Análisis de riesgos a los activos lógicos de la Infraestructura TI, en la Universidad Cooperativa de Colombia campus Arauca, basados en la norma ISO 27001:2013

Presentado Por:

Brian Enrique Romero Cueto

Director:

Ing. Carlos Eduardo Puentes Figueroa

Universidad Cooperativa de Colombia

Campus Arauca

Programa de ingeniería de Sistemas

Arauca – Arauca

2022

Notas de autor:

Brian Enrique Romero Cueto, Programa de ingeniería de Sistemas, Universidad Cooperativa de Colombia, Campus Arauca.

Correspondencia realizada con este documento ser enviada a:

brian.romeroc@campusucc.edu.co

Tabla de Contenido

Índice De Tablas

Índice De Ilustraciones

INTRODUCCIÓN

Como parte del sistema de gestión de seguridad de la información, es necesario para la empresa hacer una adecuada gestión de riesgos que le permita saber cuáles son las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que presenta.

En la medida que la empresa tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en su información.

Se permite realizar un análisis de riesgos y amenazas de la infraestructura tecnológica de la Universidad Cooperativa de Colombia Campus Arauca, utilizando el estándar ISO/ IEC 27001: 2013 y la metodología de MAGERIT, con el propósito de determinar si existe un entorno seguro para los sistemas de información y servicios que ofrecen.

1. PLANTEAMIENTO DEL PROBLEMA

> El mundo de las tecnologías es cada vez más importante en el desarrollo de las actividades de una empresa, por ende, la responsabilidad de llevar a cabo las auditorías a los sistemas y actividades relacionadas a la gestión de activos de información, deben ser periódicas. (MinTIC, 2022)

La seguridad de la información es un factor clave a la hora de mantener el funcionamiento de las organizaciones en la actualidad. Es ahí donde radica la importancia de mantener los sistemas de información seguros de amenazas y vulnerabilidades.

De lo anterior se puede concluir que con la actualización y mejoras a los controles de seguridad de la información basados en la norma ISO/ IEC 27001:2013 dominios 5. Políticas de seguridad, 13. Seguridad en las telecomunicaciones y 14. Adquisición, desarrollo y mantenimiento de los sistemas de información, se puede evitar riesgos en los sistemas de información, el cual es fundamental para la mitigación del riesgo, en la siguiente ilustración podemos ver reflejado los problemas y cusas de los problemas que se presentan o pueden presentarse.

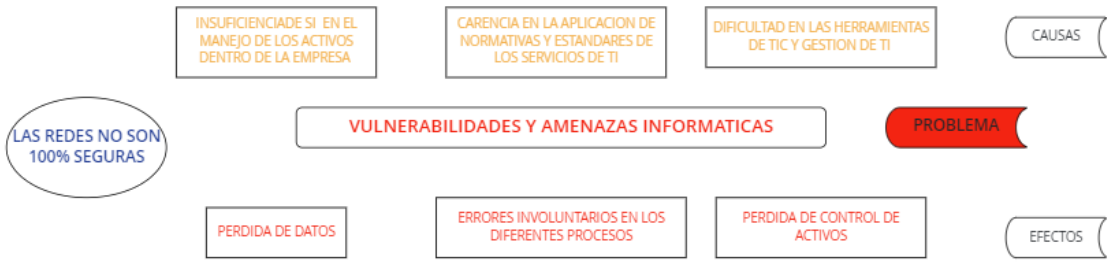

Ilustración 1, Problema, causas y efectos, elaborado por el autor del documento

2. JUSTIFICACIÓN

Según (Guerrero Julio M. , 2018)

> La incorporación acelerada de las tecnologías de la información en las organizaciones, y en general en casi todos los aspectos de la vida humana, ha posibilitado un crecimiento de las amenazas relacionadas con la falta de políticas y medidas de seguridad y falta de concienciación sobre el impacto que ellos pueda tener en la información y en los bienes organizacionales.

> En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:
> Hardware: elementos físicos del sistema informático, tales como procesadores, cableado de red, medios de almacenamiento (cabinas, discos, cintas, usb, DVDs,).
> Software: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
> Datos: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red. (Calderon Arateco, 2022)

La seguridad de la información es un factor clave a la hora de mantener el funcionamiento de las organizaciones en la actualidad. Es ahí donde radica la importancia de la seguridad informática, la UCC diariamente recolecta o almacena diferentes tipos de datos o información en diferentes procesos, dado esto es necesario un análisis de riesgo constante a este tipo de sistemas dentro de

la entidad, ya que maneja información de suma importancia, como lo son los servicios financieros, datos personales de estudiantes, docentes, personal administrativo, entre otros.
Por lo tanto, se busca identificar y evaluar los diversos factores de riesgo que presenta o puede llegar a presentar los sistemas de información de la entidad, una vez identificados se diseñaran estrategias para la mitigación de esto, y poder implementar mejoras en las políticas de seguridad, o propuestas de nuevas políticas o procesos, minimizando así los daños y perjuicios que se puedan causar por un ataque malicioso a la entidad o perdida de información.

3. OBJETIVOS

3.1 Objetivo General

Realizar un análisis de riesgos a los activos lógicos de la infraestructura TI, en la Universidad Cooperativa de Colombia, basados en la norma ISO 27001:2013 Dominios 5,13 y 14, con la metodología MAGERIT.

3.2 Objetivos Específicos.

- Caracterizar los activos de la infraestructura tecnológica de la Universidad Cooperativa de Colombia Campus Arauca.
- Analizar los riesgos en la seguridad de la información.
- Determinar los riesgos en la seguridad de la información basados en la ISO 27001:2013 dominios 5. Políticas de seguridad, 13. Seguridad en las telecomunicaciones y 14. Adquisición, desarrollo y mantenimiento de los sistemas de información, para la gestión de las vulnerabilidades detectadas en la infraestructura tecnológica.
- Generar un plan de mejoramiento en la formulación o modificación de nuevas políticas que ayuden a mitigar los riesgos existentes o los que pueden existir.

4. MARCO TEÓRICO

4.1 Metodología MAGERIT

Teniendo en cuenta lo definido por (Ministerio de Hacienda y Administraciones Públicas de España, 2012) menciona que:

> Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos". En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.

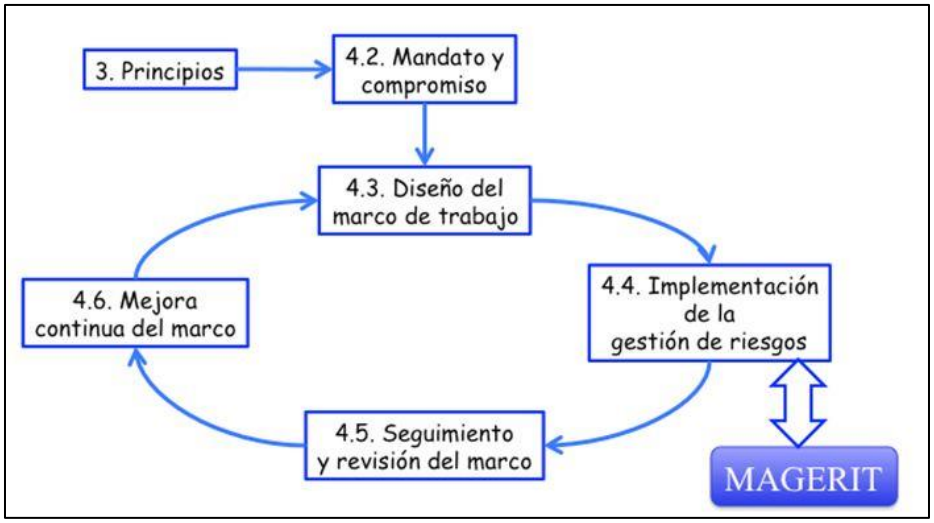

Ilustración 2, ISO 31000 - Marco de trabajo para la gestión de riesgos

Magerit persigue objetivos directos e indirectos:

Directos:

- ✓ Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.

- ✓ Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
- ✓ Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

***Indirectos**:*

- ✓ Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

De la misma manera, la metodología Magerit se articula con la norma **ISO/IEC 27001:2013**, según (ISOTools, 2022) "es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan".

Esta norma específica los requisitos para la aplicación de los controles de seguridad de la información adaptados a las necesidades de las organizaciones o partes de estas. Esta norma caracteriza los siguientes elementos:

- ***Seguridad de la Información.***

seguridad de la información tiene por objetivo preservar las características de confidencialidad, integridad y disponibilidad de la información. Este concepto tiene asociados temas en un contexto más amplio tales como: la definición de políticas y normas, el control insuficiente de cambios, los riesgos operacionales, el plan de continuidad de negocio, clasificación de la información y matrices de riesgo. (Colombia, 2014)

- ***Políticas de seguridad.***

Las políticas de seguridad informática consisten en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan. (UNIR La Universidad En Internet, 20255)

- ***Activos.***

Los activos de información son los recursos que utiliza un Sistema de Gestión de Seguridad de la Información para que las organizaciones funcionen y consigan los objetivos que se han propuesto por la alta dirección. (ISOTools Excellence, 2017)

- ***Riesgos Informáticos.***

Los riesgos informáticos son amenazas y vulnerabilidades que afectan en todos los aspectos a la empresa, y las consecuencias pueden ser muy graves en relación a la información que se está manejando. Según los autores Gonzalo Álvarez y Pedro Pérez (2004:30), consideran que "Un riesgo para un sistema informático está compuesto por la terna de activo, amenaza y vulnerabilidad, relacionados según la fórmula riesgo = amenaza + vulnerabilidad" (Muñoz Hernández, Zapata Cantero, Requena Vidal, & Ricardo, 2019)

- ***Sistema de gestión de seguridad de la información SGSI***.

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando

asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. (WIKIPEDIA, 2011)

- ***Vulnerabilidad.***

"Situación generada por la falta de controles que permite concretar una amenaza, y el riesgo es la posibilidad que una amenaza se materialice y produzca un impacto en la organización. (Guerrero y Gómez, 2012)". (Julio M. L., 2014)

- ***Activo crítico.***

Son todos aquellos bienes materiales e inmateriales que, al ser deteriorados, perdidos, divulgados sin autorización, etc., perjudican el patrimonio organizacional. (Julio M. L., 2014)

- ***Amenaza.***

"Condición del entorno organizacional relacionado con las tecnologías de información, que ante determinada circunstancia podría ser una fuente de desastre informático y afectar a los activos de la compañía (Guerrero y Gómez, 2012)". (Julio M. L., 2014)

- ***Antivirus.***

"Es un software creado específicamente para ayudar a detectar, evitar y eliminar malware (software malicioso)". (VERIZON, 2022)

- ***Autenticidad.***

Permite asegurar el origen de la información. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. (Alonso, s.f.)

- ***Confidencialidad***.

"En términos de seguridad de la información, la confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos". (Mifsud, Ministerio de Educacion, Cultura y Deporte, 2012)

- ***Disponibilidad***.

"En términos de seguridad de la información, la disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos autorizados.

El objetivo de la disponibilidad es, entonces, prevenir interrupciones no autorizadas/controladas de los recursos informáticos" (Mifsud, Ministerio de Educacion, Cultura y Deporte, 2012)

- ***Integridad***.

"En términos de seguridad de la información, la integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado". (Mifsud, Ministerio de Educacion, Cultura y Deporte, 2012)

- ***Malware.***

"Código maligno o software malicioso utilizado para cometer un delito informático". (Julio M. L., 2014)

- ***Salvaguarda.***

"Son todos aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo". (Mifsud, Ministerio de Educacion, Cultura y Deporte, 2012)

5. MARCO CONCEPTUAL

La auditoría a los sistemas de información de la UCC - Campus Arauca hace el uso de la Norma ISO 27001:2013 porque contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI). Esta normativa está compuesta por una serie de estándares de seguridad publicados por la Organización Internacional para la Estandarización (ISO), la cual, es reconocida por ser una entidad no gubernamental que promueve el desarrollo de la estandarización y las actividades.

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

Ilustración 3, control y actualización de normativas y estándares, elaborado por el autor del documento

6. INSTRUMENTOS DE RECOLECCIÓN DE LA INFORMACIÓN.

La organización debe plantearse un Sistema de Gestión de la Seguridad de la Información (SGSI). El objetivo de un SGSI es proteger la información. Para garantizar calidad e idoneidad en el proceso de recopilación de la información que es el primer paso, se hace uso de algunas herramientas o instrumentos, el análisis que se le hace a los procesos, métodos, tareas y políticas de seguridad, debe ser detallado para tener un resultado verdadero y llegar a determinar el nivel de importancia que se le debe dar a lo identificado.

6.1 Identificación Y Caracterización De Los Activos

La seguridad es un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden mitigar. Los riesgos no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad. El primer proceso es identificar los activos de información que deben ser protegidos.

El inicio de la estrategia es la recopilación de información que integra la dependencia de TI de UCC – Campus Arauca, que nos ayuda a identificar los activos y hacer un análisis de las políticas, estrategias, gestión de servicios, entre otros.

Ilustración 4, Activos UCC Campus Arauca, elaborado por el autor del documento

Como se establece en la ilustración anterior se identificaron los activos de acuerdo a los documentos brindados por la UCC Campus Arauca, donde se hallaron las políticas de la empresa, documentos relacionados a la gestión de activos, inventario de infraestructura tecnológica, entre otras. Este hallazgo ayuda a determinar los activos con los que cuenta la UCC y la importancia que tiene.

En apoyo a dar un criterio de calidad se utilizó una herramienta, checklist “Herramienta de evaluación y diagnostico bajo la norma ISO 27001_2013” Anexo A, esto con el fin de poder interpretar y exponer el estado en el dominio 5. Políticas de seguridad y 8. Gestión de activos. El dominio 8. Gestión de activos se agrega a este diagnóstico, ya que es base fundamental para poder determinar observaciones en cuanto a procesos, y demás documentaciones relacionadas a los activos y políticas de seguridad.

Para poder presentar observaciones de calidad se tuvo encuentra toda la documentación brindada por la UCC Campus Arauca, y además ciertas herramientas que nos ayudan a determinar qué tan cierto es el cumplimiento de ello. El personal de la UCC es un activo importante y de alto riesgo

ya que pueden hacer actos involuntarios, que afecten la seguridad, por tal motivo se hizo una encuesta dirigida a los usuarios administrativos de la UCC Campus Arauca, con el fin de verificar algunos procesos y políticas que deben cumplir a la hora de hacer uso de las herramientas tecnológica. En las siguientes imágenes se relaciona los resultados obtenidos en las preguntas de la encuesta sobre la percepción que tienen los profesores y administrativos sobre la seguridad de la información, evidenciando que el 87% de los encuestados conocen que existen políticas para el uso de los equipos.

Ilustración 5, Encuesta a usuarios UCC Sede Arauca, elaborado por el autor del documento

Según resultados obtenidos en la ilustración 5, los usuarios administrativos en su mayoría conocen que existen políticas de seguridad de la información, en el uso de sus equipos de cómputo, esta pregunto surge para dar inicio a los procesos.

Ilustración 6, Encuesta a usuarios UCC Sede Arauca, elaborado por el autor del documento

Podemos evidenciar que los empleados o usuarios administrativos, hacen uso del correo electrónico personal en los equipos de la UCC, esta pregunta se hace para verificar un proceso en el uso de las herramientas, los correos electrónicos personales pueden ser puentes de vulnerabilidad en los sistemas de información, ya que a menudo se presentan correos maliciosos.

Según (Caldas U. D., 2020) en su página principal en una columna nos dice que "Básicamente si un usuario abre un correo electrónico de este tipo es posible que su información o parte de la misma sea comprometida o que termine siendo víctima de una extorsión por internet."

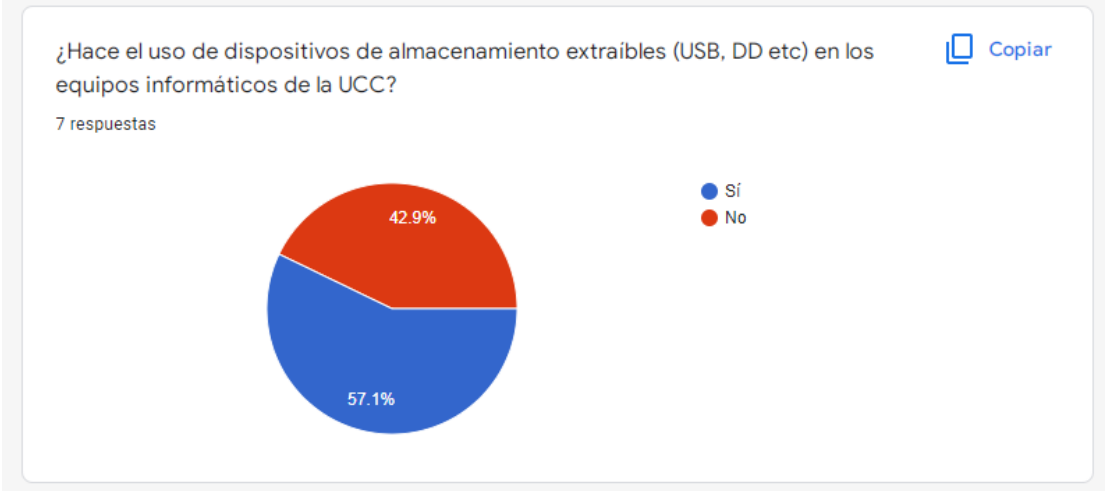

Ilustración 7, Encuesta a usuarios UCC Sede Arauca, elaborado por el autor del documento

Los dispositivos de almacenamiento externo son una forma popular de almacenar y transferir archivos; sin embargo, conllevan una serie de riesgos. Por ejemplo, a los actores de amenazas les gusta utilizar la estrategia de ingeniería social de memorias USB "perdidas" para que buenos samaritanos conecten alguna de estas memorias USB comprometidas con malware en sus computadoras.

Nombre	% Cumplimiento Total	% Alcanzado
Políticas de seguridad	**65,00%**	**26%**
Gestión de activos	**74,94%**	**45%**

Tabla 1, Cumplimiento de políticas y gestión de activos

Una vez que una unidad afectada está conectada al equipo y es abierta, su dispositivo puede infectarse con un algún tipo de código malicioso, como un keylogger o un ransomware. (Amer Owaida, 2021)

En el anexo B, podemos encontrar la relación de todos los activos, donde podemos observar la valoración individual de todos los activos de la UCC Campus Arauca.

Teniendo en cuenta resultados de la encuesta, estudio de las políticas, procesos y documentación prestada podemos obtener un resultado porcentual de las políticas de seguridad y gestión de activos, en la siguiente tabla y gráfica, podemos observar que la UCC Campus Arauca, tiene un porcentaje aceptable, ya que es menos del 80% del cumplimiento mínimo.

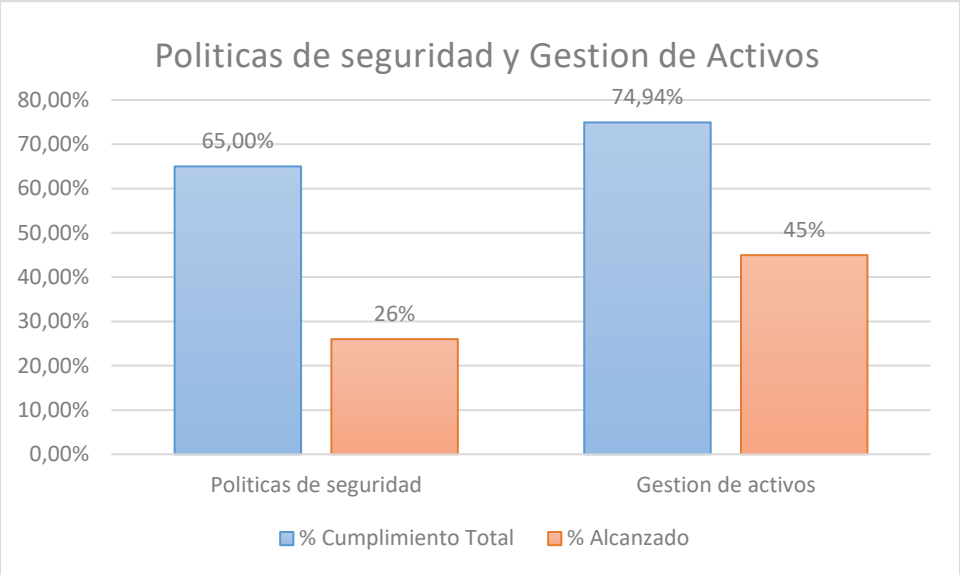

Ilustración 8, Políticas de seguridad y gestión de activos

6.2 Determinar Los Riesgos

Según la consecuencia o impacto, el riesgo puede clasificarse en bajo, medio y alto. Para poder clasificar los riesgos en esta categoría, la organización debe plantearse la pregunta ¿Qué tan malo sería si ocurriera?, por cada riesgo analizado. (Julio M. L., 2014)

Figura 14. Relación de los niveles de riesgo de Guerrero y Gómez (2010) con los criterios de seguridad de la información
Fuente: elaboración propia

Ilustración 9, Relación de los niveles de riesgo, elaborado por Guerrero Marlene Lucia

Se creó una tabla con el fin de tener facilidad a la hora de dar la valoración a cada activo de la UCC Campus Arauca, de esta manera podemos determinar qué tan importante es el activo dentro de la universidad para poder darle un nivel de importancia al riesgo o posibles riesgos que pueda tener.

Teniendo en cuenta los principios de la seguridad de la información DICAT se evalúa cada uno de los activos según posibles situaciones. En la siguiente tabla, tenemos relacionados los activos y la importancia que tiene a la hora de que un activo no esté disponible, que un activo sea utilizado por personal no autorizado, entre otras situaciones, el nivel de calificación es de 1 a 10, donde 1 es poco importante y 10 muy importante.

DISPONIBILIDAD:	¿Qué importancia tendría el activo sino está disponible?
INTEGRIDAD:	¿Qué importancia tendría que los datos fueran modificados fuera de control?
CONFIDENCIALIDAD:	¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?

AUTENTICIDAD:	¿Qué importancia tendrá que quien accede al servicio no sea realmente quien se crea?
TRAZABILIDAD:	¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?

ACTIVO	D	I	C	A	T
Equipos De Computo	8	8	8	8	8
Diseño E Instalación De Red	6	7	7	8	8
Servicio De Internet Dedicado	7	7	7	7	8
Servicio De Internet Banda Ancha	8	7	7	8	7
Formulación E Implementación De Proyectos TIC	7	8	8	8	7
Gestión De Portafolios De Servicios	6	7	7	6	7
Plan De Gestión De Incidencias	7	8	8	7	8
Instalaciones Físicas	8	8	8	7	7
Equipo De TI	7	8	8	7	7
Auxiliares De Soporte	8	7	7	6	6
Dependencias Administrativas	7	8	8	6	8
Gerencia De Dependencias	7	6	6	7	6
Jefe De Área De TI	8	7	7	6	7
Técnicos	8	7	7	7	7

Tabla 2, DICAT

En resumen, se identifican los diversos activos relacionados con la UCC Campus Arauca, evidenciando que los equipos de cómputo y servicio de internet banda ancha son los activos más importantes en el funcionamiento y procesos de las actividades del campus.

6.2.1 Identificación de los Riesgos

Una vez tener un criterio de valoración de los activos, podemos determinar los riesgos más relevantes o de mayor impacto que puedan afectar la seguridad de la información; según la importancia del activo se determina que tan alta es la amenaza o el riesgo que presenta el activo.

Para poder dar un criterio de las posibles amenazas o riesgo que ya existen se hizo uso de la herramienta el software PilarBasic el cual se nos ayuda a evaluar todos los activos y poder dar un resultado de la madurez y las medidas en varios momentos, así podremos observar la evolución de la seguridad del sistema, nos arroja el estado de los activos.

[001] A. Análisis de riesgos > A.2. Valoración de los dominios

Editar Exportar Importar

activo / dominio de seguridad	[D]	[I]	[C]	[A]	[T]
[001] Identificacion de Activos - Trabajo					
[essential] Activos esenciales	[8]	[8]	[8]	[8]	[8]
[EC] Equipos de Computo	[6]	[7]	[7]	[8]	[8]
[RDI] Diseño e instalación de redes inalámbricas	[7]	[7]	[8]	[7]	[8]
[SID] Servicio de Internet Dedicado	[8]	[7]	[8]	[8]	[7]
[SIB] Servicio de Internet Banda Ancha	[7]	[8]	[7]	[8]	[7]
[FIPT] Formulación e implementación de proyectos TIC	[6]	[7]	[7]	[6]	[7]
[GPS] Gestión del portafolio de servicios	[7]	[8]	[7]	[7]	[8]
[PAI] Plan de atención a incidencias	[8]	[8]	[8]	[7]	[7]
[IF] Intalaciones Fisicas	[7]	[8]	[8]	[7]	[7]
[ETI] Equipo de TI	[8]	[7]	[7]	[6]	[6]
[AXS] Auxiliares de Soporte	[7]	[6]	[6]	[6]	[6]
[DA] Dependencias Administrativas	[7]	[8]	[8]	[6]	[8]
[GDA] Gerencia Dependencias Administrativas	[7]	[6]	[7]	[7]	[6]
[JTI] Jefe del área de TI	[8]	[7]	[7]	[6]	[7]
[TEC] Tecnicos	[8]	[7]	[7]	[7]	[7]
Dominios de seguridad					
[base] Base	[8]	[8]	[8]	[8]	[8]

Ilustración 10, Valoración de los dominios PILARBASIC

En la siguiente ilustración se evidencia con el color rojo oscuro los activos que tienen un mayor riesgo de sufrir algun ataque.

[001] A. Análisis de riesgos > A.7. Riesgo

Exportar

potencial | current | target | PILAR

activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS	{6,0}	{6,0}	{6,0}	{5,7}	{6,3}
[EC] Equipos de Computo	{4,8}	{5,4}	{5,4}	{5,7}	{6,3}
[RDI] Diseño e instalación de redes inalámbricas	{5,4}	{5,4}	{6,0}	{5,1}	{6,3}
[SID] Servicio de Internet Dedicado	{6,0}	{5,4}	{6,0}	{5,7}	{5,7}
[SIB] Servicio de Internet Banda Ancha	{5,4}	{6,0}	{5,4}	{5,7}	{5,7}
[FIPT] Formulación e implementación de proyectos TIC	{4,8}	{5,4}	{5,4}	{4,5}	{5,7}
[GPS] Gestión del portafolio de servicios	{5,4}	{6,0}	{5,4}	{5,1}	{6,3}
[PAI] Plan de atención a incidencias	{6,0}	{6,0}	{6,0}	{5,1}	{5,7}
[IF] Intalaciones Fisicas	{5,4}	{6,0}	{6,0}	{5,1}	{5,7}
[ETI] Equipo de TI	{6,0}	{5,4}	{5,4}	{4,5}	{5,1}
[AXS] Auxiliares de Soporte	{5,4}	{4,8}	{4,8}	{4,5}	{5,1}
[DA] Dependencias Administrativas	{5,4}	{6,0}	{6,0}	{4,5}	{6,3}
[GDA] Gerencia Dependencias Administrativas	{5,4}	{4,8}	{5,4}	{5,1}	{5,1}
[JTI] Jefe del área de TI	{6,0}	{5,4}	{5,4}	{4,5}	{5,7}
[TEC] Tecnicos	{6,0}	{5,4}	{5,4}	{5,1}	{5,7}

Ilustración 11, Riesgos PILARBASIC

En conclusión, de este capítulo se establece la necesidad de generar estrategias que ayuden al proceso de mitigación de riesgos, los cuales se desarrollaran a través de la construcción de un plan de mejoramiento.

7. PLAN DE MEJORAMIENTO PARA FORMULAR O MEJORAR LAS POLITICAS DE SEGURIDAD DE LA INFORMACION

El plan de mejoramiento es una herramienta o elemento indispensable a la hora de desarrollar soluciones a las problemáticas presentes o posibles problemáticas que puedan aparecer, en este caso esas problemáticas se remplazarían por el riesgo y vulnerabilidades.

Las estrategias que se recomiendan para mejorar y cumplir con los objetivos nacen de los análisis y resultados que arrojaron en estos diferentes objetivos. La siguiente tabla está relacionada las posibles mejoras que ayude a mitigar riesgos en los sistemas de información.

ESTRATEGIA	OBJETIVO DE LA ESTRATEGIA	PRIORIDAD	ACCIONES A DESARROLLAR	RESPONSABLES
Estrategia a la gestión de activos	**Evaluar los servicios que presta cada activo y dar cumplimiento a las políticas diseñadas a ese activo.**	Muy Alta	Identificar y agregar nuevas tecnologías que ayuden el mejoramiento de los procesos en el campus	Jefe De TI/director Campus Arauca
			Evaluar los procesos existentes y validar los planes de mejoramiento continuo	Jefe De TI/director Campus Arauca
			Actualizar y mejorar los procesos, teniendo en cuenta la validación del plan de mejora	Jefe De TI/director Campus Arauca
			Evaluar el desempeño de los activos continuamente	Jefe De TI
			Evaluar la disponibilidad de los activos	Jefe De TI
Estrategia a la gestión de activos	**Evaluar, generar y actualizar continuamente las políticas de seguridad de la información**	Muy Alta	Evaluar el correcto funcionamiento de la infraestructura del área de TI	Jefe De TI
			Evaluar los avances tecnológicos para la prestación de nuevos elementos dentro de la infraestructura del área de TI	Jefe De TI
			Evaluar y mejorar los procesos de incidencias que presta a los usuarios del campus Arauca	Jefe De TI
			Mejorar las políticas de seguridad de la información continuamente	Jefe De TI/director Campus Arauca
			Mejorar las políticas en los procesos dentro de la empresa	Jefe De TI/director Campus Arauca

			Gestionar herramientas de seguimiento a las políticas, con el fin de mejorarlas continuamente	Jefe De TI
Estrategia a la gestión de activos	**Evaluar y generar mejora continua en los procesos orientado a las buenas practicas**	Alta	Formación de los empleados en la importancia del uso apropiado de las herramientas tecnológicas	Todos Los Empleados/ jefe De TI/ Director Campus Arauca
			Gestionar desarrollo de las actividades y proyectos de TI	Todos Los Empleados/ jefe De TI/ Director Campus Arauca
			Definir espacios físicos donde estén reflejadas las políticas de seguridad de la información	Todos Los Empleados/ jefe De TI/ Director Campus Arauca
			Seguimiento a los procesos del área de TI	Jefe de TI

Tabla 3, Plan de mejoramiento

Se concluye, que el plan de mejoramiento es una de las herramientas que permite la mitigación de los riesgos al interior de área de TI de la universidad cooperativa de Colombia, por lo que se recomienda poder aplicar estas políticas y ser socializadas a toda comunidad que hace uso de los activos del campus.

8. RESULTADOS

La auditoría de los sistemas de información son medidas esenciales que permiten a la UCC Campus Arauca a mejorar la seguridad de la información y tener mejoras en los procesos que llevan a cabo día a día. Este proyecto permitió hacer una evolución y análisis a los activos de la UCC que ayudan a mitigar las posibles amenazas o vulnerabilidades que presenta la seguridad de la información.

La auditoría es una verificación y/o validación única que se le hace a uno o diferentes procesos. En este proyecto la auditoria se basó en los sistemas de información, que parte de un análisis general de los activos de la infraestructura de la UCC Campus Arauca mediante diferentes

herramientas de medición de nivel de importancia, permitiendo el conocimiento integral de la seguridad de la empresa.

Se concluyó que la UCC Campus Arauca a pesar de contar con buenos parámetros de seguridad, no cuentan con políticas de seguridad actualizadas, planes estratégicos y documentación no actualizadas. A su vez como activo de importancia alta, los empleados o usuarios que hacen uso de los equipos de cómputo, redes wifi, entre otros activos, hacen mal uso involuntario en algunos procesos, que pueden causar vulnerabilidad a la seguridad de la información.

Por lo anterior se plantea crear una estrategia que ayude a mitigar dicha problemática, que seria, la UCC Campus Arauca capacite y socialice las políticas, procesos y procedimientos definidos para dar el uso correcto a las herramientas (equipos de cómputo) con las que cuenta la UCC Campus Arauca.

Mejorar los servicios de incidencias presentada por los usuarios ya que según la evaluación de la implementación de buenas prácticas en ITIL del 2017 presentadas por la UCC, nos arroja un porcentaje alto en no prestar ayuda a tiempo en las incidencias presentadas “Anexos CD”.

9. CONCLUSIONES

El proyecto ha permitido una correcta articulación en todos los procesos de los servicios y gestión de riesgos de la UCC Campus Arauca. A la UCC se le brinda los elementos de análisis actuales y que ayuden en el mejoramiento de la seguridad de la información.

Las mejoras se inician de los factores principales del proyecto como lo son el análisis y evaluación de los sistemas de información, para poder dar observaciones de mejoras que ayuden al rendimiento y a la seguridad de la información.

Podemos evidenciar que el éxito de este proyecto depende del cumplimiento y compromiso que deben tener todos los usuarios que hacen uso de los sistemas, agregando que se debe implementar medidas de evaluación constante para mitigar los posibles riesgos o los riesgos con los que se cuentan.

Seguido de la evaluación continua de los sistemas de información, se debe dar una mayor importancia al activo de formulación e implementación de proyectos de TI, ya que se pueden dar mejoras no solo en la seguridad de la información, sino en la mejora de la velocidad de la red, mejora en la infraestructura de TI, entre otras

10. ANEXOS

10.1 Anexo A

Control de seguridad de la información y seguridad informática del SGSI

AUDITORIA EN SEGURIDAD

Herramienta de Evaluación y Diagnostico bajo la Norma ISO/IEC 27002:2013

EMPRESA: **Universidad Cooperativa de Colombia - Arauca**
FUNCIONARIO: Ingeniero Carlos Puentes
CARGO: Directos de TI FECHA: 18 8 2021
AUDITOR: Brian Romero

Área de Evaluación de Cumplimiento				Resultado				
Norma	**Sección**		**Puntos a Evaluar**	**SI**	**NO**	**N/A**	**%**	**Observaciones**
5	**POLITICAS DE SEGURIDAD**						**65,0**	
5,1	**Directrices de la Dirección en seguridad de la información**						**65**	
5.1.1	Conjunto de políticas para la seguridad de la información	83	1. ¿Existen políticas de seguridad?	x			85	Archivo (DGT_Septiembre_07_2010)
			2. ¿Son todas las políticas aprobadas por la administración?	x			90	Archivo (DGT_Septiembre_07_2010)
			3. ¿Las políticas son comunicadas adecuadamente a los empleados?	x			80	Según encuesta el 87,5% saben que existen políticas

5.1.2	Revisión de las políticas para la seguridad de la información	53	1. ¿Están las políticas de seguridad sujetas a revisión?	x			70	Algunas políticas no están actualizadas, pero con este proceso no representa riegos altos
			2. ¿Regularmente se hacían revisiones?		x		20	Cuando se presentaba una circunstancia se hacía una revisión, para solucionar el problema
			3. ¿Se hacían revisiones cuando la circunstancia lo ameritaba?		x		20	
			4. ¿Las políticas son visibles para el personal?	x			90	Si, están ancladas en las plataformas de la UCC

10.2 Anexo B

VALORACION INDIVIDUAL DE ACTIVOS

ACTIVO	AMENAZA	D	I	R
[EC]EQUIPOS DE COMPUTO	[A.11] Acceso no autorizado	A	[8]	{5,7}
	[A.6] Abuso de privilegios de acceso	A	[8]	{5,7}
	[A.5] Suplantación de la identidad	A	[8]	{5,7}
	[A.15] Modificación de la información	I	[6]	{5,4}
	[A.19] Revelación de información	C	[6]	{5,4}
[RDI] Diseño e instalación de redes inalámbricas	[A.19] Revelación de información	C	[7]	{6,0}
	[A.29] Extorsión	C	[8]	{5,6}
	[A.24] Denegación de servicio	D	[7]	{5,4}
	[E.24] Caída del sistema por agotamiento de recursos	D	[6]	{5,4}
	[N.1] Fuego	D	[7]	{5,1}
	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[7]	{5,1}
	[I.*] Desastres industriales	D	[7]	{5,1}
	[A.27] Ocupación enemiga	D	[7]	{5,1}
	[N.2] Daños por agua	D	[7]	{5,1}
	[I.6] Corte del suministro eléctrico	D	[7]	{5,1}
	[A.26] Ataque destructivo	D	[7]	{5,1}
	[A.11] Acceso no autorizado	C, A	[7]	{5,1}
	[A.5] Suplantación de la identidad	C, A	[7]	{5,1}
	[A.6] Abuso de privilegios de acceso	A	[7]	{5,1}
[SID] Servicio de Internet Dedicado	[A.24] Denegación de servicio	D	[8]	{6,0}
	[E.24] Caída del sistema por agotamiento de recursos	D	[7]	{6,0}
	[A.19] Revelación de información	C	[7]	{6,0}
	[I.6] Corte del suministro eléctrico	D	[8]	{5,7}
	[A.11] Acceso no autorizado	C, A	[8]	{5,7}
	[A.6] Abuso de privilegios de acceso	A	[8]	{5,7}
	[A.5] Suplantación de la identidad	C, A	[8]	{5,7}
	[A.15] Modificación de la información	I	[6]	{5,4}
	[I.5] Avería de origen físico o lógico	D	[7]	{5,1}
	[A.18] Destrucción de la información	D	[7]	{5,1}
	[I.8] Fallo de servicios de comunicaciones	D	[7]	{5,1}
[SIB] Servicio de Internet Banda Ancha	[A.15] Modificación de la información	I	[7]	{6,0}
	[A.11] Acceso no autorizado	A	[8]	{5,7}
	[A.6] Abuso de privilegios de acceso	A	[8]	{5,7}
	[A.5] Suplantación de la identidad	I, A	[8]	{5,7}
	[A.24] Denegación de servicio	D	[7]	{5,4}
	[E.24] Caída del sistema por agotamiento de recursos	D	[6]	{5,4}
	[A.19] Revelación de información	C	[6]	{5,4}
	[I.6] Corte del suministro eléctrico	D	[7]	{5,1}
	[A.26] Ataque destructivo	D	[7]	{5,1}
[FIPT] Formulación e implementación de proyectos TIC	[A.15] Modificación de la información	I	[6]	{5,4}
	[A.19] Revelación de información	C	[6]	{5,4}

[GPS] Gestión del portafolio de servicios	[A.15] Modificación de la información	I	[7]	{6,0}
	[A.24] Denegación de servicio	D	[7]	{5,4}
	[A.19] Revelación de información	C	[6]	{5,4}
	[A.11] Acceso no autorizado	A	[7]	{5,1}
	[A.5] Suplantación de la identidad	I, A	[7]	{5,1}
	[A.6] Abuso de privilegios de acceso	A	[7]	{5,1}
[PAI] Plan de atención a incidencias	[A.24] Denegación de servicio	D	[8]	{6,0}
	[E.24] Caída del sistema por agotamiento de recursos	D	[7]	{6,0}
	[A.15] Modificación de la información	I	[7]	{6,0}
	[A.19] Revelación de información	C	[7]	{6,0}
	[A.27] Ocupación enemiga	D	[8]	{5,7}
	[A.26] Ataque destructivo	D	[8]	{5,7}
	[A.18] Destrucción de la información	D	[7]	{5,1}
	[A.5] Suplantación de la identidad	I, C, A	[7]	{5,1}
	[A.11] Acceso no autorizado	C, A	[7]	{5,1}
	[A.6] Abuso de privilegios de acceso	A	[7]	{5,1}
[IF] Instalaciones Físicas	[N.1] Fuego	D	[7]	{5,1}
	[I.7] Condiciones inadecuadas de temperatura o humedad	D	[7]	{5,1}
	[I.*] Desastres industriales	D	[7]	{5,1}
	[A.27] Ocupación enemiga	D	[7]	{5,1}
	[I.2] Daños por agua	D	[7]	{5,1}
	[I.1] Fuego	D	[7]	{5,1}
	[N.2] Daños por agua	D	[7]	{5,1}
	[I.6] Corte del suministro eléctrico	D	[7]	{5,1}
	[A.26] Ataque destructivo	D	[7]	{5,1}
	[A.11] Acceso no autorizado	C, A	[7]	{5,1}
	[A.5] Suplantación de la identidad	I, C, A	[7]	{5,1}
	[A.6] Abuso de privilegios de acceso	A	[7]	{5,1}
[ETI] Equipo de TI	[A.24] Denegación de servicio	D	[8]	{6,0}
	[N.1] Fuego	D	[8]	{5,7}
	[I.*] Desastres industriales	D	[8]	{5,7}
	[A.27] Ocupación enemiga	D	[8]	{5,7}
	[I.1] Fuego	D	[8]	{5,7}
	[A.26] Ataque destructivo	D	[8]	{5,7}
	[N.*] Desastres naturales	D	[8]	{5,4}
	[A.19] Revelación de información	C	[6]	{5,4}
	[A.15] Modificación de la información	I	[6]	{5,4}
	[A.29] Extorsión	D	[7]	{5,1}
	[A.18] Destrucción de la información	D	[7]	{5,1}
	[A.13] Repudio (negación de actuaciones)	T	[6]	{5,1}
[AXS] Auxiliares de Soporte	[A.24] Denegación de servicio	D	[7]	{5,4}
	[N.1] Fuego	D	[7]	{5,1}
	[I.*] Desastres industriales	D	[7]	{5,1}
	[A.27] Ocupación enemiga	D	[7]	{5,1}
	[I.1] Fuego	D	[7]	{5,1}
	[A.26] Ataque destructivo	D	[7]	{5,1}
	[A.13] Repudio (negación de actuaciones)	T	[6]	{5,1}

[DA] Dependencias Administrativas	[A.13] Repudio (negación de actuaciones)	T	[8]	{6,3}
	[A.15] Modificación de la información	I	[7]	{6,0}
	[A.19] Revelación de información	C	[7]	{6,0}
	[A.29] Extorsión	I, C	[8]	{5,6}
	[A.24] Denegación de servicio	D	[7]	{5,4}
	[N.1] Fuego	D	[7]	{5,1}
	[I.*] Desastres industriales	D	[7]	{5,1}
	[A.27] Ocupación enemiga	D	[7]	{5,1}
	[I.1] Fuego	D	[7]	{5,1}
	[A.26] Ataque destructivo	D	[7]	{5,1}
	[A.5] Suplantación de la identidad	I, C	[7]	{5,1}
	[A.11] Acceso no autorizado	C	[7]	{5,1}
[GDA] Gerencia Dependencias Administrativas	[A.24] Denegación de servicio	D	[7]	{5,4}
	[A.19] Revelación de información	C	[6]	{5,4}
	[N.1] Fuego	D	[7]	{5,1}
	[I.*] Desastres industriales	D	[7]	{5,1}
	[A.27] Ocupación enemiga	D	[7]	{5,1}
	[I.1] Fuego	D	[7]	{5,1}
	[A.26] Ataque destructivo	D	[7]	{5,1}
	[A.11] Acceso no autorizado	A	[7]	{5,1}
	[A.6] Abuso de privilegios de acceso	A	[7]	{5,1}
	[A.5] Suplantación de la identidad	A	[7]	{5,1}
	[A.13] Repudio (negación de actuaciones)	T	[6]	{5,1}
[JTI] Jefe del área de TI	[A.24] Denegación de servicio	D	[8]	{6,0}
	[N.1] Fuego	D	[8]	{5,7}
	[I.*] Desastres industriales	D	[8]	{5,7}
	[A.27] Ocupación enemiga	D	[8]	{5,7}
	[I.1] Fuego	D	[8]	{5,7}
	[A.26] Ataque destructivo	D	[8]	{5,7}
	[A.13] Repudio (negación de actuaciones)	T	[7]	{5,7}
	[A.15] Modificación de la información	I	[6]	{5,4}
	[A.19] Revelación de información	C	[6]	{5,4}
	[A.29] Extorsión	D	[7]	{5,1}
	[A.18] Destrucción de la información	D	[7]	{5,1}
[TEC] Técnicos	[A.24] Denegación de servicio	D	[8]	{6,0}
	[N.1] Fuego	D	[8]	{5,7}
	[I.*] Desastres industriales	D	[8]	{5,7}
	[A.27] Ocupación enemiga	D	[8]	{5,7}
	[I.1] Fuego	D	[8]	{5,7}
	[A.26] Ataque destructivo	D	[8]	{5,7}
	[A.13] Repudio (negación de actuaciones)	T	[7]	{5,7}
	[A.15] Modificación de la información	I	[6]	{5,4}
	[A.19] Revelación de información	C	[6]	{5,4}
	[A.29] Extorsión	D	[7]	{5,1}
	[A.18] Destrucción de la información	D	[7]	{5,1}
	[A.11] Acceso no autorizado	A	[7]	{5,1}
	[A.6] Abuso de privilegios de acceso	A	[7]	{5,1}
	[A.5] Suplantación de la identidad	A	[7]	{5,1}

BIBLIOGRAFÍA

Alegsa, L. (08 de 2009). *Alegsa*. Obtenido de http://www.alegsa.com.ar/Dic/antivirus.php

Alonso, P. (s.f.). *Federción de Servicios a la Ciudadanía-CCOO.* Obtenido de http://www.fsc.ccoo.es/comunes/recursos/99922/doc28596_Seguridad_informatica.pdf

Amer Owaida. (05 de enero de 2021). Obtenido de https://www.welivesecurity.com/la-es/2021/01/05/formas-comunes-dispositivos-pueden-infectarse-con-malware/

American Psychological Association. (2010). *Manual de publicaciones de la American Psychological Association.* México: Manual Moderno.

Anerdata. (s.f.). *Anerdata*. Obtenido de http://www.anerdata.com/que-es-un-servidor.html

Anonimo. (Agosto de 2012). *Welivesecurity*. Obtenido de https://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos/#:~:text=tenga%20clara%20esta-,Como%20parte%20del%20Sistema%20de%20Gesti%C3%B3n%20de%20Seguridad%20de%20la,que%20podr%C3%ADan%20explotar%20las%20vulnerabildades.

Asociación Española para la Calidad. (21 de 10 de 2014). *AEC*. Recuperado el 21 de 10 de 2014, de http://www.aec.es/web/guest/centro-conocimiento/seguridad-de-la-informacion

Bernal, J. J. (23 de 08 de 2013). *pdcahome*. Recuperado el 21 de 10 de 2014, de http://www.pdcahome.com/5202/ciclo-pdca/

Caldas, U. D. (06 de 10 de 2020). *Universidad Distrital Francisco Jose de Caldas*. Obtenido de https://ti.udistrital.edu.co/boletin/correos-maliciosos

Caldas, U. F. (06 de Octubre de 2020). Obtenido de https://ti.udistrital.edu.co/boletin/correos-maliciosos

Calderon Arateco, L. L. (2022). Obtenido de http://polux.unipiloto.edu.co:8080/00002658.pdf

Colombia, U. C. (25 de 06 de 2014). *Universidad Cooperativa De Colombia*. Obtenido de https://www.ucc.edu.co/prensa/2014/Paginas/seguridad-de-la-informacion-y-seguridad-informatica.aspx

Erb, M. (27 de 09 de 2011). Obtenido de https://protejete.wordpress.com/gdr_principal/amenazas_vulnerabilidades/

GCF Community Foundation International. (s.f.). *Gcfaprendelibre*. Obtenido de http://www.gcfaprendelibre.org/tecnologia/curso/informatica_basica/empezando_a_usar_un_computador/2.do

Google. (2015). *support.google*. Obtenido de https://support.google.com/adwords/answer/2375413?hl=es-419

Guerrero Julio, M. (2018). *Gestión de Riegos de TI.* Bucaramanga: Universidad Cooperativa de Colombia.

Guerrero Julio, M. L. (2014). *Gestión de riesgos de TI.* 09: Universidad Cooperativa de Colombia.

Hernández, R., Fernández, C., & Baptista, P. (2006). *Metodología de la investigación.* México: MacGraw-Hill.

Informática moderna. (2008). Obtenido de http://www.informaticamoderna.com/Info_dat.htm

Informaticamoderna. (2008). *Informática Moderna*. Obtenido de http://www.informaticamoderna.com/Mant_comp.htm

Instituto Nacional de Tecnologías de la comunicación de España. (2013). *INCIBE*. Obtenido de https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf

INTECO. (14 de 10 de 2014). *INTECO*. Recuperado el 14 de 10 de 2014, de https://www.inteco.es/Formacion_eu/SGSI_eu/Conceptos_Basicos_eu/Normativa_SGSI_eu/

ISOTools. (2022). Obtenido de https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISOTools Excellence. (2017). *Blog especializado en Seguridad de la Informacion y Ciberseguridad*. Obtenido de https://www.pmg-ssi.com/2017/02/realizar-inventario-activos-de-informacion/#:~:text=Los%20activos%20de%20informaci%C3%B3n%20son,indirectamente%2C%20con%20las%20dem%C3%A1s%20entidades.

Julio, M. L. (2014). *Cnseptos Generales Sobre El riesgo de Tecnologias de Informacion.* Bucaramanga: Universidad Cooperativa de Colombia.

Julio, M. L. (2014). *Gestión de riesgo de TI Unidad 1.*

Libre, U. (2020). *Universidad Libre*. Obtenido de http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/152-seguridad-de-la-informacion#:~:text=La%20Seguridad%20de%20la,confidencialidad%2C%20la%20autenticidad%20e%20Integridad.

MasterMagazine. (2009). *MasterMagazine*. Obtenido de http://www.mastermagazine.info/termino/4532.php

Mifsud, E. (2012). *Ministerio de Educacion, Cultura y Deporte.* Obtenido de http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=7

Mifsud, E. (26 de 03 de 2012). *MONOGRÁFICO: Introducción a la seguridad informática - Vulnerabilidades de un sistema informático*. Obtenido de

http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

Ministerio de Hacienda y Administraciones Públicas de España. (2012). *Magerit – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Ministerio de Hacienda y Administraciones Públicas de España. (2012). *Magerit – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

MinTIC. (2022). *Elaboración de la política general de seguridad y privacidad de la información.* Obtenido de https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-150520_G2_Politica_General.pdf

Muñoz Hernández, H., Zapata Cantero, L. G., Requena Vidal, D. M., & Ricardo. (2019). *Revista Venezolana de Gerencia.* Obtenido de https://www.redalyc.org/journal/290/29063446029/29063446029.pdf

Riesgos, M.-v. 3. (s.f.). *Magerit-versión 3.0 Metodología de Análisis Y gestión de Riesgos*. Obtenido de https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/M

Solutek. (2015). *Solutekcolombia*. Obtenido de http://www.solutekcolombia.com/servicios_tecnologicos/mantenimientos/correctivos/

Téllez, V. J. (1988). *Contratos informáticos.* Ciudad universitaria: Universidad Nacional Autónoma de México.

Gestión De Riesgos De TI Conceptos Generales Sobre El Riesgo De Tecnologías De Información (Contenidos De La Unidad 1). Autora: Marlene Lucila Guerrero Julio

Gestión De Riesgos De TI – Análisis Y Evaluación De Riesgos De Tecnologías De La Información (Contenidos De La Unidad 2). Autora: Marlene Lucila Guerrero Julio

Gestión De Riesgos De TI – Modelos Para La Gestión Del Riesgo De Tecnologías De La Información (Contenidos De La Unidad 3). Autora: Marlene Lucila Guerrero Julio

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método

UNIR La Universidad En Internet. (05 de 20255). Obtenido de https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

Universidad Nacional Autónoma de México. (19 de 04 de 2015). Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/DefinicionPolitica.php

VERIZON. (2022). *VERIZON* . Obtenido de https://espanol.verizon.com/info/definitions/antivirus/

WIKIPEDIA. (2011). *WIKIPEDIA*. Obtenido de https://es.wikipedia.org/wiki/Sistema_de_gesti%C3%B3n_de_la_seguridad_de_la_informaci%C3%B3n