DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA LA CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE

GERMÁN DARÍO RAMÍREZ TÁMARA
ROBINSON ARLEY MONTOYA URREA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SINCELEJO - SUCRE
2022

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA LA CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE

GERMÁN DARÍO RAMÍREZ TÁMARA
ROBINSON ARLEY MONTOYA URREA

Proyecto de Grado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

EDUARD ANTONIO MANTILLA TORRES
Director

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SINCELEJO - SUCRE
2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Sincelejo - Sucre

DEDICATORIA

Dedicamos principalmente este proyecto de grado como los futuros Especialistas de Seguridad Informática a Dios por permitirnos aplicar los saberes adquiridos, A nuestros familiares por apoyarnos y soportar noches de desvelo.

AGRADECIMIENTOS

A los directivos de la Corporación Universitaria Antonio José de Sucre por apoyar este proyecto y facilitar con los funcionarios levantar la información al respecto del presente proyecto.

CONTENIDO

pág.

INTRODUCCIÓN *15*

1. DEFINICIÓN DEL PROBLEMA *16*

1.1 ANTECEDENTES DEL PROBLEMA **16**

1.2 FORMULACIÓN DEL PROBLEMA **17**

2 JUSTIFICACIÓN *18*

3 OBJETIVOS *20*

3.1 OBJETIVOS GENERAL **20**

3.2 OBJETIVOS ESPECÍFICOS **20**

4 MARCO REFERENCIAL *21*

4.1 MARCO TEÓRICO **21**

4.2 MARCO CONCEPTUAL **26**

4.3 MARCO HISTÓRICO **30**

4.4 ANTECEDENTES O ESTADO ACTUAL **33**

4.5 MARCO CIENTÍFICO O TECNOLÓGICO **37**

4.6 MARCO LEGAL **39**

4.7 MARCO ESPACIAL **42**

5 DISEÑO METODOLÓGICO *44*

5.1 FUENTES DE INFORMACIÓN **44**

5.2 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN **44**

5.3 POBLACIÓN Y MUESTRA **45**

5.4 CALCULO DE LA MUESTRA **45**

5.5 METODOLOGÍA DE DESARROLLO **46**

6 DESARROLLO DE LOS OBJETIVOS *47*

6.1 DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN DE LA CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE **47**

6.1.1.1 Encuesta 47

6.1.1.2 Entrevistas 51

6.2 ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA METODOLOGÍA MAGERIT **55**

6.3 CONTROLES DE SEGURIDAD ORIENTADOS A LA NORMA ISO/IEC 27001:2013 CON EL OBJETIVO DE REDUCIR LAS VULNERABILIDADES **66**

6.4 RESUMEN EJECUTIVO **73**

7 CONCLUSIONES ***76***

8 RECOMENDACIONES ***77***

BIBLIOGRAFÍA ***78***

ANEXOS ***81***

LISTA DE TABLAS

pág.

Tabla 1 Controles y descripción de la aplicación de controles 73

LISTA DE ILUSTRACIONES

	Pág.
Ilustración 1 Organigrama Rectoría	36
Ilustración 2 Organigrama estructura académico-administrativa	37
Ilustración 3 Vicerrectoría administrativa	38
Ilustración 4 Sistema ACRATE escritorio	39
Ilustración 5 Consulta estudiantil y docente	40
Ilustración 6 Plataforma SPLAVIA	40
Ilustración 7 Mapa sede A, B, CB, D, E	46
Ilustración 8 Mapa sede C	47
Ilustración 9 Distancia entre sede A y sede C	47
Ilustración 10 Cálculo de la muestra online Feedback Networks	50
Ilustración 11 Encuesta en Google Forms	52
Ilustración 12 Consentimiento Informado Encuesta	53
Ilustración 13 Entrevista en Google Forms	56
Ilustración 14 Consentimiento Informado Entrevista	56
Ilustración 15 Evaluación de riesgos con la Metodología MAGERIT	59
Ilustración 16 control de inventario de activos	61
Ilustración 17 Inventario de activos	62
Ilustración 18 Dependencia de activos	62
Ilustración 19 Gráfica dependencia de activos	64
Ilustración 20 Probabilidad del Riesgo	65
Ilustración 21 : Impacto del Riesgo	66
Ilustración 22 Valoración cualitativa de activos	67
Ilustración 23 Valoración del riesgo	68
Ilustración 24 Relación Impacto vs Riesgo	69
Ilustración 25 Valoración de riesgo	70
Ilustración 26 Plan de tratamiento 1	71
Ilustración 27 Plan de tratamiento 2	72

LISTA DE ANEXOS

pág.

ANEXOS 1 CRONOGRAMA DE ACTIVIDADES 86
ANEXOS 2 RECURSOS NECESARIO 86
ANEXOS 3 RESULTADOS O PRODUCTOS ESPERADOS 87
ANEXOS 4 ANÁLSIS DE ENCUESTA A EMPLEADOS 87
ANEXOS 5 REGISTRO DE DILIGENCIAMIENTO DE ENCUESTA POR PARTE DE LOS COLABORADORES DE LA INSTITUCIÓN 100
ANEXOS 6 ANÁLISIS DE ENTREVISTAS A EMPLEADOS DEL ÁREA TI 100
ANEXOS 7 REGISTRO DE DILIGENCIAMIENTO DE ENTREVISTA POR PARTE DE LOS COLABORADORES TI DE LA INSTITUCIÓN 105
ANEXOS 8 INVENTARIO DE ACTIVOS GENERAL 105
ANEXOS 9 INVENTARIO DE ACTIVOS ESPECÍFICOS 107
ANEXOS 10 FORMATOS DE AUTORIZACIÓN Y CONFIDENCIALIDAD 111

GLOSARIO

ACTIVO DE INFORMACIÓN: Información o elemento que permite gestionar la información, los activos de información poseen un alto valor para las organizaciones.

AMENAZA: Es la posibilidad de ocurrencia de un evento, el cual puede afectar los activos de información negativamente.

CONFIDENCIALIDAD: Es una propiedad de la información que permite asegurar que usuarios no autorizados obtengan acceso a cierta información.

CONTROLES: Son los procesos que se implementar para garantizar que las actividades transcurran con normalidad.

DISPONIBILIDAD: Es una propiedad de la información que permite que esta esté disponible para ser consultada, modificada o eliminada en cualquier momento.

INCIDENTE DE SEGURIDAD DE LA INFORMACION: Es cuando algún individuo obtiene acceso a activos de información de manera ilegal, con fines delictivos o con el fin de afectar el desarrollo de las actividades normales.

INFORMACIÓN: Es un conjunto de datos procesados y ordenados con un propósito determinado.

INTEGRIDAD: Es una propiedad de la información que permite asegurar que esta es exacta y no ha sido modificada.

ISO27001: Es una norma internacional certificable, que describe y orienta como se debe gestionar la seguridad informática en una entidad esta norma es emitida por la organización internacional de normalización (ISO).

MAGERIT: Son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información que es una metodología enfocada al análisis y gestión de riesgos, ofrece un método semántico para realizar dicho análisis, ayudando a mantener los riesgos mitigados.

POLÍTICA DE SEGURIDAD: Es un documento donde se evidencia el alto compromiso de los directivos de una organización por la seguridad de sus activos de información, este documento define los objetivos de seguridad y procedimientos que deben llevarse a cabo en la organización con respecto al manejo de la seguridad de la información.

RIESGO: Es la posibilidad de que una amenaza se convierta en un suceso real, por el aprovechamiento de una serie de vulnerabilidades existentes, este suceso puede ser el causante de daños a los activos de información.

SGSI: Son las siglas de Sistema de Gestión de la Seguridad de la Información, que son un conjunto de políticas que dictaminan el cómo gestionar el manejo de la información para que esta esté debidamente resguardada.

TRAZABILIDAD: Cualidad que permite evidenciar el procedimiento que se lleva a cabo en la gestión de los activos de información.

VULNERABILIDAD: Es un punto débil de un sistema este puede ser a nivel de software, hardware o inclusivamente puede ser el factor humano, dicha debilidad puede permitir a un atacante comprometer la seguridad del sistema.

Las definiciones registradas en el apartado del glosario hacen parte de una sola referencia[1].

[1] COSTAS SANTOS, Jesús. Seguridad Informática. ISBN: 9789588675701. Bogotá: Ediciones de la U, 2011, 308p

RESUMEN

El presente proyecto tiene como fin realizar hasta la fase de planeación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013, para la Corporación Universitaria Antonio José de Sucre, que es una institución de educación superior ubicada en la ciudad de Sincelejo Sucre Colombia, esta organización maneja grandes volúmenes de información tanto personal, financiera como académica, es por esto que se desea implementar un sistema que permita mantener segura toda esta información.

Para realizar este proyecto se deberá realizar un diagnóstico del estado actual de la seguridad de la información en la organización utilizando diferentes instrumentos y metodologías, para posteriormente poder evidenciar las mejoras en cuanto a seguridad informática, dentro de estas mejoras es primordial el diseño de una política de seguridad de la información en la cual se dictamine las directrices de los procedimientos que se deberán llevar a cabo al momento de manipular información, con esto se buscara reducir las vulnerabilidades que posea la institución, teniendo claro cuáles son los permisos que deberá tener cada usuario de acuerdo a su rol en la organización.

Palabras clave: ISO/IEC 27001:2013, diagnóstico, información, organización, política de seguridad, vulnerabilidades.

ABSTRACT

The purpose of this project is to carry out up to the planning phase of an information security management system based on the ISO / IEC 27001:2013 standard, for the Antonio José de Sucre University Corporation, which is a higher education institution located in the city of Sincelejo Sucre Colombia, this organization handles large volumes of personal, financial and academic information, which is why we want to implement a system that allows all this information to be kept safe.

To make this project, a diagnosis of the current state of information security in the organization must be carried out using different instruments and methodologies, in order to subsequently be able to show the improvements in terms of computer security, within these improvements the design of a policy is essential of information security in which the guidelines of the procedures that must be carried out at the time of manipulating information are dictated, this will seek to reduce the vulnerabilities that the institution possesses, being clear about the permissions that each user must have according to their role in the organization.

Keywords: data, computing, standards, protocols, security, Vulnerabilities

INTRODUCCIÓN

Un Sistema de Gestión de Seguridad de la Información también conocido por su abreviación SGSI, se basa en unas normas e intrusiones de buenas prácticas para que las entidades puedan alcanzar un grado superior de aseguramiento de la información, el SGSI está en constante expansión dado a que muchas empresas han migrado de procesos y procedimientos de manera física a la digital por ende se asumen nuevos riesgo y asimilando de que la información es un activo valioso para la organización se deciden por implementar controles y buenas prácticas para evitar fuga o alteraciones de los mismos.

La normatividad a la que se sustenta un SGSI, está basada en la Organización Internacional de Estandarización (ISO), y es allí un gran motivo de su aplicabilidad en entidades como la institución educativa Corporación Universitaria Antonio José de Sucre, ya que permite a las entidades empalmar con otras entidades nacionales o internacionales los procedimientos, a su vez que está orientada en los 3 pilares de seguridad informática, que son la integridad, la confidencialidad y la disponibilidad, la forma de identificar el SGSI dentro de la ISO es mediante la numeración 27000.

Por lo dicho anteriormente, este proyecto busca ser una guía para evidenciar de manera práctica la puesta en marcha de un diseño de SGSI y de esta manera evaluar los pilares de seguridad informática en la institución Corporación Universitaria Antonio José de Sucre.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La institución universitaria, Corporación Universitaria Antonio José de Sucre, es una institución de educación superior, que de ahora en adelante será la Corporación, de carácter privado que ofrece programas técnicos, tecnológicos, profesionales, postgrado y de educación continuada en modalidad presencial y a distancia, actualmente su oferta está presente en la ciudad de Sincelejo, Montería y en otras ciudades como Cartagena y Barranquilla mediante un convenio interinstitucional con la Universidad Fundación Antonio de Arévalo, UNITECNAR. Dentro de los actores que intervienen en la institución se encuentran interesados, estudiantes, egresados, docentes, administrativos, proveedores, instituciones en convenios y entidades gubernamentales.

Dentro del Sistema de Gestión de la Calidad, el cual se encuentra certificado bajo la norma ISO-9001, la División de Tecnologías, Sistemas de Información y Recursos Educativos (SIRET), cuenta con un análisis de riesgo, un plan y un procedimiento; en cuanto al análisis de riesgo existen 2 eventos potenciales como lo son el daño a equipos de cómputo de usuarios finales categorizado de nivel medio y daño a servidores institucionales de nivel catastrófico, que ambos son intervenidos en el plan y el procedimiento que se enfoca en el mantenimiento preventivo y realización de backup sin embargo no se tiene contemplado otros posibles riesgos que se enfocan no solo en la disponibilidad sino también en la integridad y en la confidencialidad de los datos.

Cabe señalar que la División SIRET, es un área de apoyo transversal tanto a las áreas administrativas como académicas por lo tanto no existe una persona a cargo de las funciones específica de inconvenientes en seguridad informática por lo que el Director debe distribuir sus labores de tal manera de que pueda solventar todos los requerimientos afectando los tiempos de respuesta, motivo por el cual no se tiene debidamente documentado los casos de posible ataque o problema de seguridad informática, como

punto adicional el Director SIRET solo administra los sistemas de información y la base de datos institucional debido a que dichos sistemas son desarrollado por el área de la División de Tecnología y Sistemas de Información de UNITECNAR, mediante el convenio ya mencionado.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cómo el diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2013 contribuirá al aseguramiento de la integridad, la disponibilidad y la confidencialidad de la información en la Corporación Universitaria Antonio José de Sucre?

2 JUSTIFICACIÓN

Los ataques cibernéticos no dan tregua para las organizaciones ya que cada día los intentos son más constantes, aunque cabe resaltar que existe la posibilidad de que la información sobre el número de los ataques reportados por las organizaciones sean aún mayores, teniendo en cuenta que muchas organizaciones prefieren no publicarlos para evitar que su imagen institucional se vea afectada; la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) ha realizado un reporte de ciberseguridad 2020 denominado “Tendencias del cibercrimen 2021 - 2022 nuevas amenazas al comercio electrónico”[2], en donde se obtuvieron las siguientes tendencias:

Al finalizar noviembre de 2021, hubo 46.527 eventos por ciberdelitos en el país, que con respecto al año anterior se registró un incremento del 21%, estos datos corresponden solo a los casos denunciados en la Fiscalía General de la Nación, la Policía Nacional (DIJIN-SIJIN) y las policías judiciales del CTI.

En los primeros 9 meses del año 2021 se presentaron más de 500 casos de Ransomware en empresas PYME.

En el año 2021 se reportaron 3.806 empresas víctimas de Ransomware en el mundo y también se identificaron 53 bandas criminales dedicadas al cibercrimen.[3]

La institución Corporación Universitaria Antonio José de Sucre, hoy día opera diariamente un gran flujo de información, como los datos sus clientes (estudiantes), empleados (docentes y administrativos) y proveedores, manejando de ellos datos sensibles y confidenciales propios de la institución mediante los sistemas de información a través de

[2] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias del cibercrimen 2021 -2022 Nuevas amenazas al comercio electrónico. Bogotá. 2021

[3] Ibíd.

su intranet e internet; adicional a ello, ofrece a la comunidad servicio de WIFI por lo que no está exenta de sufrir algún tipo de ataque mediante su red u otra técnica de hacking con el objetivo de vulnerar algunos de los principios de seguridad informática como la disponibilidad, integridad o confidencialidad de los datos, causando con ello posibles problemas leves o graves que puedan afectar estructuralmente a la institución

Ahora bien, las directivas de la institución han trazado una meta institucional, la cual apunta a mejorar los servicios tecnológicos en aras de la transformación digital y entendiendo el contexto global que apunta en asegurar los datos de las organizaciones, necesita al mismo tiempo implementar buenas prácticas en materia de la seguridad de los datos y conscientes de dicha necesidad ha definido en su Plan Estratégico de Desarrollo 2020-2025, el siguiente objetivo "7.1.4 Implementar sistema de gestión de la seguridad de la información basados en el estándar de seguridad de la información ISO 27001"[4] ; por lo que en efecto, la aplicación de este proyecto permite apoyar la ejecución de este objetivo así como también los compromisos que como Institución de Educación Superior está sujeta a cumplir como la Ley 1581 de 2012; la cual define la Política de Protección de Datos Personales, cuya adaptación fue realizada bajo el Acuerdo No. 001-2018 emanado por la Corporación.

Otras de las razones subyacentes en la realización de este proyecto se basan en que en el departamento de Sucre no existen o son carentes los trabajos, estudios o estadísticas relacionada a la seguridad informática y con este trabajo se pretende ser referente en el departamento y en la región. Como complemento final existe una razón en el ámbito personal y se enfoca en la posibilidad de la creación de una Dirección de Ciberseguridad y consecuente a ello; como autores del presente proyecto es muy factible perfilarse a dicha nueva área proyectada por la institución

[4] CORPORACIÓN UNIVERSITARIA ANTONIO JOSE DE SUCRE. Plan Estratégico de Desarrollo para la Corporación Universitaria Antonio José de Sucre – CORPOSUCRE 2020-2025. Sincelejo. 2020

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar un Sistema de Gestión de Seguridad de la Información para la Corporación Universitaria Antonio José de Sucre teniendo como referencia la norma ISO/IEC 27001:2013.

3.2 OBJETIVOS ESPECÍFICOS

- Elaborar un diagnóstico del estado actual de la seguridad de la información de la Corporación Universitaria Antonio José de Sucre.

- Compilar los activos de información que tiene la institución para realizar el análisis de los riesgos de seguridad mediante la aplicación de la metodología MAGERIT.

- Desarrollar los controles de seguridad orientados a la norma ISO/IEC 27001:2013 con el objetivo de reducir las vulnerabilidades

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La era digital está en constante crecimiento, se hace necesario realizar la pregunta de que sí ese crecimiento es directamente proporcional a la seguridad informática que debería contar estos sistemas informáticos

Si bien los sistemas de información son la base de la era digital, estos son desarrollados por humanos por lo tanto es posible que estos presenten errores que puede ser aprovechados por los atacante y de esta manera irrumpir la confidencialidad, integridad o disponibilidad de la información, esto se puede evidenciar en el trabajo desarrollado por GARCÍA, Juliana denominado “Uso de tecnologías de pruebas de penetración para validación de seguridad de aplicaciones web basado en el top 10 de vulnerabilidades de OWASP” [5]. En donde se describe las grandes vulnerabilidades que presentan muchos sistemas de información como la inyección SQL, pérdida de autenticación y gestión de sesión, exposición de datos sensible entre otras; Dado a lo anteriormente mencionado, existen técnicas cómo el Hacking ético que le permite a las entidades y organizaciones a realizar pruebas controladas para establecer un diagnóstico del estado de la seguridad informática, es por ello que RODRÍGUEZ Cuadros, Oscar en su trabajo de grado, ha diseñado un manual básico de Hacking ético el cual tiene 3 particiones fundamentales que son la fase de reconocimiento, fase de descubrimiento de vulnerabilidades y por último el ataque controlado[6], el trabajo de Rodríguez permite evidenciar que a pesar que existan vulnerabilidades es posible disminuirlas con la ayuda de diferentes herramientas; Es importante señalar que adicional a los sistemas de información, la interconexión entre 2 o más dispositivos a lo cual se le denominan redes son parte fundamental de la era digital por lo tanto es el vector más usado por los atacantes para escalar privilegios o

[5] GARCÍA, Juliana. Uso de tecnologías de pruebas de penetración para validación de seguridad de aplicaciones web basado en el top 10 de vulnerabilidades de OWASP. Sabaneta, 2018, 41 p. Trabajo de Grado de tipo Monografía para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

[6] RODRÍGUEZ CUADRADOS, Oscar Alberto. Diseño de manual básico de pruebas de Hacking Ético: escaneo de red, de vulnerabilidades y ataques. Bucaramanga, 2018, 78p. Trabajo de grado. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas.

realizar ataque como la denegación de servicios, en consecuencia a esto SUESCUN, Jonhatan Alexander realizó una monografía sobre "La importancia de los sistemas de monitoreo de redes de datos en las empresas" sobre este estudio, se identifica que muchas grandes empresas y organizaciones como la Registraduría Civil de Colombia han sido atacadas y en ocasiones han perdido datos, por lo tanto en la actualidad muchas empresas han identificado la necesidad de implementar seguridad de la información contratando personal especializado o subcontratando los servicios con una agencia especializada en el tema[7].

En Colombia la cibercriminalidad es en efecto un vector que está ligado al avance tecnológico y no solo ha afectado el robo de datos personales sino que también el dinero electrónico de empresas y personas de modo que según la investigación realizada en la monografía de MARIN, Ana Milena y CARVAJAL, Oscar Javier "Estudio monográfico sobre casos más comunes de cibercrimen en las pymes colombianas" nos brinda datos muy importantes sobre la cibercriminalidad en el país como los siguientes: "Durante el periodo del 2014 al 2016 se recibieron cerca de 13.774 denuncias de violación a la ley 1273 de 2009, en el transcurso del año 2017 aumento este número a 15.565". [8] A pesar de lo anterior, El Gobierno Colombiano ha identificado que es pertinente regular aspectos sobre la protección de datos de sus ciudadanos por ello ha establecido una serie de normatividad que han sido analizadas en el trabajo de PARRA, Jairo Andrés[9] en su monografía de grado "Delitos informáticos y marco normativo en Colombia" indaga sobre aquellas normatividad dirigidas a la seguridad de la información establecida por el gobierno de Colombia durante los años 1980 a 2018, en la monografía se puede evidenciar el método análisis-síntesis en donde el autor construye un normograma que

[7] SUESCUN PINEDA, Jonhatan Alexander. Estudio sobre la importancia de los sistemas de monitoreo de redes de datos en las empresas. Medellín, 2019, 95- 98p. Monografía de grado. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas.

[8] MARIN GUINEME, Ana Milena & CARVAJAL CARVAJAL Oscar Javier. Estudio monográfico sobre casos más comunes de cibercrimen en las pymes colombianas. Bogotá, 2018, 84p. Trabajo de Grado tipo Monografía para optar por el título de Especialista en Seguridad Informática. Universidad Nacional

[9] PARRA CALDERON, Jairo Andres. Delitos informáticos y marco normativo en Colombia. Huila, 2019, 121p. Monografía presentada como requisito parcial para optar al título de: Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas.

permite observar el consolidado histórico de las normatividades implementada, del cual se puede concluir que el gobierno de Colombia aumentó en los últimos años (2000 al 2011) la implementación de normatividad a la vanguardia internacional; Al igual que PARRA, HERNÁNDEZ, Sandra realizó una investigación sobre "Las implicaciones de la seguridad informática en la legislación colombiana"[10] en donde sí bien resaltó los esfuerzo del Gobierno Colombiano, también resaltó que estos deben estar en constante actualización ya que de esta manera se garantiza los derechos de sus ciudadanos. En Departamentos como Boyacá se han presentados delitos informáticos en donde la gran mayoría violan datos personales pero este tipo de ataques no ha crecido con respecto a los ocurridos a nivel mundial es necesario la búsqueda de los cibercriminales para su respectiva judicialización[11], Unos de los aspectos importante dentro de la seguridad informática se encuentra la investigación forense la cual le permite a las autoridades oficiales encargadas de la seguridad informática en Colombia, ciertas herramientas y metodologías que serán de apoyo fundamental como material probatorio, como lo demostró GUEVARA, Estefani en su trabajo de grado[12], de igual forma es importante que cuando las autoridades obtengan el material probatorio, estos realicen el proceso de cadena de custodia de dichas evidencias digitales, para que estas sean lo suficientemente completas para condenar al ciberdelincuente, es por ello que PATERNIA, Ramón Andrés en su proyecto aplicado identificó 4 vulnerabilidades de este proceso en el Cuerpo Técnico de Investigación – CTI Seccional Bolívar.[13]

---

[10] HERNÁNDEZ, Sandra Milena. Implicaciones de la Seguridad Informática en la Legislación Colombiana. Manizales, 2018, 65 p. Trabajo de Grado de tipo Monografía para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

[11] ORDUZ BARRERA, Diana Maria. Análisis de emergencias cibernéticas que se presentan en las ciudades de Tunja, Duitama y Sogamoso con respecto al resto del país en los últimos 2 años. Sogamoso, 2018, 75p. Trabajo de grado. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas.

[12] GUEVARA, Estefani. Alcances que puede tener una investigación forense dentro de un proceso legal en Colombia. Bogotá, 2018, 61 p. Trabajo de Grado de tipo Monografía para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

[13] PATERNINA CUESTA, Ramon Andres. Estudio de vulnerabilidades en el proceso de cadena de custodia de evidencias en delitos informáticos en la ciudad de Cartagena. Cartagena, 2018, 71p. Proyecto de grado aplicado. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas.

El ministerio de las TICS de Colombia, quien lidera el enfoque de las tecnologías en el país junto con el gobierno Colombiano mediante su programa de Gobierno en Línea (GEL) han orientado sus esfuerzos en la implementación del SGSI, cuyos avances se encuentran identificados en el trabajo de grado de CELY, Ronald Mauricio en donde se denota que la Federación Colombiana de Municipios cuentan con un SGSI y están preparadas para dar cumplimiento a los requisitos de GEL en el mediano plazo lo cual daría buenos indicios de la importancia que el Gobierno Colombiano le ha dado a la seguridad informática[14]

Con todo lo expuesto anteriormente, las organizaciones deben implementar una Gobernabilidad en Seguridad Informática como lo sugiere RODRIGUEZ, Juan Hernán en donde establece los siguientes elementos claves: Modelo de referencia para la Gestión de Seguridad, Modelo de Madurez de Seguridad, Esquema de Medición y Diagnóstico y por último elemento clave Procesos adicionales de seguridad de la información[15]

Muchas empresas y organizaciones al notar la realidad de la situación con la cibercriminalidad han optado por la implementación de normatividad orientadas a la seguridad informática pero para ello se hace necesario una planeación como lo denota el trabajo de grado de MENDOZA GAMBOA, Denís Celín[16], denominado “Diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para la Secretaría de Educación Departamental del Norte de Santander” en donde se puede apreciar que comparte algunos objetivos del proyecto aplicado que se desea

[14] CELY, Ronald Mauricio. Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) con base al Modelo de Seguridad y Privacidad de la Información según lineamientos del Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia GEL (Gobierno en Línea) y en cumplimiento del Decreto 1078 De 2015 y 2573 De 2014. Bogotá. 2018. 424 p. Proyecto aplicado para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

[15] RODRIGUEZ MAHECHA, Juan Hernan.Modelo para la definición e implementación de Gobernabilidad de Seguridad. Bogotá, 2009, 63p. Trabajo de grado. Universidad de los Andes. Departamento de Ingeniería de Sistemas y Computación.

[16] MENDOZA GAMBOA, Denys Celin. Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la Secretaría de Educación Departamental del Norte de Santander. Cúcuta, 2019, 33p. Trabajo de Grado tipo Proyecto Aplicado para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería

presentar como el título, el alcance hasta la planeación, la implementación de la metodología MAGERIT.

Aunque el sector educativo actualmente no es el más atacado por los cibercriminales porque representa un 3% de los ataques en el año 2017 según MARIN GUINEME, Ana Milena y CARVAJAL[17] es importante la implementación de medidas orientadas a la seguridad informática ya que el ataque puede ser concedido a través de un dispositivo personal previamente atacado de un miembro o usuario de la institución, dicho ataque de acuerdo con los autores anteriormente citados equivale a un 66% en el 2017, es por ello que investigaciones como la del proyecto de grado de MEDINA RINCÓN, Luz Amanda[18] cuyo título es "Análisis y diseño de un sistema de gestión de la seguridad de la información para la Dirección de Sistemas de la Universidad de la Sabana" se correlaciona con la utilización de la norma ISO/IEC 27001:2013 con otro objetivo del proyecto que se desea implementar, además que también es de gran referencia no solo por los aspectos en común sino por las nociones sobre qué información se puede publicar a sabiendas de que es un proyecto aplicado en una Universidad real y genera parte de tranquilidad a los directivos de la institución al conocer la viabilidad de la realización de un proyecto de esta categoría. Para finalizar, otro trabajo de grado de alta referencia a la intención del proyecto es el realizado por BAQUERO, Magda Mayery quien diseñó el SGSI para la empresa COMFENALCO QUÍNDIO el cual al igual que el anterior su alcance fue hasta la etapa de diseño[19].

---

[17] MARIN GUINEME, Ana Milena & CARVAJAL CARVAJAL Oscar Javier. Estudio monográfico sobre casos más comunes de cibercrimen en las pymes colombianas. Bogotá, 2018, 84p. Trabajo de Grado tipo Monografía para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

[18] MEDINA RINCÓN, Luz Amanda. Análisis y diseño de un sistema de gestión de la seguridad de la información para la Dirección de Sistemas de la Universidad de la Sabana. Chía, 2019, 36p. Trabajo de Grado tipo Proyecto Aplicado para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería

[19] BAQUERO, Magda Mayery. Diseño Del Sistema De Gestión De Seguridad De La Información Para La Empresa Comfenalco Quindío. Armenia, 2019, 63 p. Trabajo de Grado para optar al título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

4.2 MARCO CONCEPTUAL

4.2.1 SEGURIDAD DE LA INFORMACIÓN.

Partiendo del concepto de que la información es el conjunto de datos que se interrelacionan entre sí con un objetivo en común, está a pesar de estar presente en nuestro entorno, se convierte en el activo más importante de todo negocio ya que en ella se contempla por ejemplo la información de sus proveedores, clientes, fórmulas de administración y sí esta es accedida por agentes no autorizados puede conllevar fácilmente en la quiebra del negocio, por lo tanto independientemente del medio en donde está contenida dicha información debe ser resguardada de tal forma que solo el personal autorizado tenga acceso a ella y esto se ve reflejado en el top 10 de hallazgo de la encuesta realizada por la Asociación Colombiana de Ingenieros de Sistemas, ACIS[20] sobre las tendencias informáticas (2012-2013) en donde cabe resaltar la posición #1 de dicho top en donde manifiesta que "cada vez, las organizaciones están más preocupadas por las anomalías electrónicas que acechan en Internet; de ahí que para este año el hecho más relevante es el significativo incremento del 27 al 87% de las organizaciones que buscan mantener contactos con autoridades nacionales o internacionales para atender ciber ataques o incidentes que afectan las infraestructuras de las organizaciones."

4.2.2 PILARES DE LA SEGURIDAD INFORMÁTICA

Para alcanzar el aseguramiento en la seguridad de la información se ha establecido 3 pilares fundamentales que son: confidencialidad, integridad y disponibilidad por lo tanto en base a estos pilares se diseñan normatividad referente a la ciberseguridad, a continuación, se describen cada uno de los conceptos

- Confidencialidad: Se trata de la cualidad que debe poseer un documento o archivo

[20] ALMANZA, Andrés Ricardo. REVISTA SISTEMAS. {En línea}. {17 de mayo de 2013} Disponible en: (http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-no127/item/132-seguridad-inform%C3%A1tica-en-colombia-tendencias-2012-2013)

para que esté solo se entienda de manera comprensible o sea leído por la persona o sistema que esté autorizado. De esta manera se dice que un documento (o archivo o mensaje) es confidencial si y sólo si puede ser comprendido por la persona o entidad a quien va dirigido o está autorizada. En el caso de un mensaje esto evita que exista una intercepción de este y que pueda ser leído por una persona no autorizada. Por ejemplo, si Andrea quiere enviar un mensaje a Bruno y que sólo pueda leerlo Bruno, Andrea cifra el mensaje con una clave (simétrica o asimétrica), de tal modo que solo Bruno sepa la manera de descifrarlo, así ambos usuarios están seguros de que solo ellos van a poder leer el mensaje[21].

- Integridad: La integridad es la cualidad que posee un documento o archivo que no ha sido alterado y que además permite comprobar que no se ha producido manipulación alguna en el documento original. Aplicado a las bases de datos sería la correspondencia entre los datos y los hechos que refleja. En el caso del envío de la información y su no modificación durante su viaje a través de una red, teniendo como muestra el ejemplo anterior, Andrea envía tanto el propio mensaje como un resumen cifrado del mismo. Finalmente, Bruno en el lado receptor, compara el mensaje como resumen (aplicando la misma función que Andrea) y el resumen cifrado enviado. Si en el transcurso de la comunicación el mensaje ha sido alterado por fallos en el canal de comunicación o por algún usuario intruso, la comparación será errónea, y si está da como resultado "iguales", quiere decir que no ha existido manipulación del mensaje[22].

- Disponibilidad: Se trata de la capacidad de un servicio de unos datos o de un sistema, a ser accesible y utilizable por los usuarios (o procesos) autorizados cuando estos lo requieran. También se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida

[21] COSTAS SANTOS, Jesús. Seguridad Informática. ISBN: 9789588675701. Bogotá: Ediciones de la U, 2011, 308p

[22] Ibíd.

o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor. Por ejemplo, siguiendo con el ejemplo de Andrea y Bruno, se supone que en el momento que Andrea se encontraba redactando el mensaje que sería enviado a bruno, el fluido eléctrico fue bruscamente interrumpido, pero gracias a qué Andrea tenía su equipo conectado a una UPS no sufrió pérdida de la información y pudo enviar el mensaje a Bruno para luego apagar su equipo de forma controlada sin sufrir posibles daños en el hardware[23].

4.2.3 CIBERDELINCUENCIA

Con la evolución de la tecnología para agilizar los procesos en las distintas organizaciones, también nace este término de ciberdelincuencia, el cual se refiere a los delitos contra sistemas informáticos que tienen como fin lograr accesos no autorizados a un sistema o negar el acceso a un usuario que sea legítimo.

También este término abarca la evolución de la delincuencia tradicional puesto que las organizaciones delictivas han empezado a utilizar el internet para cometer delitos como robo, extorsión, fraude, entre otros[24].

4.2.4 NORMA ISO

(International Organization for Standardization) Las normas ISO son herramientas que utilizan las organizaciones para garantizar que los productos o servicios ofrecidos por ellas son de calidad.

Las normas ISO sirven para optimizar procesos reduciendo así costos en las organizaciones y satisfaciendo al cliente con productos y servicios de calidad, estas normas dan acceso a las organizaciones a nuevos mercados puesto que estas normas son a nivel internacional[25].

---

[23] COSTAS SANTOS, Jesús. Seguridad Informática. ISBN: 9789588675701. Bogotá: Ediciones de la U, 2011, 308p

[24] ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL INTERPOL. Ciberdelincuencia. Francia. 2020

[25] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN ICONTEC. Certificación ISO 27001, Sistemas de Gestión de seguridad de la información. Bogotá. 2020

4.2.5 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La información de una empresa es su activo más valioso, por lo tanto, está siempre está expuesta ante amenazas de ataques, errores, ambientales, fallas en los sistemas, entre otras vulnerabilidades que pueden representar puntos débiles para poder preservar los 3 pilares fundamentales de la información (confidencialidad, integridad y disponibilidad), los cuales son de vital importancia para que la organización realice sus procesos de una forma eficiente.

Para lograr lo anterior mencionado la organización debe definir políticas, objetivos y procesos que definan el modo en el cual se va a llevar a cabo la protección de dicha información aquí es donde se define un sistema de gestión de seguridad de la información como un conjunto de políticas, directrices y procedimientos para la protección de sus activos de información.

4.2.6 MAGERIT

Es una metodología de análisis y gestión de riesgos, esta herramienta generaliza el uso de las tecnologías mostrando los beneficios que estas traen consigo, pero también dando lugar a identificar los riesgos que deben minimizarse para mantener la seguridad de estas tecnologías. MAGERIT busca concientizar a las organizaciones que la información está expuesta a riesgos los cuales hay que gestionarlos y mediante esta información se lograra una aproximación metódica que busca ser más precisa, la opinión de un analista, todo este proceso prepara la organización para procesos de auditoría, certificaciones y evaluaciones[26].

[26] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN ICONTEC. Certificación ISO 27001, Sistemas de Gestión de seguridad de la información. Bogotá. 2020

4.3 MARCO HISTÓRICO

La institución inició sus actividades en el año 1996 como organización de carácter Limitada en convenio con el Instituto de Administración y Finanzas de Cartagena – IAFIC cuyo objetivo fue la administración de carreras técnicas en la ciudad de Sincelejo, luego obtuvo 2 convenios tendientes a la profesionalización de las carreras de Contaduría Pública con la Fundación Universitaria Los Libertadores, (Agosto 2020) y Administración con la Corporación Educativa Mayor del Desarrollo Simón Bolívar, como resultado de actividades académicas de calidad la CORPOSUCRE Ltda. Y a otras personas naturales crearon la Corporación Universitaria de Sucre – CORPOSUCRE la cual quedó registrada con la Personería Jurídica No. 2302 el 26 de septiembre del 2003 por el Ministerio de Educación Nacional y el 3 de enero de 2004 obtuvo el registro 2850 por el Sistema Nacional de Información de Educación Superior (SNIES)

Luego del otorgamiento de la Personería Jurídica, se le concedió la creación de los 2 primeros programas profesionales, Psicología y Fisioterapia, La Corporación Universitaria de Sucre - CORPOSUCRE, inicia labores con el Programa de Fisioterapia con 57 alumnos, en el Segundo Semestre de 2005.

El 1 de septiembre de 2011, con el objetivo de fortalecer ampliar la cobertura académica realizó un convenio con la Fundación Tecnológica Antonio de Arévalo – TECNAR logrando así extender los programas en las ciudades de Cartagena y Barranquilla.

A partir del año 2012, la Corporación Universitaria de Sucre – CORPOSUCRE aumente su oferta debido a la aprobación de una serie de registros calificados aprobados por el Ministerio de Educación Nacional, los cuales son:

8 programas de pregrado profesional en la modalidad presencial (Sincelejo)
2 programa profesional en la modalidad presencial (Barranquilla)

5 programas académicos profesionales presenciales (Cartagena)
1 programa Técnico Profesional (Barranquilla)
1 programa Tecnológico (Barranquilla)
2 programas Técnicos Profesionales (Sincelejo)
2 programas Tecnológicos (Sincelejo)
2 programas Técnicos Profesionales (Cartagena)
2 programas Tecnológicos (Cartagena)
9 programas Tecnológicos en Convenio con la Fundación Tecnológica Antonio de Arévalo - TECNAR.

El 18 de febrero de 2013, la Corporación Universitaria de Sucre – CORPOSUCRE cambió su denominación por Corporación Universitaria Antonio José de Sucre - CORPOSUCRE

En el año 2013 la Institución fue seleccionada en una convocatoria del Ministerio de Educación Nacional para el Fomento de Acreditación Institucional con el acompañamiento de la Universidad de Medellín, con esta convocatoria se generó el Sistema de Acreditación Institucional para Corposucre (SAMCI), como un mecanismo que permite consolidar los procesos de autoevaluación y mejoramiento continuo de los programas académicos

En el año 2016, se crearon las primeras especializaciones universitarias: Especialización en Seguridad y Salud en el Trabajo y Especialización en Gerencia Tributaria, que obtuvieron su registro calificado por parte del Ministerio de Educación Nacional el 18 de mayo de 2016 y el 01 de junio de 2016 respectivamente.

En este mismo año, la Corporación crea el Sistema de Gestión de la Calidad y es certificada por Bureau Veritas con la norma ISO-9001 versión 2008 con alcance de los procesos administrativos. Posterior a esto, la Institución continuó trabajando en la mejora de su sistema, vinculando a este los procesos académicos y ajustándose a la versión de

la norma 2015. En octubre de 2017, obtiene certificación del sistema de gestión de la calidad en la norma ISO-9001 versión 2015 por Bureau Veritas.

En el año 2017, logra la Certificación de Responsabilidad Social Empresarial otorgada por Fenalco, dado a las acciones realizadas por la institución la cual obtuvo más de 15 mil beneficiarios

A la fecha actual, la Corporación Universitaria Antonio José de Sucre - CORPOSUCRE cuenta con el Plan de Desarrollo 2020-2025 que en sincronía con el Plan Educativo Institucional (PEI) buscan fortalecer sus procesos académicos y administrativos tomando como referencia normatividades nacionales e internacionales como La Organización para la Cooperación y el Desarrollo Económicos (OCDE)[27]

[27] CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE. Historia. Sincelejo. 2020

4.4 ANTECEDENTES O ESTADO ACTUAL

La Corporación Universitaria Antonio José de sucre es una institución de educación superior que oferta programas de pregrado posgrado y educación continuada, está regida por los lineamientos del ministerio de educación nacional de Colombia. Cuenta con 10 procesos certificados bajo la norma ISO 9001, con la firma Bureau Verita, dentro de los cuales se encuentran los procesos estratégicos, procesos misionales y procesos de apoyo, dentro de las políticas de calidad se encuentra el cumplimiento de la normatividad legal vigente y de las metas institucionales a través del fortalecimiento de la docencia, la investigación e innovación y la proyección social como ejes misionales, y de la internacionalización como eje transversal, el mejoramiento de la infraestructura física y tecnológica, el talento humano necesario, el crecimiento y permanencia de la población estudiantil, la atención de los servicios ofrecidos y la mejora continua del Sistema de Gestión.

La institución cuenta con un plan estratégico de desarrollo (PEI) 2020-2025 el cual es la hoja de ruta de los procesos académicos y administrativos que concretara la institución en dicho periodo[28], este proyecto está basado en el contexto de las políticas y tendencias nacionales e internacionales, por ende, dentro de sus acciones a ejecutar se encuentra la implementación del sistema de gestión de seguridad de la información.

El PEI está alineado con la misión y visión de la institución el cual se define a continuación.

Misión

La Corporación Universitaria Antonio José de Sucre es una Institución de Educación Superior de carácter privado, que, a través del ejercicio de la docencia, la investigación e innovación y la proyección social, propende por la formación integral, para contribuir al mejoramiento del entorno globalizado, al desarrollo sostenible, la convivencia y la paz, permitiendo el acceso de los diversos grupos sociales y generando procesos de calidad.

[28] CORPORACIÓN UNIVERSITARIA ANTONIO JOSE DE SUCRE. Plan Estratégico de Desarrollo para la Corporación Universitaria Antonio José de Sucre – CORPOSUCRE 2020-2025. Sincelejo. 2020

Visión

En el año 2025 la Corporación Universitaria Antonio José de Sucre será una Institución de alta calidad, reconocida por su gran compromiso con la docencia, la investigación e innovación, la proyección social y la formación integral de profesionales, que atiendan con responsabilidad social, las necesidades del sector productivo, social y el desarrollo sostenible de su entorno regional, nacional y global.

Aunque la institución no cuenta con una política de seguridad de la información si presenta una política de protección de datos personales[29] referenciada en el decreto 1377 de 2013 y la ley 1581 de 2012, también desde la dirección de tecnologías, sistemas de información y recursos educativos se ha implementado la política de infraestructura tecnológica la cual presenta ciertos estándares orientados a la seguridad informática[30].

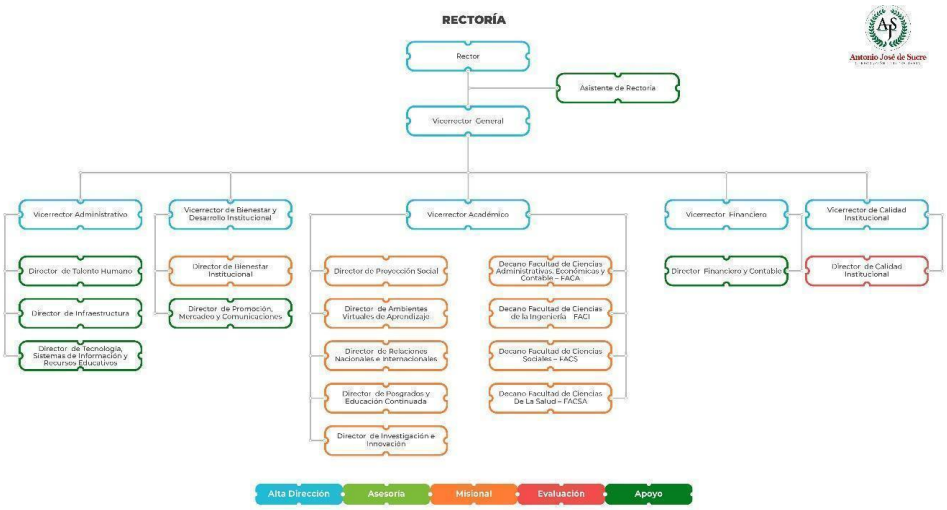
ORGANIGRAMA

A continuación, se evidencia cómo está constituida la institución, desde los cargos de la alta dirección, seguido por los asesores, los cargos misionales, las áreas de evaluación y por último las áreas de apoyo. La Dirección de Tecnologías, Sistemas de Información y Recursos Educativos, depende de la Vicerrectoría Administrativa.

Ilustración 1 Organigrama Rectoría

[29] CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE. Política de Protección de datos personales. Sincelejo. 2020

[30] CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE. Políticas de Infraestructura Física y Tecnológica. Sincelejo. 2020



Fuente: https://www.corposucre.edu.co/sites/default/files/Organigramas2.jpg

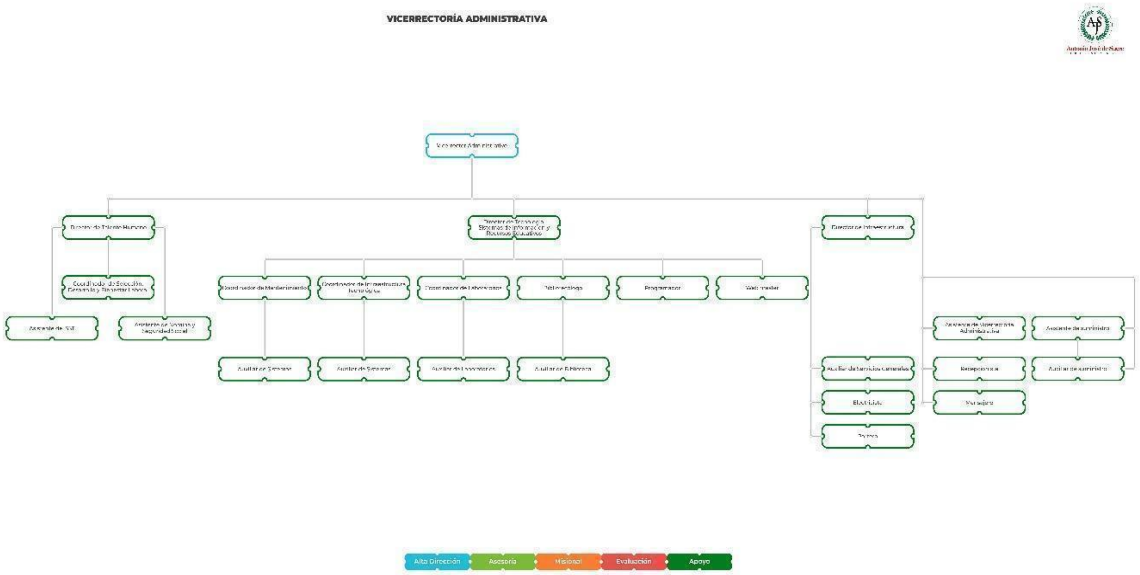
En la siguiente ilustración, se detalla los comités creados por la institución, los cuales tienen como función principal asesorar a la alta dirección sobre nuevas estrategias y realizar un seguimiento a las acciones para alcanzar sus respectivas metas; se puede identificar que no existe un comité exclusivo referente a la seguridad informática.

Ilustración 2 Organigrama estructura académico-administrativa

Fuente: https://www.corposucre.edu.co/sites/default/files/Organigramas1.jpg

La Dirección de Tecnologías, Sistemas de Información y Recursos Educativos tiene a cargo 6 coordinadores y de estos dependen los auxiliares, de igual forma se logra identificar que no existe un cargo exclusivo para el área de la Ciberseguridad; sin embargo, distribuye dichas actividades con algunos coordinadores.

Ilustración 3 Vicerrectoría administrativa

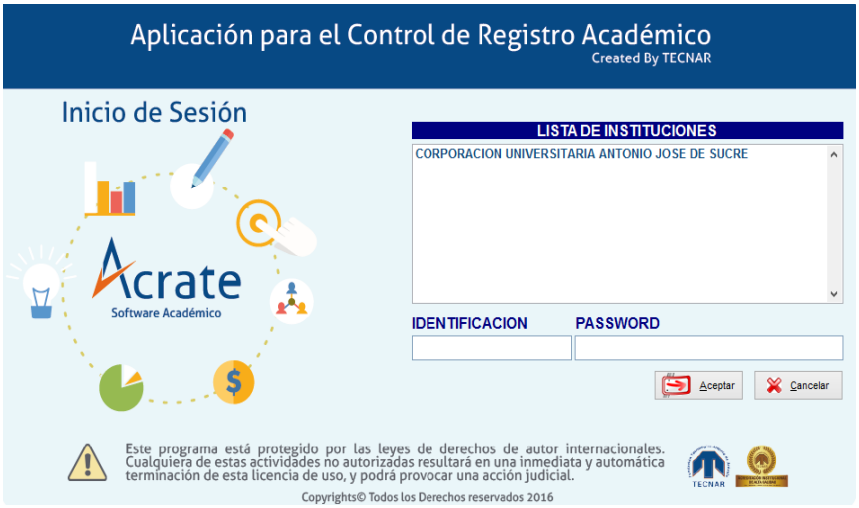


Fuente: https://www.corposucre.edu.co/sites/default/files/Organigramas6.jpg

4.5 MARCO CIENTÍFICO O TECNOLÓGICO

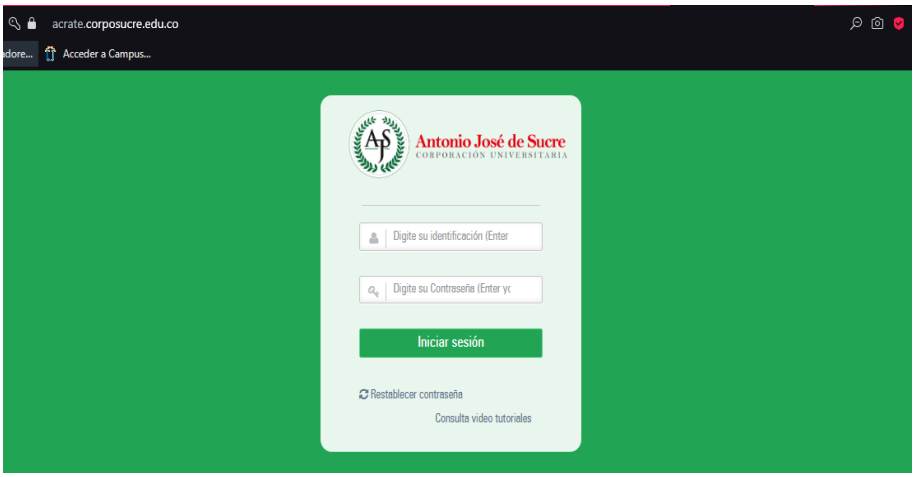
La Corporación Universitaria Antonio José de Sucre, cuenta con una infraestructura tecnológica y de red propia y en convenio con la Fundación Antonio de Arévalo a nivel de los aplicativos institucionales, la institución a nivel de red ofrece el servicio de internet a diferentes áreas como la administrativa, estudiantil y docente, salas de sistemas, biblioteca, laboratorios e invitados, cada una de ella cuenta con parámetros de seguridad de acuerdo al uso o servicio que se requieran, a nivel de los aplicativos cuenta con un sistema de escritorio denominado ACRATE (Ilustración 4) (Aplicativo de Control y Registro Académico), el cual tiene extensiones web como la consulta estudiantil y docente https://acrate.corposucre.edu.co (Ilustración 5), en el cual se encuentran una serie de accesos directos que direccionan a los diferentes aplicativos de acuerdo al rol como la plataforma virtual SPLAVIA dirigida a estudiantes y docentes (Ilustración 6).

Ilustración 4 Sistema ACRATE escritorio



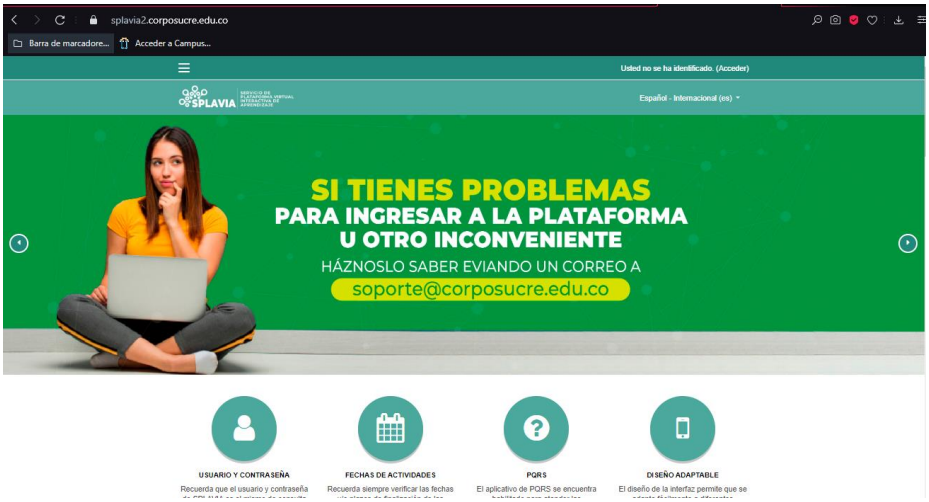
Fuente: División de Tecnologías, Sistemas de Información y Recursos Educativos

Ilustración 5 Consulta estudiantil y docente



Fuente: https://acratenew.corposucre.edu.co/

Ilustración 6 Plataforma SPLAVIA



Fuente: https://splavia2.corposucre.edu.co

Con respecto a la tecnología a utilizar en el presente proyecto se encuentran software de carácter Open Source, en el caso de herramientas de auditorías informáticas se encuentran las distribuidas en los sistemas operativos de la familia GNU LINUX, los cuales son potentes y también de carácter Open Source, en el caso de los aplicativos ofimáticos se encuentran Microsoft Office y la Suite de Google Apps otorgados por la Corporación Universitaria Antonio José de Sucre para la ejecución del presente proyecto.

4.6 MARCO LEGAL

El Gobierno de Colombia ha adelantado mediante su poder legislativo la creación de leyes orientadas a la protección de datos del usuario final que vendría siendo un ciudadano de dicha nacionalidad, en el mismo ejercicio de creación se ha visto obligado en derogar con fines de actualización con el fin de actualizar o modificar normatividad ya creadas, a continuación, se detallan las normas vigentes en la realización del presente proyecto:

LEY 1221 DE 2008

“Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones”.

En el año 2020 el teletrabajo se volvió un tema de moda en las organizaciones, ya que la mayoría de las instituciones lo implementaron puesto que se vieron enfrentadas a una pandemia mundial, esta ley promueve y regula el teletrabajo como una forma de trabajar mediante el uso de tecnologías de la información y telecomunicaciones[31].

LEY 1266 DE 2008

“Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”.

Esta ley busca dar a conocer a las personas el derecho que tienen sobre conocer su información contenida en bases de datos y garantizarle el manejo de esta además de mantenerla actualizada.

[31] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1221 de 2008. Bogotá. 2008

La ley es aplicable al proyecto puesto que Corposucre maneja información en sus bases de datos de los aspirantes estudiantes, docentes, personal administrativo y proveedores los cuales podrían acceder en cualquier momento mediante esta ley a ejercer su derecho de rectificar su información y actualizarla[32].

LEY 1273 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”.

Esta ley busca identificar los delitos informáticos y darle un valor ante la justicia para poder procesar a los individuos que infrinjan los artículos expresados en esta.
La ley es congruente con el proyecto puesto que la institución maneja distintos softwares, cuenta con un sitio web, numerosos activos informáticos y maneja información personal y financiera de personas[33].

DECRETO NÚMERO 1377 DE 2013

Dicta Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1, 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”.

[32] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley Estatutaria 1266 de 2008. Bogotá. 2008
[33] Ibíd. Ley 1273 de 2009. Bogotá. 2009

Este decreto es aplicable al proyecto ya que la institución tiene sistemas para correcta recolección de los datos de las personas (estudiantes, docentes y administrativos), y estos pueden verificar su correcto almacenamiento y tratamiento a sus datos[34].

LEY 1712 DE 2014

“Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.

Esta ley también es llamada ley de transparencia puesto que les da las facultades a las personas de poder acceder a la información pues esta se considera publica, sin dejar de lado las condiciones y procedimientos que se requieren para esto, cuando se dice condiciones se refiere a que existe información que es considerada constitucionalmente como excepción[35].

DECRETO 1008 DE 2018

“Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones”.

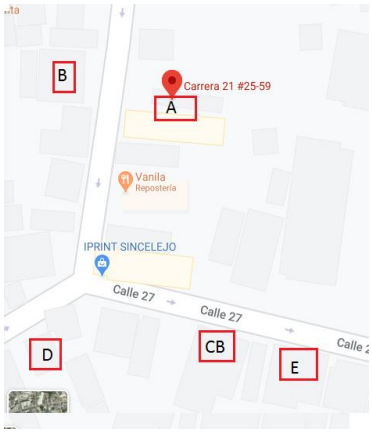
Este decreto es aplicable al proyecto puesto que busca promover la seguridad para con el usuario final mediante reglamentaciones que garanticen el acceso a la información en línea de una forma ininterrumpida y actualizada[36].

[34] MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1377 de 2013. Bogotá. 2013.
[35] CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1712 de 2014. Bogotá. 2014
[36] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1008 del 14 de junio de 2018. Bogotá. 2018

4.7 MARCO ESPACIAL

La Corporación Universitaria Antonio José de Sucre se encuentra ubicada en el departamento de Sucre y en la capital Sincelejo, cerca de la zona céntrica de la ciudad en donde actualmente cuenta con sedes administrativa y académicas muy cercana entre una y otra permitiendo la fácil movilización de los estudiantes y docentes, además de las sedes la institución cuenta con un consultorio jurídico ubicado un poco más en la zona céntrica, en la ilustración 7 presentada a continuación se describen las zonas geográficas de las respectivas sedes:

Ilustración 7 Mapa sede A, B, CB, D, E

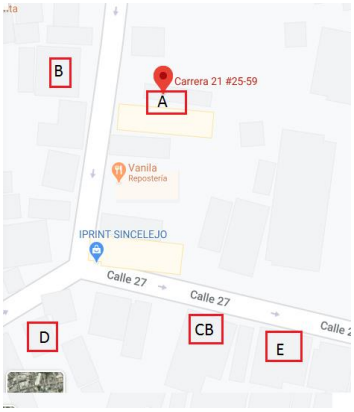


Fuente: Google Maps

A: Sede A, punto de referencia, se encuentran Área administrativa y académica, ubicada en Carrera 21 # 25-59 Barrio La María
B: Sede B, Área académica
D: Sede D, Área académica
E: Sede E, Edificio nuevo, Área administrativa y académica
CB: Área administrativa
La sede C ubicada en la dirección Carrera 19 A # 28A - 109 Avenida Alfonso López, es

la sede un poco más lejana de las demás sin embargo según Google Maps cuenta con una distancia de 500 metros lo que equivale a 7 minutos de desplazamiento caminando, las anteriores informaciones se muestran en las ilustraciones 8 y 9.

Ilustración 8 Mapa sede C



Fuente: Google Maps

Ilustración 9 Distancia entre sede A y sede C

Fuente: Google Maps

5 DISEÑO METODOLÓGICO

El proyecto está orientado en una investigación aplicada con la cual se busca generar conocimiento a partir de su implementación en una entidad real, la metodología es de carácter cualitativa y cuantitativa ya que se utilizó instrumentos que permiten realizar un diagnóstico orientado al contexto real de la organización para el diseño del Sistema de Gestión de Seguridad de la Información.

La investigación tiene factor cualitativo a causa de las entrevistas realizadas a los funcionarios del área encargada para conocer los procedimientos de aseguramiento de la disponibilidad, la confidencialidad y la integridad de los datos, de igual manera se realizó la observación de la infraestructura tecnológica. Con respecto al factor cuantitativo se realizó encuestas al actor con mayor frecuencia de uso de las instalaciones y aplicativos de la institución como lo es el personal administrativo, además que se utilizó otras herramientas como el análisis de riesgo.

Adicional a las metodologías anteriormente enunciadas, se implementó 2 tipos de metodología: la explorativa y la descriptiva. Explorativa porque se indagó procesos similares aplicados. Descriptiva porque se documentó el diagnóstico del estado actual de la seguridad de la información.

5.1 FUENTES DE INFORMACIÓN

La información es de carácter documental por lo que la fuente que refiriere es primaria teniendo en cuenta que la información se obtuvo a través de visitas, entrevistas y encuestas; es de tipo documental a causa de las referencias en cuanto a los documentos de carácter público como la historia, misión, visión, objetivos, organigrama entre otras e información de carácter privada como informes de la institución

5.2 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

Dentro de las técnicas de tipo cualitativa se puede listar la entrevista al personal que administra los sistemas de información, encargado del Sistema de Gestión de la Calidad, talento humano y alta dirección, la visita realizada a las instalaciones de la institución como el DATACENTER y diferentes sedes en Sincelejo y sede Montería

De las técnicas de recolección de tipo cuantitativa, se puede enunciar el cuestionario orientado a cada tipo de actor principal de la institución y la lista de chequeo para el análisis de la brecha.

5.3 POBLACIÓN Y MUESTRA

La población es conformada por el personal administrativo de la institución Corporación Universitaria Antonio José de Sucre, a sabiendas que dicha población es finita, la muestra probabilística se define en la siguiente fórmula:

$$n = \frac{N.Z_{\alpha}^{2}.p.q}{d^{2}(N-1)+Z_{\alpha}^{2}.p.q}$$

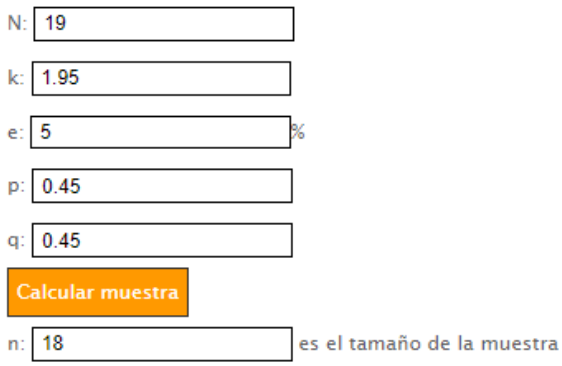
Donde:
N: tamaño de la población
Z: nivel de confianza en %, se referencia en décima con la letra K
p: probabilidad de éxito
q: probabilidad de fracaso
d: margen de error máximo permitido.

5.4 CALCULO DE LA MUESTRA

Para la identificación de la muestra (n) de manera segura, se utiliza la herramienta online Feedback Networks utilizando los valores reflejados en la ilustración 10

N: 19 (dependencias) k: 1.95 p: 0,5 q: 0,5 e: 4,5%

Ilustración 10 Cálculo de la muestra online Feedback Networks



Fuente: Autor

5.5 METODOLOGÍA DE DESARROLLO

La metodología consiste en la gestión del riesgo de los procesos establecido en la norma ISO el cual consiste en la metodología PHVA (Planear, Hacer, Verificar y Actuar), cabe resaltar que la implementación del presente proyecto tiene como alcance contemplar la primera fase, planear, adicional a ello para el inicio del presente trabajo se solicita con antelación la autorización de la institución para el desarrollo de las actividades inherentes a los procesos del presente trabajo de grado

6 DESARROLLO DE LOS OBJETIVOS

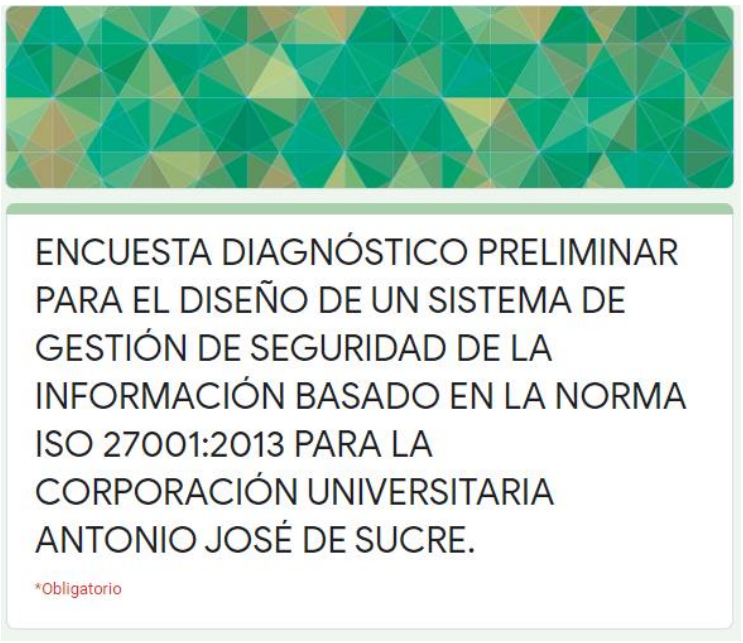
6.1 DIAGNÓSTICO DEL ESTADO ACTUAL DE LA SEGURIDAD DE LA INFORMACIÓN DE LA CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE

Los instrumentos utilizados para realizar un diagnóstico preliminar del estado de la seguridad informática en la institución fueron una encuesta dirigida al personal administrativo y académico de la institución y una entrevista dirigida al personal TI, cuyos resultados se describen a continuación:

6.1.1.1 Encuesta

La encuesta dirigida al personal de la Corporación Universitaria Antonio José De Sucre tiene como fin recolectar información sobre el estado inicial de la seguridad de la información en dicha institución, para ello se diseñó mediante la herramienta en línea Google Forms, teniendo en cuenta la situación de cuarentena ocasionada por la Pandemia COVID-19, fue aplicada a un total de 18 participantes y tiene como nombre “ENCUESTA DIAGNÓSTICO PRELIMINAR PARA EL DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA LA CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE”.

Ilustración 11 Encuesta en Google Forms



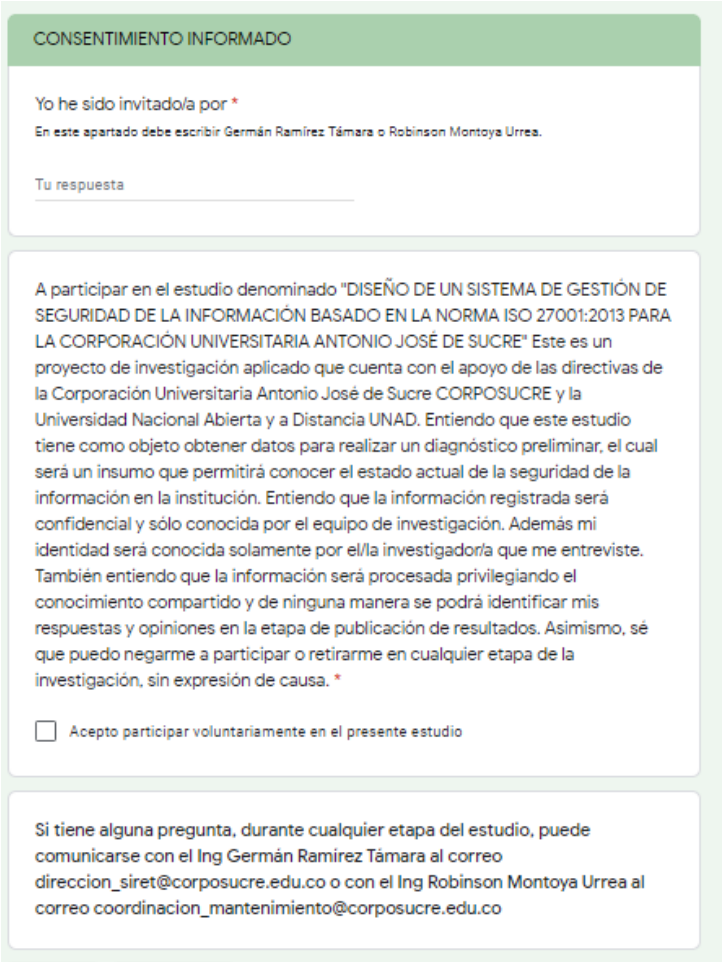
Fuente: Autores

La encuesta cuenta con 3 secciones:

- Información Contextual del funcionario participante
- Conceptos relacionados con la seguridad de la información
- Activos de seguridad de la información

Antes del diligenciamiento de este se solicita el consentimiento informado como se evidencia a continuación:

Ilustración 12 Consentimiento Informado Encuesta



Fuente: Autores

Dentro de los resultados de la encuesta que cuya ampliación de cada punto se evidencia en el anexo A6 se analizaron diferentes puntos de los controles del Anexo A de la norma ISO 27001 versión 2013, de los cuales se permite resaltar los siguientes:

Sección 1. Información Contextual del funcionario participante

- El 31,8% de los participantes tiene el cargo de Director.

- El 44,4% su nivel es profesional
- Hubo una participación de 11 áreas distinta
- El 33,3% es líder de proceso

Sección 2. Conceptos relacionados con la seguridad de la información

- El 55,6% no conocen la Política de Datos Personales.
- De los encuestados que contestaron que sí conocen la Política de Datos Personales el 50% comprenden completamente la política.
- De los encuestados que no contestaron que no conocen la Política de Datos Personales, el 88,9% manifiestan que no la han socializado.
- El 88,9% no conocen sus responsabilidades en un SGSI
- El 100% de los encuestados, no han recibido socialización sobre seguridad de la información
- El 94,4% de los participantes tiene acceso a los aplicativos institucionales, es decir que cuenta con usuarios y módulos asignados.
- El 100% de los encuestados, trabajan desde sus oficinas y desde la casa, se deduce por el cambio temporal causado por la cuarentena.
- 7 empleados cumplen 3 roles, Operativo, Administrativo y de Auditoría.
- El 58,8% comparten su contraseña de acceso a los sistemas de información.
- El 53% de los encuestados, utilizan la contraseña asignada por el departamento de sistemas
- El 47,1% de los encuestados no permiten que otros empleados accedan a su equipo de cómputo
- De los encuestados que sí comparten las credenciales de acceso, el 71% le han suministrado su contraseña a otro colaborador
- El 52,9% cambian sus contraseñas de los sistemas de información y correo electrónicos entre 4 a 6 meses.

Sección 3. Activos de seguridad de la información

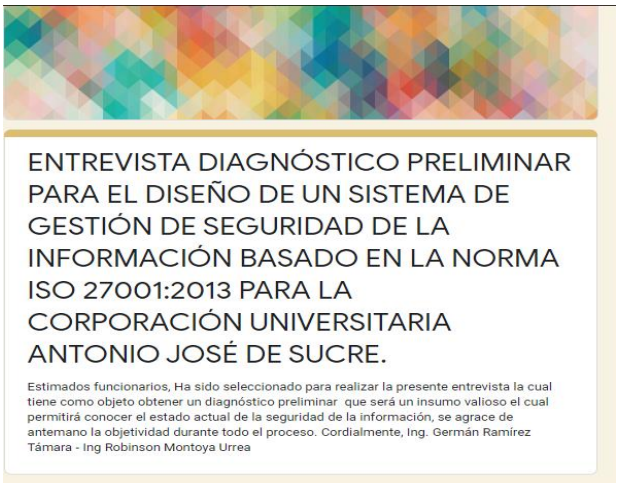
- El 40% de los usuarios manejan datos de gestión interna
- El 49% solo almacena información de gestión.
- Los softwares que utilizan los empleados son el sistema operativo Windows, ACRATE, Paquete de Ofimática y los navegadores.
- El 47% de los empleados tienen asignado un equipo de cómputo de escritorio.
- El 100% de los encuestados utilizan como medio de almacenamiento el Disco Duro del Computador, Disco duro portátil o USB y la Nube
- El 76,5% realizan copias de respaldo de manera semestral
- El 41% de los empleados cuando salen a comisión o visita oficial, utiliza el equipo suministrado por la institución.

En el anexo A6, se identifican los controles que se deberían reforzar en caso de la implementación de un SGSI

6.1.1.2 Entrevistas

Para la entrevista, se utilizó la misma herramienta que se utilizó para las encuestas, a esta se le dio el nombre de “ENTREVISTA DIAGNÓSTICO PRELIMINAR PARA EL DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA LA CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE” como se evidencia en la ilustración 13 y se aplicó el consentimiento informado como se evidencia en la ilustración 14:

Ilustración 13 Entrevista en Google Forms

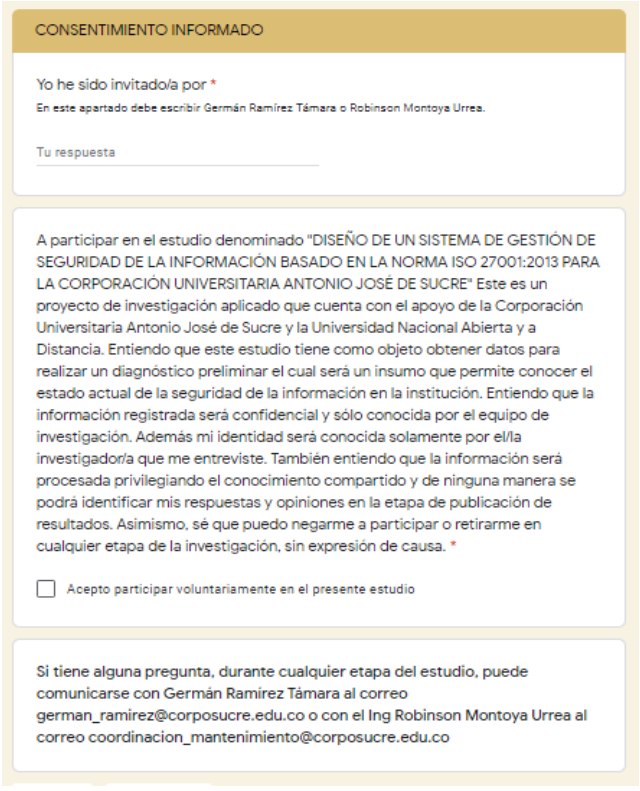


ENTREVISTA DIAGNÓSTICO PRELIMINAR PARA EL DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA LA CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE.

Estimados funcionarios, Ha sido seleccionado para realizar la presente entrevista la cual tiene como objeto obtener un diagnóstico preliminar que será un insumo valioso el cual permitirá conocer el estado actual de la seguridad de la información, se agrace de antemano la objetividad durante todo el proceso. Cordialmente, Ing. Germán Ramírez Támara - Ing Robinson Montoya Urrea

Fuente: Autores

Ilustración 14 Consentimiento Informado Entrevista



CONSENTIMIENTO INFORMADO

Yo he sido invitado/a por *

En este apartado debe escribir Germán Ramírez Támara o Robinson Montoya Urrea.

Tu respuesta

A participar en el estudio denominado "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001:2013 PARA LA CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE" Este es un proyecto de investigación aplicado que cuenta con el apoyo de la Corporación Universitaria Antonio José de Sucre y la Universidad Nacional Abierta y a Distancia. Entiendo que este estudio tiene como objeto obtener datos para realizar un diagnóstico preliminar el cual será un insumo que permite conocer el estado actual de la seguridad de la información en la institución. Entiendo que la información registrada será confidencial y sólo conocida por el equipo de investigación. Además mi identidad será conocida solamente por el/la investigador/a que me entreviste. También entiendo que la información será procesada privilegiando el conocimiento compartido y de ninguna manera se podrá identificar mis respuestas y opiniones en la etapa de publicación de resultados. Asimismo, sé que puedo negarme a participar o retirarme en cualquier etapa de la investigación, sin expresión de causa. *

☐ Acepto participar voluntariamente en el presente estudio

Si tiene alguna pregunta, durante cualquier etapa del estudio, puede comunicarse con Germán Ramírez Támara al correo german_ramirez@corposucre.edu.co o con el Ing Robinson Montoya Urrea al correo coordinacion_mantenimiento@corposucre.edu.co

Fuente: Autores

En este instrumento se utilizaron preguntas abiertas referentes a aspectos de seguridad informática, los cuales fueron analizados y dentro de los resultados se encuentran:

- Los empleados TI, enfatizan en la gran acogida de las tecnologías, por ende, la Seguridad Informática es vital para la protección de los activos de información.
- A pesar de que la institución no cuenta con un SGSI, desde el liderazgo de la alta gerencia se han trazado la implementación de este y se encuentra plasmado en el Plan de Desarrollo 2020 – 2025
- Ante la apreciación de que existen trabajos de grados orientados a la implementación completa o parcial de un SGSI, los entrevistados ven viable la aplicación de una tesis en la institución siempre se mantenga el principio de confidencialidad
- Aunque la institución a la fecha no cuenta con la Política de Seguridad de la Información, presentan una Política de Protección de Datos Personales y una Política de la División de Tecnologías, Sistemas de Información y Recursos Educativos recientemente creada, las cuales fueron revisadas y contemplan varios aspectos de la seguridad informática.
- A nivel de acceso a la información, la institución cuenta con un menú para la asignación de permisos de acuerdo con el perfil y el área que lo autoriza es Talento Humano
- La institución cuenta con dispositivos móviles para la asignación a sus empleados, la medida de control se realiza mediante la aplicación de correo electrónico que brinda informes sobre el uso
- La institución no realiza teletrabajo, sin embargo, por motivos de cuarentena por el virus COVID-19 les tocó implementar el trabajo remoto asistido por tecnología, por lo tanto, no le aplica el control A.6.2.2 Teletrabajo.
- Se demuestra cumplimiento del control A.7.1.2 Términos y condiciones del empleo
- La institución no realiza capacitaciones referentes a la seguridad de la información

- La División de Sistemas de Información, Tecnologías y Recursos Educativos, cuenta con un control de activo fijos, donde se contemplan el ciclo de vida de los equipos de cómputos y tecnológicos. Cumpliendo con los ítems A.11.2.1 Ubicación y protección de los equipos, A.11.2.2 Servicios de suministro, A.11.2.4 Mantenimiento de equipos y A.11.2.5 Retiro de activos de la norma ISO/IEC 27001
- La institución cuenta con perímetro de seguridad física, controles de acceso físico, seguridad de oficinas, recintos e instalaciones cumpliendo de esta forma con los ítems A.11.1.1, A.11.1.2 Y A.11.3 respectivamente
- Se contempla la gestión del cambio a través del Sistema de Gestión de la Calidad.
- A nivel de copia de respaldo, se manejan desde los usuarios finales utilizando como medio de almacenamiento la nube y en cuento a los sistemas de información se realiza a través de procesos automatizados a los cuales se realizan pruebas de verificación, cumpliendo con el anexo A.12.3.1 Respaldo de la información

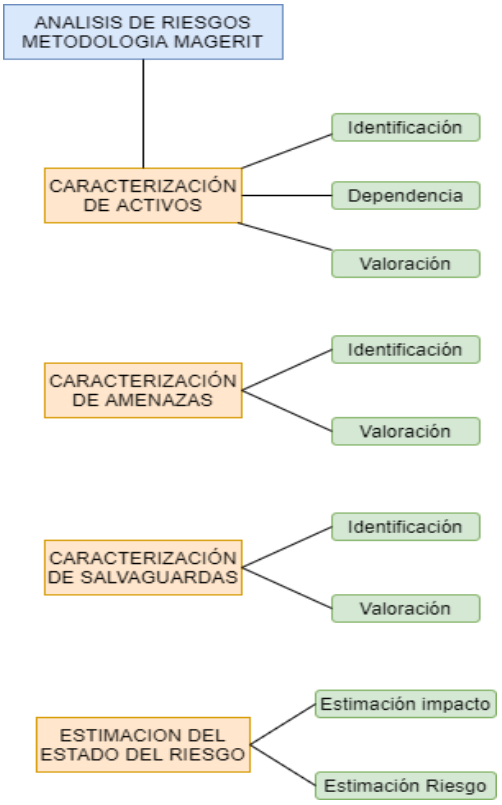
6.2 ANÁLISIS DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA METODOLOGÍA MAGERIT

Evaluar los riesgos es el principio para obtener una buena seguridad de la información, esto se lleva a cabo con el fin de identificar las vulnerabilidades y amenazas que puedan llegar a representar un impacto negativo en los activos de información trayendo consigo pérdidas económicas para la organización y afectando así la imagen de la empresa, es por esto que se debe realizar la identificación de riesgos mediante una metodología adecuada para poder tomar acciones preventivas y correctivas que eliminen o minimicen la posibilidad de un incidente.

La norma ISO/IEC 27001:2013 en el apartado 6.1 se refiere a las acciones para el tratamiento de riesgos y oportunidades y hace referencia a la importancia de realizar este procedimiento para posteriormente minimizarlos, también hace referencia a la importancia de la identificación de los riesgos para poder realizar un buen diseño de un sistema de gestión de seguridad de la información.

Para realizar la identificación de riesgos en la CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE se utilizará la metodología MAGERIT, la cual es una metodología bastante conocida en cuando a identificación y análisis de riesgos, dicha metodología utiliza una estrategia basada en la caracterización de activos, amenazas salvaguardas y estimación del estado del riesgo.

Ilustración 15 Evaluación de riesgos con la Metodología MAGERIT



Fuente: autores

Caracterización de los activos:

Consiste en identificar y establecer los activos de información con los cuales cuenta la CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE, definir el valor que estos poseen para la organización y la dependencia que tienen entre ellos, en esta fase la metodología MAGERIT dictamina el desarrollo de 3 actividades y estas son:

- Identificación de activos
- Definición de la dependencia de activos
- Valoración de activos

Identificación de activos:

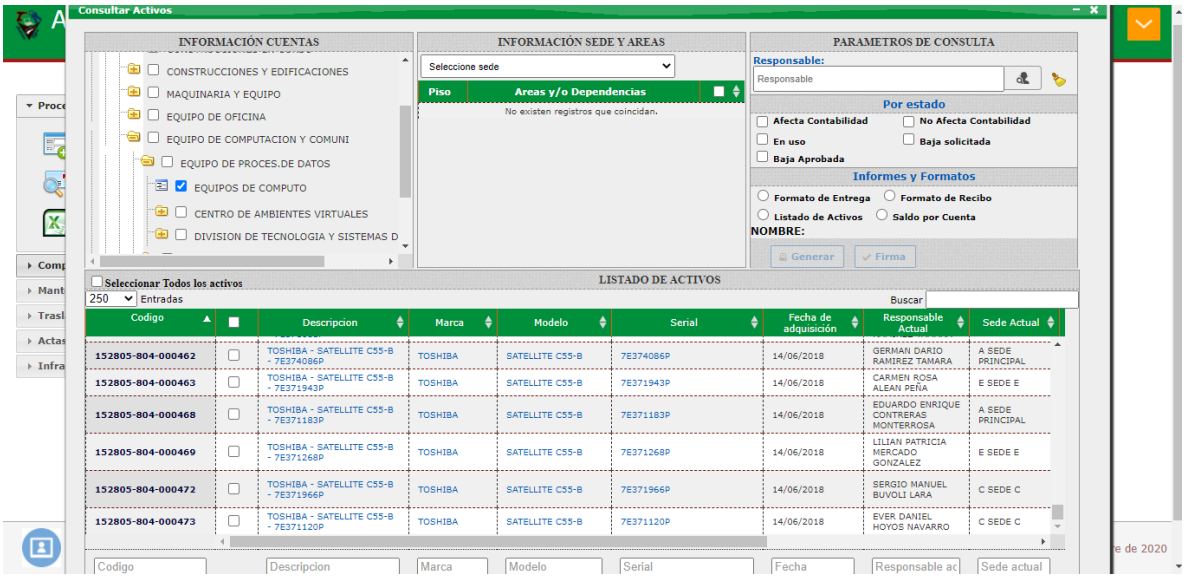
La CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE, posee activos de información y los medios para gestionarlos, es importante garantizar la confidencialidad, disponibilidad e integridad de estos para esto se diseñan las políticas de seguridad de la información.

Para realizar el proceso de identificación de activos se debe tener en cuenta el inventario general donde se detallan los equipos con los que cuenta la organización y basándose en la metodología MAGERIT los activos de información se clasificará de acuerdo con la configuración del perfil, basados en esto las computadoras personales serán denominados como (PC) solamente una vez por cada dependencia ya que todos cuentan con los mismos softwares y almacenan datos de gestión interna.

Apoyados en lo descrito anteriormente se realizó la clasificación de activos de la CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE, para facilitar los pasos venideros de la metodología MAGERIT.

A continuación, se mostrará la aplicación web SIA donde se lleva a cabo el registro y control del inventario de los activos de la corporación.

Ilustración 16 control de inventario de activos



Fuente: https://sia.corposucre.edu.co

Este es un informe en formato .xls que se puede generar sobre el inventario de activos que posee en el momento la corporación en el cual se evidencia el responsable de cada activo.

Nota: Por temas de confidencialidad con la Corporación, la información se visualiza de manera difuminada

Ilustración 17 Inventario de activos

Fuente: https://sia.corposucre.edu.co

DEPENDENCIA ENTRE ACTIVOS: En esta sección se buscará describir la dependencia que tiene un activo de otro y los efectos que estos pueden desencadenar sobre los activos que son subordinados de algún activo en caso de que ocurra un incidente.
Para determinar la dependencia entre activos se clasificaron en 4 fases.

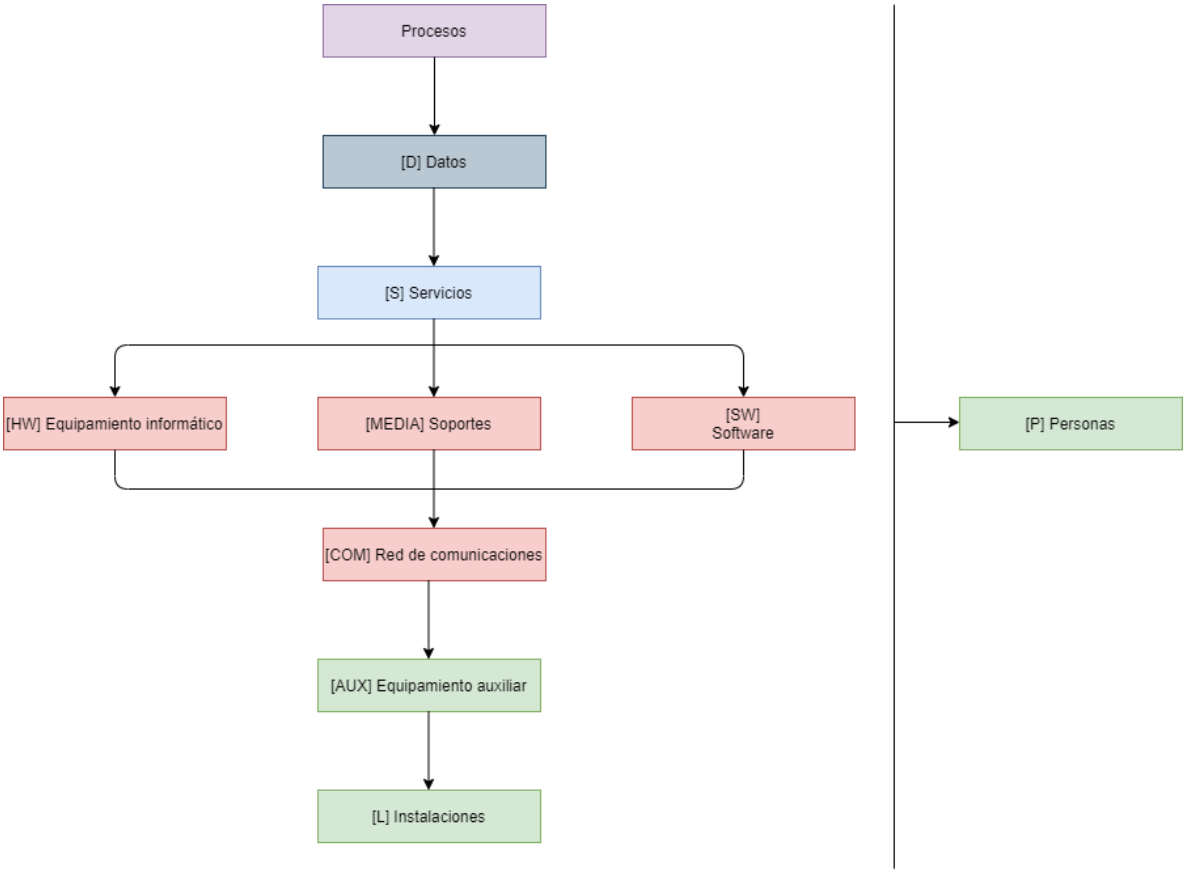
Ilustración 18 Dependencia de activos

FASE	TIPO ACTIVO	CODIGO
Fase 1: Entorno	[AUX]	[formiture], [ac], [gen], [ups], [power]
	[P]	[ue], [ui], [op], [adm], [sub], [prov]
	[L]	[bulding]
Fase 2: Sistemas de información	[HW]	[ipphone], [wap], [router], [switch], [modem], [scan], [print], [pc], [mid]
	[SW]	[os], [av], [office], [browser], [ap], [cont], [sub]
	[COM]	[LAN], [wifi], [adsl], [internet]
	[MEDIA]	[printed], [dvd], [cd], [usb]
Fase 3: Servicios	[S]	[ipm], [idm], [email], [www], [internet]
Fase 4: Datos e información	[D]	[source], [password], [int], [conf], [backup], [files], [classified],[per], [vr], [adm]

Fuente: Autores

En las 4 fases se identificaron y clasificaron los activos de información que poseen similitudes o tendrían afectaciones en caso de que otro activo sufriera un incidente.
Las fases fueron ubicadas en forma ascendente de manera que los activos que están debajo dependen de los activos que se encuentran en los niveles superiores.

Ilustración 19 Gráfica dependencia de activos



Fuente: autores

Este punto de la metodología permite establecer un valor a los siguientes niveles:

- Sin instalaciones no sería posible la existencia de equipamiento auxiliar.
- La inexistencia de equipamiento auxiliar afectaría la red de comunicaciones.
- Si no se hiciera uso de una red de comunicaciones no sería necesario la existencia de equipamiento informático, no sería necesario realizar soportes y no sería necesario el uso de software.

- Sin equipamiento informático, soportes ni software, no sería posible la prestación de servicios.
- Si no se prestan servicios no se hará gestión de información.
- Sin información los procesos no tienen un horizonte u objetivo.
- Por último, el personal afecta a todos los activos puesto que este es el que ejecuta los procesos y se encarga de que la organización sea funcional.

VALORACIÓN DE ACTIVOS: Para realizar la valorización de equipos se utilizaron matrices y se tuvo en cuenta que existen activos que son idénticos en diferentes dependencias, pero a pesar de esto no poseen el mismo valor ya que estos son utilizados de forma diferente y en procesos distintos, entonces la gestión de información en estos no es de igual valor.

- Valoración cualitativa: se desarrolló una tabla en la cual se le asignó un valor en cada uno de los pilares referentes a la seguridad informática.

Ilustración 20 Probabilidad del Riesgo

PROBABILIDAD DEL RIESGO			
	Nomenclatura	**Categoría**	**Valoración**
Probabilidad	MA	**Prácticamente seguro**	5
	A	**Probable**	4
	M	**Posible**	3
	B	**Poco probable**	2
	MB	**muy raro**	1

Fuente: ZAMBRANO HERNANDEZ, Luis Fernando; Curso de Administración y Gestión de Riesgos.

Ilustración 21 : Impacto del Riesgo

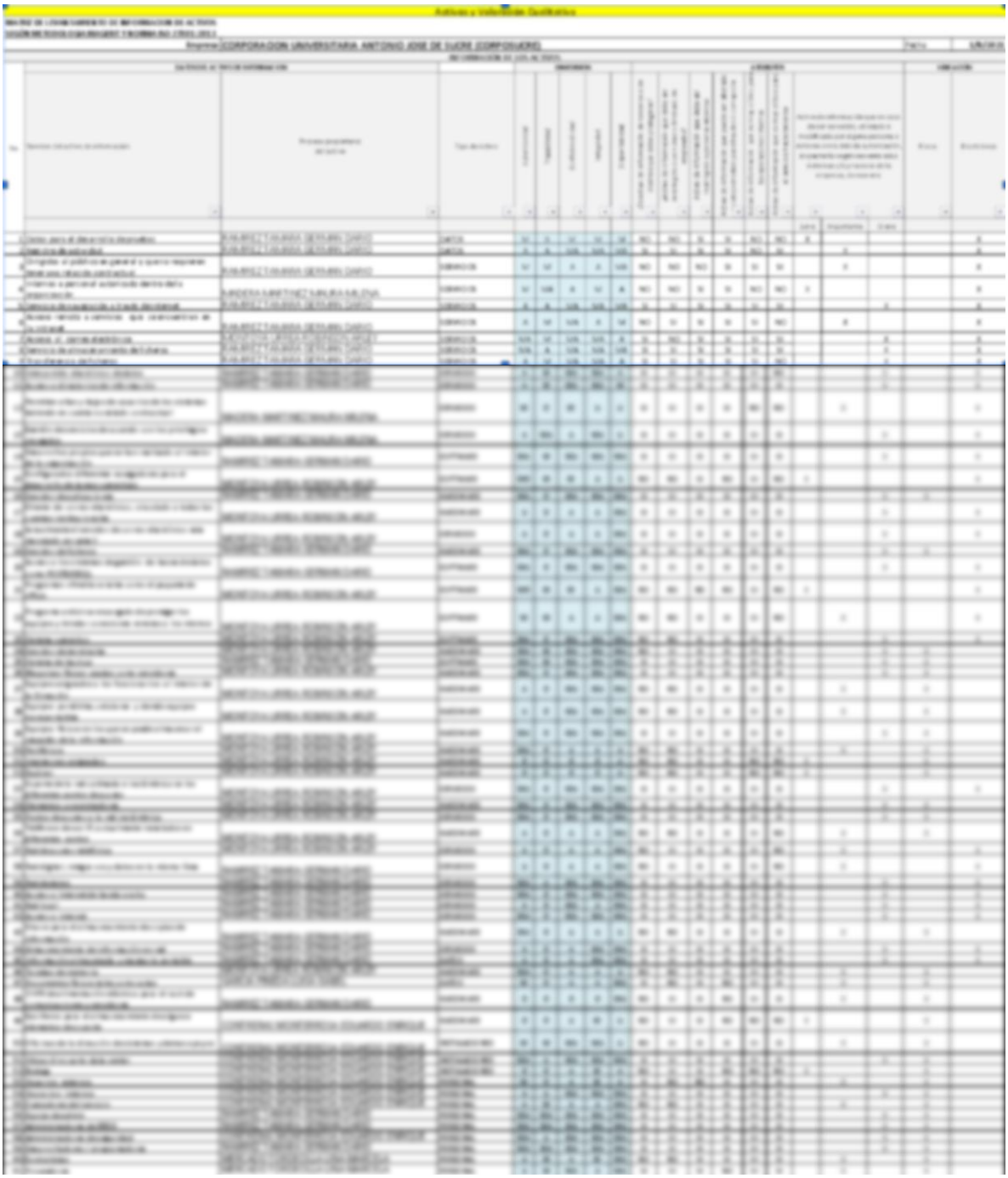
IMPACTO DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Impacto	MA	**Muy Alto**	5
	A	**Alto**	4
	M	**Medio**	3
	B	**Bajo**	2
	MB	**Muy Bajo**	1

Fuente: ZAMBRANO HERNANDEZ, Luis Fernando; Curso de Administración y Gestión de Riesgos.

A continuación, se observa la valoración que fue asignada a los activos pertenecientes a la institución de acuerdo con la criticidad y gestión del riesgo.

Nota: Por temas de confidencialidad con la Corporación, la información se visualiza de manera difuminada

Ilustración 22 Valoración cualitativa de activos



Fuente: ZAMBRANO HERNANDEZ, Luis Fernando; Curso de Administración y Gestión de Riesgos.

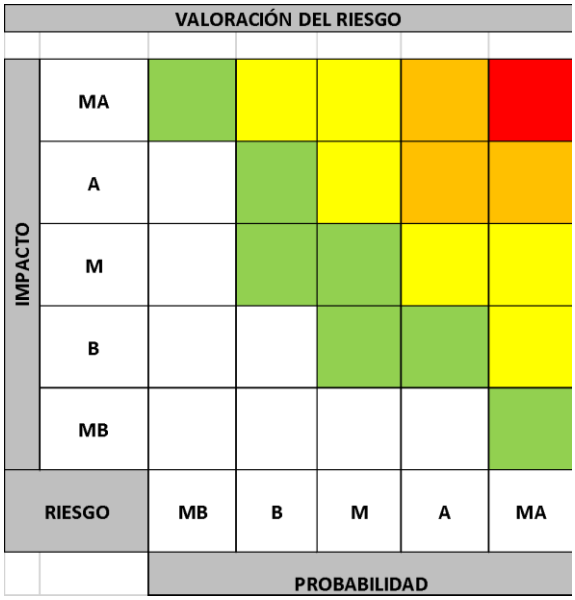
Valoración cuantitativa: para realizar la valoración cuantitativa se tiene en cuenta los valores obtenidos en la valoración cualitativa esto con el fin de darle valores a cada dimensión, se sacó un promedio y este fue asignado a cada categoría y de acuerdo con el puntaje obtenido en la valoración cualitativa el activo de información será ubicado en la escala correspondiente.

Ilustración 23 Valoración del riesgo

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: ZAMBRANO HERNANDEZ, Luis Fernando; Curso de Administración y Gestión de Riesgos.

Ilustración 24 Relación Impacto vs Riesgo



Fuente: ZAMBRANO HERNANDEZ, Luis Fernando; Curso de Administración y Gestión de Riesgos.

En la anterior tabla se muestra una variación de 1 a 25 dividida en 5 escalas, que permitirán ubicar los activos de información en cada categoría de riesgo, se entiende que la categoría crítica es la categoría con el mayor riesgo y la categoría Despreciable corresponde al menor riesgo.

Nota: Por temas de confidencialidad con la Corporación, la información se visualiza de manera difuminada

Ilustración 25 Valoración de riesgo

Fuente: ZAMBRANO HERNANDEZ, Luis Fernando; Curso de Administración y Gestión de Riesgos.

6.3 CONTROLES DE SEGURIDAD ORIENTADOS A LA NORMA ISO/IEC 27001:2013 CON EL OBJETIVO DE REDUCIR LAS VULNERABILIDADES

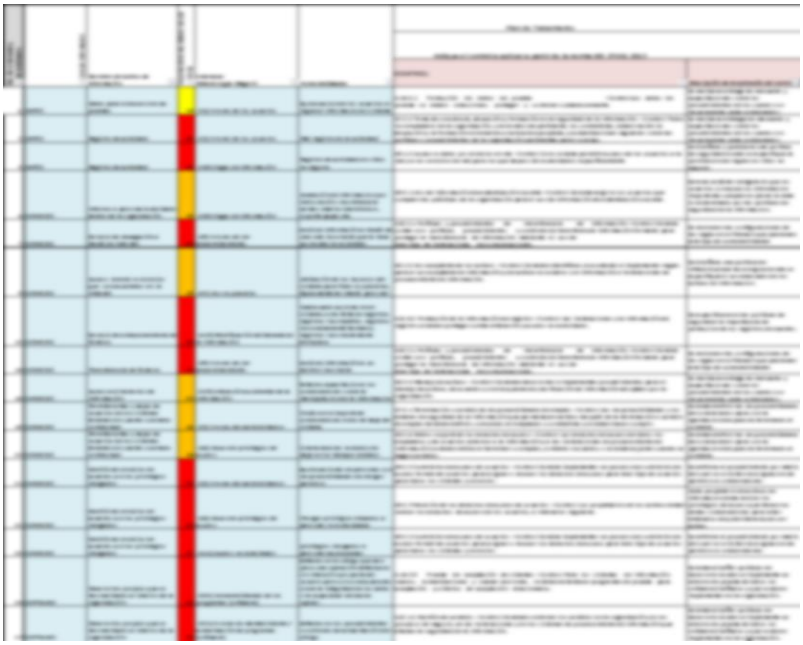
Basados en el nivel de aceptación de riesgos en el cual se determinó que solo se iban a tratar los riesgos que estén en nivel Inaceptable, se procede a identificar los controles que se consideran adecuados para mitigar o eliminar las vulnerabilidades y amenazas, también se describe la aplicación que se deberá realizar al control elegido.

En la siguiente ilustración se evidencian los activos de información y los niveles de vulnerabilidad que cada uno posee, aplicando la norma se determina el control que se debe aplicar para mitigar o eliminar la amenaza y se muestra la descripción de la aplicabilidad de dicho control.

En las ilustraciones 26 y 27 se evidencian los activos de información, las amenazas que estos poseen según la metodología Magerit y los niveles de vulnerabilidad de cada uno, aplicando la norma se determina el control que se debe aplicar para mitigar o eliminar la amenaza y se muestra la descripción de la aplicabilidad de dicho control.

Nota: Por temas de confidencialidad con la Corporación, la información se visualiza de manera difuminada

Ilustración 26 Plan de tratamiento 1



Fuente: ZAMBRANO HERNANDEZ, Luis Fernando; Curso de Administración y Gestión de Riesgos.

Nota: Por temas de confidencialidad con la Corporación, la información se visualiza de manera difuminada

Ilustración 27 Plan de tratamiento 2

Fuente: ZAMBRANO HERNANDEZ, Luis Fernando; Curso de Administración y Gestión de Riesgos.

Tabla 1 Controles y descripción de la aplicación de controles

CONTROL	DESCRIPCIÓN DE LA APLICACIÓN DEL CONTROL
A.14.2.9 Prueba de aceptación de sistemas --Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados.	Se deben diseñar políticas de desarrollo donde se implemente un entorno de prueba de todos los softwares diseñados y que se deseen implementar en la organización.
A.14.3.1 Protección de datos de prueba --Control: Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.	Se realizará entrega de manuales y capacitaciones sobre los procedimientos de los cuales son responsables cada colaborador.
A11.1.4 Protección contra amenazas externas y ambientales. --Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Se debe implementar un plan de mantenimiento preventivo para evitar fallas en los equipos antes de culminar su tiempo de vida útil.
A11.1.4 Protección contra amenazas externas y ambientales. --Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Se realizará una reparación a los equipos de refrigeración y en caso de seguir presentando fallas se procederá a reemplazarlos por nuevos equipos.
A11.1.4 Protección contra amenazas externas y ambientales. --Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	Se debe implementar un plan de mantenimiento preventivo, además se debe contar con una UPS que soporte por cierto tiempo el funcionamiento de los equipos en caso de cortes en el fluido eléctrico.

A11.2.1 Ubicación y protección de los equipos --Control: Los equipos deben de estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	Se alertará al personal de vigilancia para monitorear los dispositivos por medio del circuito cerrado de tv
A11.2.2 Servicios de suministro --Control: Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	Se realizará revisión del cableado, picos y del polo a tierra del servicio de fluido eléctrico.
A11.2.4 Mantenimiento de los equipos. --Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	Se debe implementar un plan de mantenimiento preventivo para evitar fallas en los equipos antes de culminar su tiempo de vida útil.
A12.1.1 Procedimientos de operación documentados --Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.	Se realizará la entrega de manuales de procedimientos a cada colaborador y se realizarán capacitaciones.
A12.1.2 Gestión de cambios --Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Se deben diseñar políticas de desarrollo donde se implemente un entorno de prueba de todos los softwares diseñados y que se deseen implementar en la organización.
A12.1.2 Gestión de cambios --Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Será de carácter obligatorio tener las actualizaciones automáticas activadas para garantizar que todos los softwares estén actualizados.
A12.1.2 Gestión de cambios --Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	Se actualizarán todos los equipos de cómputo al paquete de office más actualizado.

A12.4.2 Protección de la información de registro --Control: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	Se especificará en las políticas de seguridad la importancia de protección de los registros de eventos.
A13.1.2 Seguridad de los servicios de red --Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Se verificará que este equipo cumpla con los requisitos mínimos para prestar un óptimo servicio, de no ser así se procederá a realizar cambio de equipo.
A13.1.2 Seguridad de los servicios de red --Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	Diseñar acuerdos de servicio de red, donde se especifiquen las configuraciones con las que cuenta la red de la organización.
A13.2.1 Políticas y procedimientos de transferencia de información --Control: Se debe contar con políticas, procedimientos y controles de transferencia información formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	Se revisarán las configuraciones de las reglas en el firewall que previenen este tipo de vulnerabilidades
A18.1.3 Protección de registros --Control: Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	Se almacenarán los documentos que estén en físico en un lugar adecuado para evitar el deterioro y se irán digitalizando para que perduren en el tiempo sin correr tanto riesgo de daño.
A7.2.2 Toma de conciencia, educación y formación en la seguridad de la información. --Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización	Se realizará entrega de manuales y capacitaciones sobre los procedimientos de los cuales son responsables cada colaborador.

pertinentes para su cargo.	
A7.2.3 Proceso disciplinario --Control: Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	En el contrato firmado con la organización se debe especificar el horario que debe estar disponible el colaborador y en qué casos es justificable su ausencia.
A7.3.1 Terminación o cambio de responsabilidades de empleo --Control: Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	Se deben definir las responsabilidades del colaborador para con la organización después de terminado el contrato.
A8.1.3 Uso aceptable de los activos --Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	Se diseñará una política de infraestructura tecnológica donde se especifique el uso adecuado de los activos de información.
A8.2.3 Manejo de activos --Control: Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	Se realizará entrega de manuales y capacitaciones sobre los procedimientos de los cuales son responsables cada colaborador.
A9.3.1 Uso de información de autenticación secreta --Control: Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	Será de carácter obligatorio que los usuarios con acceso a información importante cumplan al pie de la letra lo dictaminado por las políticas de seguridad de la información.

Fuente: Autores.

6.4 RESUMEN EJECUTIVO

El presente resumen ejecutivo está basado en el análisis de los resultados obtenidos por la aplicación de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) en su versión 3, cuyo entorno técnico fue enfocado en los activos de información de la Corporación, el cual se desglosa de la siguiente manera:

Clasificación general de los activos

La Corporación Universitaria Antonio José de Sucre, transacciona sobren más de 50 activos clasificados en Tipo Dato, Tipo Claves Criptográficas, Tipo Servicio, Tipo Software, Tipo Hardware, Tipo Comunicaciones, Tipo Soporte de Información, Tipo Equipamiento Auxiliar, Tipo Instalaciones y Tipo Personal ; de los cuales, existe una mayor proporción en los activos clasificados como de Servicio, por lo que es proporcional al objeto social de la Corporación.

Ubicación

A la fecha existe un equilibrio en cuanto la cantidad de disposición de los datos entre físico y electrónicos, por ende, se entiende la necesidad de apropiar sus procesos a los servicios tecnológicos

Clasificación de activos según su valor

En el análisis realizado, se identifica la clasificación de activos según su valor, de los cuales se sugiere una revisión interna sobre aquellos datos que deben ser restringidos a personas externas, esto con el motivo principal de controlar en su mayor esfuerzo la fuga de datos innecesarios, otros de los activos importantes a revisar son aquellos que pueden ser alterados o comprometidos para fraudes o corrupción ya que como lo demuestra los controles definidos, el apoyo a las medidas que actualmente se implementa debe ser enfocado en aquellos usuarios que operan constantemente con los datos; ahora bien, se resalta que la institución dentro de sus medidas se logra mapear que persona iteró con

cierto proceso, se puede robustecer el sistema de acceso inicial con técnicas de verificación de 2 pasos para consolidar la autentificación.

Como toda entidad, existen activos con diferentes niveles de criticidad, por lo tanto, gracias al ejercicio realizado con MAGERIT, su completa identificación permite tomar decisiones en cuanto a los controles que apunten a la integridad, confidencialidad y disponibilidad; de igual forma, se ha identificado en menor medida activos de información que deben ser restringidos a un número limitado de empleados, aunque es un comportamiento muy común en las organizaciones en donde en ocasiones hay personas que poseen más privilegios a nivel de menú de sistema u otras configuraciones, lo que puede conllevar al escalamiento de privilegios y aunque en el caso de la Corporación, esta condición fue evidenciada en situaciones mínimas se sugiere tomar medidas en cuanto a lo hallado. Para finalizar, en cuanto a los activos clasificados según su valor y enfocados en los clientes, existen unos activos de este tipo de usuario que deben fortalecerse con el fin de que todo su historial se resguarde ya que los estudiantes quienes son los clientes consultan de ella cualquier día de la semana y a cualquier hora, inclusive cuando ya son egresados.

Clasificación según el impacto a la seguridad

Si bien, cuando se hace referencia a la seguridad informática es diciente enfocarse en lo que se debe hacer (control) para que algo no ocurra (vulnerabilidad); sin embargo, una consigna propia de la seguridad informática se basa en que no se puede asegurar en un 100% todo un sistema, por ello se hace necesario contemplar un escenario en el cual el hecho ocurra para poder medir las consecuencias y en efecto las acciones para restablecer la continuidad del negocio y el resultado de este análisis ha remitido que son mayores los impacto de seguridad grave que los importantes o leve, dado a que el CORE del negocio ya está en funcionamiento en los servicios tecnológicos a lo que es consecuente su priorización emanada de una constante actualización en materia de seguridad.

Resumen de nivel de riesgo en los activos

Para concluir y como es natural, los activos que cada vez más son incluidos a los sistemas informáticos se transforma o se adicionan los riesgos inherentes de este, a lugar que se debe realizar un especial énfasis en aquellos identificado como “Extremo” y “Alto” porque sin la aplicación adecuada de los controles y una planificación para restablecer los servicios tras un ataque exitoso tanto las operaciones como el status de la institución pueden tener repercusiones inclusive en el ámbito legal.

Resultado de Encuesta y Entrevistas

Dentro de los resultados del levantamiento de información contextual de carácter cualitativo y cuantitativo se logra concluir que la Corporación a nivel de la Seguridad Informática, a pesar de que no cuenta con la implementación de un Sistema de Gestión de la Seguridad de La Información (SGSI), posee fortalezas que le permite responder a las necesidades tecnológicas con aspectos relevantes de seguridad y a su vez le permite responder a las normativas legales vigentes; sin embargo, dentro de los hallazgo de la encuesta se logra evidenciar que se requieren esfuerzos de sensibilización sobre las responsabilidades de dicha normatividad; adicionalmente, existen opciones de mejoras en cuanto a la operación de los usuarios finales, que se pueden atender además de tecnologías y procedimientos estandarizados con un acompañamiento y seguimiento de cumplimiento que se podrá lograr con la implementación completa del SGSI, El cual ya se encuentra contemplado por lo manifestado en la entrevista y constatado con el Plan de Desarrollo.

7 CONCLUSIONES

La institución actualmente en términos de seguridad informática presenta ciertas desventajas al no tener consolidado el Sistema de Gestión de la Seguridad Informática en donde se resaltan aspectos como falta de sensibilización al personal sobre aspectos referentes sobre el SGSI y su rol o responsabilidades, así como malas prácticas como compartir las credenciales de acceso con otros colaboradores y la poca frecuencia de cambio de dichas credenciales.

Se debe resaltar que la institución demuestra voluntad propia en pro de optimizar sus procesos y tecnologías en aras de mejorar la seguridad de la información, reconociendo los datos como un activo valioso de la institución.

El análisis de riesgos realizado por medio de la metodología MAGERIT, permitió identificar vulnerabilidades y la probabilidad de estas materializarse, también el impacto que estas tendrían en la organización, se identificaron 33 riesgos en clasificación extrema, 21 riesgos en clasificación alta, 2 riesgos en media y 5 en baja.

Concluyendo los estudios realizados se puede afirmar que es urgente que se implemente un sistema de gestión de seguridad de la información en la institución ya que se pudo evidenciar que existen muchos riesgos que aún no son tratados y que en cualquier momento se pueden materializar y causar grandes pérdidas a la organización.

8 RECOMENDACIONES

Con respecto a las Políticas actuales relacionadas con la Seguridad de la Información como la Política de Protección de Datos Personales y Política de Infraestructura Tecnológica se sugiere diseñar estrategias que permitan la fácil receptividad por los empleados, así como una evaluación para conocer dicho nivel de receptividad.

Conformar un comité de seguridad informática, independientemente de la aplicación completa del SGSI o el tiempo de ejecución de las otras fases, teniendo en cuenta que constantemente se debe estar a la vanguardia con el fin de cerrar las oportunidades de vulneración con nuevas técnicas.

Continuar con las fases para completar el esquema de implementación del SGSI y en su efecto que se permita ser certificado, lo anterior no solo aportará un gran plus para los usuarios de la institución, sino que también aporta a la sociedad local y nacional el concepto de la importancia que tienen los datos en una entidad como lo es una Institución Educativa.

BIBLIOGRAFÍA

ALMANZA, Andrés Ricardo. REVISTA SISTEMAS. {En línea}. {17 de mayo de 2013} Disponible en: (http://52.0.140.184/revsistemas1/index.php/ediciones-revista-sistemas/edicion-no127/item/132-seguridad-inform%C3%A1tica-en-colombia-tendencias-2012-2013)

BAQUERO, Magda Mayery. Diseño Del Sistema De Gestión De Seguridad De La Información Para La Empresa Comfenalco Quindío. Armenia, 2019, 63 p. Trabajo de Grado para optar al título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias del cibercrimen 2021 -2022 Nuevas amenazas al comercio electrónico. Bogotá. 2021

CELY, Ronald Mauricio. Diseño del Sistema de Gestión de Seguridad de la Información (SGSI) con base al Modelo de Seguridad y Privacidad de la Información según lineamientos del Ministerio de las Tecnologías de la Información y las Comunicaciones en el marco de la estrategia GEL (Gobierno en Línea) y en cumplimiento del Decreto 1078 De 2015 y 2573 De 2014. Bogotá. 2018. 424 p. Proyecto aplicado para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1273 de 2009. Bogotá. 2009

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1221 de 2008. Bogotá. 2008.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley 1712 de 2014. Bogotá. 2014.

CONGRESO DE LA REPÚBLICA DE COLOMBIA. Ley Estatutaria 1266 de 2008. Bogotá. 2008.

CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE. Historia. Sincelejo. 2020.

CORPORACIÓN UNIVERSITARIA ANTONIO JOSE DE SUCRE. Plan Estratégico de Desarrollo para la Corporación Universitaria Antonio José de Sucre – CORPOSUCRE 2020-2025. Sincelejo. 2020.

CORPORACIÓN UNIVERSITARIA ANTONIO JOSÉ DE SUCRE. Política de Protección de datos personales. Sincelejo. 2020.

CORPORACIÓN UNIVERSITARIA ANTONIO JOSE DE SUCRE. Políticas de Infraestructura Física y Tecnológica. Sincelejo. 2020.

COSTAS SANTOS, Jesús. Seguridad Informática. ISBN: 9789588675701. Bogota: Ediciones de la U, 2011, 308p.

GARCÍA, Juliana. Uso de tecnologías de pruebas de penetración para validación de seguridad de aplicaciones web basado en el top 10 de vulnerabilidades de OWASP. Sabaneta, 2018, 41 p. Trabajo de Grado de tipo Monografía para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

GUEVARA, Estefani. Alcances que puede tener una investigación forense dentro de un proceso legal en Colombia. Bogotá, 2018, 61 p. Trabajo de Grado de tipo Monografía para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

HERNÁNDEZ, Sandra Milena. Implicaciones de la Seguridad Informática en la Legislación Colombiana. Manizales, 2018, 65 p. Trabajo de Grado de tipo Monografía para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN ICONTEC. Certificación ISO 27001, Sistemas de Gestión de seguridad de la información. Bogotá. 2020.

ISOTOOLS EXCELENT. Pilares fundamentales SGSI. Argentina. 2015.

MARIN GUINEME, Ana Milena & CARVAJAL CARVAJAL Oscar Javier. Estudio monográfico sobre casos más comunes de cibercrimen en las pymes colombianas. Bogotá, 2018, 84p. Trabajo de Grado tipo Monografía para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

MEDINA RINCÓN, Luz Amanda. Análisis y diseño de un sistema de gestión de la seguridad de la información para la Dirección de Sistemas de la Universidad de la Sabana. Chía, 2019, 36p. Trabajo de Grado tipo Proyecto Aplicado para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería

MENDOZA GAMBOA, Denys Celin. Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/IEC 27001 para la Secretaría de Educación Departamental del Norte de Santander. Cúcuta, 2019, 33p. Trabajo de Grado tipo

Proyecto Aplicado para optar por el título de Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Facultad Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO. Decreto 1377 de 2013. Bogotá. 2013.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1008 del 14 de junio de 2018. Bogotá. 2018.

ORDUZ BARRERA, Diana Maria. Análisis de emergencias cibernéticas que se presentan en las ciudades de Tunja, Duitama y Sogamoso con respecto al resto del país en los últimos 2 años. Sogamoso, 2018, 75p. Trabajo de grado. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas.

ORGANIZACIÓN INTERNACIONAL DE POLICÍA CRIMINAL INTERPOL. Ciberdelincuencia. Francia. 2020.

PARRA CALDERON, Jairo Andres. Delitos informáticos y marco normativo en Colombia. Huila, 2019, 121p. Monografía presentada como requisito parcial para optar al título de: Especialista en Seguridad Informática. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas.

PATERNINA CUESTA, Ramon Andres. Estudio de vulnerabilidades en el proceso de cadena de custodia de evidencias en delitos informáticos en la ciudad de Cartagena. Cartagena, 2018, 71p. Proyecto de grado aplicado. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas.

RODRÍGUEZ CUADRADOS, Oscar Alberto. Diseño de manual básico de pruebas de Hacking Ético: escaneo de red, de vulnerabilidades y ataques. Bucaramanga, 2018, 78p. Trabajo de grado. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas.

RODRIGUEZ MAHECHA, Juan Hernan.Modelo para la definición e implementación de Gobernabilidad de Seguridad. Bogotá, 2009, 63p. Trabajo de grado. Universidad de los Andes. Departamento de Ingeniería de Sistemas y Computación.

SUESCUN PINEDA, Jonhatan Alexander. Estudio sobre la importancia de los sistemas de monitoreo de redes de datos en las empresas. Medellín, 2019, 95- 98p. Monografía de grado. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas.

ANEXOS

ANEXOS 1 CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD	MES1	MES2	MES3	MES4	MES5	MES6	MES7	MES8	MES9
Identificación de las partes que tendrán participación dentro del SGSI	x								
Aplicación de entrevistas y encuestas	x								
Análisis del contexto de la organización y determinación del alcance			x						
Análisis de los riesgos de seguridad mediante la aplicación de la metodología MAGERIT.			x	x					
Definir los controles de seguridad orientados					x	x			
Socialización del ejercicio realizado a las directivas de la institución									x

ANEXOS 2 RECURSOS NECESARIO

RECURSO	DESCRIPCIÓN	PRESUPUESTO
Equipo Humano	Líder de proyecto y asesor	$50.000.000
Equipos y Software	Computador portátil para líder de proyecto	$3.000.000
Viajes y Salidas de Campo	Viajes a Unitecnar Cartagena	$2.000.000
Materiales y suministros	Elementos de apoyo como tarjetas de red inalámbrica, tarjeta de red pci, memoria usb, entre otros	$500.000
Bibliografía		

TOTAL= $55.500.000

ANEXOS 3 RESULTADOS O PRODUCTOS ESPERADOS

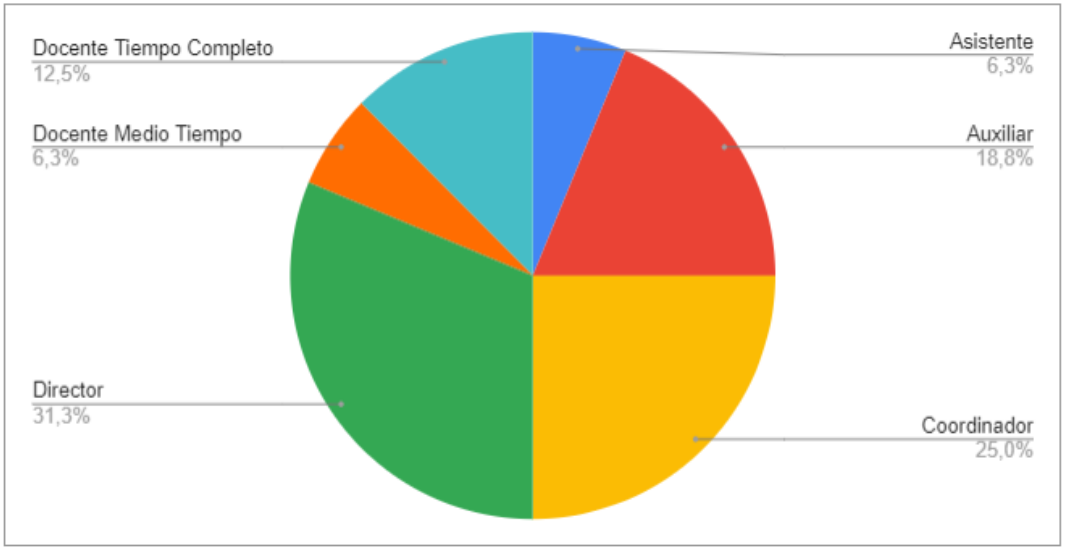
RESULTADO/PRODUCTO ESPERADO	INDICADOR	BENEFICIARIO
Diagnóstico del estado actual de la seguridad de la información	Informe del diagnóstico	División SIRET
Identificación de los activos de información y su respectiva clasificación	Implementación de la Metodología MAGERIT	División SIRET
Reducción de vulnerabilidades	Número de controles diseñados	Corporación

ANEXOS 4 ANÁLSIS DE ENCUESTA A EMPLEADOS

SECCIÓN UNO: Información Contextual del funcionario participante

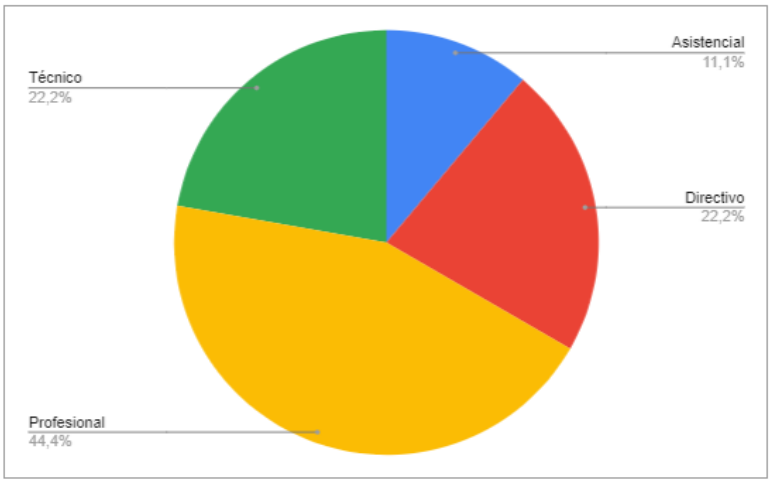
La presente encuesta tiene como propósito conocer el estado actual de la aplicabilidad de algunos aspectos referentes a la seguridad informática desde la perspectiva de los usuarios finales.

Cargo actual



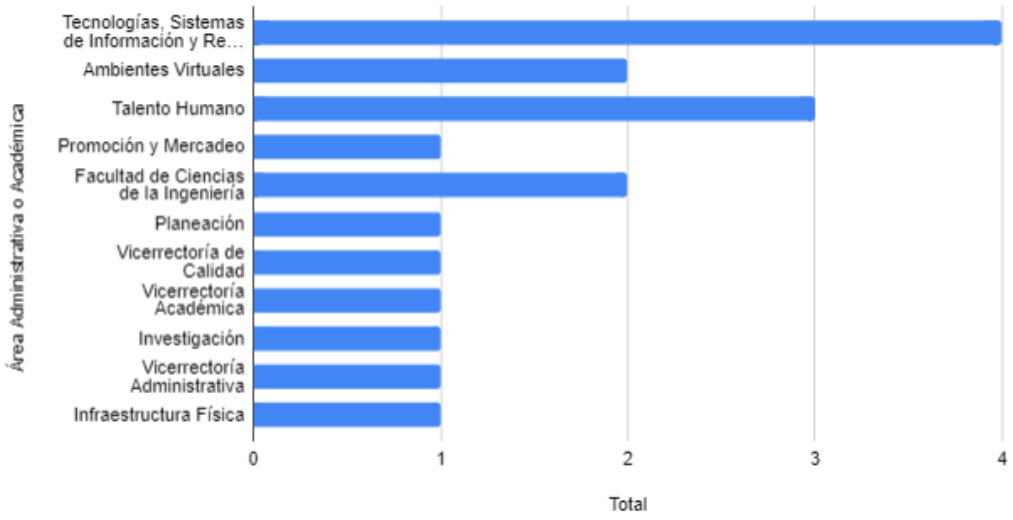
La mayor participación que se obtuvo fue la del personal con cargo de Director con un 31,3%, seguido por el cargo de Coordinador con un 25,0%, Auxiliar con 18,8%, Docente Tiempo Completo con 12,5%, Asistente y Docente Medio Tiempo con un total de 6,3% de participación cada uno, de lo anterior se deduce que hubo una participación de varias áreas de la institución.

Nivel Jerárquico



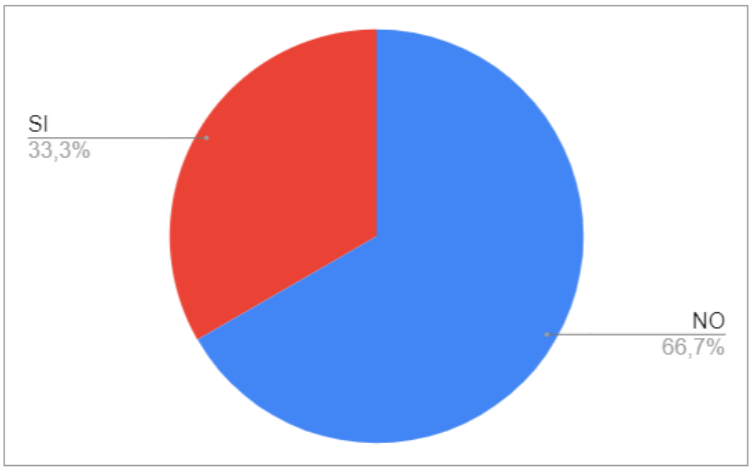
El nivel jerárquico de los empleados en su mayoría corresponde a Profesional con un 44,4%, seguido por el cargo Directivo y Técnico con un 22,2%, por último, Asistencial con un 11,1%

Área Administrativa o Académica



De las 18 participaciones, el área de Tecnologías, Sistemas de Información y Recursos Educativos tuvo mayor participación con un total de 4, seguido de Talento Humano con 3, Ambientes Virtuales y Facultad de Ciencias de la Ingeniería con 2 y con una participación las áreas de Promoción y Mercadeo, Planeación, Vicerrectoría de Calidad, Vicerrectoría Administrativa, Investigación e Infraestructura Física, para un total de 11 áreas distintas.

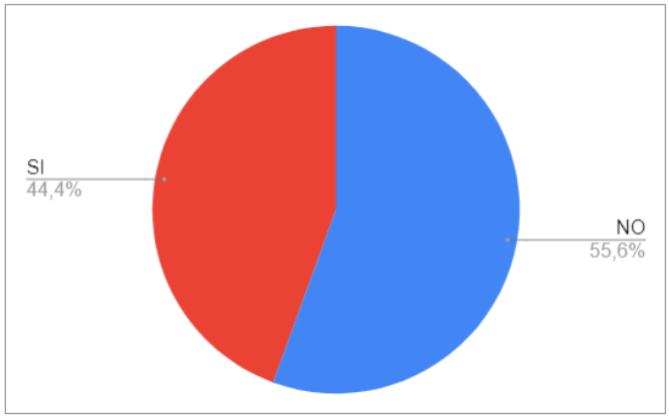
¿Es usted líder de proceso?



De los encuestados el 33,3% son líderes de los diferentes procesos establecidos en el Sistema de Gestión de Calidad de la institución, esto indica que poseen un mayor grado de responsabilidad sobre la información que maneja la entidad sobre el 66,7% de empleados restantes.

SECCIÓN DOS: Conceptos relacionados con la seguridad de la información

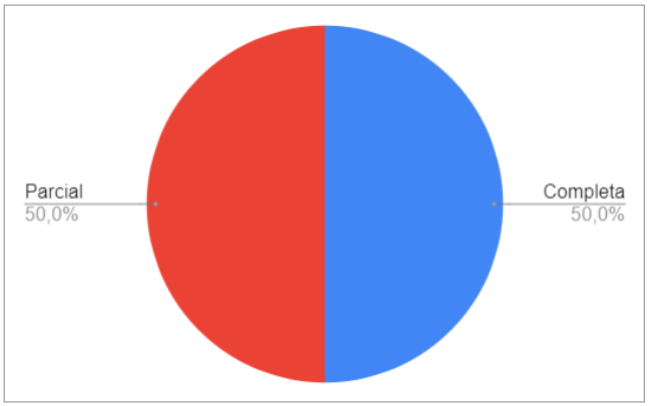
¿Conoce usted la política de protección de datos personales?



Más de la mitad de los encuestados (55,6%) no conocen la Política de Datos Personales, la cual es la más relacionada en la institución con el aspecto a SGSI, es decir la apropiación de la política es parcial.

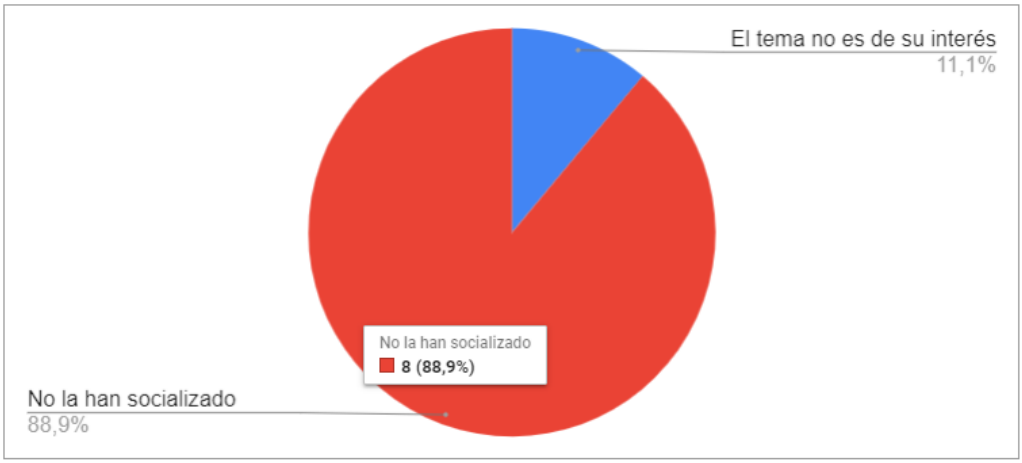
Continuación Respuesta SI

¿Su comprensión del texto de la política de protección de datos personales, es?



De los encuestados que contestaron que, sí conocen la Política de Datos Personales, la mitad de ellos comprenden completamente la política y la otra que su comprensión fue parcial, no hubo respuesta de comprensión nula, es decir que se debe idear estrategias para que la información sea más clara y tenga mayor retentiva.

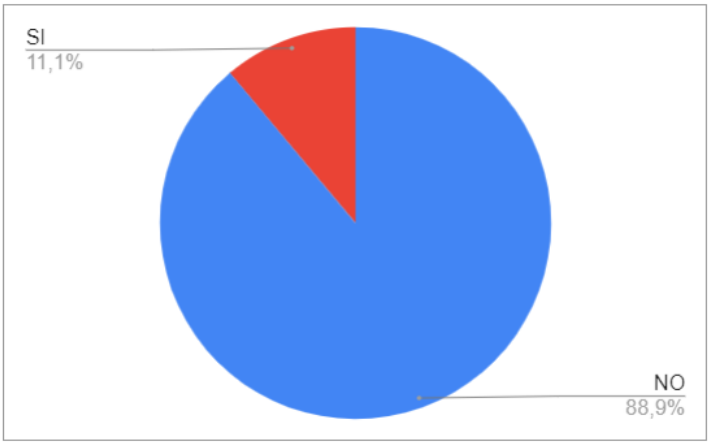
Continuación Respuesta NO



De los encuestados que no contestaron que no conocen la Política de Datos Personales, la mayoría contestaron que no la han socializado (88,9%) mientras que el 11,1% consideró que el tema no es de su interés, por lo anterior, al implementar el SGSI, se debe tener un mayor énfasis en el Anexo A de la ISO 27001, en especial el control A.6

Organización de la Seguridad de la Información, A.6.1.1 Roles y responsabilidades para la seguridad de la información

¿Sabe usted la responsabilidad que cumple dentro de un SGSI?

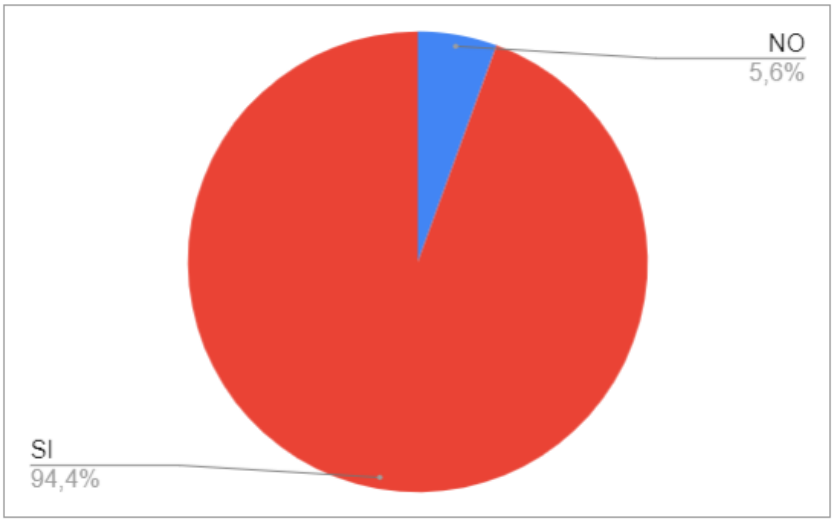


Aunque la institución no tiene implementado un SGSI, el 11% de la población sabe qué responsabilidades tienen, el 88,9% no conoce que sus responsabilidades en un SGSI

Durante el proceso de inducción o reinducción, ¿Le han socializado sobre seguridad de la información?

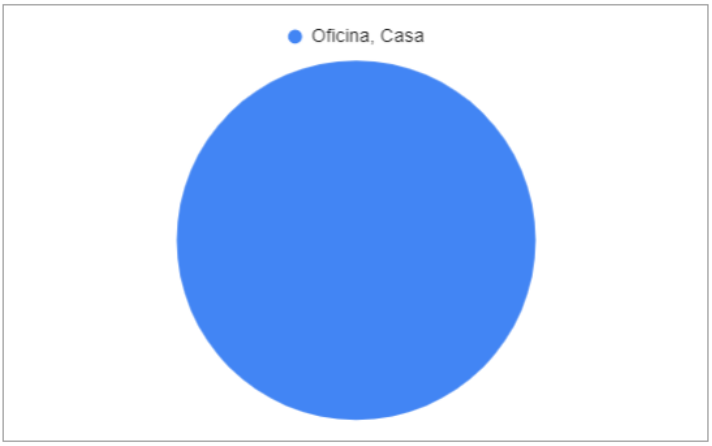
El 100% de los encuestados, no han recibido socialización sobre seguridad de la información

¿Tiene acceso a los aplicativos webs institucionales?



Casi que en la totalidad (94,4%) de los participantes tiene acceso a los aplicativos institucionales, es decir que cuenta con usuarios y módulos asignados

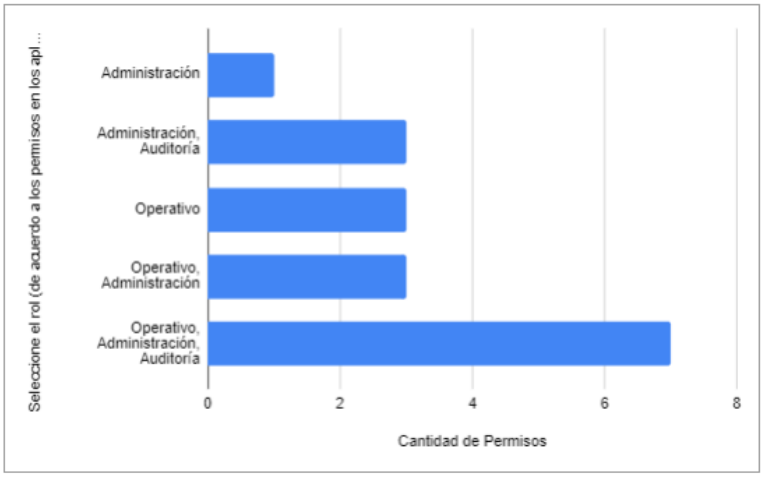
¿Desde qué lugares ha ingresado a los aplicativos webs institucionales? (selección múltiple)



El 100% de los encuestados, trabajan desde sus oficinas y desde la casa, se deduce por el cambio temporal causado por la cuarentena, pero la institución no cuenta con reglamentación para el Teletrabajo.

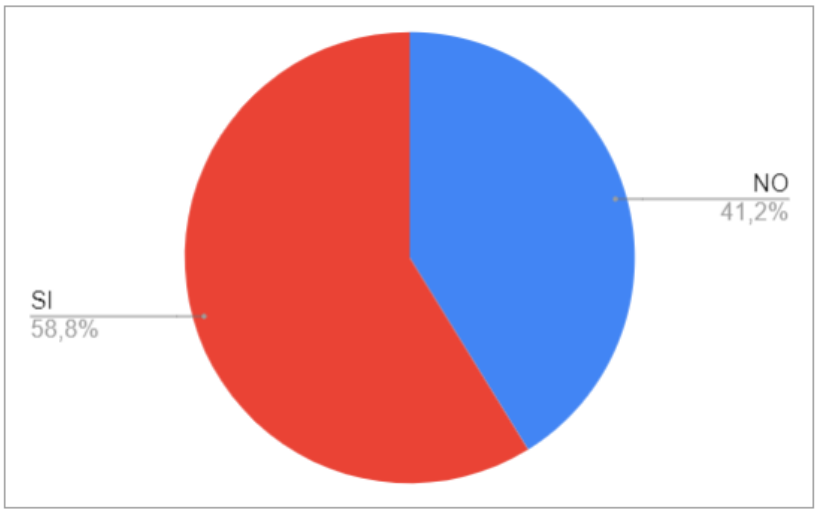
Seleccione el rol (de acuerdo con los permisos en los aplicativos) que más se orienta a su labor, siendo OPERATIVO: Ejecuta procesos secuenciales,

ADMINISTRACIÓN; Función principal de realizar informes, AUDITORÍA: Revisión de informes



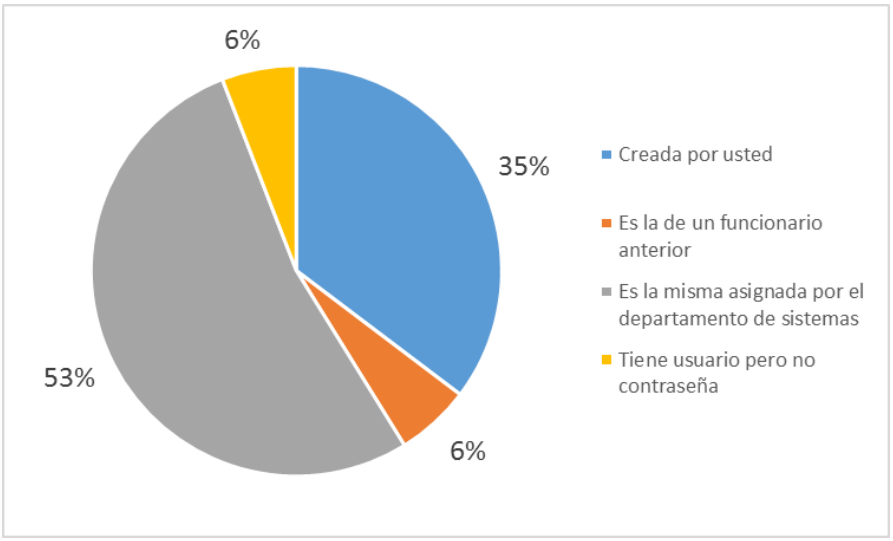
Del gráfico anterior, se puede señalar que los empleados no tienen un rol en específico a nivel de los permisos de aplicación, es un riesgo que no se puede eliminar, pero sí se debe controlar según el control A.6.1.2 Separación de deberes de la ISO/IEC 27001.

¿Comparte con otro funcionario (compañero o subalterno) las contraseñas de acceso a los sistemas de información?



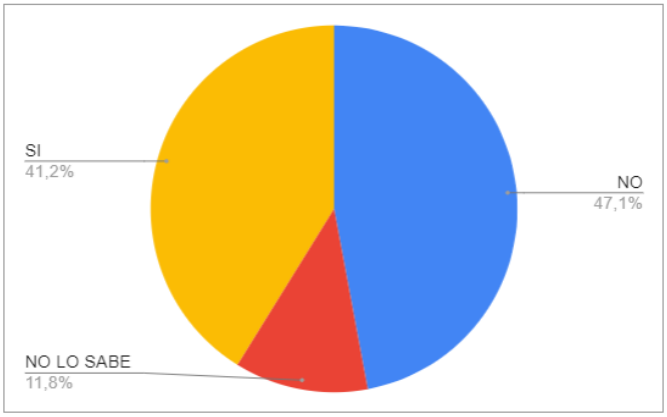
Más de la mitad de los encuestados, comparten su contraseña de acceso a los sistemas de información (58,8%), siendo un riesgo de acuerdo con el 9.4.3 Gestión de contraseñas de usuario de la ISO/IEC 27001.

La contraseña del equipo de cómputo (escritorio o portátil) asignado actualmente es:



El 53% de los encuestados, utilizan la contraseña asignada por el departamento de sistemas, el 35% tiene contraseñas creadas por el mismo, el 6% utilizan la contraseña de un funcionario anterior y este mismo porcentaje manifiesta que el computador tiene usuario más no contraseña, se evidencia posible riesgo de acuerdo con el control A.9.4.3 Sistema de gestión de Contraseñas de la ISO/IEC 27001.

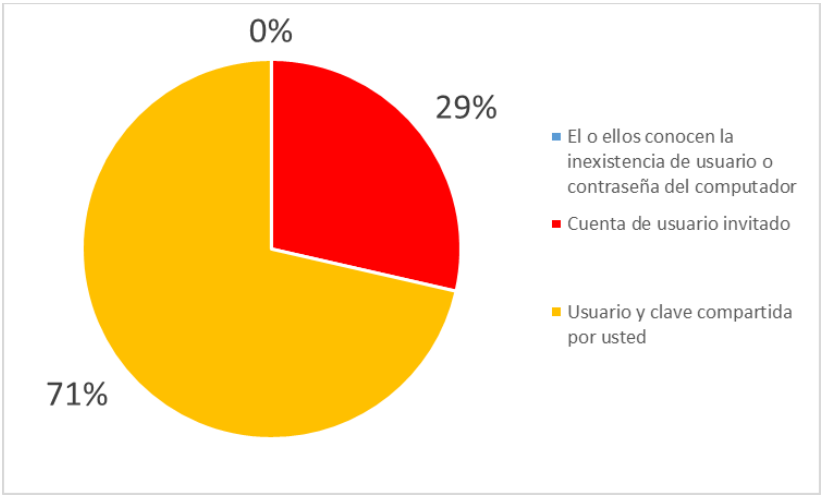
¿Cuándo usted no se encuentra en el lugar de trabajo, los funcionarios de su área pueden ingresar a su equipo para consultar información almacenada allí?



Aunque el 47,1% de los participantes no permiten que otros empleados accedan a su equipo de cómputo, el 41,2% si realiza esta práctica y el 11,8% no lo sabe, de lo anterior se evidencia que existe carencia del procedimiento de ingreso seguro, en este caso operativo de acuerdo con el control A.9.4.2 de la ISO/IEC 27001.

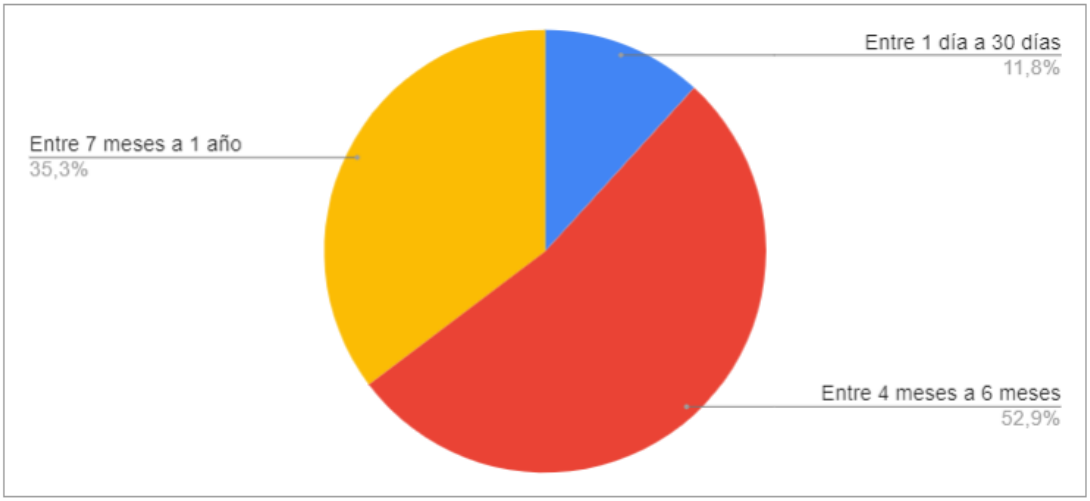
Continuación respuesta SI

¿Con cuál clave realizan el ingreso las otras personas?



De los empleados que dijeron que otros empleados tienen acceso a su equipo de trabajo, la mayoría el 71% le han suministrado su contraseña a otro colaborador, el 29% acceden mediante un usuario invitado y 0% El o ellos conocen la inexistencia de usuario o contraseña del computador.

¿Con qué frecuencia en promedio cambia usted las claves de los sistemas de información y CUENTAS DE CORREOS?

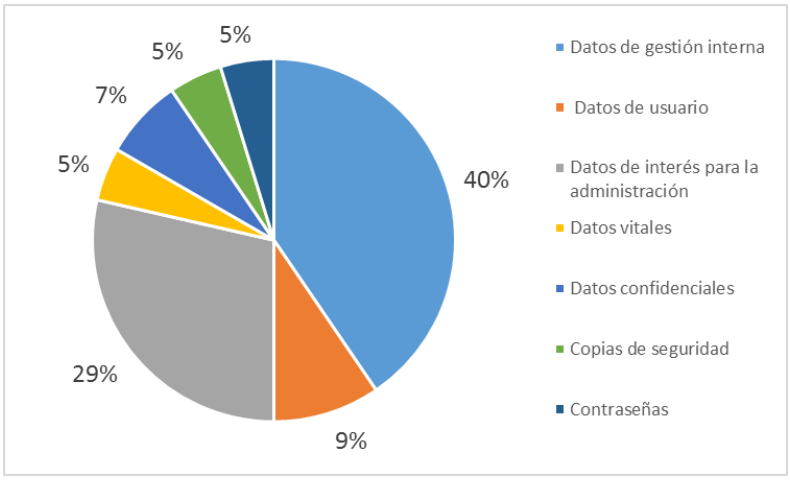


52,9% realizan el cambio de contraseña de los sistemas de información y correo electrónicos entre 4 y 6 meses, el 35,3% entre 7 meses a 1 año y el 11,8% entre 1 a 30

días, lo cual es una fortalece en el control A.9.4.3 Sistema de gestión de Contraseñas de la ISO/IEC 27001.

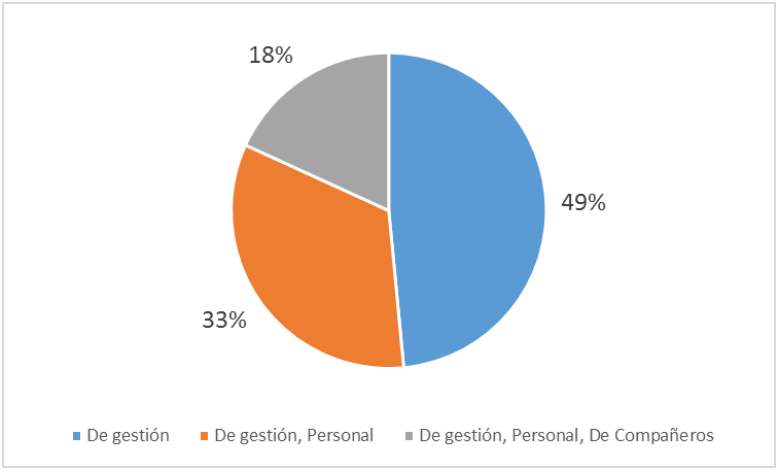
SECCIÓN TRES: Activos de seguridad de la información

¿Qué tipo de información usted maneja dentro de sus funciones? (selección múltiple)



Todos los encuestados manifiestan que manejan diferentes tipos de funciones, la principal se basa en gestión interna con un 40%, seguido de un 29% sobre datos interés para la administración, también se encuentra empleados que manejan informaciones vitales, confidenciales y copia de seguridad

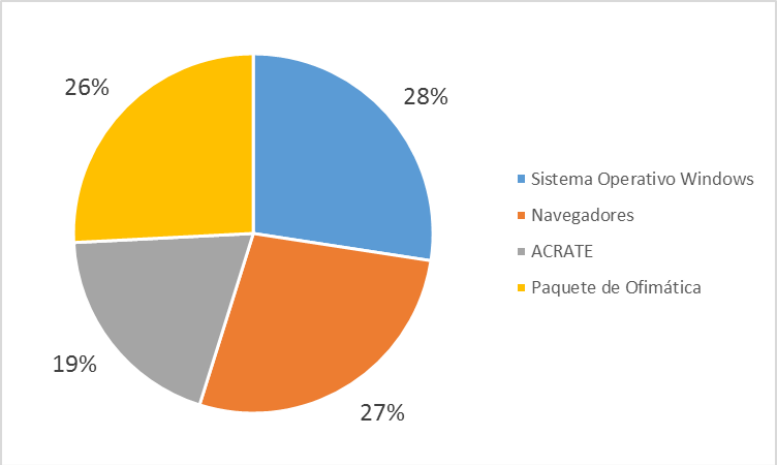
¿Qué tipo de información guarda usted en el equipo de cómputo de su puesto de trabajo? (selección múltiple)



Casi la mitad de los empleados, solo almacenan información de gestión (49%), mientras que el 33% además de esta información almacena información personal y el 18%

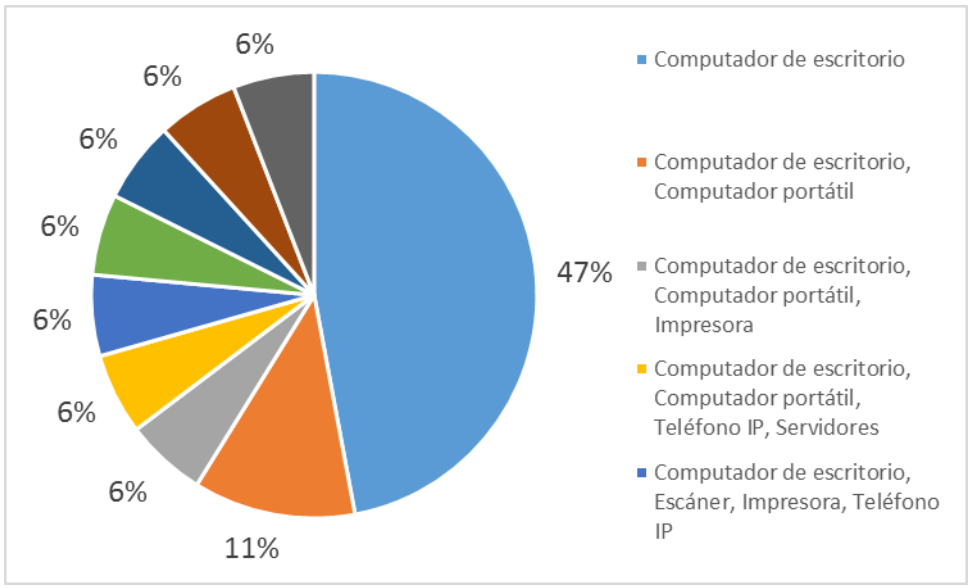
manejan las 2 anteriores más información de los compañeros, siendo un riesgo para el control A.11.2.9 Política de escritorio y pantalla limpia

¿Qué software instalado usa en el equipo de cómputo de su puesto de trabajo? (selección múltiple)



Del gráfico anterior ningún empleado seleccionó la opción de antivirus, puede ser que la institución no cuenta con uno o no tienen conocimiento de la instalación de este, por lo que se debe tener un mayor seguimiento al control A.12.2.1 contra códigos maliciosos

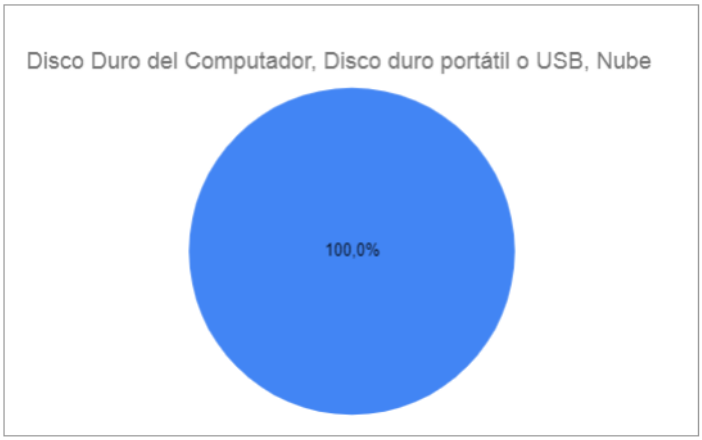
Seleccione los equipos que usted tiene asignado (selección múltiple)



El principal tipo equipo o activo fijo que poseen los empleados es el computador de escritorio con un total del 47%, también se evidencia que de acuerdo con las funciones

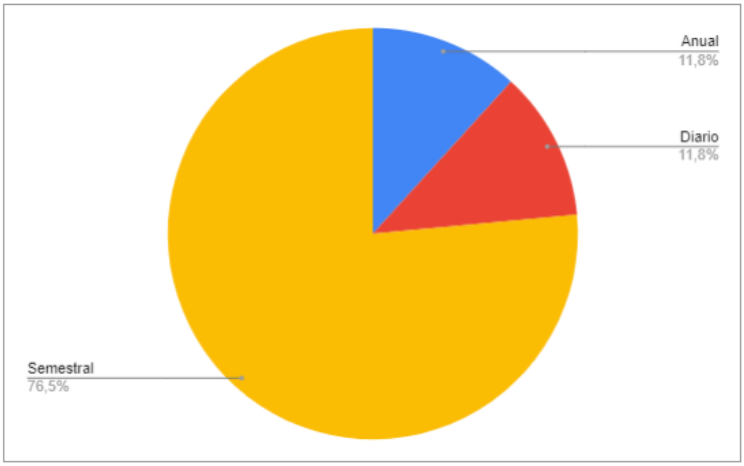
un empleado puede tener más de 1 equipo asignado por lo que se debe tener un mayor seguimiento de acuerdo con el control A.11.2 Equipos de la norma ISO/IEC 27001

¿En qué medios usted almacena la información? (selección múltiple)



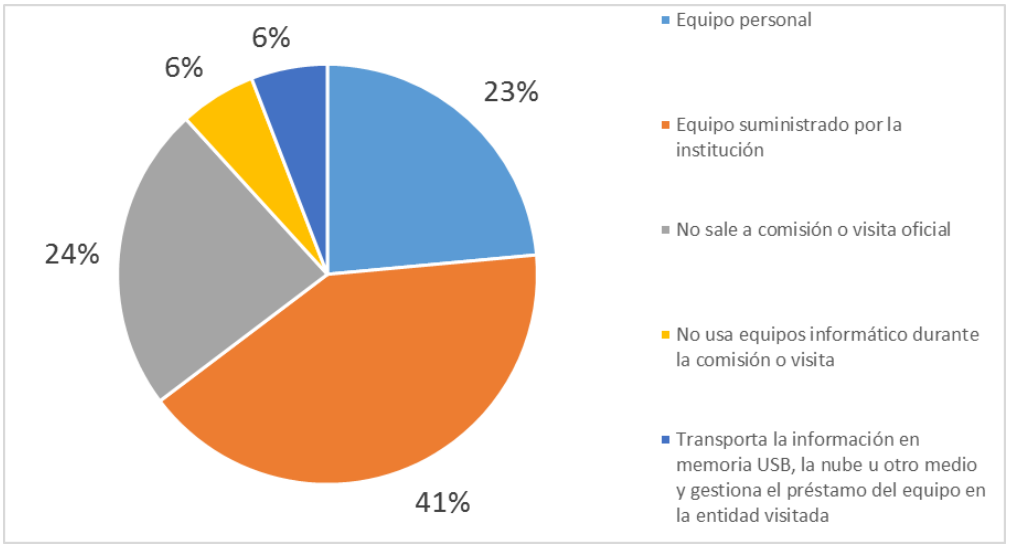
El 100% de los encuestados utilizan como medio de almacenamiento el Disco Duro del Computador, Disco duro portátil o USB y Nube, al tener los empleados varios tipos de almacenamiento habilitado se debe enfatizar en los controles A.12.4.1 Registro de eventos, A.8.3.1 Gestión de medios
Removibles, A.8.3.3 Transferencia de medios físicos de la norma ISO/IEC 27001

¿Con qué frecuencia hace copia de respaldo o backup de la información?



La mayoría de los empleados tienen la cultura de realizar las copias de respaldo de manera semestral, que equivale a un 76,5%, seguido a una realización de backup de manera diaria y anual cada uno con un 11,8%, se debe focalizar las acciones para que la población que realiza el proceso anual lo haga en una periodicidad menor, para no afectar el control A.12.3.1 Respaldo de la información de la norma ISO/IEC 27001

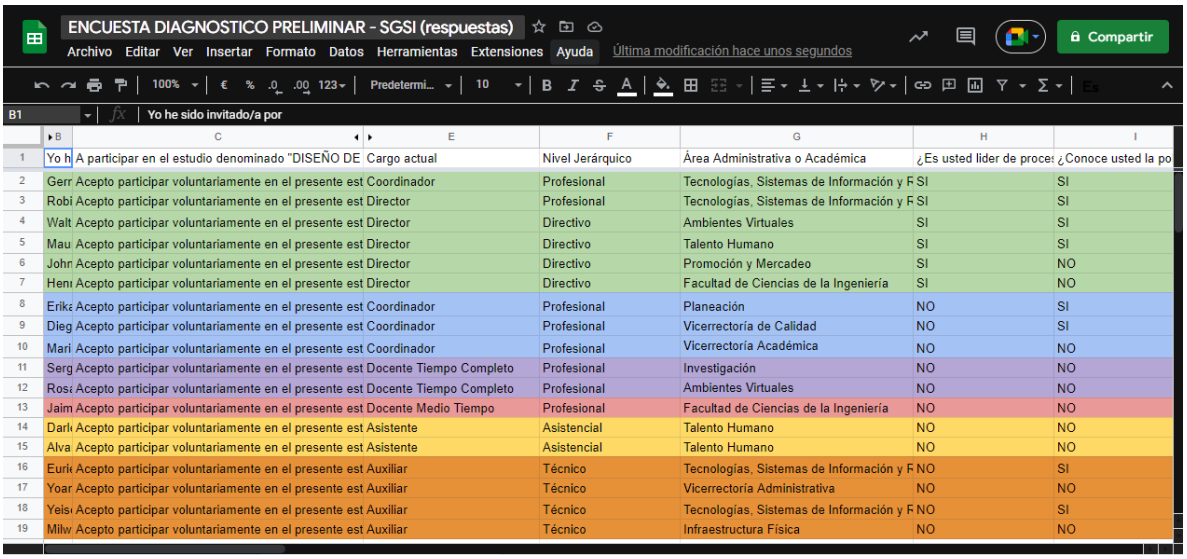
¿Cuándo sale de comisión o visita oficial, que elemento o equipo utiliza para la gestión de la información?



El 41% de los empleados cuando salen a comisión o visita oficial, utiliza el equipo suministrado por la institución por lo que se debe tener seguridad de equipos y activos fuera de las instalaciones, según el anexo A.11.2.6 de la norma ISO/IEC 27001.

De esta manera, se obtiene un insumo importante para conocer el estado actual de la seguridad de la información, desde la perspectiva del usuario final, la cual es muy relevante debido a que ellos son los que a diario operan los sistemas de información y a pesar de que en un escenario ideal pueda existir todo un sistema robusto a nivel de seguridad de la información sí los usuarios finales, lo desconocen o no desean aplicarla es imposible asegurar que dicha entidad está logrando reducir las posibles brechas de seguridad.

ANEXOS 5 REGISTRO DE DILIGENCIAMIENTO DE ENCUESTA POR PARTE DE LOS COLABORADORES DE LA INSTITUCIÓN



ENCUESTA DIAGNOSTICO PRELIMINAR - SGSI (respuestas)

Archivo Editar Ver Insertar Formato Datos Herramientas Extensiones Ayuda Última modificación hace unos segundos

Compartir

B1: Yo he sido invitado/a por

	B	C	E	F	G	H	I
1	Yo h	A participar en el estudio denominado "DISEÑO DE	Cargo actual	Nivel Jerárquico	Área Administrativa o Académica	¿Es usted líder de proce	¿Conoce usted la po
2	Gerr	Acepto participar voluntariamente en el presente est	Coordinador	Profesional	Tecnologías, Sistemas de Información y F	SI	SI
3	Robi	Acepto participar voluntariamente en el presente est	Director	Profesional	Tecnologías, Sistemas de Información y F	SI	SI
4	Walt	Acepto participar voluntariamente en el presente est	Director	Directivo	Ambientes Virtuales	SI	SI
5	Mau	Acepto participar voluntariamente en el presente est	Director	Directivo	Talento Humano	SI	SI
6	John	Acepto participar voluntariamente en el presente est	Director	Directivo	Promoción y Mercadeo	SI	NO
7	Henı	Acepto participar voluntariamente en el presente est	Director	Directivo	Facultad de Ciencias de la Ingeniería	SI	NO
8	Erik	Acepto participar voluntariamente en el presente est	Coordinador	Profesional	Planeación	NO	SI
9	Dieg	Acepto participar voluntariamente en el presente est	Coordinador	Profesional	Vicerrectoría de Calidad	NO	SI
10	Mari	Acepto participar voluntariamente en el presente est	Coordinador	Profesional	Vicerrectoría Académica	NO	NO
11	Serg	Acepto participar voluntariamente en el presente est	Docente Tiempo Completo	Profesional	Investigación	NO	NO
12	Rosa	Acepto participar voluntariamente en el presente est	Docente Tiempo Completo	Profesional	Ambientes Virtuales	NO	NO
13	Jaim	Acepto participar voluntariamente en el presente est	Docente Medio Tiempo	Profesional	Facultad de Ciencias de la Ingeniería	NO	NO
14	Darl	Acepto participar voluntariamente en el presente est	Asistente	Asistencial	Talento Humano	NO	NO
15	Alva	Acepto participar voluntariamente en el presente est	Asistente	Asistencial	Talento Humano	NO	NO
16	Eurí	Acepto participar voluntariamente en el presente est	Auxiliar	Técnico	Tecnologías, Sistemas de Información y F	NO	SI
17	Yoar	Acepto participar voluntariamente en el presente est	Auxiliar	Técnico	Vicerrectoría Administrativa	NO	NO
18	Yeis	Acepto participar voluntariamente en el presente est	Auxiliar	Técnico	Tecnologías, Sistemas de Información y F	NO	SI
19	Milw	Acepto participar voluntariamente en el presente est	Auxiliar	Técnico	Infraestructura Física	NO	NO

ANEXOS 6 ANÁLISIS DE ENTREVISTAS A EMPLEADOS DEL ÁREA TI

Este tipo de recolección de la información, es de carácter cualitativo, y es dirigida principalmente a personal que trabaja en la Dirección de Tecnologías, Sistemas de Información y Recursos Educativos, quienes son los responsables más afín en cuanto a la seguridad informática

¿Qué entiende usted con seguridad informática y qué importancia tiene la aplicación de la misma en la institución (negocio)?

R1: En un entorno enfocado en la era digital, ha permeado diferentes sectores como la educación por lo tanto en la institución la tecnología es la herramienta por excelencia para la ejecución de los procesos por ende es de gran importancia implementar la seguridad para evitar incumplimiento de los pilares de la seguridad informática

R2: Con un mercado invadido en casi su totalidad por la tecnología, la información es un activo muy valioso para todas las organizaciones, este activo por lo general se gestiona a través de sistemas informáticos por lo que es de vital importancia contar con una seguridad alta para resguardar todos los activos de información.

- *Los empleados TI, enfatizan en la gran acogida de las tecnologías, por ende, la Seguridad Informática es vital para la protección de los activos de información.*

¿En qué estado se encuentra el SGSI en el negocio?

R1: La institución actualmente no cuenta con un SGSI, sin embargo, cuenta con un SGC certificado bajo la norma ISO 9001:2013 en cuanto al SGSI la alta dirección han decidido la implementación del SGSI para luego ser certificada por lo tanto es una acción para ejecutar en el Plan de Desarrollo 2020 – 2025

R2: En la organización actualmente no se encuentra implementado un SGSI, pero las directivas tienen contemplada la implementación y certificación de un sistema de gestión de la seguridad de la información en el plan de desarrollo 2020 - 2025.

- *A pesar de que la institución no cuenta con un SGSI, desde el liderazgo de la alta gerencia se han trazado la implementación de este y se encuentra plasmado en el Plan de Desarrollo 2020 – 2025*

Actualmente existen tesis de grados orientadas a la implementación completa o parcial de un SGSI, con base a esto ¿Qué le parece la idea de permitir desarrollar la fase de planeación a través de una tesis de grado?

R1: Es una excelente idea y sí es posible realizar otra fase sería un proceso de enriquecimiento mutuo, sin embargo, se debe respetar los datos de confidencialidad y reserva en cuanto a datos sensibles

R2: Me parece que para la organización sería un gran avance, puesto que hasta la fase de planeación permitirá a los directivos analizar el alcance del proyecto y contemplar los beneficios que esto les traería.

- *Ante la apreciación de que existen trabajos de grados orientados a la implementación completa o parcial de un SGSI, los entrevistados ven viable la aplicación de una tesis en la institución siempre se mantenga el principio de confidencialidad*

¿Qué políticas referentes a la seguridad informática han implementado en el negocio?

R1: Aunque en la institución no se cuenta con la Política de Seguridad de la Información, sí se cuenta con la Política de la División de Tecnologías, Sistemas de Información y Recursos Educativos (reciente) en donde se mencionan diferentes aspectos en donde se presencia ítems referentes a la seguridad informática, por otro lado también se cuenta con la Política de Protección de Datos Personales la cual se encuentra publicada en la página web www.corposucre.edu.co en la sección de reglamentación y un link en el footer de la página

R2: Por el momento la organización no cuenta con una política de seguridad de la información, con relación a esto cuenta con una Política de la División de Tecnologías,

Sistemas de Información y Recursos Educativos y también cuenta con una Política de Protección de Datos Personales.

- *Aunque la institución a la fecha no cuenta con la Política de Seguridad de la Información, presentan una Política de Protección de Datos Personales y una Política de la División de Tecnologías, Sistemas de Información y Recursos Educativos recientemente creada, las cuales fueron revisadas y contemplan varios aspectos de la seguridad informática*

En cuanto a acceso de la información ¿Se regula el acceso a la misma de acuerdo con el perfil del funcionario?

Si, contamos con un sistema que mediante perfiles de sistema se asigna de acuerdo con las necesidades, en caso de existir un cargo nuevo, Talento Humano remite el listado de permisos del perfil nuevo

Si, esto se realiza mediante un sistema de asignación de roles que van de acuerdo con el cargo que ocupa el funcionario.

- *A nivel de acceso a la información, la institución cuenta con un menú para la asignación de permisos de acuerdo con el perfil y el área que lo autoriza es Talento Humano*

¿Los funcionarios tienen asignado dispositivos móviles? en caso de ser afirmativa la respuesta ¿Cuenta el negocio con medidas de control de la información?

R1: Si, el control se basa en la aplicación del servicio de correo electrónico el cual brinda informes sobre el uso de este y permite aplicar reglas.

R2: Los funcionarios si usan dispositivos móviles, en los cuales hacen uso del correo institucional, el correo brinda informes sobre su uso.

- *La institución cuenta con dispositivos móviles para la asignación a sus empleados, la medida de control se realiza mediante la aplicación de correo electrónico que brinda informes y permite aplicar reglas, por lo tanto, le aplica el control A.6.2.1 Política para dispositivos móviles*

¿En el negocio se realiza teletrabajo? En caso de ser así ¿Cuentan con normatividad que lo regule?

R1: No, sin embargo, como consecuencia de la pandemia Covid-19 la institución se ha visto obligada a flexibilizarse en la implementación de teletrabajo

R2: En la organización no se realiza teletrabajo, pero a raíz de la calamidad mundial por el covid-19 la institución he hecho uso de las herramientas virtuales para mitigar el

impacto de dicha pandemia, en cuanto a una normatividad que regule el teletrabajo en la institución no se cuenta con ninguna.

- *La institución no realiza teletrabajo, sin embargo, por motivos de cuarentena por el virus COVID-19 les tocó implementar el trabajo remoto asistido por tecnología, por lo tanto, no le aplica el control A.6.2.2 Teletrabajo.*

Dentro de los términos de contratación con empleados y contratistas ¿Se contemplan las responsabilidades en cuanto a la seguridad de la información que el funcionario va a tener acceso?

R1: La institución en los términos y condiciones del contrato en los términos y condiciones, en específico en el término Décimo sexta contempla el manejo de la Confidencialidad de la información

R2: Dentro de los términos de contratación se plasma que los usuarios se harán responsables por el tratamiento de la información.

- *Se demuestra cumplimiento del control A.7.1.2 Términos y condiciones del empleo de la norma ISO/IEC 27001*

¿Los funcionarios reciben capacitaciones en cuanto a seguridad de la información, con qué frecuencia se realiza?

R1: Al momento no se realiza

R2: En la organización por el momento no se realizan capacitaciones sobre seguridad de la información.

- *La institución no realiza capacitaciones referentes a la seguridad de la información*

¿Se implementa un inventario de activos, en caso de ser afirmativa la respuesta que procesos se realizan con este?

R1: Si, se cuenta con un sistema que permite el control de activos fijos de cómputo en donde se realiza toda la trazabilidad en cuanto a préstamos permanente (durante contrato) o de préstamo, así como el historial de mantenimiento, tal cual como se contempla en el SGC

R2: Si se implementa un inventario de activos, los procesos que se realizan con este es llevar la trazabilidad de los préstamos y mantenimientos de cada activo, también este inventario cuenta con información financiera sobre el valor de cada activo y cuenta con la descripción detallada del activo y sus accesorios, partes o complementos.

- *La División de Sistemas de Información, Tecnologías y Recursos Educativos, cuenta con un control de activo fijos, donde se contemplan el ciclo de vida de los equipos de cómputos y tecnológicos. Cumpliendo con los ítems A.11.2.1 Ubicación y protección de los equipos, A.11.2.2 Servicios de suministro, A.11.2.4 Mantenimiento de equipos y A.11.2.5 Retiro de activos de la norma ISO/IEC 27001*

¿El negocio cuenta con seguridad física que permita el control de acceso a personal autorizado, así como el registro de los elementos informáticos al momento del ingreso o retiro de la persona?

R1: Se cuenta con personal con funciones de vigilancia en las zonas de acceso perimetral, así como un CCTV

R2: Actualmente en la organización se cuenta con personal destinado a permitir el acceso solo al personal autorizado, estos funcionarios cuentan con una minuta donde se registran todos los elementos informáticos que ingresan y salen de la institución.

- *La institución cuenta con perímetro de seguridad física, controles de acceso físico, seguridad de oficinas, recintos e instalaciones cumpliendo de esta forma con los ítems A.11.1.1, A.11.1.2 Y A.11.3 respectivamente*

¿Cómo se controla la gestión del cambio?

R1: Si, se contempla en el SGC cada cambio es registrado en un documento macro y en el histórico del mismo procedimiento

R2: La gestión de cambio se controla a través de un documento macro donde se lleva el registro de los procedimientos.

- *Se contempla la gestión del cambio a través del Sistema de Gestión de la Calidad.*

¿Cómo se manejan las copias de respaldo en el negocio, se realizan pruebas de verificación?

R1: De 2 maneras, por parte de los funcionarios se realiza backup antes de la jornada de mantenimiento preventivo y se les ha socializado el procedimiento de realización de backup mediante la nube, el usuario final es el responsable del procedimiento.

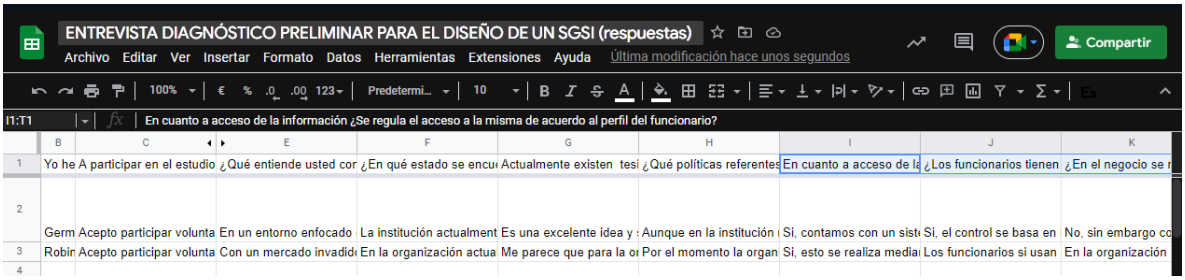
En cuanto a los sistemas de información, se ejecuta procedimientos automáticos de generación y se almacenan en 2 infraestructuras distintas, con respecto a las pruebas si se han realizado

R2: Las copias de seguridad son realizadas por cada usuario diariamente esta copia es almacenada en la nube, y las copias de seguridad de los sistemas de información se

ejecutan automáticamente guardando la copia de seguridad generada en dos partes distintas.

- *A nivel de copia de respaldo, se manejan desde los usuarios finales utilizando como medio de almacenamiento la nube y en cuanto a los sistemas de información se realiza a través de procesos automatizados a los cuales se realizan pruebas de verificación, cumpliendo con el anexo A.12.3.1 Respaldo de la información*

ANEXOS 7 REGISTRO DE DILIGENCIAMIENTO DE ENTREVISTA POR PARTE DE LOS COLABORADORES TI DE LA INSTITUCIÓN



ANEXOS 8 INVENTARIO DE ACTIVOS GENERAL

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	DESCRIPCIÓN	RESPONSABLE
ARQUITECTURA DEL SISTEMA	[ARCH]	Elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.	
DATOS	[D]	La información es un activo abstracto que será almacenado en equipos o soportes de información.	
SERVICIOS	[S]	Función que se encarga de satisfacer una necesidad de los usuarios del servicio.	

SOFTWARE (APLICACIONES)	[SW]	En cualquier denominación (programas, aplicaciones, desarrollos, etc.) tareas automatizadas para su desempeño por un equipo informático, las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la presentación de los servicios.	
HARDWARE	[HW]	Referida a los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.	
COMUNICACIONES	[COM]	Incluye instalaciones dedicadas como servicios de comunicación contratados a terceros; centrada en que son medios de transporte que llevan datos de un sitio a otro.	
CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	DESCRIPCIÓN	
SOPORTE DE INFORMACION	[MEDIA]	Dispositivos físicos que permiten almacenar información de forma permanente o durante un largo periodo de tiempo.	

EQUIPOS AUXILIARES	[AUX]	Se consideran como otros equipos que sirven de soporte a los sistemas de información.	
INSTALACIONES	[L]	Lugares en los que se hospedan los sistemas de información y comunicaciones.	
PERSONAS	[P]	Personal relacionado con los sistemas de información.	

ANEXOS 9 INVENTARIO DE ACTIVOS ESPECÍFICOS

No.	**DATOS DEL ACTIVO DE INFORMACIÓN**		
	NOMBRE DEL ACTIVO DE INFORMACIÓN	PROCESO PROPIETARIO DEL ACTIVO	TIPO DE ACTIVO
1	Datos para el desarrollo de pruebas		DATOS
2	Registro de actividad		DATOS
3	Dirigidos al público en general y que no requieren tener una relación contractual		SERVICIOS

4	Internos a personal autorizado dentro de la organización		SERVICIOS
5	Servicio de navegación a través de internet		SERVICIOS
6	Acceso remoto a servicios que se encuentran en la intranet		SERVICIOS
7	Acceso al correo electrónico		SERVICIOS
8	Servicio de almacenamiento de ficheros		SERVICIOS
9	Transferencia de ficheros		SERVICIOS
10	Intercambio electrónico de datos		SERVICIOS
11	Acceso a directorios de información		SERVICIOS
12	Permiten altas y bajas de usuarios de los sistemas teniendo en cuenta su estado contractual		SERVICIOS
13	Gestión de servicios de acuerdo con los privilegios otorgados		SERVICIOS
14	Desarrollos propios que se han realizado al interior de la organización		SOFTWARE
15	Configurados diferentes navegadores para el desarrollo de tareas operativas		SOFTWARE
16	Servidor de aplicaciones		HARDWARE
17	Cliente de correo electrónico, vinculado a todas las cuentas institucionales		HARDWARE

18	Actualmente el servidor de correo electrónico esta manejado por Gmail		SERVICIOS
19	Servidor de ficheros		HARDWARE
20	Acceso a los sistemas de gestión de bases de datos como POSTGRESQL		SOFTWARE
21	Programas ofimáticos tales como el paquete de office.		SOFTWARE
22	Programa antivirus encargado de proteger los equipos y brindar conexiones remotas a los mismos		SOFTWARE
23	Sistema operativo		SOFTWARE
24	Servidor de terminales		HARDWARE
25	Sistema de backup		SOFTWARE
26	Maquinas físicas usadas como servidores		HARDWARE
27	Equipos asignados a los funcionarios al interior de la Dirección		HARDWARE
28	Equipos portátiles, celulares y demás equipos transportables		HARDWARE
29	Equipos físicos en los que se puede almacenar el respaldo de la información		HARDWARE
30	Periféricos		HARDWARE
31	Impresoras asignadas		HARDWARE
32	Escáner		HARDWARE

33	Soporte de la red cableada e inalámbrica en los diferentes puntos de acceso		SERVICIOS
34	Elementos concentradores		HARDWARE
35	Puntos de acceso a la red inalámbrica		SERVICIOS
36	Teléfonos de voz IP, actualmente instalados en diferentes puntos		HARDWARE
37	Red de acceso telefónica		SERVICIOS
38	Red digital, integra voz y datos en la misma línea		SERVICIOS
39	Red de datos		SERVICIOS
40	Acceso a Internet de banda ancha		SERVICIOS
41	Red local		SERVICIOS
42	Acceso a internet		SERVICIOS
43	Discos para el almacenamiento de copias de información		HARDWARE
44	Almacenamiento de información en red		SERVICIOS
45	Información almacenada y necesaria portable		DATOS
46	Tarjetas de memoria		HARDWARE
47	Documentos físicos tales como actas		DATOS
48	2 UPS de alimentación eléctrica para el rack de comunicaciones y servidores		HARDWARE

49	Casilleros para el almacenamiento de algunos elementos de soporte		HARDWARE
50	Oficinas de la dirección de sistemas y demás apoyos		INSTALACIONES
51	Ubicación-cuarto data center		INSTALACIONES
52	Bodega		INSTALACIONES
53	Usuarios externos		PERSONAL
54	Usuarios internos		PERSONAL
55	Operadores del servicio		PERSONAL
56	Equipo de ADMIN		PERSONAL
57	Administradores de BBDD		PERSONAL
58	Administradores de seguridad		PERSONAL
59	Desarrolladores / programadores		PERSONAL
60	Contratistas		PERSONAL
61	Proveedores		PERSONAL

ANEXOS 10 FORMATOS DE AUTORIZACIÓN Y CONFIDENCIALIDAD

En conversación con la Secretaría General de la Corporación Universitaria Antonio José de Sucre, no autorizó colocar los anexos con las firmas institucionales en el presente documento que será de carácter público

Cordial saludo Robinson y German,

A continuación algunas recomendaciones de forma:

- Tener en cuenta aplicar lo siguiente al documento, por que algunas hojas no tienen la configuración correcta.

Tipo de Letra y Espaciado

Para la ESI, se plantea trabajar con:

• Fuente Arial

• Tamaño 12

• Interlineado 1.5

Márgenes

Superior 3 cm

Izquierdo 3 cm

Derecho 2 cm

Inferior 3 cm

- Colocar como anexos Autorización Empresa V1 y el Acuerdo de confidencialidad - Empresa Estudiante V1
- Tener presente que deben tener un mínimo de 5 referencias bibliográficas en inglés.
- Tener en cuenta la ortografía y redacción de las palabras resaltadas en amarillo.
- Tener en cuenta algunos comentarios que se dejaron en el documento.
- Diseñar el Resumen Analítico Especializado RAE del cual adjunto formato

Atentamente,

Eduard Mantilla T.