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

LUZ AMANDA MEDINA RINCÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

CHÍA

2019

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

LUZ AMANDA MEDINA RINCÓN

Trabajo de Grado Proyecto Aplicado

Asesor y Director de Curso: Juan José Cruz

Director de proyecto: Salomón Gonzales García

Gabriel Alberto Puerta Aponte

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

CHÍA

2019

CONTENIDO

INTRODUCCIÓN - 8 -
1. TITULO - 9 -
2. FORMULACIÓN DEL PROBLEMA - 10 -
3. JUSTIFICACIÓN - 13 -
4. OBJETIVOS - 15 -
4.1. OBJETIVO GENERAL - 15 -
4.2. OBJETIVOS ESPECÍFICOS - 15 -
5. MARCO DE REFERENCIA - 16 -
5.1. MARCO TEÓRICO - 16 -
5.1.1. Normas ISO - 16 -
5.1.2. Sistema De Gestión De La Seguridad De La Información (SGSI) - 20 -
5.1.3. MAGERIT - 22 -
5.2. MARCO CONCEPTUAL - 23 -
5.2.1. Amenazas - 23 -
5.2.2. Vulnerabilidades - 23 -
5.2.3. Riesgos - 24 -
5.2.4. Activos - 24 -
5.2.5. Impacto - 24 -
5.2.6. Desastre - 24 -
5.3. MARCO CONTEXTUAL - 25 -
5.3.1. Estado Actual - 26 -
5.3.2. Descripción de la Universidad - 26 -
5.3.3. Reseña Histórica - 27 -
5.3.4. Misión, Visión - 28 -
5.3.5. Organigrama Institucional - 28 -
5.3.6. Principales Procesos Y Servicios - 30 -
5.3.7. Análisis Diferencial - 33 -
5.4. MARCO LEGAL - 33 -
6. DISEÑO METODOLÓGICO - 36 -

6.1. OBJETO DE ESTUDIO - 36 -
6.2. FUENTE DE INFORMACIÓN - 36 -
6.3. MEDICIÓN Y ANÁLISIS DE LA INFORMACIÓN - 36 -
6.4. TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN - 37 -
6.5. METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS - 37 -
6.6. ANÁLISIS Y GESTIÓN DE RIESGOS EN LA ORGANIZACIÓN - 38 -
6.6.1. Inventario De Activos - 39 -
6.6.2. Dimensiones de valoración - 40 -
6.6.3. Valoración de activos - 42 -
6.6.4. Identificación y Análisis de amenazas - 44 -
6.6.5. Análisis de riesgo - 46 -
6.6.6. Salvaguardas - 48 -
6.6.7. Diseño de políticas y controles - 62 -
7. NOMBRE DE LAS PERSONAS QUE PARTICIPAN EN EL PROYECTO **Error! Bookmark not defined.**
8. RECURSOS DISPONIBLES (Materiales, Financieros, Institucionales). - 70 -
RECOMENDACIONES - 71 -
CONCLUSIONES - 72 -
DIVULGACIÓN - 73 -
BIBLIOGRAFÍA - 74 -
ANEXOS - 77 -

LISTA DE TABLAS

Pág.

TABLA 1 IDENTIFICACIÓN DE ACTIVOS INFORMÁTICOS - 40 -

TABLA 2 DIMENSIÓN DE VALORACIÓN **ERROR! BOOKMARK NOT DEFINED.**

TABLA 3 CRITERIOS DE VALORACIÓN - 42 -

TABLA 4 VALORACIÓN DE ACTIVOS CANTIDADES - 43 -

TABLA 5 VALORACIÓN DE ACTIVOS **ERROR! BOOKMARK NOT DEFINED.**

TABLA 6 ESCALA DE RANGO DE PROBABILIDAD DE AMENAZAS - 44 -

TABLA 7 DIMENSIONES DE SEGURIDAD - MAGERIT - 45 -

TABLA 8 RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO **ERROR! BOOKMARK NOT DEFINED.**

TABLA 9 ANÁLISIS - IDENTIFICACIÓN DE AMENAZAS **ERROR! BOOKMARK NOT DEFINED.**

TABLA 10 MAPA DE RIESGO - 46 -

TABLA 11 NIVEL DE RIESGO - 47 -

TABLA 12 MATRIZ DE ANÁLISIS DE RIESGOS INFORMÁTICOS **ERROR! BOOKMARK NOT DEFINED.**

TABLA 13 SALVAGUARDAS - 50 -

TABLA 14 PORCENTAJES / DOMINIOS / CUMPLIMIENTO - 53 -

TABLA 15 MATRIZ DE CONTROLES **ERROR! BOOKMARK NOT DEFINED.**

TABLA 16 RECURSOS DISPONIBLES - 70 -

LISTA DE FIGURAS

Pág.

FIGURA. 1 GESTIÓN DEL RIESGO - 19 -

FIGURA. 2 RIESGOS DE LA INFORMACIÓN - 21 -

FIGURA. 3 MODELO MAGERIT - 23 -

FIGURA. 4 ORGANIGRAMA GENERAL - 29 -

FIGURA. 5 DIVISIÓN ADMINISTRATIVA - 29 -

FIGURA. 6 DIVISIÓN DE LA DIRECCIÓN DE SISTEMAS - 30 -

FIGURA. 7 SISTEMA DE GESTIÓN DE LA CALIDAD PARA LA PRESTACIÓN DE SERVICIOS DE APOYO A LA ACADEMIA - 32 -

FIGURA. 8 EXTRACTO INVENTARIO DE ACTIVOS **ERROR! BOOKMARK NOT DEFINED.**

FIGURA. 9 ESCALA DE MADUREZ REFERENCIA - 51 -

FIGURA. 10 CALIFICACIONES - 52 -

FIGURA. 11 PORCENTAJE DE CUMPLIMIENTO - 55 -

FIGURA. 12 TABLA DE BARRAS CONTROLES - 56 -

FIGURA. 13 NIVEL DE MADURACIÓN - 57 -

ANEXOS

ANEXOS 1 - A1 – INVENTARIO DE ACTIVOS GENERAL - 77 -
ANEXOS 2 - A1 – INVENTARIO DE ACTIVOS ESPECÍFICO - 79 -
ANEXOS 3 - A2 – DIMENSIÓN DE VALORACIÓN - 89 -
ANEXOS 4 - A3 – VALORACIÓN DE ACTIVOS - 109 -
ANEXOS 5 - A4 – ANÁLISIS - IDENTIFICACIÓN DE AMENAZAS - 132 -
ANEXOS 6 - A5 – ANÁLISIS – RIESGOS - 147 -
ANEXOS 7 - A6 – SALVAGUARDAS - MATRIZ DE CONTROLES_27002 - 155 -

INTRODUCCIÓN

El SGSI es la abreviatura que se utiliza para el sistema de gestión de la seguridad de la información, el cual es uno de los procesos que a nivel empresarial actualmente genera un alto impacto ya sea positivo o negativo, según la madurez de los procesos internos de la organización, En tal contexto se debe hablar de información ya que corresponde al conjunto de datos organizados en poder de una organización y que a su vez posean un alto valor para la misma, independiente de la forma en la que esta se encuentre almacenada, su origen o la fecha en la se creó, según la norma ISO 27001, un sistema de gestión de la seguridad de la información consiste en la preservación de tres pilares fundamentales los cuales son la confidencialidad, integridad y disponibilidad, de la información, al igual que los sistemas implicados al interior de una organización.

Por lo tanto, el contenido de este documento busca ser una guía, el cual permitirá evaluar la integridad, confidencialidad y disponibilidad de los activos de información que actualmente afectan ya seguridad de la información en la Dirección de Sistemas de La Universidad De La Sabana,

En consecuencia, actualmente los procesos que se llevan al interior de la Dirección de Sistemas de la Universidad de la Sabana, no logran optimizar su funcionamiento y seguridad en el manejo de la información ya que actualmente no es posible identificar y garantizar la preservación de los procesos que pueden ser afectados en su confidencialidad, integridad y disponibilidad, es por este motivo que se busca el desarrollar un sistema de gestión de la seguridad de la información para la Dirección de Sistemas de la Universidad de la Sabana impactando positivamente sus procesos, teniendo como referencia la norma ISO/IEC 27001:2013, norma internacional emitida por la organización internacional de normalización ISO, encargada de describir cómo se debería gestionar la seguridad de la información al interior de una organización, esta norma puede ser implementada al interior de cualquier organización, sin mencionar que ha sido creada por los mejores especialistas del mundo en este tema y proporciona una metodología para la implementación de la gestión de la seguridad de la información en una organización,

con el propósito de agregar valor a la organización, mediante un Sistema de Gestión de la Seguridad de la Información.

1. **TITULO**

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

2. **FORMULACIÓN DEL PROBLEMA**

En un contexto general la seguridad de la información se ha convertido en uno de los temas centrales en el mundo para las organizaciones[1] es por este motivo que se requiere que cuenten con un sistema de información, el cual puede variar sus características según el tamaño de la empresa y el sistema de información que puede llegar a requerir la organización.

Teniendo en cuenta un informe presentado por la organización de los estados americanos (OEA) en el año 2014[2], en el cual se realiza un enfoque frente a las tendencias de Seguridad Cibernética en América Latina y el Caribe, este informe muestra los resultados de un estudio realizado en el año 2013 y publicado como ya se menciona en el año 2014, en este se indica que el ciberespionaje, la privacidad de la información y el personal interno malintencionado ocupan los principales lugares, varias de las violaciones de información a gran escala pusieron de manifiesto que los delitos cibernéticos siguen en un constante aumento y que este tipo de amenazas sigue acechando a gobiernos, empresas privadas y usuarios finales. En la actualidad se estima que los altos costos de delitos informático podrán ascender si se tiene en cuenta que para el periodo evaluado los delitos informáticos costaban almeno unos USD 113.000 millones. Solamente en Brasil los costos alcanzaron los USD 8.000 millones, seguidos de México con USD 3.000 millones y finalmente Colombia con USD 464 millones.

En Colombia se han presentado dos casos, el primer caso en una Universidad de la ciudad de Medellín en el 2013 que se vio afectada por fallas de seguridad de la información, en donde dos funcionarios cambiaban notas de estudiantes por dinero, este evento causo pérdida de reputación y por poco la pérdida de certificación como

[1] VON, Solms, y VAN Niekerk, J. From information security to cyber security. Cybercrime in the Digital Economy, [En linea]. 1ª ed. 2013., [17 – noviembre -29017]. Disponible en internrt: https://doi.org/http://dx.doi.org.ezproxy.unisabana.edu.co/10.1016/j.cose.2013.04.004

[2] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y SYMANTEC. Tendencias De Seguridad Cibernética En América Latina Y El Caribe [En línea] 1ª ed. 2014 [18 – noviembre - 2017]. Disponible en internet: https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf

institución de alta calidad dada por el Ministerio de Educación[3]. También está el caso de una Universidad en la ciudad de Bogotá en el 2013 en donde un estudiante destacado y becado, logro por medio de programas Key loggers descifrar contraseñas de algunos profesores en el sistema de notas y luego ofrecía este servicio a otros estudiantes a cambio de dinero[4]

Los procesos que actualmente se llevan al interior de la Dirección de Sistemas de la Universidad de la Sabana, posiblemente no logran optimizar su funcionamiento y seguridad en el manejo de la información ya que actualmente no es posible identificar y garantizar la preservación de los procesos que pueden ser afectados en su confidencialidad, integridad y disponibilidad, es por este motivo que se busca el desarrollar un sistema de gestión de la seguridad de la información para la Dirección de Sistemas de la Universidad de la Sabana buscando impactar positivamente sus procesos, teniendo como referencia la norma ISO/IEC 27001:2013 y ISO/IEC 27002, y que de este modo se responda a la pregunta de investigación del ¿cómo aporta la administración de un sistema de gestión de seguridad de información al interior de una organización?, lo anterior teniendo en cuenta la evaluación de la problemática actual de la organización.

El problema actual radica en la manera en la que se gestionan los procesos administrativos, que actualmente se manejan en la Dirección de Sistemas, procesos que no se encuentran documentados, no tienen asignado un responsable o que simplemente no tienen una gestión ni una trazabilidad, la dirección se comporta como un área transversal a todos los procesos de la universidad, prestando servicios a todas las direcciones académico administrativas de la universidad, por lo cual afecta a todas las áreas retrasando la correcta gestión de los procesos articulares, se requiere que esta realice una mejor gestión de la información, identificando con claridad cuáles son las falencias actuales para tomar acciones y realizar procesos de mejora continua que permitan definir controles y políticas sobre la correcta gestión y administración de la información, teniendo en cuenta que se trata de un área trasversal se deben crear procesos globales que puedan ser acogidas por las demás áreas y de este modo permitan generar valor en su quehacer, lo anterior basados en una evaluación y análisis de riesgos,

[3] EL TIEMPO, N. Rector de la UPB habla sobre escándalo de alteración de notas - Archivo Digital de Noticias de Colombia y el Mundo desde 1.990 - eltiempo.com. [2013] Retrieved from [En línea]. 1ª ed. Colombia – Bogotá: Universidad de la Sabana, [Citado 17 – Noviembre - 2017] Disponible en internet: http://www.eltiempo.com/archivo/documento/CMS-13084882

4 EL ESPECTADOR. N. Universidades, víctimas de “hackers” | ELESPECTADOR.COM. Retrieved from . [2015] Retrieved from [En línea]. 1ª ed. Colombia – Bogotá: Universidad de la Sabana, [Citado 17 – Noviembre - 2017] Disponible en https://www.elespectador.com/noticias/judicial/universidades-victimas-de-hackers-articulo-560884

tomando como base fundamental el cumplimiento de la política de seguridad de la información que actualmente se encuentra abalada por la universidad, lo anterior para identificar el nivel de cumplimiento de la misma con respecto a lo sugerido por el SGSI, y que de esta manera se pueda llegar a articular el SGSI con respecto a la política de seguridad de la información, sin llegar a modificar su matriz de gobernabilidad.

El SGSI, permite establecer políticas y procedimientos en relación a los propósitos de negocio de la Universidad [5] y por ende de la Dirección de Sistemas, entendiendo en cuenta que la universidad es una entidad de educación superior de alta calidad, actualmente certificada por la norma ISO 9001 y con 35 años de experiencia en el campo de la educación superior, ofreciendo alrededor de 120 programas de formación superior, entre programas de doctorados, maestrías, especializaciones y pregrados, hoy la universidad tiene más de 44000 egresados y un total de 44952 estudiantes activos, la Dirección de Sistemas al ser un área transversal brinda soporte a todas las plataformas a través de un catálogo de servicios, que se encuentra alineado a los requerimientos de la organización, partiendo de la gran diversidad de usuarios que por su labor tiene. Por consiguiente, entiende que es posible presentar riesgos de seguridad de la información que como consecuencia pueden afectar el funcionamiento y la credibilidad en la institución, es por este motivo que se busca la implementación de un sistema de gestión de seguridad de la información, que permita mitigar y gestionar los riesgos de la Dirección de Sistemas como eje central del tratamiento de la información en la Universidad de la Sabana[6].

[5]UNIVERSIDAD DE LA SABANA. Proyecto Educativo Institucional. [En línea]. 1ª ed. Colombia – Chía: Universidad de la Sabana, [Citado 17 – Noviembre - 2017] Disponible en internet: https://www.unisabana.edu.co/nosotros/proyecto-educativo-institucional/

[6] UNIVERSIDAD DE LA SABANA. La Sabana En Sifras. Chía 2017 [En línea]. 1ª ed. Colombia – Chía: Universidad de la Sabana, [Citado 17 – Noviembre - 2017 Disponible en internet: https://www.unisabana.edu.co/nosotros/la-sabana-en-cifras/

3. **JUSTIFICACIÓN**

El desarrollo del presente proyecto tiene como principal objetivo, el lograr que en la organización se pueda gestionar de una manera adecuada y segura la información, tomando como punto de referencia las diferentes normas que existen y que se pueden aplicar en la actualidad para la correcta gestión de la información, es necesario tomar como punto de partida el prefacio de que, la seguridad de la información surge como una necesidad de asegurar que la información tenga los niveles adecuados de protección en cuanto a elementos tales como confidencialidad, integridad y disponibilidad de la información.

De ahí la importancia de implementar un sistema de gestión de la seguridad de la información, que permita garantizar al interior de la organización la disminución de los riesgos, ya que si bien es cierto no es posible eliminar por completo los riesgos, es posible controlarlos o aplacarlos en gran medida, a través de la generación de políticas adecuadas y útiles se puedan mitigar dichas amenazas.

Las amenazas que actualmente sufren al interior de las organizaciones, es un dato que día con día tiende a dar un alto crecimiento según una encuesta realizada en el año 2016 sobre tendencias de ciber riesgo y seguridad de la información en Latinoamérica, dicho sondeo indica que las principales tendencias identificadas son[7]:

- 4 de cada 10 organizaciones sufrieron una brecha de seguridad en los últimos 24 meses, menos del 20% de las organizaciones cuentan con un SOC[8].
- A pesar de contar con mayor presupuesto, la principal barrera que enfrentan

[7] DELOITTE CYBER RISK & INFORMATION SECURITY STUDY – Latinoamérica. Para más información contacte a Deloitte & Touche SRL 2016. [En línea]. 1ª ed., [Citado 17 – Noviembre - 2017] Disponible en internet: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%C3%A9rica%20-%20Resultados%20Generales%20vf%20(Per%C3%BA).pdf

[8] DELOITTE CYBER RISK & INFORMATION SECURITY STUDY – Latinoamérica. Para más información contacte a Deloitte & Touche SRL 2016. [En línea]. 1ª ed., [Citado 17 – Noviembre - 2017] Disponible en internet: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%C3%A9rica%20-%20Resultados%20Generales%20vf%20(Per%C3%BA).pdf

los casos sigue siendo la falta de presupuesto y/o de recursos suficientes
- Menos del 10% de las organizaciones cuenta con un tablero con indicadores, que permita evaluar la gestión de ciber riesgos y de seguridad de la información.
- La capacidad y concientización es la iniciativa de seguridad que mayor cantidad de organizaciones ejecutaron durante el 2016[9].

La seguridad informática puede tener factores buenos y elementos que se deben mantener en una mejora continua, en la actualidad los países latinoamericanos o que se encuentran en vía de desarrollo como es el caso de Colombia pueden llegar a ser más atractivos para los delincuentes informáticos.

Por lo tanto, un sistema de gestión de la seguridad de la información es necesario al interior de las organizaciones ya que permite solventar y manejar adecuadamente los riesgos y las vulnerabilidades a los que se pueden ver enfrentado, por el mal manejo de la información y lo que su seguridad implica, un sistema de gestión de seguridad de la información teniendo como referencia la norma ISO/IEC 27001:2013, y la norma ISO/IEC 27002, tendrá las condiciones que se requieren para que la seguridad de la información pueda fortalecer los objetivos que actualmente tiene designados la Dirección de Sistemas para el cumplimiento y apoyo al macro posesión del cual hace parte, de tal manera que se garantice la gestión académico administrativa y operacional del área de interés en este particular caso la correcta gestión de la seguridad de la información al interior de la Dirección de Sistemas de la Universidad de la Sabana.

[9] DELOITTE CYBER RISK & INFORMATION SECURITY STUDY – Latinoamérica. Para más información contacte a Deloitte & Touche SRL 2016. [En línea]. 1ª ed., [Citado 17 – Noviembre - 2017] Disponible en internet: https://www2.deloitte.com/content/dam/Deloitte/pe/Documents/risk/Deloitte%202016%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Latinoam%C3%A9rica%20-%20Resultados%20Generales%20vf%20(Per%C3%BA).pdf

4. **OBJETIVOS**

4.1. **OBJETIVO GENERAL**

- Diseñar un sistema de gestión de seguridad de la información para la Dirección de Sistemas de la Universidad de la Sabana, teniendo como referencia las normas ISO/IEC 27001:2013 y ISO/IEC 27002.

4.2. **OBJETIVOS ESPECÍFICOS**

- Desarrollar los procedimientos y documentación requeridos para el diseño y gestión del planteamiento del SGSI, con forme a lo requerido por las normas ISO/IEC 27001:2013 y ISO/IEC 27002.

- Realizar un análisis de brechas GAP, basados en las normas seleccionadas, que permita identificar el estado actual de la Dirección de Sistemas en cuanto a la gestión de la seguridad de la información.

- Establecer y determinar el estado del cumplimiento actual que tiene la Dirección de Sistemas y las brechas respecto a lo requerido por las normas seleccionadas.

- Diseñar políticas del SGSI, que permitan mitigar o solucionar los riesgos y vulnerabilidades evidenciadas, tras los análisis identificados.

5. MARCO DE REFERENCIA

5.1. MARCO TEÓRICO

5.1.1. Normas ISO

- ISO

  Es actualmente un sistema de gestión normalizados, que busca a través de un conjunto de normas orientar la gestión de una empresa, en sus diferentes procesos[10].

  La organización internacional de normas (ISO), fue creada en el año 1947 y en la actualidad cuenta con más de 90 estados miembros los cuales son representados por organismos locales de normalización.

  Esta organización tiene como una de sus principales finalidades el trabajar para lograr una forma común de conseguir el establecimiento de un sistema de calidad, es decir. Busca ya estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional, el cual propende por garantizar las necesidades y expectativas de los clientes o consumidores finales.

  Inicialmente la ISO, designo un grupo de comités técnicos con el propósito de trabajar en el desarrollo de una norma común y universal, es de este resultado que se encuentra la norma ISO 9000, generada 7 años más tarde tras el compendio del aseguramiento de la calidad.

  ISO es el organismo encargado de promover el correcto desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales, con excepción de la eléctrica y la electrónica.

  Las normas ISO no son gubernamentales, ya que ISO es un organismo no gubernamental y por lo tanto no depende de ningún otro organismo internacional, por lo que no tiene autoridad para imponer sus normas en ningún país.

[10] ISOTOOLS. Normas ISO - Sistemas de Gestión Normalizados Colombia. Bogotá 2017 [En línea]. 1ª ed. Colombia – Chía: Universidad de la Sabana, [Citado 17 – Noviembre - 2017 Disponible en internet: https://www.isotools.org/normas/

- ISO 9000

  Normas de gestión de la calidad, estas normas se enfocan a homogeneizar los estándares de calidad de los diferentes productos y servicios que tienen las organizaciones ya sean públicas o privadas, sin importar su tamaño o actividad[11].

- ISO 14000

  Normas para la gestión del medio ambiente son un instrumento claro y eficaz para que las organizaciones puedan establecer actividades parametrizadas con el entorno, cumpliendo con las legislaciones vigentes y dando respuesta a las exigencias actuales de la sociedad[12].

- ISO 26000

  Norma referente a la gestión de la responsabilidad social, enfocada a ayudar a las organizaciones en todo momento a tener un comportamiento transparente y ético el cual fomente parte indisoluble de su modelo de gestión[13].

- ISO 22000, OHSAS 18001, ISO 27001, ISO 22301 etc.

  Normas sobre la gestión de riesgos y seguridad estas son normas y sistemas desarrollados con la finalidad de evitar o tratar de mitigar los distintos riesgos que se presentan relativos a las diferentes amenazas y vulnerabilidades originadas por la actividad empresarial[14].

- ISO 27001

[11] ISOTOOLS. Normas ISO - Sistemas de Gestión Normalizados Colombia. Bogotá 2017 [En línea]. 1ª ed. Colombia – Chía: Universidad de la Sabana, [Citado 17 – Noviembre - 2017 Disponible en internet: https://www.isotools.org/normas/

[12] ISOTOOLS. Normas ISO - Sistemas de Gestión Normalizados Colombia. Bogotá 2017 [En línea]. 1ª ed. Colombia – Chía: Universidad de la Sabana, [Citado 17 – Noviembre - 2017 Disponible en internet: https://www.isotools.org/normas/

[13] ISOTOOLS. Normas ISO - Sistemas de Gestión Normalizados Colombia. Bogotá 2017 [En línea]. 1ª ed. Colombia – Chía: Universidad de la Sabana, [Citado 17 – Noviembre - 2017 Disponible en internet: https://www.isotools.org/normas/

[14] ISOTOOLS. Normas ISO - Sistemas de Gestión Normalizados Colombia. Bogotá 2017 [En línea]. 1ª ed. Colombia – Chía: Universidad de la Sabana, [Citado 17 – Noviembre - 2017 Disponible en internet: https://www.isotools.org/normas/

Se parte de lo ya expuesto anteriormente en el cual se define que hace parte de un grupo de normas que trata sobre la gestión de riesgos y seguridad, son normas y sistemas desarrollados con la finalidad de evitar o tratar de mitigar los distintos riesgos que se presentan relativos a las diferentes amenazas y vulnerabilidades originadas por la actividad empresarial.

Con forme a lo anterior se define como una norma internacional emitida por la organización internacional de normalización ISO, la cual se encarga de describir cómo se debería gestionar la seguridad de la información al interior de una organización, la última verificación de esta norma fue publicada en el año 2013, y en la actualidad el nombre completo de esta norma es ISO/IEC 27001:2013.

Esta norma puede ser implementada al interior de cualquier organización, sin mencionar que esta norma ha sido creada por los mejores especialistas del mundo en este tema y proporciona una metodología para la implementación de la gestión de la seguridad de la información en una organización, con el propósito de agregar valor a la organización, permite que estas sean certificadas, esto quiere decir, que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en dicha organización en cumplimiento con la norma ISO 27001[15].

La información es parte de la gestión global del riesgo al interior de una organización, hay ásperos que se superponen con la ciberseguridad, la gestión de la continuidad y las tecnologías de la información, para entender un como mejor en donde interviene la gestión de la seguridad de la información en la organización es necesario visualizar la siguiente información:

[15] 27001 ACADEMY. ¿Qué Es La Norma ISO 27001? [En línea]. 1ª ed. Colombia: ISO 27001 Academia [Citado 17 – Noviembre - 2017] Disponible en internet: https://advisera.com/27001academy/es/que-es-iso-27001/

Figura. 1 Gestión del riesgo

Fuente: https://advisera.com/

Para el desarrollo de un sistema de gestión de seguridad de la información[16] se utilizan diferentes conceptos referentes a la seguridad que aplican a cualquier tipo de entidad y público, como se pudo visualizar en las normas anteriormente descritas, ahora se busca identificar las diferentes características del SGSI, para su implementación.

[16] GONZÁLEZ MARTÍNEZ, J. Elaboración de un plan de implementación de la norma ISO/IEC 27001:2013. [2015] (U. O. de Catalunya & A. Tortajada Gallego, Eds.), En línea]. 1ª ed. Colombia: ISO 27001 Academia [Citado 17 – Noviembre - 2017] Disponible en internet: http://creativecommons.org/licenses/by-nc-nd/3.0/es/. Universitat Oberta de Catalunya; Universitat Obert

5.1.2. **Sistema De Gestión De La Seguridad De La Información (SGSI)**

El SGSI es la abreviatura que se utiliza para el sistema de gestión de la seguridad de la información, en este contexto se habla de información o se denomina información al conjunto de datos organizados en poder de una entidad y que a su vez posean valor para la misma, independiente de la forma en la que esta se encuentre almacenada, su origen o la fecha en la se creó.

Teniendo en cuenta la definición de los SGSI, según la norma ISO 27001, esta consiste en la preservación de tres pilares fundamentales los cuales son la confidencialidad, integridad y disponibilidad, de la misma manera que los sistemas implicados al interior de una organización.

Según la norma ISO 27001, estos tres términos son la base de toda la seguridad de la información y los define de la siguiente manera:

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados[17].

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso[18].

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran[19].

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI[20].

Como se puede visualizar a continuación, la información puede estar expuesta a diferentes fuentes de riesgos, los cuales deben ser tratados por medio o a través de un sistema de gestión de la seguridad de la información.

---

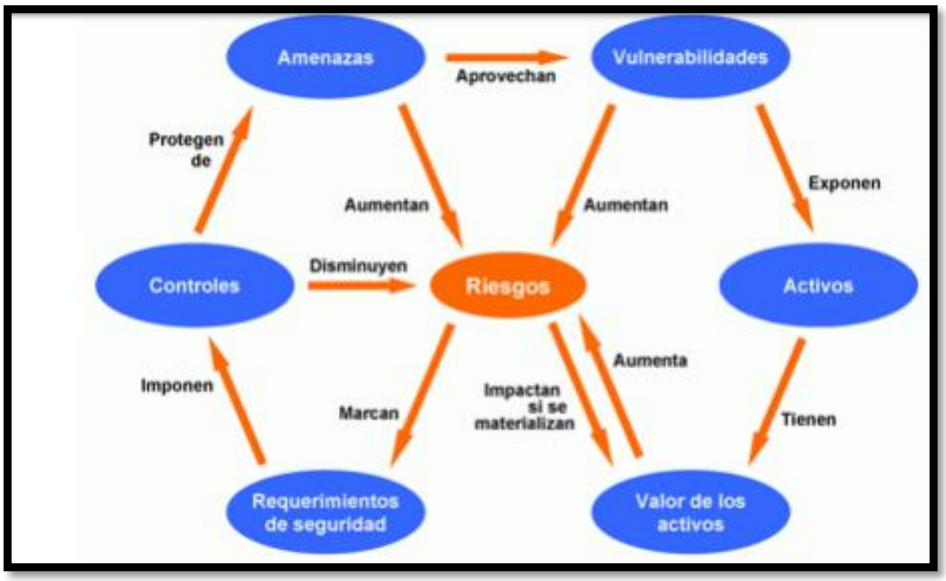
[17] EL PORTAL DE ISO 27001 EN ESPAÑOL [EN línea] 1ª ed. [2012]. Disponible en internet: http://www.iso27000.es/sgsi.html

[18] EL PORTAL DE ISO 27001 EN ESPAÑOL [En línea] 1ª ed. [2012]. Disponible en internet: http://www.iso27000.es/sgsi.html

[19] EL PORTAL DE ISO 27001 EN ESPAÑOL [En línea] 1ª ed. [2012]. Disponible en internet: http://www.iso27000.es/sgsi.html

[20] ISO27000 Sistema de Gestión de la Seguridad de la Información [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: http://www.iso27000.es/download/doc_sgsi_all.pdf

Figura. 2 Riesgos de la información



Fuente: http://www.iso27000.es

La información en conjunto con los procesos y los sistemas que hacen uso de la información, son activos demasiado importantes para la empresa, la confidencialidad, integridad y disponibilidad de esta información puede ser esencial para mantener los niveles de competitividad, conformidad, rentabilidad e imagen de la empresa necesarios para conseguir los objetivos de la empresa y asegurase de que haya beneficios económicos[21].

A continuación, los elementos necesarios para la implementación de un SGSI, PROPUESTOS POR LA Norma ISO 27001[22].

1. Definición de políticas
2. Definir el alcance del SGSI
3. Análisis de riesgo
4. Selección de controles a implementar
5. Declaración de aplicabilidad
6. Revisión del sistema
7. Auditorías internas.

[21] ISOTOOLS EXCELLENCE. Blog especializado en Sistemas de Gestión de Seguridad de la Información. [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: http://www.pmg-ssi.com/2015/07/que-es-sgsi/
[22] NORMAS ISO. ISO 27001 Gestión de la Seguridad de la Información. En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: http://www.normas-iso.com/iso-27001

5.1.3. **MAGERIT**

La metodología de análisis y gestión de riesgos de los sistemas de información o mejor conocida como MAGERIT, elaborada por el Consejo Superior de Administración Electrónica de España, esta metodología se encarga de cubrir la fase AGR o análisis y gestión de riesgos, se habla de una gestión global de la seguridad de la información basada en la norma ISO 27001. Es por lo tanto el núcleo de toda actualización organizacional, ya que debe ser incluida en todas las fases que sean de tipo estratégico y se condiciona la fase a profundidad de tipo logístico, se basa en analizar el impacto que puede llegar a tener para la empresa la violación de la seguridad, realizando una adecuada búsqueda de las posibles amenazas, que pueden afectar a la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando de este modo tener una claridad de las medidas que se deben tomar para la prevención y corrección de riesgos que sean más apropiadas para la organización.

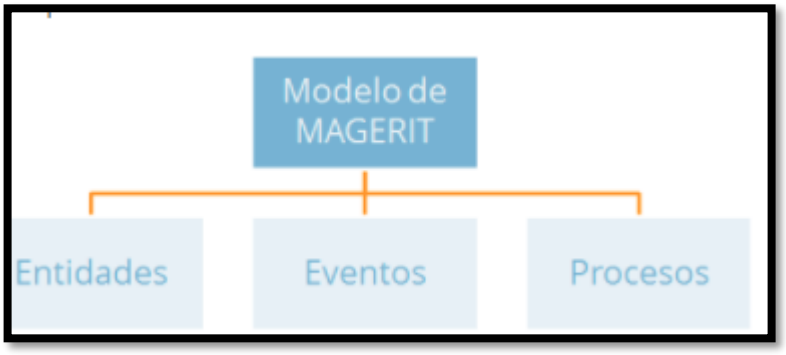
MAGERIT está relacionada con el uso de las nuevas tecnologías de la información y la comunicación, por lo que genera grandes beneficios, pero también riesgos los cuales se deben identificar y minimizar, MAGERIT indica que se puede llevar a cabo:

1. El análisis de riesgo en cualquier tipo de sistema de seguridad de la información.
2. La gestión de los riesgos, basada en todos los resultados obtenidos durante todo el proceso realizado durante el análisis y la identificación de los riesgos.

MAGERIT tiene por objetivo la evaluación, homologación y certificación de seguridad de los sistemas de información según la norma ISO 27001[23]. La visión global de la seguridad de los sistemas de información de ISO 27001, comienza con un modelo de análisis de la gestión de los riesgos la cual comprende tres modelos como se muestra en la siguiente imagen.

[23] (ISOTOOLS EXCELLENCE. Blog especializado en Sistemas de Gestión de Seguridad de la Información. ISO 27001: El método MAGERIT 2015 [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit/

Figura. 3 Modelo MAGERIT



Fuente: http://www.pmg-ssi.com

5.2. **MARCO CONCEPTUAL**

5.2.1. **Amenazas**

Son aquellas acciones que pueden ocasionar consecuencias negativas en la operatividad de la organización[24].

5.2.2. **Vulnerabilidades**

Son definidas como debilidades del sistema informático el cual puede ser utilizado para causar un daño, estas pueden aparecer en cualquier elemento ya sea software, hardware o sistemas operativo[25].

[24] TUTORIAL DE SEGURIDAD INFORMÁTICA. [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: Tutoriales De Seguridad. http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html
[25] TUTORIAL DE SEGURIDAD INFORMÁTICA. [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: Tutoriales De Seguridad. html http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html#14

5.2.3. **Riesgos**

- Gestión Del Riesgo

  Se define como una actividad capas de coordinar para dirigir y controlar los aspectos que se encuentran asociados al riesgo al interior de una organización[26].

- Análisis De Riesgo

  Puede ser un proceso de carácter cualitativo o cuantitativo el cual permite que se realice una evaluación del riesgo[27].

5.2.4. **Activos**

Son todos aquellos relacionados con los sistemas de información[28].

5.2.5. **Impacto**

Es la consecuencia inherente cuando ocurren las distintas amenazas y siempre son de carácter negativo, ya que las pérdidas que estas acarrean pueden ser financiaras, de corto mediano o largo plazo.

5.2.6. **Desastre**

Eventos adversos de mayor magnitud que las emergencias, por lo que superan la capacidad de respuesta de la comunicación afectada y exige apoyo externo.

---

[26] MINTIC. Guía de gestión de riesgos [2017]. [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

[27] MINTIC. Guía de gestión de riesgos [2017]. [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

[28] ANÁLISIS DE INFORMACIÓN SOBRE RIESGOS. [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: https://www.cepal.org/publicaciones/xml/8/33658/ColombiaCapII.pdf

5.3. **MARCO CONTEXTUAL**

El desarrollo de este proyecto se llevará a cabo en la Dirección de Sistemas de la Universidad de la Sabana, se encuentra ubicada en Chía Cundinamarca, a 15 minutos de la zona norte de Bogotá Colombia.

Existe como base para el desarrollo del presente proyecto, diferentes análisis y documentos que se han venido tratando a lo largo de este documento, para buscar la implementación de mejores prácticas al interior de la organización, haciendo referencia de este modo a documentación que se puede encontrar ya el marco conceptual y teórico, así mismo un numero notorio de referencias bibliografías que brindan soporte a las diferentes teorías y levantamientos de información, que se buscan soportar, analizar y diseñar en el presente proyecto, de tal manera que puedan ser de utilidad para la Dirección de sistemas, de la universidad.

Como fuente de apoyo se buscan algunos elementos referenciales como tesis, normas, artículos y demás elementos útiles para el correcto desarrollo de la investigación y solución al problema planteado, el cual radica en que los procesos que actualmente se llevan al interior de la Dirección de Sistemas de la Universidad de la Sabana, no logran optimizar su funcionamiento y seguridad en el manejo de la información ya que actualmente no es posible identificar y garantizar la preservación de los procesos que pueden ser afectados en su confidencialidad, integridad y disponibilidad, es por este motivo que se busca el desarrollar un sistema de gestión de la seguridad de la información para la Dirección de Sistemas de la Universidad de la Sabana impactando positivamente sus procesos, teniendo como referencia la norma ISO/IEC 27001:2013 y ISO/IEC 27002..

Conforme a lo anteriormente mencionado y a modo de contextualización se puede mencionar que el problema actual radica en la mala gestión administrativa de los procesos que actualmente se manejan en la Dirección de Sistemas, teniendo en cuenta que la dirección se comporta como un área transversal, la cual presta servicios a todas las direcciones académico administrativas de la universidad, se requiere que esta realice una mejor gestión de la información, identificando con claridad cuáles son las falacias actuales para tomar acciones y realizar procesos de mejora continua que permitan definir controles y políticas sobre la correcta gestión y administración de la información, basados en una evaluación y análisis de riesgos y una probable medición de eficacia de los mismos.

Según una estadística realizada durante el año 2014, por los niveles de certificación reportados en la norma ISO 27001, se nota in crecimiento con respecto al año inmediatamente anterior del 7%, teniendo para este periodo de tiempo 23,972, El estándar de seguridad de la información experimentó una leve desaceleración, con un crecimiento modesto del 7%, contradiciendo los prometedores resultados de años anteriores. Como un innovador en tecnología digital, Japón encabeza históricamente las listas de éxitos en el sector de la seguridad de la información, aunque el Reino Unido también ocupa un lugar destacado con el crecimiento más importante en términos absolutos (340 certificados emitidos), como resultado de un organismo de certificación que informó la emisión de más certificados que en 2013[29].

5.3.1. **Estado Actual**

Al interior de este punto se identifica las actividades propuestas para la identificación del manejo de riesgos de la seguridad de la información, que actualmente tiene la organización con respecto a las mejores prácticas de la norma ISO/IEC 27001 para de este modo poder diseñar un sistema de gestión de seguridad de la información para la organización.

Inicialmente y como se encuentra programado en el cronograma de actividades, lo primero es identificar los principales objetivos y procesos del negocio en este caso de la Dirección de Sistemas y tecnologías de la información, para de este modo determinar los puntos trabajables.

Una vez se pueda determinar el alcance del proyecto con respecto a la información contenida en los objetivos y a la delimitación ya expuesta, a continuación, se describe en términos generales la organización, identificando la misión y visión, de la misma manera se realiza identificación del principal proceso.

5.3.2. **Descripción de la Universidad**

La Universidad de la Sabana es una entidad de educación superior, que se encuentra certificada ante el Ministerio de Educación Nacional de Colombia como una de las universidades que actualmente cumple con altos niveles de calidad en la educación superior.

La Universidad de la Sabana, en su condición de universidad, es una comunidad

[29] GLOBALSTD CERTIFICATION. [En línea] 1ª ed. [20 – Octubre -2014]. Disponible en internet: Estadísticas ISO 2014 http://www.globalstd.com/component/k2/estadisticas-iso-2014

de personas, vinculadas por el fin participado de crecimiento superior, gracias al cual se constituye una comunidad de saberes.

En tanto el conocimiento es un bien, difusivo como bien, se impone una comunicación que se traduce en una tarea académica.

Así, mediante la investigación y la docencia, la Universidad se proyecta, con vocación de servicio, en los distintos servicios de la sociedad.

La Universidad, que, en una de sus notas esenciales, articula, de conformidad con la unidad de lo real, la necesidad de coherencia de los fines que orientan la misión de la Universidad con la singularidad de las personas, la pluralidad de sus posturas ideológicas o científicas y la diversidad de los saberes.

Por lo tanto, la Dirección de Sistemas y Tecnologías, en conformidad con la línea educativa que tiene la organización, se línea a todas las directrices de la universidad y propicia de manera activa escenarios que permitan fortalecer los diferentes procesos necesarios para el cumplimiento de los objetivos institucionales.

5.3.3. **Reseña Histórica**

La Universidad de La Sabana es el resultado de años de trabajo de una comunidad académica en busca de cultivar profesionales y seres humanos excelentes que trabajen por el desarrollo del país y la sociedad.

Fue San Monseñor Josemaría Escrivá de Balaguer en 1964 quien impulsó la fundación de colegios por padres de familia, lo que años más tarde daría origen a la Asociación para la Enseñanza (Aspaen). Más tarde en 1971 gracias a esta Asociación nace el INSE, Instituto Superior de Educación, pionero en educación a distancia en el país y Latinoamérica.

Entre los aspectos esenciales de la Universidad de La Sabana expresados en el Proyecto Educativo Institucional se destacan: la universalidad respecto a todas las ciencias, las técnicas y las artes, y de todas las personas; la apertura a la verdad, el diálogo permanente y el respeto por la discrepancia; la libertad de enseñanza, aprendizaje, investigación y cátedra dentro de las exigencias de la verdad y del bien común; la proyección de la Universidad, con vocación de servicio, en todos los sectores de la sociedad; la autonomía para darse sus normas y gobernarse con base en ellas; la responsabilidad respecto a la coherencia y calidad de su proyecto educativo ante sí misma y ante la entidad fundadora, la comunidad científica, la sociedad y el Estado; el régimen de decisión colegiada en su gobierno; el reconocimiento en los profesores como el centro de la vida universitaria; la apertura a toda persona con las condiciones

para la educación superior que desee acudir a la Universidad para preparase con competencia profesional; la asesoría académica como medio constante de atención personalizada a los estudiantes; y la formación integral de todos los miembros de la comunidad universitaria.

Actualmente, la Universidad ofrece 23 programas de pregrado, 17 especializaciones médico-quirúrgicas, 49 especializaciones, 28 maestrías y 3 doctorados.[30]

5.3.4. **Misión, Visión**

A continuación, se sita la misión y la visión de la Universidad de la Sabana[31]

5.3.4.1. Misión

Formar profesionales en filosofía y ciencias humanas con inspiración cristiana del hombre y el mundo, mediante la docencia, la investigación y la proyección social con enfoque integral y multidisciplinar[32].

5.3.4.2. Visión

Al año 2019, será reconocida ante la comunidad académica y empresarial por su pensamiento estructurado en Filosofía y ciencias humanas con programas de pregrado y posgrado de alta calidad con prestigio internacional[33].

5.3.5. **Organigrama Institucional**

En este organigrama se representan los cargos hasta nivel profesional que dependen directamente de los directivos de la Universidad: Rector, Vicerrectores, secretario del Consejo Fundacional, Secretario General, Decanos y Directores de Unidades Académicas de Carácter Especial, y Directores de Unidades Administrativas.

---

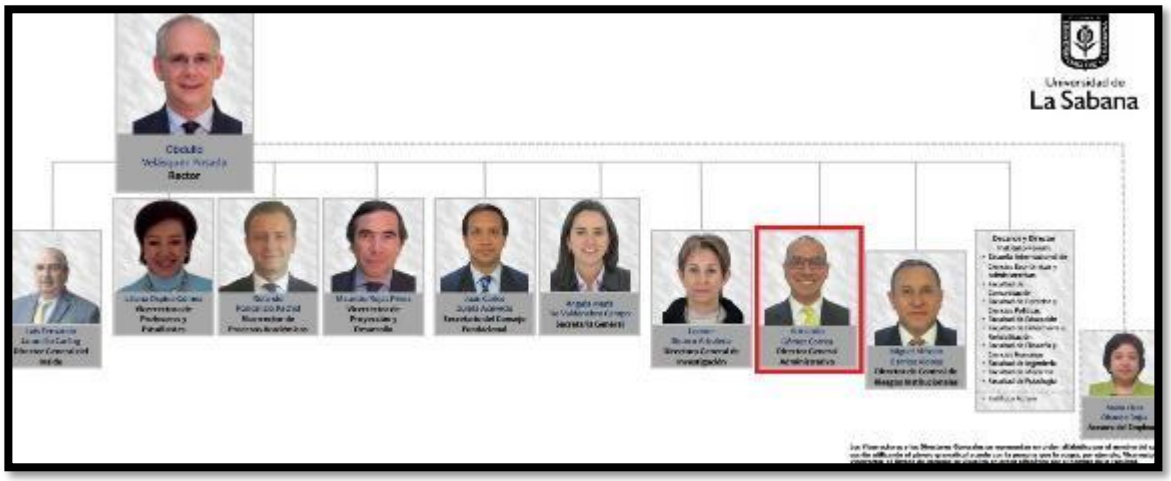
[30] UNIVERSIDAD DE LA SABANA – Nuestra historia [En línea] 1ª ed. [11 – Febrero -2018]. Disponible en internet: https://www.unisabana.edu.co/nosotros/nosotros/historia/

[31] UNIVERSIDAD DE LA SABANA. [En línea] 1ª ed. [11 – Febrero -2018]. Disponible en internet: https://www.unisabana.edu.co/programas/carreras/facultad-de-filosofia-y-ciencias-humanas/filosofia/mision-y-vision/

[32] UNIVERSIDAD DE LA SABANA. [En línea] 1ª ed. [11 – Febrero -2018]. Disponible en internet: https://www.unisabana.edu.co/programas/carreras/facultad-de-filosofia-y-ciencias-humanas/filosofia/mision-y-vision/

[33] UNIVERSIDAD DE LA SABANA. [En línea] 1ª ed. [11 – Febrero -2018]. Disponible en internet: https://www.unisabana.edu.co/programas/carreras/facultad-de-filosofia-y-ciencias-humanas/filosofia/mision-y-vision/

Figura. 4 Organigrama General



Fuente: www.unisabana.edu.co

División administrativa:

Figura. 5 División Administrativa

Fuente: www.unisabana.edu.co

División de la Dirección de Sistemas y Tecnologías de Información

Figura. 6 División de la Dirección de Sistemas

Fuente: www.unisabana.edu.co

5.3.6. **Principales Procesos Y Servicios**

A continuación, se mencionan los principales procesos y servicios, que presta la Dirección de Sistemas a las demás dependencias de la organización, así como la recolección de información acerca de las políticas y procedimientos de seguridad informática existentes en la Dirección de Sistemas y Tecnologías de Información, sin embargo, para realizar este proceso de identificación se mencionan los principales procesos del negocio, para lo cual se utiliza el sistema de gestión de calidad con el cual cuenta actualmente la organización, este sistema tiene definidos e identificados los principales procesos del negocio.

La Universidad de la Sabana cuenta con un sistema de gestión de calidad, cobijado bajo la norma ISO 9001:2008 para los procesos de apoyo a la academia, El SGC es consistente con la misión institucional, está alineado con la Acreditación Institucional, promueve una adecuada gestión por procesos y aporta al eficiente uso de los recursos de la Universidad. Además, está alineado con el Plan Estratégico

Institucional y los Planes de Desarrollo de las unidades académicas y administrativas[34].

El SGC obtuvo la primera certificación bajo la norma ISO 9001:2008 por parte de Bureau Veritas Certification, a partir del 5 de enero de 2010. Este reconocimiento fue otorgado por un término de 3 años, con visitas anuales de seguimiento por parte del organismo certificador[35].

En diciembre de 2012, Bureau Veritas Certification certificó una vez más que el Sistema de Gestión de la Calidad (SGC) de la Universidad de La Sabana se encontraba acorde con los requerimientos de la norma internacional.

En diciembre de 2014, el SGC recibió la certificación de ampliación de alcance por parte Bureau Veritas Certification, en la cual se incluyó el proceso de Gestión de Infraestructura Física (Aseo de Instalaciones, Mantenimiento de Infraestructura y Gestión de Servicios de la Dirección de Operaciones). La vigencia de la certificación fue otorgada hasta el 4 de enero de 2016[36].

En noviembre de 2015, la Universidad inició un nuevo ciclo de evaluación del SGC con otro organismo certificador, el ICONTEC, el cual certificó al SGC en la norma ISO 9001:2008 a partir del 27 de noviembre de 2015 y hasta el 26 de noviembre de 2018 con visitas anuales de seguimiento[37].

El principal objetivo del sistema de gestión de calidad es establecer la forma en que se gestiona la calidad en los procesos que se encuentran al servicio de la academia y el alcance que está dirigido para la prestación de servicios de apoyo a la académica en los 11 siguientes procesos[38].

- Planeación
- PIAMI – Promoción, inscripción, admisión, matricula e inducción.
- Becas y Financiación

[34] SISTEMA DE GESTIÓN DE LA CALIDAD PARA LA PRESTACIÓN DE SERVICIOS DE APOYO A LA ACADEMIA - Universidad de la Sabana [En línea] 1ª ed. [22 – Enero -2016]. Disponible en internet: https://www.unisabana.edu.co/nosotros/planeacion/sistema-de-gestion-de-calidad/

[35] SISTEMA DE GESTIÓN DE LA CALIDAD PARA LA PRESTACIÓN DE SERVICIOS DE APOYO A LA ACADEMIA - Universidad de la Sabana [En línea] 1ª ed. [22 – Enero -2016]. Disponible en internet: https://www.unisabana.edu.co/nosotros/planeacion/sistema-de-gestion-de-calidad/

[36] SISTEMA DE GESTIÓN DE LA CALIDAD PARA LA PRESTACIÓN DE SERVICIOS DE APOYO A LA ACADEMIA - Universidad de la Sabana [En línea] 1ª ed. [22 – Enero -2016]. Disponible en internet: https://www.unisabana.edu.co/nosotros/planeacion/sistema-de-gestion-de-calidad/

[37] SISTEMA DE GESTIÓN DE LA CALIDAD PARA LA PRESTACIÓN DE SERVICIOS DE APOYO A LA ACADEMIA - Universidad de la Sabana [En línea] 1ª ed. [22 – Enero -2016]. Disponible en internet: https://www.unisabana.edu.co/nosotros/planeacion/sistema-de-gestion-de-calidad/

[38] SISTEMA DE GESTIÓN DE LA CALIDAD PARA LA PRESTACIÓN DE SERVICIOS DE APOYO A LA ACADEMIA - Universidad de la Sabana [En línea] 1ª ed. [22 – Enero -2016]. Disponible en internet: https://www.unisabana.edu.co/nosotros/planeacion/sistema-de-gestion-de-calidad/

- Administración del registro académico
- Administración de la biblioteca
- Gestión de la información
- Gestión para el desarrollo humano
- Administración financiera
- Gestión de compras y contratación
- Gestión de la mejora continua
- Gestión de infraestructura física

En la siguiente figura se muestran los procesos que cubre el SGC[39].

Figura. 7 Sistema de Gestión de la Calidad para la Prestación de Servicios de Apoyo a la Academia

Fuente: www.unisabana.edu.co

[39] SISTEMA DE GESTIÓN DE LA CALIDAD PARA LA PRESTACIÓN DE SERVICIOS DE APOYO A LA ACADEMIA - Universidad de la Sabana [En línea] 1ª ed. [22 – Enero -2016]. Disponible en internet: https://www.unisabana.edu.co/nosotros/planeacion/sistema-de-gestion-de-calidad/

Todos los procesos anteriormente mencionados están soportados por las tecnologías de la información, utilizadas para el normal desarrollo de los mismos, por tal razón se hace necesaria que los activos de seguridad de la información del área de sistemas y tecnología cuente con un sistema de gestión de la seguridad de la información.

Los principales servicios que presta la Dirección de Sistemas y Tecnologías de información para los procesos del SGC y el normal desarrollo de la academia son:

- Sistema de información académica
- Sistema de información administrativa
- Sistema de información financiera
- Sistema de información gestión documental
- Servicios de internet
- Servicios de redes de datos
- Servicios de telefonía
- Servicios de correo electrónico
- Servicios de escritorios virtuales
- Servicios de soporte tecnológico

5.3.7. **Análisis Diferencial**

Para realizar el proceso de planificación del sistema de gestión de la seguridad de la información, se hace necesario conocer el estado actual de la Dirección de Sistemas, con respecto al seguimiento de las mejores prácticas. Conocer dicha información ayudara a la identificación del cumplimiento de la normativa.

Se toma como base documentación brindada por la Dirección de Sistemas tomada de un análisis para la implementación de un sistema de gestión de seguridad de la información realizada en el año 2014.

Reglamentación 056 políticas de seguridad de la información.

5.4. **MARCO LEGAL**

La implementación de un sistema de seguridad de la información requiere al interior de una organización, sin lugar a dudas que se tengan en cuenta una serie de normas, leyes y reglamentos que puedan brindar seguridad de la información a la que se tiene acceso, por lo que se hace referencia en este

documento a la 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.[40]

Hace un especial énfasis al capítulo uno en el cual se expresa la importancia de la protección de los datos y la información, De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos[41].

A continuación, se citan textualmente algunos de los artículos que se consideran de mayor relevancia en el desarrollo de este proyecto[42].

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes[43].

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes[44].

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos

[40] LEY 1273 DE 2009 NIVEL NACIONAL [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[41] LEY 1273 DE 2009 NIVEL NACIONAL [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[42] LEY 1273 DE 2009 NIVEL NACIONAL [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[43] LEY 1273 DE 2009 NIVEL NACIONAL [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[44] LEY 1273 DE 2009 NIVEL NACIONAL [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

legales mensuales vigentes[45].

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave[46].

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave[47].

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito[48].

Estas leyes de una forma u otra buscan complementar el concepto que actualmente se tiene de seguridad, así como también se encuentran normas obligatorias de cumplimiento, tales como la ley estatutaria 1581 de 2012, relacionada con la protección de datos personales[49] y la ley de acceso electrónico de los ciudadanos a los servicios públicos[50], también pueden intervenir regulaciones sectoriales que pueden afectar diferentes ámbitos dentro de la organización.

[45] LEY 1273 DE 2009 NIVEL NACIONAL [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[46] LEY 1273 DE 2009 NIVEL NACIONAL [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[47] LEY 1273 DE 2009 NIVEL NACIONAL [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[48] LEY 1273 DE 2009 NIVEL Nacional [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[49] LEY ESTATUTARIA 1581 DE 2012. [En línea] 1ª ed. [17 – Octubre -2012]. Disponible en internet: Diario Oficial 48587 de octubre 18 de 2012. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

[50] RESUMEN DE LA LEY DE SERVICIOS PÚBLICOS ELECTRÓNICOS. [En línea] 1ª ed. [1-Junio- 2007]. Disponible en internet: www.notariosyregistradores.com https://www.notariosyregistradores.com/doctrina/resumenes/servicios-publicos-electronicos.htm

6. DISEÑO METODOLÓGICO

6.1. OBJETO DE ESTUDIO

La investigación pude ser definida, de acuerdo con el investigador Francisco Abranza, la profundización científica y metódica hacia lo desconocido en orden de prever información para la resolución de problemas, de este modo lo más importante de la investigación es que busca la solución de un problema y esto se aplica a las investigaciones aplicada y pura que pueden intervenir al interior de un proyecto que plantea algún caso de estudio.

Teniendo en cuenta lo anterior, se indica que el presente proyecto se guía a través del objetivo de estudio de la investigación aplicada, ya que puede tomar decisiones para la correcta aplicación del proyecto, de a la manera que se dé solución al problema identificado,

6.2. FUENTE DE INFORMACIÓN

La información que se encuentra actualmente en su gran mayoría es información de carácter documental, por lo cual se basa principalmente en una investigación de tipo documental, sin embargo, no se puede descartar el hecho de realizar algunas validaciones de campo.

La fuente documental aquí mencionada hace referencia a los diferentes documentos habilitadas por parte de la Dirección de Sistemas para dar inicio y gestión al desarrollo de la evaluación del estado actual de la unidad, entre las cuales se encuentra documentación de carácter publico como la historia de la organización, misión, visión, objetivos entre otras, e información de carácter privada, como acceso al organigrama institucional, política de seguridad de la información, informes y repositorios de carácter institucional.

6.3. MEDICIÓN Y ANÁLISIS DE LA INFORMACIÓN

Para el desarrollo de este trabajo se utilizarán cuestionarios para el análisis de la información, entrevistas y la observación de los diferentes elementos, funciones y personal encargado, esta información puede ser visualizada en los

resultados de este proyecto, principalmente en los anexos los cuales resumen este primer segmento de análisis y medición de la información, de la misma manera se utilizarán fuentes documentales y de información tales como textos, artículos, revistas, medios físicos y magnéticos etc, estos a su vez se han referenciado y citado a lo largo del desarrollo del proyecto.

Se tendrán en cuenta los métodos de investigación cualitativos y cuantitativos, ya que se requiere realizar obtener resultados claros mediante la ayuda de mediciones objetivas y reales de la información, pero a su vez la descripción de datos, identificación de los procesos y profundización en algunos puntos cuando de esta manera se requiera.

6.4. **TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN**

Las técnicas de investigación para tener en cuenta de acuerdo con el tipo de proyecto seleccionado corresponden a entrevistas, sondeo de opinión ya que se requiere el uso de diferentes tipos de recolección de información, observación y análisis de documentos de información. Esta información será analizada y plasmada al interior de los anexos de este proyecto, la documentación adicional usada se encuentra publicada en la pagina principal de la Universidad de la Sabana y en la intranet correspondiente a información privada y usada exclusivamente en las secciones requeridas para el correcto desarrollo del análisis y la gestión de los riesgos de la Dirección de Sistemas.

6.5. **METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS**

Un sistema de gestión de la seguridad de la información en los requisitos de planificación y soporte requiere que se tenga en cuenta una metodología para el análisis y la gestión de los riesgos para apoyar las decisiones de valoración y tratamiento de los riesgos de la seguridad de la información.

Esta metodología debe ser utilizada por la organización y revisada por los menos una vez en el año, con el objetivo de valorar las nuevas amenazas a las que se pueden ver expuestos los activos de seguridad de la información, para el presente proyecto se plantea el uso de la metodología MAGERIT Versión 3.0 que está desarrollada por el Consejo Superior de Administración Electrónica de España, al consulta los diferentes proyectos relacionados con la planeación de la ISO/IEC 27001:2013 todos utilizan esta metodología.

A continuación, se mencionan cada una de las etapas de la metodología de análisis y gestión de riesgos a seguir.

1. Inventario de activos: Se realiza una clasificación de activos de seguridad de la información, delimitado por el alcance del SGSI. Se utilizan los tipos de activos según la clasificación de activos que propone la metodología MAGERIT.
2. Valoración de activos: Se valoran los activos de acuerdo a las escalas definidas, los valores se clasifican de acuerdo al nivel de impacto que estos tienen al interior de la organización.
3. Dimensiones de seguridad: Se realiza la valoración de los activos en las dimensiones de seguridad (disponibilidad, confidencialidad, integridad, autenticidad y trazabilidad), para tal valoración se utilizan las escalas propuestas por MAGERIT.
4. Análisis de amenazas: Se analizan las amenazas a las que están expuestos los activos, considerando los cuatro tipos (desastres naturales, origen industrial, ataques intencionados y ataques no intencionados).
5. Impacto potencial: Se procede a realizar el cálculo del impacto potencial que puede causar la materialización de las amenazas sobre los activos identificados. Para hallar los valores se utiliza la valoración de activos y impactos que pueden causar las amenazas sobre estos.
6. Análisis de riesgos: con la información de todo el cálculo de los riesgos realizado sobre los activos, se procede a realizar un análisis sobre la información y se identifican los riesgos de los activos que tienen mayor valor dentro de la organización. Este análisis sugiere el orden de prioridad para el tratamiento de los riesgos.
7. Definición de niveles de riesgo: Se definen los niveles de riesgo, los cuales debe ser aprobados por la alta dirección, estos niveles servirán para la toma de decisiones en el tratamiento de los riesgos. Los niveles que deben definirse son los de riesgos gestiónales y riesgos aceptables.

6.6. **ANÁLISIS Y GESTIÓN DE RIESGOS EN LA ORGANIZACIÓN**

La Dirección de Sistemas y tecnologías de Información, tiene la necesidad de la detección de oportunidades y amenazas provenientes de su entorno, el cual puede estar afectado por factores internos o externos. Por lo cual es necesario determinar el comportamiento del entorno para la formulación de estrategias gerenciales que permitan su aprovechamiento y en el caso de las amenazas, poder mitigarlas y de este modo reducir al máximo sus repercusiones. Por consiguiente, se hace necesario el uso de que permita compilar la información

para facilitar la competición del comportamiento del entorno y de este modo poder tomar las decisiones adecuadas, la metodología de análisis y la gestión de riesgos contribuye con la identificación de las amenazas que pueden estar afectando al desarrollo de la operación en la organización, por lo que a continuación se realiza el desarrollo de la metodología planteada.

6.6.1. **Inventario De Activos**

El primer paso del análisis de riesgos es la identificación de los activos de la seguridad de la información, el cual a su vez corresponde a uno de los objetivos planteados al interior del desarrollo de este proyecto. Teniendo en cuenta la delimitación planteada al inicio se realiza la identificación de activos para la Dirección de Sistemas y tecnologías de Información que actualmente soporta los 11 procesos del sistema de gestión de calidad que brinda apoyo al normal funcionamiento de la academia.

A continuación, se muestra un extracto general de la identificación de activos, para este se tuvo en cuenta la clasificación de activos sugerida por la metodología de MAGERIT y los activos actualmente administrados por la Dirección de Sistemas y Tecnologías de Información, esta información se relaciona en una tabla final y será suministro para continuar con los siguientes pasos para el análisis de riesgos, el inventario de activos se puede consultar en el anexo A1 denominado inventario de activos.

Tabla 1 Extracto inventario de activos

NOMBRE DEL ACTIVOS	CANTIDAD GENERAL
Aplicaciones Informáticas	16
Arquitectura del sistema	3
Datos	11
Equipamiento auxiliar	6
Equipos informáticos	15
Instalaciones	3
Personas	10
Redes de comunicación	7
Servicios	13
Soportes de información	7
Grand Total	**91**

Fuente: Amanda Medina

Para conocer el documento completo de inventario de activos diríjase al Anexo: A1 – Inventario De Activos

Tabla 2 Identificación de activos informáticos

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Arquitectura del sistema	[ARCH]	[SAP]	Puntos de acceso al servicio definidas por la organización las cuales recaen sobre terceros.	Director de sistemas y tecnologías

Fuente: Amanda Medina

Para conocer todo el contenido tenga en cuenta consultar el ANEXO: A1 – Inventario De Activos.

6.6.2. **Dimensiones de valoración**

Una vez identificados los tipos de activos se hace necesario tener las dimensiones de valoración, las cuales se refieren a las características o atributos que hacen valioso un activo. Una dimensión corresponde a una faceta o aspecto de un activo independientemente de otras facetas.

Las dimensiones se requieren para realizar la valoración del activo y de este modo para valorar las consecuencias de la materialización de una amenaza.

A continuación, se hace referencia al tipo de dimensión, posteriormente se anexa el documento denominado como dimensiones de valoración, en el que se encuentran las categorías de los activos según MAGERIT, las vulnerabilidades, amenazas de seguridad encontrados en la Dirección de Sistemas y Tecnologías de Información.

- Disponibilidad: es una propiedad o característica de los activos consiste en que las entidades y los procesos que se encuentren autorizados tienen acceso a estos siempre que se requiera.

- Integridad de los datos: es una característica del activo de información significa que dicho activo no ha sido alterado de manera no autorizada.
- Confidencialidad de la información: es una propiedad de la información indicando que esta no se pone a disposición, tampoco se revela o divulga a individuos o proceso no autorizados.
- Autenticidad: consiste en que la entidad es quien dice o garantiza la fuente de la que proceden los datos.
  Trazabilidad: es la que permite identificar la actuación de la entidad teniendo en cuenta que puede ser imputada exclusivamente a dicha entidad.

Tabla 3 Dimensión de valoración

Tipo de Amenaza [N.1] Fuego	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar [L] Instalaciones	**Dimensiones:** [D] Disponibilidad [I] Integridad de los datos
Descripción: Incendios: posibilidad de que el fuego acabe con activos informáticos de la organización. Explosiones: probabilidad de que las estructuras colapsen y se genere daños materiales y perdida de información.	

Fuente: Amanda Medina

- En el ANEXO: A2 – Dimensión de valoración, se puede visualizar con mayor claridad la clasificación de las dimensiones según su criticidad.
- Para conocer todo el contenido tenga en cuenta consultar ANEXO: A2 – Dimensión de valoración

6.6.3. **Valoración de activos**

Criterios de valoración:

Es necesario valorar los activos y teniendo en cuenta la metodología que se está implementando, se hace necesario tener en cuenta, el uso de la escala común, logarítmica y homogénea para cada una de las dimensiones anteriormente expuestas.

Se seleccionó la escala determinada por MAGERIT en la cual se brindan 10 valores, seleccionando el valor 0 como determinante de lo que sería un valor despreciable y 10 como estreno o grave, para una mayor especificación véase la tabla 4.

Tabla 4 Criterios de Valoración

Criterios de Valoración		
Valor		**Criterio**
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
8	Alto	Daño grave
7	Alto	Daño grave
6	Alto	Daño grave
5	Medio	Daño importante
4	Medio	Daño importante
3	Medio	Daño importante
2	Bajo	Daño menor
1	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: Amanda Medina

En la tabla número 6 valoración de activos, se muestra un extracto de la tabla final de la valoración de los activos de seguridad de la información, a su vez muestra las respectivas dimensiones de seguridad, esta valoración se realizó según las tablas propuestas en la metodología MAGERIT, libro número 2, la

tabla numero 6 completa puede ser consultada en el ANEXO: A3 – Valoración de activos.

Tabla 5 Valoración de activos cantidades

Cuenta de VALOR	Etiquetas de columna					
Etiquetas de fila	Autenticidad	Confiabilidad	Disponibilidad	Integridad	Trazabilidad	Total general
Daño extremadamente grave	8	23	38	14	2	85
Daño grave	32	27	16	32	24	131
Daño importante	11	10	7	7	29	64
Daño menor	3	2	1	6	24	36
Daño muy grave	28	23	26	28	2	107
Irrelevante a efectos prácticos	7	4	1	2	8	22
Total general	**89**	**89**	**89**	**89**	**89**	**445**

Fuente: Amanda Medina

Tabla 6 Valoración de activos

TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
[ARCH]Arquitectura del sistema	[SAP]	7	7	1	9	9
[ARCH]Arquitectura del sistema	[IP]	3	6	5	7	1
[ARCH]Arquitectura del sistema	[EXT]	9	7	7	4	3

Fuente: Amanda Medina

Para conocer todo el contenido tenga en cuenta consultar ANEXO: A3 – Valoración de activos

6.6.4. **Identificación y Análisis de amenazas**

Para realizar el análisis de las amenazas sobre los activos anteriormente identificados fue necesario realizar el siguiente procedimiento.

Teniendo en cuenta la cantidad de amenazas a las que se pueden ver expuestos los diferentes tipos de activos, se realiza una tabla que facilita la verificación de los tipos de activos y las amenazas que los afectan.

Las amenazas son todos aquellos factores externos que de alguna manera pueden causar daños en los activos de información o también hace referencia a personas que aprovechan las vulnerabilidades de seguridad que pueden estar expuestas y que existen para cometer ataques a los sistemas o a los activos de información que actualmente tiene la organización.

En el libro número 2 de la metodología MAGERIT se detalla cada uno se los factores externos de amenaza y su respectiva clasificación, por medio del cual se realiza la identificación y análisis a continuación presentado. La evaluación de las amenazas se realiza teniendo en cuenta la frecuencia o probabilidad de materialización de las amenazas, en cada uno de los activos de información existentes, la valoración del impacto en cada una de las dimensiones de seguridad según la metodología MAGERIT. La escala que se muestra en la tabla 7 a continuación se puede visualizar la probabilidad de amenaza,

Tabla 7 Escala de rango de Probabilidad de amenazas

TABLA DE PROBABILIDAD		
Valor	**Rango**	**Vulnerabilidad**
5	1 vez al día	Probabilidad muy alta
4	1 vez cada semana	Probabilidad alta
3	1 vez cada 2 meses	Probabilidad media
2	1 vez cada 6 meses	Probabilidad baja
1	1 vez al año	Probabilidad muy baja

Fuente: Amanda Medina

Tabla 8 Dimensiones de seguridad - MAGERIT

DIMENSIÓN DE SEGURIDAD	
TABLA DE CONVERSIONES	
Disponibilidad	[D]
Integridad	[I]
Confiabilidad	[C]
Autenticidad	[A]
Trazabilidad	[T]

Fuente: Amanda Medina

En la tabla 9 se muestra un extracto de las amenazas identificadas, también se muestra el impacto o afectación que pueda causar cada amenaza en su respectiva dimensión de seguridad, teniendo en cuenta que este procedimiento se ha realizado para cada uno de los activos de información, determinando su probabilidad o frecuencia y el impacto que tiene en cada una de las dimensiones de seguridad.

Tabla 9 Relación de amenazas por activo identificando su frecuencia e impacto

Relación de amenazas por activo identificando su frecuencia e impacto								
Grupo	**Amenaza**	**Activo**	**Probabilidad**	[D]	[I]	[C]	[A]	[T]
[N] Desastres naturales	[N.1] Fuego	[HW] equipos informáticos.	1 vez al año	9	5	7	6	4
		[Media] soportes de información.	1 vez al año	9	8	10	9	6
		[AUX] equipamento auxiliar.	1 vez al año	9	9	9	7	2

		[L] instalaciones.	1 vez al año	9	9	10	4	2
	[N.2] Daños por agua	[HW] equipos informáticos.	1 vez al año	9	6	7	6	4
		[Media] soportes de información.	1 vez al año	9	9	10	9	6
		[AUX] equipamento auxiliar.	1 vez al año	9	9	9	7	2
		[L] instalaciones.	1 vez al año	9	9	10	4	2
	[N.*] Desastre natural	[HW] equipos informáticos.	1 vez cada 2 meses	9	6	7	6	4
		[Media] soportes de información.	1 vez cada 2 meses	9	9	10	9	6
		[AUX] equipamento auxiliar.	1 vez cada 2 meses	9	9	9	7	2
		[L] instalaciones.	1 vez al año	9	9	10	4	2

Fuente: Amanda Medina

Para conocer todo el contenido de la tabla 9 tenga en cuenta consultar ANEXO: A4 - Análisis - identificación de amenazas

6.6.5. **Análisis de riesgo**

- Estimación del riesgo

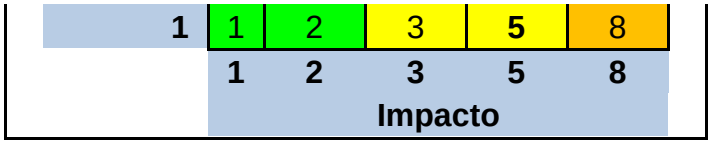
Este valor se obtiene como resultado de la siguiente formula:

Riesgo (R)= Probabilidad (F) x Impacto

El valor **NR** (Nivel de Riesgo) obedece al Mapa de Riesgos:

Tabla 10 Mapa de riesgo

Riesgo = Probabilidad * Impacto						
Probabilidad	5	5	10	15	25	40
	4	4	8	12	20	32
	3	3	6	9	15	24
	2	2	4	6	10	16



Fuente: Amanda Medina

La tabla 12 corresponde a la valoración que se tiene de acuerdo con los colores y elementos mostrados en la tabla 11 anterior.

Tabla 11 Nivel de Riesgo

4	Extremo
3	Intolerable
2	Tolerable
1	Aceptable

Fuente: Amanda Medina

En la tabla 13 se muestra un extracto de los resultados obtenidos en la matriz de análisis de riesgos informáticos.

Tabla 12 Matriz de análisis de riesgos informáticos

Matriz de análisis de riesgos informáticos															
Grupo	**Amenaza**	**Activo**	IMPACTO					**P**	RIESGOS				
			[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
[_] Desastres naturales		[HW] equipos informáticos.	9	5	7	5	3	1	9	5	7	5	3
	[N.1] Fuego	[Media] soportes de información.	9	8	9	9	6	1	9	8	9	9	6
		[AUX] equipamento auxiliar.	9	9	9	7	2	1	9	9	9	7	2
		[L] instalaciones.	9	9	10	4	2	1	9	9	10	4	2
	[N.2] Daños por agua	[HW] equipos informáticos.	9	6	7	6	4	1	9	6	7	6	4
		[Media] soportes de información.	9	9	10	9	6	1	9	9	10	9	6
		[AUX] equipamento auxiliar.	9	9	9	7	2	1	9	9	9	7	2
		[L] instalaciones.	9	9	10	4	2	1	9	9	10	4	2
	[N.*] Desastre natural	[HW] equipos informáticos.	9	6	7	6	4	3	27	18	21	18	12
		[Media] soportes de información.	9	9	10	9	6	3	27	27	30	27	18
		[AUX] equipamento auxiliar.	9	9	9	7	2	3	27	27	27	21	6
		[L] instalaciones.	9	9	10	4	2	1	9	9	10	4	2

Matriz de análisis de riesgos informáticos											
Grupo	**Amenaza**	**Activo**	IMPACTO					**P**	RIESGO		
			[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]

Fuente: Amanda Medina

Para conocer todo el contenido de la tabla 13 tenga en cuenta consultar ANEXO: A5- Análisis - Riesgos

6.6.6. **Salvaguardas**

Salvaguardas, contramedidas o controles de seguridad:

Los controles de seguridad o salvaguardas denominados como los procedimientos o mecanismos tecnológicos que se encargan de reducir en gran medida los riesgos, en los cuales se deben establecer controles para cada amenaza de cada activo que se ha identificado con anterioridad.

Por lo tanto, se tiene que las salvaguardas son medidas, procedimientos o mecanismos tecnológicos que reducen el riesgo al que se encuentra expuesto la organización.

Algunas de las amenazas identificadas se solucionan al interior de la empresa con organización, otras requieren elementos técnicos entiéndase estos como programas o equipos, otras por su parte requieren seguridad física y finalmente enquisten otras que requieren políticas orientadas a las personas en particular.

Se hace indispensable la identificación de las salvaguardas existentes que tengan los activos, sistemas de información, para determinar su nivel de eficiencia y de esta manera proponer nuevas salvaguardas, eliminarlas o simplemente mantener las que actualmente se encuentran cumpliendo con los respectivos estándares o criterios de seguridad.

Una vez que se ha realizado el inventario de activos, la identificación de las amenazas y las vulnerabilidades se procede a la estimación de los riesgos mediante el análisis de los mismos, finalmente se definen las salvaguardas que no son más que procedimientos tecnológicos que reducen el riesgo, de acuerdo a los activos que se van a proteger, en este caso se han tenido en cuenta las salvaguardas definidas en el libro número 3 de MAGERIT.

Extracto del documento final de Salvaguardas, para consultar el documento completo ir al ANEXSO: A6 – Salvaguardas - Matriz de Controles_27002

Tabla 13 Salvaguardas

#	Política	#	Dominio de Control	Objetivos de Control	#	Titulo Control	Descripción del Control	APLICABILIDAD SI / NO		Evidencia Solicitada	Área Responsable Secundaria	Responsable	Revisión de la Evidencia	Obs.	Calificación	Comentarios Adicionales
5.0	Políticas de Seguridad de la Información	A.5.1	Directrices de la Dirección en seguridad de la información	Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes.	A.5.1.1	Políticas para la seguridad de la información	La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.	**X**		Reglamento No. 056 – política de seguridad de la información	Jefatura de infraestructura	Área de seguridad y telecomunicaciones	Conforme a lo requerido en la guía de implementación de la norma GTC-ISO/IEC 27002 …	D	**Definido**	

Fuente: Amanda Medina

Como se puede visualizar en la muestra anterior, se realizó un estudio inicial respecto al nivel de maduración de los procesos ajustados a los dominios y a los controles, para realizar una evaluación del estado actual de los procesos y de este modo brindar una calificación para cada uno de los controles.

Para realizar la anterior evaluación se tuvo en cuenta el diseño de un análisis de brechas o análisis GAP, respecto a las Políticas Globales de Seguridad. En base a entrevistas, observaciones y revisión de la documentación, los cuales se encuentra resumidos en la revisión de controles que se visualizan en el anexo A6 – Salvaguardas - Matriz de Controles_27002, al que se refiere la tabla 14, se asigna una puntuación a cada uno de los controles como se plantea en la norma (controles/ISO 27002_2013 - 113 Controles).

Para este proceso se tiene la siguiente escala de maduración:

Figura. 8 Escala de Madurez referencia

Escala de Madurez según marco de refencia CobIT 4.1	
Puntuación	**Descripción**
0	Se carece totalmente de un proceso. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
1	Existe evidencia que la empresa ha reconocido la necesidad del proceso. No existe un proceso formal – estandarizado si no que existe enfoques ad-hoc que se aplican de manera individual o caso a caso. La gestión del mismo es desorganizada. La implementación de un control depende de cada individuo y es principalmente reactiva.
2	El proceso se encuentra suficientemente desarrollado y distintas personas ejecutan más o menos los mismos procedimientos. No existe una comunicación ni entrenamiento formal de los procedimientos, y la responsabilidad es individual. Existe una gran dependencia del conocimiento que tiene los individuos y, por tanto existe una probabilidad de error importante.
3	El proceso está estandarizado, documentado y difundido mediante entrenamiento. Sin embargo, se deja a voluntad de los individuos la aplicación de los procedimientos del proceso y es poco probable que se detecten las desviaciones en su uso. Los procedimientos en sí no son sofisticados y corresponden a la formalización de las prácticas existentes.
4	Es posible monitorear y medir la conformidad en la aplicación de los procedimientos del proceso y es posible tomar acciones cuando el proceso no está operando adecuadamente. Los procesos están mejorándose continuamente. Se dispone de automatizaciones y de herramientas que son usadas de una manera limitada o fragmentada.
5	El proceso ha sido refinado al nivel de las mejores prácticas, basado en los resultados del mejoramiento continuo y de los modelos ya maduros de otras compañías. Las TI son usadas integralmente para automatizar workflow, entregando herramientas que mejoran la calidad y efectividad, aumentando la capacidad de adaptación de la empresa.

Autor: https://msaffirio.wordpress.com

Se tiene en cuenta la siguiente escala de calificación teniendo en cuenta la puntuación que se puede asignar en conformidad con os porcentajes que pueden tener cada uno y la escala de madurez anteriormente identificada:

Figura. 9 Calificaciones

Calificación - Modelo Genérico de Madurez			
Puntuación	**Porcentaje de cumplimiento**	**Descripción**	**Color**
N/A	No aplica	No aplica	N/A
0	**Inexistente** (0% de cumplimiento)	Universidad De La Sabana no cuenta con los elementos necesarios para cumplir con lo requerido por el control.	0
1	**Inicial** (entre 0% y 20% de cumplimiento)	Universidad De La Sabana cuenta con elementos, no obstantes, éstos no alcanzan para cumplir con los requerimientos del control.	1
2	**Repetible** (entre 20% y 40% de cumplimiento)	Universidad De La Sabana cuenta con elementos y responsables para el cumplimiento de los requerimientos mas se depende del conocimiento de individuos para su ejecución.	2
3	**Definido** (entre 40% y 70% de cumplimiento)	Universidad De La Sabana cuenta con elementos, responsables y capacitación para el cumplimiento de los requerimientos, no obstante, no se hace seguimiento a su ejecución.	3
4	**Gestionado** (entre 70 y 90% de cumplimiento)	Universidad De La Sabana cuenta con los elementos necesarios para cumplir con los requerimientos del control. Éstos se encuentran en mejora continua.	4
5	**Optimizado** (entre 90% y 100% de cumplimiento)	Universidad De La Sabana cuenta con los elementos necesarios acorde a las mejores prácticas para cumplir con los requerimientos del control.	5

Autor: https://msaffirio.wordpress.com

Con forme a los datos anteriores, los resultados del análisis expuesto muestra una matriz de valoración nivel de madurez y cumplimiento, para cada uno de los dominios.

Tabla 14 porcentajes / Dominios / Cumplimiento

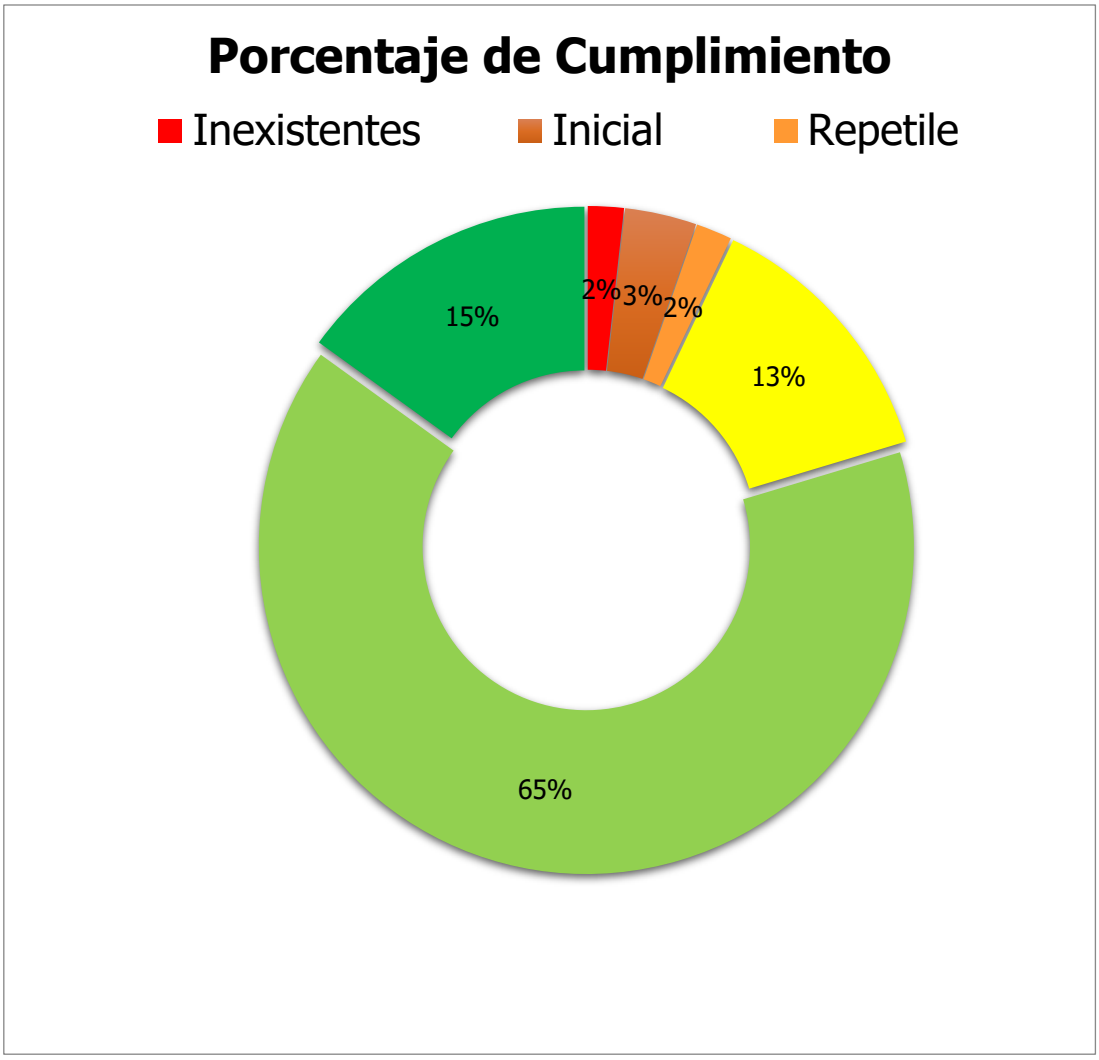
Dominio	Controles 27002 2013	Inexistentes 0%	Inicial 20%	Repetile 40%	Definido 70%	Gestionado 90%	Optimizado 100%	% Cumplimiento
Políticas de Seguridad de la Información	2	0	1	0	1	0	0	45%
Organización de Seguridad de la Información	7	0	1	0	1	3	2	80%
Gestión de Activos de la Información	10	0	1	0	4	3	2	77%
Seguridad en los Recursos Humanos	6	0	1	0	0	3	2	82%
Seguridad Física y Medio Ambiental	15	1	0	1	2	9	2	79%
Operaciones de Seguridad	14	0	0	0	2	12	0	87%
Control de acceso (lógico)	13	1	0	0	1	7	4	85%
Adquisición, desarrollo y mantenimiento de sistemas de información	13	0	0	0	2	10	1	88%
Gestión de incidentes de seguridad de información	7	0	0	0	1	6	0	87%
Gestión de la Continuidad de Negocio	4	0	0	0	0	4	0	90%
Cumplimiento Regulatorio	8	0	0	1	0	6	1	85%
Seguridad en relación con los proveedores	5	0	0	0	0	3	2	94%
Seguridad en las Comunicaciones	7	0	0	0	1	5	1	89%

Criptografía	2	0	0	0	0	2	0	90%
Total Controles	**113**	2	4	2	15	73	17	

Fuente: Amanda Medina.

La tabla 15 muestra un resumen del estado actual de cada uno de los dominios implementados al interior de la Dirección de Sistemas de la Universidad de la Sabana, esto en cuanto a madurez y cumplimiento, cada uno de los estados tiene un nivel de porcentual, que sumados brindan un valor de cumplimiento y de este modo es posible evidenciar el estado actual de la dirección y los puntos trabajables, así como los puntos que pueden requerir de una mayor prioridad teniendo en cuenta la matriz de riesgos y vulnerabilidades.

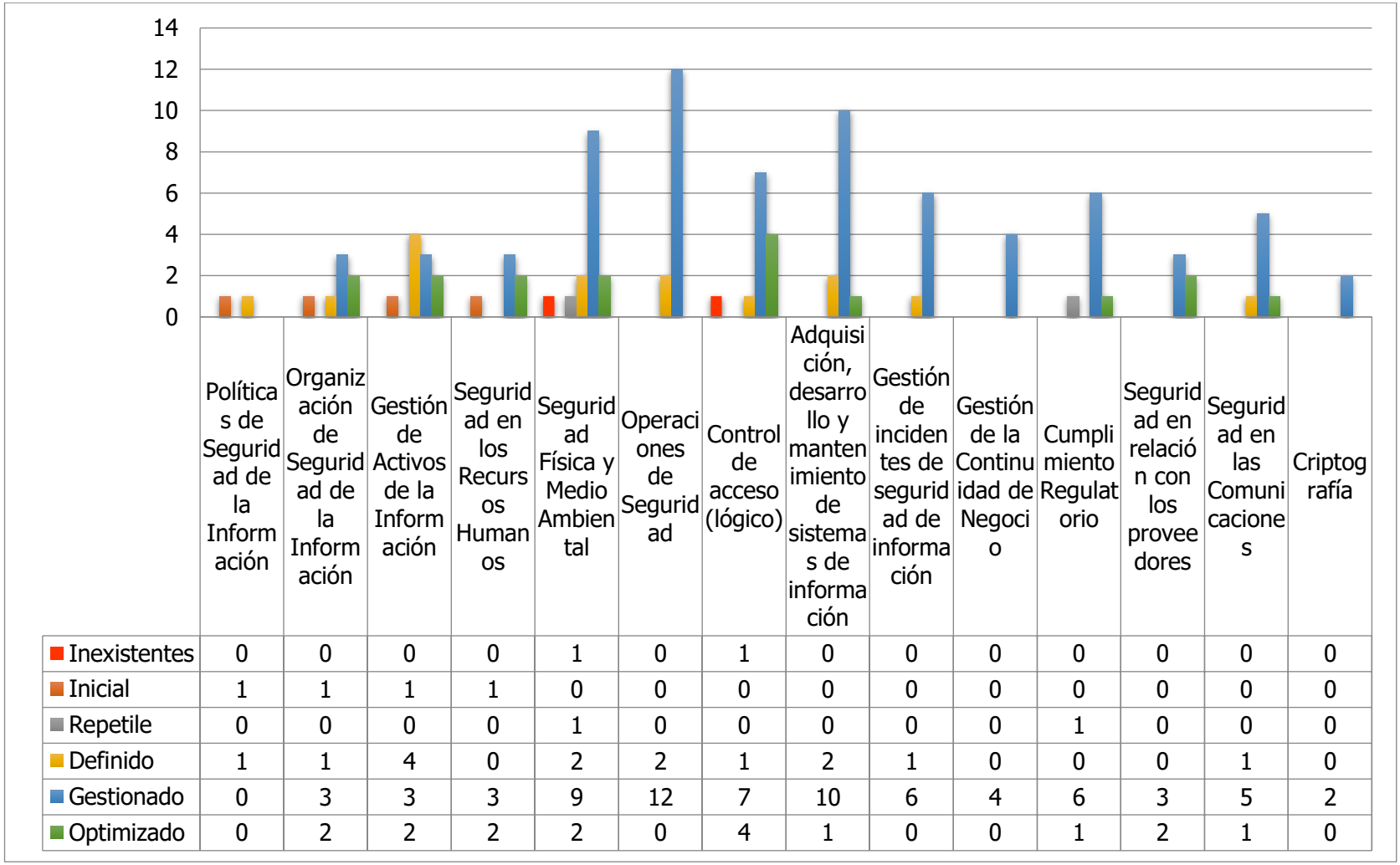
Figura. 10 Porcentaje de cumplimiento



Fuente: Amanda Medina

En la figura 11 es posible apreciar de manera gráfica la escala porcentual de cumplimiento que actualmente tiene la Dirección de Sistemas en cuanto a cada uno de los dominios.

Figura. 11 Tabla de barras controles



	Políticas de Seguridad de la Información	Organización de Seguridad de la Información	Gestión de Activos de la Información	Seguridad en los Recursos Humanos	Seguridad Física y Medio Ambiental	Operaciones de Seguridad	Control de acceso (lógico)	Adquisición, desarrollo y mantenimiento de sistemas de información	Gestión de incidentes de seguridad de información	Gestión de la Continuidad de Negocio	Cumplimiento Regulatorio	Seguridad en relación con los proveedores	Seguridad en las Comunicaciones	Criptografía
Inexistentes	0	0	0	0	1	0	1	0	0	0	0	0	0	0
Inicial	1	1	1	1	0	0	0	0	0	0	0	0	0	0
Repetile	0	0	0	0	1	0	0	0	0	0	1	0	0	0
Definido	1	1	4	0	2	2	1	2	1	0	0	0	1	0
Gestionado	0	3	3	3	9	12	7	10	6	4	6	3	5	2
Optimizado	0	2	2	2	2	0	4	1	0	0	1	2	1	0

Fuente: Amanda Medina

La figura 12 muestra de manera más específica las cantidades que se tienen por cada una de las calificaciones asignadas para cada dominio.

Figura. 12 Nivel de maduración

Fuente: Amanda Medina

En la anterior grafica número 13 se puede observar el nivel de madurez por cada uno de los dominós.

Para mayor especificación visualizar ANEXO A6– Salvaguardas - Matriz de Controles 27002 Y Nivel de madurez asociado por dominio

Tabla 15 Matriz de Controles

#	Política	#	Dominio de Control	Objetivos de Control	#	Titulo Control	Descripción del Control	APLICABILIDAD SI / NO		Evidencia Solicitada	Área Responsable Secundaria	Responsable	Revisión de la Evidencia	Obs.	Calificación
A.5.- Políticas de Seguridad de la Información															
5.0	Políticas de Seguridad de la Información	A.5.1	Directrices de la Dirección en seguridad de la información	Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos	A.5.1.1	Políticas para la seguridad de la información	La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los emplea	**X**		Reglamento No. 056 – política de seguridad de la información	Jefatura de infraestructura	Área de seguridad y telecomunicaciones	Conforme a lo requerido en la guía de implementación de la norma GTC-ISO/IEC 27002, actualmente la organización	D	**Definido**

				comerciales y leyes y regulaciones relevantes.			dos y entidades externas relevantes.						cuenta con una política de seguridad de la información avalada por la comisión de asuntos generales del consejo superior, según acta No.1504 de 2015, por lo anterior esta política ha sido avalada por el consejo superior, es esta se		

													establece el enfoque de la universidad para la gestión y objetivos de la seguridad de la información.		
5.0	Políticas de Seguridad de la Información	A.5.1	Directrices de la Dirección en seguridad de la información	Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerci	A.5.1.2	Revisión de las Políticas para la Seguridad de la Información	La política de seguridad de la información debe ser revisada regularmente a intervalos planea	**X**		Comité de seguridad, solicitud de actas, validación de seguimientos	Jefatura de infraestructura	Área de seguridad y telecomunicaciones	Actualmente no se tiene un comité de seguridad de la información y no se realiza una verificación periódica de las políticas, sin	PNP	**Inicial**

				ales y leyes y regulaciones relevantes.			dos o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.						embargo, todos los cambios en cuanto a seguridad deben pasar por un comité de cambios que actualmente tiene la dirección de sistemas, en el cual se realiza evaluación del impacto.		

Fuente: Amanda Medina

6.6.7. **Diseño de políticas y controles**

Las políticas y controles que se diseñaron tienen como objetivo principal mitigar los riesgos identificados bajo los dominios y que actualmente tienen un nivel de cumplimiento que se encuentre comprendido en un 0% a 40%, los cuales representan un mayor riesgo para la organización, por lo que se deben evaluar y diseñar metodologías que permitan mitigar en gran medida las vulnerabilidades identificadas y generar un mayor cumplimiento del dominio especificado.

1. **Política: A.5.- Políticas de Seguridad de la Información: Revisión de las Políticas para la Seguridad de la Información.**

    1.1. Política: Políticas de Seguridad de la Información

    SOA: A 5.1 Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes.

    1.2. Integración de controles a la política
    Política con controles: Directrices de la Dirección en seguridad de la información, teniendo en cuenta que actualmente no se tiene un comité de seguridad de la información y no se realiza una verificación periódica de las políticas, se debe realizar la implementación de una directriz por parte de la Dirección de Sistemas, en el cual se efectué la creación de un comité de seguridad de la información y se realice una verificación periódica de las políticas de seguridad.

    1.3. Procedimiento para la creación de un comité de seguridad de la información:

    A. Establecer integrantes del comité de seguridad informativa, es importante que el comité se encuentre integrado por representantes de todas las áreas sustantivas de la organización, destinados a garantizar el apoyo manifiesto de las autoridades a las diferentes iniciativas de seguridad.
    B. El comité debe estar en la capacidad de revisar y proponer a los órganos de gobierno para su consideración y posterior aprobación, las políticas de seguridad de la información y demás requerimientos o cambios que requieran ser aprobados por un ente que el comité considere deben ser aprobadas por un ente superior.
    C. El comité deberá está en la capacidad de monitorear cambios considerados como significativos en los riesgos que afectan los

recursos y disponibilidad de la información, frente a posibles amenazas sean estas internas o externas.

D. El comité deberá realizar seguimiento periódico de las incidencias de seguridad presentados, para su gestión, revisión y análisis.
E. El comité deberá establecer un alcance que le permita realizar gestión sobre la aprobación de las principales iniciativas sobre procesos y metodologías, para incrementar la seguridad de la información, teniendo en cuenta las competencias y responsabilidades adquiridas.
F. El comité deberá promover la difusión y apoyo de las temáticas relacionadas con seguridad de la información al interior de la Dirección de Sistemas y posteriormente de la universidad.

2. **Política: A.6.- Organización de Seguridad de la Información: relación con los dispositivos móviles y el teletrabajo (Trabajo Remoto)**

2.1. Política: Organización de Seguridad de la Información

SOA: A 6.2 Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles

2.2. Integración de controles a la política
Política con controles: Se debe desarrollar e implementar una política, y procedimientos y planes operaciones de actividades de trabajo remoto.

2.3. Procedimiento para realizar análisis los controles y políticas requeridos para la implementación del proyecto planteado:

A. Se debe garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles que se definan al interior de la organización.
B. Se debe documentar e implementar procedimientos que contengan estándares de niveles de seguridad, para proteger la información a la que se tiene acceso, que puede ser procesada o almacenada en los diferentes lugares en los que se vean relacionados al teletrabajo.

3. **Política: A.7.- Seguridad en los Recursos Humanos**:

3.1. Política: Seguridad en los Recursos Humanos

SOA: A 7.2 Asegurar que los empleados, contratistas y usuarios de terceras partes sean conscientes de las amenazas y de las preocupaciones de la seguridad de la información, de sus responsabilidades y obligaciones, y estén preparados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y para reducir el riesgo de errores humanos

3.2. Integración de controles a la política
Política con controles: Todos los empleados de la organización y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.

3.3. Procedimiento para realizar análisis los controles y políticas requeridos para la implementación del proyecto planteado:

De acuerdo con OCTAVE Allegro, se puede evaluar un riesgo en los siguientes 8 pasos:

A. Desarrollar un perfil de activos de información
B. Identificar contenidos de activos de información
C. Identificar áreas de preocupación
D. Identificar esa nación de amenaza
E. Identificar riesgos
F. Analizar riesgos
G. Seleccionar un enfoque de mitigación
H. Asegurar que los colaboradores entiendan cada una de las responsabilidades que les son asignadas y que deben ser idóneos para el desempeño de sus funciones u obligaciones que se hayan tenido en su contratación.

4. Política: A.8.- Gestión de Activos de la Información:

4.1. Política: Gestión de Activos de la Información

SOA: A 8.3 Prevenir o evitar la divulgación no autorizada, modificación, borrado o destrucción de los activos e interrupción de las actividades del negocio.

4.2. Integración de controles a la política

Política con controles: Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.

4.3. Procedimiento para realizar análisis los controles y políticas requeridos para la implementación del proyecto planteado:

A. Es necesario que se realice un inventario de activos de información, el cual deberá estar alineado a los diferentes requisitos legales y regulatorios que tenga la organización, en el que se deben tener registrados los propietarios, los responsables y clasificación de cada activo.
B. Realizar procedimientos para el correcto etiquetado de la información, teniendo en cuenta la clasificación de información que tenga adoptada la dirección.
C. Documentar e implementar criterios para que los diferentes colaboradores realicen devolución de todos los activos que sean de propiedad de la Dirección de Sistemas, al finalizar los contratos, acuerdo o retiro de la entidad, de tener estos procesos se deben llevar estadísticas y realizar seguimiento del cumplimiento de los mismos.
D. Disponer en forma segura de los medios de almacenamientos de información cuando ya no se requieran, llevando procedimientos formales para cada cambio que se realice.

5. Política: A.9.- Control de acceso (lógico):

5.1. Política: Control de acceso (lógico)

SOA: A 9.2 Asegurar el acceso autorizado a los usuarios e impedir el acceso no autorizado a sistemas de información.

5.2. Integración de controles a la política
Política con controles: La dirección debe establecer un proceso formal de revisión periódica de los derechos de acceso de los usuarios.

5.3. Procedimiento para realizar análisis los controles y políticas requeridos para la implementación del proyecto planteado:

A. Limitar el acceso a información y a instalaciones de manejo de información, siempre que el funcionario no debe tener acceso a dicha información, se debe tener especial atención a los accesos

a privilegiados, implementando un procedimiento formal del registro, ajuste, cancelación y revisión periódica de accesos.

B. Implementar mecanismos adecuados de autenticación del usuario a los diferentes sistemas de información, teniendo en cuenta si el usuario se encuentra activo o inactivo, que en tal caso se deberán definir los alcance para la eliminación de los permisos actuales de los usuarios en el caso en el que el usuario se encuentre inactivo.

6. Política: A.11.- Seguridad Física y Medio Ambiental:

6.1. Política: Seguridad Física y Medio Ambiental

SOA: A 11.2 Prevenir pérdida, hurto o el compromiso de los activos, así como la interrupción de las actividades de la organización.

6.2. Integración de controles a la política
Política con controles: El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad o integridad.

6.3. Procedimiento para realizar análisis los controles y políticas requeridos para la implementación del proyecto planteado:

A. Proteger mediante controles de acceso apropiados para segura que solo se permita el acceso a personal autorizado a la información haciendo uso de mecanismos de seguridad apropiados que aseguren la permanente disponibilidad y cuidado en la integridad de la información.
B. Aplicar protección física contra desastres naturales, ataques maliciosos o accidentes para evitar daños a causa de incendios, inundaciones, terremotos, explicaciones, disturbios civiles y otras formas de desastres naturales a los cuales se pueda encontrar expuesta la información.
C. Tomar acciones para la perdida, daño, robo o compromiso de activos de información y la interrupción de las operaciones de la dirección.
D. Los equipos de información deberán estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las posibilidades de acceso no autorizado, protegidos adecuadamente contra fallos de energía y demás interrupciones que puedan ser

causadas por el suministro de energía, los servicios deben estar protegidos contra la interrupción, interferencia o daño.

E. Se debe implementar la cultura de bloqueo de los equipos de cómputo cuando estén desatendidos, cerrar las sesiones de las aplicaciones o servicios de red cuando ya no se necesiten, adoptar la política de escritorio limpio de papeles y medios de almacenamiento removibles y tener la pantalla del computador despejada, libre de archivos o accesos directos a los programas, esto teniendo en cuenta las políticas que actualmente tenga la dirección.

7. Política: A.11.- Seguridad Física y Medio Ambiental:

7.1. Política: Seguridad Física y Medio Ambiental

SOA: A 11.2 Prevenir pérdida, hurto o el compromiso de los activos, así como la interrupción de las actividades de la organización.

7.2. Integración de controles a la política
Política con controles: Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.

7.3. Procedimiento para realizar análisis los controles y políticas requeridos para la implementación del proyecto planteado:

A. Proteger mediante controles de acceso apropiados para segura que solo se permita el acceso a personal autorizado a la información haciendo uso de mecanismos de seguridad apropiados que aseguren la permanente disponibilidad y cuidado en la integridad de la información.
B. Aplicar protección física contra desastres naturales, ataques maliciosos o accidentes para evitar daños a causa de incendios, inundaciones, terremotos, explicaciones, disturbios civiles y otras formas de desastres naturales a los cuales se pueda encontrar expuesta la información.
C. Tomar acciones para la perdida, daño, robo o compromiso de activos de información y la interrupción de las operaciones de la dirección.
D. Los equipos de información deberán estar ubicados y protegidos para reducir los riesgos de amenazas, peligros del entorno y las

posibilidades de acceso no autorizado, protegidos adecuadamente contra fallos de energía y demás interrupciones que puedan ser causadas por el suministro de energía, los servicios deben estar protegidos contra la interrupción, interferencia o daño.

E. Se debe implementar la cultura de bloqueo de los equipos de cómputo cuando estén desatendidos, cerrar las sesiones de las aplicaciones o servicios de red cuando ya no se necesiten, adoptar la política de escritorio limpio de papeles y medios de almacenamiento removibles y tener la pantalla del computador despejada, libre de archivos o accesos directos a los programas, esto teniendo en cuenta las políticas que actualmente tenga la dirección.

8. Política: A.18.- Cumplimiento Regulatorio:

8.1. Política: Cumplimiento Regulatorio

SOA: A 18.2 Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de los requisitos de seguridad.

8.2. Integración de controles a la política
Política con controles: Se deben utilizar controles criptográficos que cumplan con todos los acuerdos, leyes y regulaciones pertinentes.

8.3. Procedimiento para realizar análisis los controles y políticas requeridos para la implementación del proyecto planteado:

A. Garantizar el cumplimiento adecuado de las obligaciones legales, regulatorias o contractuales que se encuentren relacionadas con la seguridad de la información y de cualquier otro requisito de seguridad que relacionado y que deba ser aplicado.
B. Implementar elementos constantes de privacidad, protección y tratamiento de la información.
C. El incumplimiento a la política de seguridad y privacidad de la información aplicada por la Dirección de Sistemas debe tener consecuencias legales según sea definido por la normativa expuesta por la universidad.
D. Es necesario que los criterios, acuerdos, leyes y regulaciones se encuentren socializados entre las partes interesadas de los controles, todos los procesos deberán ser documentados y

especificados con forme a lo que se disponga, es necesario que estos procesos sean revisados almenas una vez al año.

7. **RECURSOS DISPONIBLES (Materiales, Financieros, Institucionales).**

Tabla 16 Recursos Disponibles

RECURSO	DESCRIPCIÓN	PRESUPUESTO
1. Equipo Humano	Gestor del proyecto: Luz Amanda Medina Rincón Personal de la Dirección de Sistemas	$ 6,000,000,000
1. Equipo Humano	Consultoría	
2. Equipos y Software	Se utilizarán herramientas Gratuitas para la evaluación de los riesgos, de ser requeridas.	$ -
3. Viajes y Salidas de Campo	N/A	$ -
4. Materiales y suministros	Equipo de cómputo, Fuentes documentales los cuales contengan la información requerida para el desarrollo de la investigación, esta información puede ser física o magnética.	$ 3,000,000,000
TOTAL:		$ 9,000,000,000

Fuente: autor

RECOMENDACIONES

El profesional en seguridad de la información no se debe limitar a las herramientas y normativas presentadas al interior del presente proyecto aplicado, se sugiere realizar un análisis completo de cada una de las normas que permiten el diseño análisis e implementación de un SGSI, ya que el campo que enmarca un sistema de gestión de seguridad de la información es muy grande y es necesario entender, que requiere de un estudio a profundidad para que se pueda de este modo cubrir a profundidad cada una de las fases que lo componen.

A consideración de que el presente proyecto se enmarco al diseño de un sistema de seguridad de la información para la Dirección de Sistemas de la Universidad de la Sabana, se recomienda tener en cuenta la identificación y valoración de activos realizada, ya que corresponden a dos puntos clave para el análisis de amenazas y el análisis de riesgos elaborados, dado el procedimiento anterior se realizó un planteamiento de las posibles acciones que se consideran pertinentes para la gestión de la seguridad de la información al interior de la organización, generando de esta manera un grupo de controles o salvaguardas que pueden llegar a intervenir en los procesos identificados de una manera positiva, esto debido a todo el análisis realizado durante el desarrollo de la metodología de análisis de riesgos.

CONCLUSIONES

El presente trabajo aplicado busca servir como un insumo base para la Dirección de Sistemas y Tecnologías De Información, de la Universidad de la Sabana, de tal manera que se continúen las actividades que permitan mejorar todos los procesos y procedimientos de la organización, soportados siempre en el manejo de las mejores prácticas de seguridad de la información, que se pueden ver en el desarrollo de la metodología de análisis y gestión de riesgos, implementado en el presente proyecto, basado en las normas ISO/IEC 27001 Y 27002.

La aplicación de la metodología de gestión de riesgos sobre los activos de seguridad de la información, logro categorizar con claridad los principales riesgos a los que está expuesta la Dirección de Sistemas, con la información compilada, se realizó un planteamiento de las posibles acciones que se consideran pertinentes para la correcta gestión, teniendo en cuenta que hacen parte de los principales riesgos encontrados, los cuales pueden llegar a causar grandes pérdidas económicas, jurídicas o de reputación para la organización.

Mediante el análisis de riesgo fue posible generar los controles de seguridad que permiten mitigar los riesgos identificados en la Dirección de Sistemas, para lograr el avance que busca la implementación de las mejores prácticas en seguridad de la información, para que a futuro la dirección pueda llevar a cabo la implementación de un SGSI que abarque a toda la organización.

DIVULGACIÓN

Este documento fue creado con el propósito de efectuar un SGSI para la Dirección de Sistemas de la Universidad de la Sabana, quien en conformidad de las leyes de la republica de Colombia e identificada tributariamente con el NIT 860.070.558, como proyecto aplicado para fines educativos y privados, actualmente este documento no se encuentra autorizado para ser divulgado bajo ninguna circunstancia, es de uso exclusivo para el proceso que aquí se a mencionado, lo anterior teniendo en cuenta que el documento cuenta con información de carácter confidencial relacionados con aspectos internos y de operación, por lo cual se hace necesario proteger la mencionada información confidencial por medio del presente acuerdo de divulgación.

Para el uso de los datos suscritos en el presente proyecto aplicado la Universidad Nacional Abierta y Distancia, a través del representante legal de la universidad deberá solicitar y suscribir un acuerdo de confidencialidad de la información que será determinado por la Universidad de la Sabana a través del representante legal de esta, de así requerirlo, de la misma manera el Jefe de Infraestructura tecnológica de la Universidad de la Sabana puede brindar un aval para el uso de los datos que fueron usados en este documento, el cual ya se encuentra avalado por esta jefatura, para su análisis y diseño, alcance que fue definido en los objetivos de este proyecto, mas no para la publicación o divulgación de esta información, ya que no corresponde a un rol que se encuentre habilitado para desarrollar, en tal caso debería ser avalado por el representante legal de la Universidad de la Sabana.

BIBLIOGRAFÍA

LEY 1273 DE 2009 NIVEL NACIONAL [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. (s.f.).

(ISOTOOLS EXCELLENCE. Blog especializado en Sistemas de Gestión de Seguridad de la Información. ISO 27001: El método MAGERIT 2015 [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: http://www.pmg-ssi.com/2015/03/iso-27001-el-metodo-magerit. (s.f.).

27001 ACADEMY. ¿Qué Es La Norma ISO 27001? [En línea]. 1ª ed. Colombia: ISO 27001 Academia [Citado 17 – Noviembre - 2017] Disponible en internet: https://advisera.com/27001academy/es/que-es-iso-27001/. (s.f.).

ANÁLISIS DE INFORMACIÓN SOBRE RIESGOS. [En línea] 1ª ed. [15 – noviembre - 2017]. Disponible en internet: https://www.cepal.org/publicaciones/xml/8/33658/ColombiaCapII.pdf. (s.f.).

DELOITTE CYBER RISK & INFORMATION SECURITY STUDY – Latinoamérica. Para más información contacte a Deloitte & Touche SRL 2016. [En línea]. 1ª ed., [Citado 17 – Noviembre - 2017] Disponible en internet: https://www2.deloitte.com/content/dam/Deloitte/pe/Docu. (s.f.).

DINERO. El 2015 fue un año de “altas y bajas” para la seguridad informática. Colombia – Bogotá 2016. [En línea]. 1ª ed. [Citado 20– Noviembre - 2017 Disponible en internet: http://www.dinero.com/pais/articulo/informe-certicamara-sobre-seguridad-informati. (s.f.).

EL ESPECTADOR. N. Universidades, víctimas de “hackers” | ELESPECTADOR.COM. Retrieved from . [2015] Retrieved from [En línea]. 1ª ed. Colombia – Bogotá: Universidad de la Sabana, [Citado 17 – Noviembre - 2017] Disponible en https://www.elespectador.com/no. (s.f.).

EL PORTAL DE ISO 27001 en español [En línea] 1ª ed. [2012]. Disponible en internet: http://www.iso27000.es/sgsi.html. (s.f.).

EL TIEMPO, N. Rector de la UPB habla sobre escándalo de alteración de notas - Archivo Digital de Noticias de Colombia y el Mundo desde 1.990 - eltiempo.com. [2013] Retrieved from [En línea]. 1ª ed. Colombia – Bogotá: Universidad de la Sabana, [Citado 17 . (s.f.).

GLOBALSTD CERTIFICATION. [En línea] 1ª ed. [20 – Octubre -2014]. Disponible en internet: Estadísticas ISO 2014 http://www.globalstd.com/component/k2/estadisticas-iso-2014. (s.f.).

GONZÁLEZ MARTÍNEZ, J. Elaboración de un plan de implementación de la norma ISO/IEC 27001:2013. [2015] (U. O. de Catalunya & A. Tortajada Gallego, Eds.), En línea]. 1ª ed. Colombia: ISO 27001 Academia [Citado 17 – Noviembre - 2017] Disponible en internet:. (s.f.).

ISO27000 Sistema de Gestión de la Seguridad de la Información [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: http://www.iso27000.es/download/doc_sgsi_all.pdf. (s.f.).

ISOTOOLS EXCELLENCE. Blog especializado en Sistemas de Gestión de Seguridad de la Información. [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: http://www.pmg-ssi.com/2015/07/que-es-sgsi/. (s.f.).

ISOTOOLS. Normas ISO - Sistemas de Gestión Normalizados Colombia. Bogotá 2017 [En línea]. 1ª ed. Colombia – Chía: Universidad de la Sabana, [Citado 17 – Noviembre - 2017 Disponible en internet: https://www.isotools.org/normas/. (s.f.).

Ley 1273 de 2009 Nivel Nacional [En línea] 1ª ed. [5 – Enero de 2009]. Disponible en internet: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492. (s.f.).

LEY ESTATUTARIA 1581 DE 2012. [En línea] 1ª ed. [17 – Octubre -2012]. Disponible en internet: Diario Oficial 48587 de octubre 18 de 2012. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. (s.f.).

MINTIC. Guía de gestión de riesgos [2017]. [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf. (s.f.).

NORMAS ISO. ISO 27001 Gestión de la Seguridad de la Información. En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: http://www.normas-iso.com/iso-27001. (s.f.).

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS y SYMANTEC. Tendencias De Seguridad Cibernética En América Latina Y El Caribe [En línea] 1ª ed. 2014 [18 – noviembre - 2017]. Disponible en internet: https://www.symantec.com/content/es/mx/enterprise/other_resources/. (s.f.).

RESUMEN DE LA LEY DE SERVICIOS PÚBLICOS ELECTRÓNICOS. [En línea] 1ª ed. [1-Junio- 2007]. Disponible en internet: www.notariosyregistradores.com

https://www.notariosyregistradores.com/doctrina/resumenes/servicios-publicos-electronicos.htm. (s.f.).

SISTEMA DE GESTIÓN DE LA CALIDAD PARA LA PRESTACIÓN DE SERVICIOS DE APOYO A LA ACADEMIA - Universidad de la Sabana [En línea] 1ª ed. [22 – Enero -2016]. Disponible en internet: https://www.unisabana.edu.co/nosotros/planeacion/sistema-de-gestion-de-calidad. (s.f.).

TUTORIAL DE SEGURIDAD INFORMÁTICA. [En línea] 1ª ed. [15 – noviembre -2017]. Disponible en internet: Tutoriales De Seguridad. html http://redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap2.html#14. (s.f.).

UNIVERSIDAD DE LA SABANA – Nuestra historia [En línea] 1ª ed. [11 – Febrero -2018]. Disponible en internet: https://www.unisabana.edu.co/nosotros/nosotros/historia/. (s.f.).

UNIVERSIDAD DE LA SABANA. [En línea] 1ª ed. [11 – Febrero -2018]. Disponible en internet: https://www.unisabana.edu.co/programas/carreras/facultad-de-filosofia-y-ciencias-humanas/filosofia/mision-y-vision/ . (s.f.).

UNIVERSIDAD DE LA SABANA. La Sabana En Sifras. Chía 2017 [En línea]. 1ª ed. Colombia – Chía: Universidad de la Sabana, [Citado 17 – Noviembre - 2017 Disponible en internet: https://www.unisabana.edu.co/nosotros/la-sabana-en-cifras/. (s.f.).

UNIVERSIDAD DE LA SABANA. Proyecto Educativo Institucional. [En línea]. 1ª ed. Colombia – Chía: Universidad de la Sabana, [Citado 17 – Noviembre - 2017] Disponible en internet: https://www.unisabana.edu.co/nosotros/proyecto-educativo-institucional/. (s.f.).

VON, Solms, y VAN Niekerk, J. From information security to cyber security. Cybercrime in the Digital Economy, [En linea]. 1ª ed. 2013., [17 – noviembre -29017]. Disponible en internrt: https://doi.org/http://dx.doi.org.ezproxy.unisabana.edu.co/10.1016/j. (s.f.).

ANEXOS

Anexos 1 - A1 – Inventario de Activos General

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	DESCRIPCIÓN	RESPONSABLE
ARQUIRECTURA DEL SISTEMA	[ARCH]	Elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior.	Director de sistemas y tecnologías
DATOS	[D]	La información es un activo abstracto que será almacenado en equipos o soportes de información.	Director de sistemas y tecnologías
SERVICIOS	[S]	Función que se encarga de satisfacer una necesidad de los usuarios del servicio.	Director de sistemas y tecnologías
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.	Director de sistemas y tecnologías
HARDWARE	[HW]	referida a los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización.	Director de sistemas y tecnologías
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.	Director de sistemas y tecnologías

A1 - Continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	DESCRIPCIÓN	RESPONSABLE
SOPORTE DE INFORMACION	[MEDIA]	Dispositivos físicos que permiten almacenar información de forma permanente o durante un largo periodo de tiempo.	Director de sistemas y tecnologías
EQUIPOS AUXILIARES	[AUX]	Se consideran como otros equipos que sirven de soporte a los sistemas de información.	Director de sistemas y tecnologías
INSTALACIONES	[L]	Lugares en los que se hospedan los sistemas de información y comunicaciones.	Director de sistemas y tecnologías
PERSONAS	[P]	Personal relacionado con los sistemas de información.	Director de sistemas y tecnologías

Anexos 2 A1 – Inventario de Activos Específico

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Arquitectura del sistema	[ARCH]	[SAP]	Puntos de acceso al servicio definidas por la organización las cuales recaen sobre terceros.	Director de sistemas y tecnologías
Arquitectura del sistema	[ARCH]	[IP]	Puntos de interconexión entre diferentes sistemas	Director de sistemas y tecnologías
Arquitectura del sistema	[ARCH]	[EXT]	Servicios que dependen de terceros para su correcto funcionamiento	Director de sistemas y tecnologías
Datos	[D]	[FICHEROS]	Datos almacenados en ficheros	Director de sistemas y tecnologías
Datos	[D]	[BACKUP]	Copias de respaldo de los datos	Director de sistemas y tecnologías
Datos	[D]	[CONF]	Datos necesarios de configuración del sistema	Director de sistemas y tecnologías
Datos	[D]	[INT]	Datos de gestión interna	Director de sistemas y tecnologías
Datos	[D]	[PASSWORD]	Credenciales de acceso	Director de sistemas y tecnologías
Datos	[D]	[AUTH]	Datos de validación de credenciales	Director de sistemas y tecnologías
Datos	[D]	[ACL]	Datos de control de acceso	Director de sistemas y tecnologías

A1 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Datos	[D]	[LOG]	Datos de registro de actividad	Director de sistemas y tecnologías
Datos	[D]	[TEST]	Datos de pruebas	Director de sistemas y tecnologías
Datos	[D]	[LOG]	Registro de actividad	Director de sistemas y tecnologías
Datos	[D]	[TEST]	Datos para el desarrollo de pruebas	Director de sistemas y tecnologías
Servicios	[S]	[ANON]	Servicio que no requiere autenticación del usuario	Director de sistemas y tecnologías
Servicios	[S]	[PUB]	Dirigidos al público en general y que no requieren tener una relación contractual	Director de sistemas y tecnologías
Servicios	[S]	[INT]	Internos a personal autorizado dentro de la organización	Director de sistemas y tecnologías
Servicios	[S]	[WWW]	Servicio de navegación a través de internet	Director de sistemas y tecnologías
Servicios	[S]	[TELNET]	Acceso remoto a servicios que se encuentran en la intranet	Director de sistemas y tecnologías
Servicios	[S]	[EMAIL]	Acceso al correo electrónico	Director de sistemas y tecnologías

A1 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Servicios	[S]	[FILE]	Servicio de almacenamiento de ficheros	Director de sistemas y tecnologías
Servicios	[S]	[FTP]	Transferencia de ficheros	Director de sistemas y tecnologías
Servicios	[S]	[EDI]	Intercambio electrónico de datos	Director de sistemas y tecnologías
Servicios	[S]	[DIR]	Acceso a directorios de información	Director de sistemas y tecnologías
Servicios	[S]	[IDM]	Permiten altas y bajas de usuarios de los sistemas teniendo en cuenta su estado contractual	Director de sistemas y tecnologías
Servicios	[S]	[IPM]	Gestión de servicios de acuerdo con los privilegios otorgados	Director de sistemas y tecnologías
Servicios	[S]	[PKI]	Servicio de infraestructura de claves públicas, relacionada con los certificados y marca de agua	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[PRP]	Desarrollos propios que se han realizado al interior de la organización	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[STD]	Estándar	Director de sistemas y tecnologías

A1 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Aplicaciones Informáticas	[SW]	[BROWSER]	Configurados diferentes navegadores para el desarrollo de tareas operativas	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[WWW]	Servidor de presentación	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[APP]	Servidor de aplicaciones	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[EMAIL_CLIENT]	Cliente de correo electrónico, vinculado a todas las cuentas institucionales	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[EMAIL_SERVER]	Actualmente el servidor de correo electrónico esta manejado por office365	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[FILE]	Servidor de ficheros	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[DBMS]	Acceso a los sistemas de gestión de bases de datos como SQLDEVELOPER.	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[TM]	Monitor transaccional	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[OFFICE]	Programas ofimáticos tales como el paquete de office.	Director de sistemas y tecnologías

A1 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Aplicaciones Informáticas	[SW]	[AV]	Programa antivirus encargado de proteger los equipos y brindar conexiones remotas a los mismos	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[OS]	Sistema operativo	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[HYPERVISOR]	Citrix es actualmente el gestor de máquinas virtuales que maneja la organización	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[TS]	Servidor de terminales	Director de sistemas y tecnologías
Aplicaciones Informáticas	[SW]	[BACKUP]	Sistema de backup	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[HOST]	Maquinas físicas usadas como servidores	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[PC]	Equipos signados a las funcionarias al interior de la Dirección	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[MOBILE]	Equipos portátiles, celulares y demás equipos transportables	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[VHOST]	Maquinas Thin Client distribuidas en la organización	Director de sistemas y tecnologías

A1 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Equipos informáticos	[HW]	[BACKUP]	Equipos físicos en los que se puede almacenar el respaldo de la información	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[PERIPHERAL]	Periféricos	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[PRINT]	Impresoras asignadas	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[SCAN]	Escáner	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[NETWORK]	Soporte de la red cableada e inalámbrica en los diferentes puntos de acceso	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[HUB]	Elementos concentradores	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[SWITCH]	Conmutadores muy necesarios en la distribución de la red	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[ROUTER]	Encaminadores de red	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[FIREWALL]	Cortafuegos para brindar seguridad en los servicios que se brinda en la organización	Director de sistemas y tecnologías

A1 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Equipos informáticos	[HW]	[WAP]	Puntos de acceso a la red inalámbrica	Director de sistemas y tecnologías
Equipos informáticos	[HW]	[IPPHONE]	Teléfonos de vos IP, actualmente instalados en diferentes puntos con el software de Avaya	Director de sistemas y tecnologías
Redes de comunicación	[COM]	[PSTN]	Red de acceso telefónica	Director de sistemas y tecnologías
Redes de comunicación	[COM]	[ISDN]	Red digital, integra voz y datos en la misma línea	Director de sistemas y tecnologías
Redes de comunicación	[COM]	[X25]	Red de datos	Director de sistemas y tecnologías
Redes de comunicación	[COM]	[ADSL]	Acceso a Internet de banda ancha	Director de sistemas y tecnologías
Redes de comunicación	[COM]	[WIFI]	Red de acceso inalámbrico	Director de sistemas y tecnologías
Redes de comunicación	[COM]	[LAN]	Red local	Director de sistemas y tecnologías
Redes de comunicación	[COM]	[INTERNET]	Acceso a internet	Director de sistemas y tecnologías
Soportes de información	[MEDIA]	[DISK]	Discos para el almacenamiento de copias de información	Director de sistemas y tecnologías

A1 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Soportes de información	[MEDIA]	[VDISK]	Discos de almacenamiento virtual	Director de sistemas y tecnologías
Soportes de información	[MEDIA]	[SAN]	Almacenamiento de información en red	Director de sistemas y tecnologías
Soportes de información	[MEDIA]	[DVD]	Almacenamiento de algunos datos en DVD	Director de sistemas y tecnologías
Soportes de información	[MEDIA]	[USB]	Información almacenada y necesaria portable	Director de sistemas y tecnologías
Soportes de información	[MEDIA]	[MC]	Targetas de memoria	Director de sistemas y tecnologías
Soportes de información	[MEDIA]	[PRINTED]	Documentos físicos tales como actas	Director de sistemas y tecnologías
Equipamiento auxiliar	[AUX]	[UPS]	1 UPS de alimentación eléctrica para el rack de comunicaciones y servidor de sistema de alarmas comunitarias	Director de sistemas y tecnologías
Equipamiento auxiliar	[AUX]	[POWER]	Planta de energía eléctrica para el datacenter y algunos puntos específicos	Director de sistemas y tecnologías
Equipamiento auxiliar	[AUX]	[GEN]	Generadores eléctricos	Director de sistemas y tecnologías
Equipamiento auxiliar	[AUX]	[AC]	Ventiladores ubicados en algunos puntos requeridos	Director de sistemas y tecnologías

A1 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Equipamiento auxiliar	[AUX]	[CABLING]	Distribuido según corresponda en cada punto al interior de la organización	Director de sistemas y tecnologías
Equipamiento auxiliar	[AUX]	[FURNITURE]	Casilleros para el almacenamiento de algunos elementos de soporte	Director de sistemas y tecnologías
Instalaciones	[L]	[SITE]	Oficinas de la dirección de sistemas y demas apoyos	Director de sistemas y tecnologías
Instalaciones	[L]	[LOCAL]	Ubicación - cuarto data cebter	Director de sistemas y tecnologías
Instalaciones	[L]	[SHELTER]	Bodega	Director de sistemas y tecnologías
Personas	[P]	[UE]	Usurarios externos	Director de sistemas y tecnologías
Personas	[P]	[UI]	Usurarios internos	Director de sistemas y tecnologías
Personas	[P]	[OP]	Operadores del servicio	Director de sistemas y tecnologías
Personas	[P]	[ADM]	Equipo de admin	Director de sistemas y tecnologías
Personas	[P]	[COM]	Administradores de comunicaciones	Director de sistemas y tecnologías
Personas	[P]	[DBA]	Administradores de BBDD	Director de sistemas y tecnologías

A1 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	DESCRIPCIÓN	RESPONSABLE
Personas	[P]	[SEC]	Administradores de seguridad	Director de sistemas y tecnologías
Personas	[P]	[DES]	Desarrolladores / programadores	Director de sistemas y tecnologías
Personas	[P]	[SUB]	Contratistas	Director de sistemas y tecnologías
Personas	[P]	[PROV]	Proveedores	Director de sistemas y tecnologías

Anexos 3 - A2 – Dimensión de valoración

Tipo de Amenaza [N.1] Fuego	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar [L] Instalaciones	**Dimensiones:** [D] Disponibilidad [I] Integridad de los datos
Descripción: Incendios: posibilidad de que el fuego acabe con activos informáticos de la organización. Explosiones: probabilidad de que las estructuras colapsen y se genere daños materiales y perdida de información.	

Tipo de Amenaza [N.2] Daños por agua	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar [L] Instalaciones	**Dimensiones:** [D] Disponibilidad [I] Integridad de los datos
Descripción: inundaciones: posibilidad de que el agua acabe con activos informáticos de la organización, y posibilidad de que los datos almacenados puedan ser dañados.	

A2 – continuación

Tipo de Amenaza [N.*] Desastres naturales	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar [L] Instalaciones	**Dimensiones:** [D] Disponibilidad [I] Integridad de los datos
Descripción: otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras.	

Tipo de Amenaza [I.1] Fuego	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar [L] Instalaciones	**Dimensiones:** [D] Disponibilidad [I] Integridad de los datos
Descripción: Incendios: posibilidad de que el fuego acabe con activos informáticos de la organización. Explosiones: probabilidad de que las estructuras colapsen y se genere daños materiales y perdida de información. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

A2 – continuación

Tipo de Amenaza [I.2] Daños por agua	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar [L] Instalaciones	**Dimensiones:** [D] Disponibilidad [I] Integridad de los datos
Descripción: inundaciones: posibilidad de que el agua acabe con activos informáticos de la organización, y posibilidad de que los datos almacenados puedan ser dañados. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

Tipo de Amenaza [I.*] Desastres industriales	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar [L] Instalaciones	**Dimensiones:** [D] Disponibilidad [I] Integridad de los datos
Descripción: otros desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

A2 – continuación

Tipo de Amenaza [I.3] Contaminación mecánica	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar	**Dimensiones:** [D] Disponibilidad
Descripción: vibraciones, polvo, suciedad. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

Tipo de Amenaza [I.4] Contaminación electromagnética	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar	**Dimensiones:** [D] Disponibilidad
Descripción: interferencias de radio, campos magnéticos, luz ultravioleta. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

A2 – continuación

Tipo de Amenaza [I.5] Avería de origen físico o lógico	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar [SW] aplicaciones (software)	**Dimensiones:** [D] Disponibilidad
Descripción: Se representan a través de fallos en los sistemas o fallos físicos, estos pueden ser de fabrica o presentados por el uso, deterioro y manejo de los servicios. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

Tipo de Amenaza [I.6] Corte del suministro eléctrico	
Tipos de activos: [HW] Equipos informáticos [MEDIA] Soportes de información [AUX] Equipamiento auxiliar	**Dimensiones:** [D] Disponibilidad
Descripción: indisponibilidad del servicio de energía cese de la alimentación a los diferentes activos. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

A2 – continuación

Tipo de Amenaza [I.8] Fallo de servicios de comunicaciones	
Tipos de activos: [COM] redes de comunicaciones	**Dimensiones:** [D] Disponibilidad
Descripción: indisponibilidad por incapacidad para la transmisión de datos de un liga a otro, por cualquier causa. **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

Tipo de Amenaza [I.9] Interrupción de otros servicios y suministros esenciales	
Tipos de activos: [AUX] equipamiento auxiliar	**Dimensiones:** [D] Disponibilidad
Descripción: indisponibilidad de recursos necesarios para la correcta operación de los equipos, se hace referencia papel de impresiona, toner,refrigerantes. Origen: **Entorno** (accidental) Humano (accidental o deliberado)	

A2 – continuación

Tipo de Amenaza [I.10] Degradación de los soportes de almacenamiento de la información	
Tipos de activos: [Media] soportes de información	**Dimenciones:** [D] Disponibilidad
Descripción: como consecuencia del uso a traves del tiempo **Origen:** Entorno (accidental) Humano (accidental o deliberado)	

Tipo de Amenaza [E.1] Errores de los usuarios	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [Media] soportes de información	**Dimenciones:** [I] integridad [C] confidencialidad [D] disponibilidad
Descripción: Mal uso por parte del usuario de los servicios, también pueden ser equivocación por desconocimiento.	

A2 – continuación

Tipo de Amenaza [E.1] Errores de los usuarios	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (software) [Media] soportes de información	**Dimenciones:** [I] integridad [C] confidencialidad [D] disponibilidad
Descripción: Mal uso por parte del usuario de los servicios, también pueden ser equivocación por desconocimiento.	

Tipo de Amenaza [E.3] Errores de monitorización (log)	
Tipos de activos: [D.log] registros de actividad	**Dimenciones:** [I] integridad
Descripción: inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrec tamente fechados, registros **incorrectamente atribuidos**.	

Tipo de Amenaza [E.7] Deficiencias en la organización	
Tipos de activos: [P] personal	**Dimenciones:** [D] disponibilidad
Descripción: Cuando no se tiene claridad sobre la ejecución de los procesos, no se sabe quién hace que en la organización.	

A2 – continuación

Tipo de Amenaza [E.8] Difusión de software dañino	
Tipos de activos: [SW] aplicaciones	**Dimenciones:** [D] disponibilidad [I] integridad [C] confidencialidad
Descripción: Cuando se realiza propagación de un virus sin conocimiento de causa.	

Tipo de Amenaza [E.9] Errores de [re-]encaminamiento	
Tipos de activos: [SW] aplicaciones	**Dimenciones:** [C] confidencialidad
Descripción: Cuando se realiza el envió de información por error a través de una ruta que no está autorizada o no es debida.	

Tipo de Amenaza[E.14] Escapes de información	
Tipos de activos: [S] servicios [SW] aplicaciones [COM] redes de comunicaciones	**Dimenciones:** [C] confidencialidad
Descripción: la información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	

A2 – continuación

Tipo de Amenaza [E.15] Alteración accidental de la información	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones [Media] soportes de información [L] instalaciones	**Dimenciones:** [I] integridad
Descripción: La alteración de la información puede llegar a ser validada sobre datos en general, ya que cuando se encuentra en algún soporte informático se valida a través de amenazas específicas.	

Tipo de Amenaza [E.18] Destrucción de información	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones [Media] soportes de información [L] instalaciones	**Dimenciones:** [D] disponibilidad
Descripción: Descrita como la perdida accidental de la información y puede llegar a ser validada sobre datos en general, ya que cuando se encuentra en algún soporte informático se valida a través de amenazas específicas.	

A2 – continuación

Tipo de Amenaza [E.19] Fugas de información	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones [Media] soportes de información [L] instalaciones [P] personal	**Dimenciones:** [C] confidencialidad
Descripción: La revelación por indiscreción puede ser verbal, no verbal o escrita.	

Tipo de Amenaza [E.21] Errores de mantenimiento / actualización de programas (software)	
Tipos de activos: [SW] aplicaciones	**Dimenciones:** [I] integridad [D] disponibilidad
Descripción: Puede ser error a la hora de ejecutar los procesos de mantenimiento y actualización, como puede ser error al ejecutar actualizaciones enviadas por el fabricante.	

A2 – continuación

Tipo de Amenaza [E.25] Pérdida de equipos	
Tipos de activos: [[HW] equipos informáticos [Media] soportes de información [AUX] equipamiento auxiliar	**Dimenciones:** [I] integridad [C] confidencialidad
Descripción: la pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	

Tipo de Amenaza[A.4] Manipulación de la configuración	
Tipos de activos: [D.log] registros de actividad	**Dimenciones:** [I] integridad [C] confidencialidad [A] disponibilidad
Descripción: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc	

A2 – continuación

Tipo de Amenaza [A.5] Suplantación de la identidad del usuario	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones [COM] redes de comunicaciones	**Dimenciones:** [I] integridad [C] confidencialidad [A] autenticidad
Descripción: Cuando un atacante normalmente externo logra acceder un usuario sin autorización aprovechándose para realizar proceso no autorizados.	

Tipo de Amenaza [A.6] Abuso de privilegios de acceso	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones [HW] equipos informáticos [COM] redes de comunicaciones	**Dimenciones:** [I] integridad [C] confidencialidad [A] disponibilidad
Descripción: Cundo un usuario tiene más permisos de los que debería tener según su cargo y rol, así mismo cuando pese a los permisos asignados realiza tareas abusivas que no le corresponden	

A2 – continuación

Tipo de Amenaza [A.7] Uso no previsto	
Tipos de activos: [S] servicios [SW] aplicaciones (software) [HW] equipos informáticos [COM] redes de comunicaciones [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	**Dimenciones:** [I] integridad [C] confidencialidad [A] disponibilidad
Descripción: utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: juegos, consultas personales en Internet, bases de datos personales, programas personales, almacenamiento de datos personales entre otras.	

Tipo de Amenaza [A.11] Acceso no autorizado	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones [HW] equipos informáticos [COM] redes de comunicaciones [Media] soportes de información [AUX] equipamiento auxiliar [L] instalaciones	**Dimenciones:** [I] integridad [C] confidencialidad
Descripción: Cuando el atacante consigue acceder al sistema de forma no autorizada, aprovechando cualquier falencia para acceder.	

A2 – continuación

Tipo de Amenaza [A.12] Análisis de tráfico	
Tipos de activos: [COM] redes de comunicaciones	**Dimenciones:** [C] confidencialidad
Descripción: El atacante es capaz de extraer información únicamente con realizar un análisis con el contenido de las comunicaciones.	

Tipo de Amenaza [A.14] Interceptación de información	
Tipos de activos: [COM] redes de comunicaciones	**Dimenciones:** [C] confidencialidad
Descripción: El atacante tiene acceso a la información, pero no realiza ninguna modificación a la misma para que esta no se vea afectada.	

A2 – continuación

Tipo de Amenaza [A.15] Modificación deliberada de la información	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios (acceso) [SW] aplicaciones (SW) [COM] comunicaciones [Media] soportes de información [L] instalaciones	**Dimenciones:** [I] Integridad
Descripción: Cuando se realiza alteración de la información de forma intencionada	

Tipo de Amenaza [E.18] Destrucción de información	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones [Media] soportes de información [L] instalaciones	**Dimenciones:** [D] disponibilidad
Descripción: Descrita como la eliminación de forma intencionada de la información con ánimo de obtener beneficios.	

A2 – continuación

Tipo de Amenaza [A.19] Divulgación de información	
Tipos de activos: [D] datos / información [keys] claves criptográficas [S] servicios [SW] aplicaciones (SW) [COM] comunicaciones [Media] soportes de información [L] instalaciones	**Dimenciones:** [C] confidencialidad
Descripción: Descrita como dibulgación de información	

Tipo de Amenaza [A.22] Manipulación de programas	
Tipos de activos: [SW] aplicaciones	**Dimenciones:** [I] integridad [C] confidencialidad [A] disponibilidad
Descripción: Definida como la intención para alterar el funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	

A2 – continuación

Tipo de Amenaza [A.22] Manipulación de programas	
Tipos de activos: [HW] equipos [Media] soportes de información [AUX] equipamiento auxiliar	**Dimenciones:** [C] confidencialidad [A] disponibilidad
Descripción: Definida como la intención para alterar el funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	

Tipo de Amenaza [A.24] Denegación de servicio	
Tipos de activos: [S] servicios [HW] equipos informáticos (hardware) [COM] redes de comunicaciones	**Dimenciones:** [A] disponibilidad
Descripción: Definida como la carencia de recursos para soportar demasiada carga de trabajo	

A2 – continuación

Tipo de Amenaza [A.25] Robo	
Tipos de activos: [HW] equipos informáticos [Media] soportes de información [AUX] equipamiento auxiliar	**Dimenciones:** [C] confidencialidad [A] disponibilidad
Descripción: La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas contratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias.	

Tipo de Amenaza [A.28] Indisponibilidad del personal	
Tipos de activos: [P] personal interno	**Dimenciones:** [A] disponibilidad
Descripción: Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos.	

A2 – continuación

Tipo de Amenaza [A.30] Ingeniería social (picaresca)	
Tipos de activos: [P] personal interno	**Dimenciones:** [A] disponibilidad [C] confidencialidad [I] integridad
Descripción: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	

Anexos 4 - A3 – Valoración de activos

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Arquitectura del sistema	[ARCH]	[SAP]	Disponibilidad	7	Daño grave
			Integridad	7	Daño grave
			Confiabilidad	1	Daño menor
			Autenticidad	9	Daño muy grave
			Trazabilidad	9	Daño muy grave
Arquitectura del sistema	[ARCH]	[IP]	Confiabilidad	5	Daño importante
			Integridad	6	Daño grave
			Autenticidad	7	Daño grave
			Disponibilidad	3	Daño importante
			Trazabilidad	1	Daño menor
Arquitectura del sistema	[ARCH]	[EXT]	Confiabilidad	7	Daño grave
			Integridad	7	Daño grave
			Autenticidad	4	Daño importante
			Disponibilidad	9	Daño muy grave
			Trazabilidad	3	Daño importante
Datos	[D]	[FICHEROS]	Confiabilidad	5	Daño importante
			Integridad	5	Daño importante
			Autenticidad	8	Daño grave
			Disponibilidad	3	Daño importante
			Trazabilidad	3	Daño importante

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Datos	[D]	[BACKUP]	Confiabilidad	8	Daño grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	5	Daño importante
Datos	[D]	[CONF]	Confiabilidad	2	Daño menor
			Integridad	2	Daño menor
			Autenticidad	5	Daño importante
			Disponibilidad	5	Daño importante
			Trazabilidad	1	Daño menor
Datos	[D]	[INT]	Confiabilidad	7	Daño grave
			Integridad	7	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	5	Daño importante
			Trazabilidad	4	Daño importante
Datos	[D]	[PASSWORD]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	7	Daño grave
			Trazabilidad	1	Daño menor

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Datos	[D]	[AUTH]	Confiabilidad	0	Irrelevante a efectos prácticos
			Integridad	1	Daño menor
			Autenticidad	5	Daño importante
			Disponibilidad	5	Daño importante
			Trazabilidad	5	Daño importante
Datos	[D]	[ACL]	Confiabilidad	5	Daño importante
			Integridad	3	Daño importante
			Autenticidad	8	Daño grave
			Disponibilidad	2	Daño menor
			Trazabilidad	0	Irrelevante a efectos prácticos
Datos	[D]	[LOG]	Confiabilidad	7	Daño grave
			Integridad	6	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	3	Daño importante
Datos	[D]	[TEST]	Confiabilidad	7	Daño grave
			Integridad	3	Daño importante
			Autenticidad	3	Daño importante
			Disponibilidad	6	Daño grave
			Trazabilidad	3	Daño importante

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Servicios	[S]	[ANON]	Confiabilidad	0	Irrelevante a efectos prácticos
			Integridad	3	Daño importante
			Autenticidad	0	Irrelevante a efectos prácticos
			Disponibilidad	5	Daño importante
			Trazabilidad	0	Irrelevante a efectos prácticos
Servicios	[S]	[PUB]	Confiabilidad	6	Daño grave
			Integridad	6	Daño grave
			Autenticidad	6	Daño grave
			Disponibilidad	8	Daño grave
			Trazabilidad	3	Daño importante
Servicios	[S]	[INT]	Confiabilidad	9	Daño muy grave
			Integridad	8	Daño grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	6	Daño grave
Servicios	[S]	[WWW]	Confiabilidad	3	Daño importante
			Integridad	6	Daño grave
			Autenticidad	3	Daño importante
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	5	Daño importante

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Servicios	[S]	[TELNET]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	8	Daño grave
			Trazabilidad	8	Daño grave
Servicios	[S]	[EMAIL]	Confiabilidad	9	Daño muy grave
			Integridad	8	Daño grave
			Autenticidad	7	Daño grave
			Disponibilidad	8	Daño grave
			Trazabilidad	5	Daño importante
Servicios	[S]	[FILE]	Confiabilidad	5	Daño importante
			Integridad	6	Daño grave
			Autenticidad	4	Daño importante
			Disponibilidad	5	Daño importante
			Trazabilidad	4	Daño importante
Servicios	[S]	[FTP]	Confiabilidad	4	Daño importante
			Integridad	4	Daño importante
			Autenticidad	4	Daño importante
			Disponibilidad	6	Daño grave
			Trazabilidad	5	Daño importante

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Servicios	[S]	[EDI]	Confiabilidad	5	Daño importante
			Integridad	6	Daño grave
			Autenticidad	5	Daño importante
			Disponibilidad	7	Daño grave
			Trazabilidad	3	Daño importante
Servicios	[S]	[DIR]	Confiabilidad	10	Daño extremadamente grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	7	Daño grave
Servicios	[S]	[IDM]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	10	Daño extremadamente grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	7	Daño grave
Servicios	[S]	[IPM]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	10	Daño extremadamente grave
			Disponibilidad	7	Daño grave
			Trazabilidad	8	Daño grave

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Servicios	[S]	[PKI]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	10	Daño extremadamente grave
			Disponibilidad	8	Daño grave
			Trazabilidad	7	Daño grave
Aplicaciones Informáticas	[SW]	[PRP]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	8	Daño grave
Aplicaciones Informáticas	[SW]	[STD]	Confiabilidad	10	Daño extremadamente grave
			Integridad	9	Daño muy grave
			Autenticidad	10	Daño extremadamente grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	0	Irrelevante a efectos prácticos
Aplicaciones Informáticas	[SW]	[BROWSER]	Confiabilidad	3	Daño importante
			Integridad	0	Irrelevante a efectos prácticos
			Autenticidad	3	Daño importante
			Disponibilidad	7	Daño grave
			Trazabilidad	2	Daño menor

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Aplicaciones Informáticas	[SW]	[WWW]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	8	Daño grave
Aplicaciones Informáticas	[SW]	[APP]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	10	Daño extremadamente grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	7	Daño grave
Aplicaciones Informáticas	[SW]	[EMAIL_CLIENT]	Confiabilidad	6	Daño grave
			Integridad	6	Daño grave
			Autenticidad	1	Daño menor
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	6	Daño grave
Aplicaciones Informáticas	[SW]	[EMAIL_SERVER]	Confiabilidad	8	Daño grave
			Integridad	9	Daño muy grave
			Autenticidad	8	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	7	Daño grave

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Aplicaciones Informáticas	[SW]	[FILE]	Confiabilidad	6	Daño grave
			Integridad	6	Daño grave
			Autenticidad	6	Daño grave
			Disponibilidad	6	Daño grave
			Trazabilidad	6	Daño grave
Aplicaciones Informáticas	[SW]	[DBMS]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	5	Daño importante
Aplicaciones Informáticas	[SW]	[TM]	Confiabilidad	8	Daño grave
			Integridad	9	Daño muy grave
			Autenticidad	8	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	9	Daño muy grave
Aplicaciones Informáticas	[SW]	[OFFICE]	Confiabilidad	8	Daño grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	1	Daño menor

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Aplicaciones Informáticas	[SW]	[AV]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	10	Daño extremadamente grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	10	Daño extremadamente grave
Aplicaciones Informáticas	[SW]	[OS]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	3	Daño importante
Aplicaciones Informáticas	[SW]	[HYPERVISOR]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	4	Daño importante
Aplicaciones Informáticas	[SW]	[TS]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	7	Daño grave

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Aplicaciones Informáticas	[SW]	[BACKUP]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	6	Daño grave
Equipos informáticos	[HW]	[HOST]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	10	Daño extremadamente grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	7	Daño grave
Equipos informáticos	[HW]	[PC]	Confiabilidad	7	Daño grave
			Integridad	7	Daño grave
			Autenticidad	7	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	3	Daño importante
Equipos informáticos	[HW]	[MOBILE]	Confiabilidad	7	Daño grave
			Integridad	7	Daño grave
			Autenticidad	7	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	3	Daño importante

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Equipos informáticos	[HW]	[VHOST]	Confiabilidad	9	Daño muy grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	3	Daño importante
Equipos informáticos	[HW]	[BACKUP]	Confiabilidad	10	Daño extremadamente grave
			Integridad	9	Daño muy grave
			Autenticidad	7	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	7	Daño grave
Equipos informáticos	[HW]	[PERIPHERAL]	Confiabilidad	6	Daño grave
			Integridad	6	Daño grave
			Autenticidad	6	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	4	Daño importante
Equipos informáticos	[HW]	[PRINT]	Confiabilidad	0	Irrelevante a efectos prácticos
			Integridad	1	Daño menor
			Autenticidad	0	Irrelevante a efectos prácticos
			Disponibilidad	6	Daño grave
			Trazabilidad	2	Daño menor

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Equipos informáticos	[HW]	[SCAN]	Confiabilidad	3	Daño importante
			Integridad	1	Daño menor
			Autenticidad	0	Irrelevante a efectos prácticos
			Disponibilidad	7	Daño grave
			Trazabilidad	1	Daño menor
Equipos informáticos	[HW]	[NETWORK]	Confiabilidad	8	Daño grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	1	Daño menor
Equipos informáticos	[HW]	[HUB]	Confiabilidad	8	Daño grave
			Integridad	1	Daño menor
			Autenticidad	0	Irrelevante a efectos prácticos
			Disponibilidad	9	Daño muy grave
			Trazabilidad	1	Daño menor
Equipos informáticos	[HW]	[SWITCH]	Confiabilidad	3	Daño importante
			Integridad	1	Daño menor
			Autenticidad	1	Daño menor
			Disponibilidad	8	Daño grave
			Trazabilidad	1	Daño menor

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Equipos informáticos	[HW]	[ROUTER]	Confiabilidad	7	Daño grave
			Integridad	4	Daño importante
			Autenticidad	3	Daño importante
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	5	Daño importante
Equipos informáticos	[HW]	[FIREWALL]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	10	Daño extremadamente grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	10	Daño extremadamente grave
Equipos informáticos	[HW]	[WAP]	Confiabilidad	9	Daño muy grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	6	Daño grave
Equipos informáticos	[HW]	[IPPHONE]	Confiabilidad	8	Daño grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	5	Daño importante

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Redes de comunicación	[COM]	[PSTN]	Confiabilidad	8	Daño grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	5	Daño importante
Redes de comunicación	[COM]	[ISDN]	Confiabilidad	9	Daño muy grave
			Integridad	7	Daño grave
			Autenticidad	7	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	4	Daño importante
Redes de comunicación	[COM]	[X25]	Confiabilidad	8	Daño grave
			Integridad	5	Daño importante
			Autenticidad	7	Daño grave
			Disponibilidad	8	Daño grave
			Trazabilidad	3	Daño importante
Redes de comunicación	[COM]	[ADSL]	Confiabilidad	8	Daño grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	6	Daño grave

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Redes de comunicación	[COM]	[WIFI]	Confiabilidad	8	Daño grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	6	Daño grave
Redes de comunicación	[COM]	[LAN]	Confiabilidad	9	Daño muy grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	6	Daño grave
Redes de comunicación	[COM]	[INTERNET]	Confiabilidad	8	Daño grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	6	Daño grave
Soportes de información	[MEDIA]	[DISK]	Confiabilidad	10	Daño extremadamente grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	6	Daño grave

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Soportes de información	[MEDIA]	[VDISK]	Confiabilidad	10	Daño extremadamente grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	6	Daño grave
Soportes de información	[MEDIA]	[SAN]	Confiabilidad	10	Daño extremadamente grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	1	Daño menor
Soportes de información	[MEDIA]	[DVD]	Confiabilidad	10	Daño extremadamente grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	1	Daño menor
Soportes de información	[MEDIA]	[USB]	Confiabilidad	10	Daño extremadamente grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	1	Daño menor

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Soportes de información	[MEDIA]	[MC]	Confiabilidad	10	Daño extremadamente grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	1	Daño menor
Soportes de información	[MEDIA]	[PRINTED]	Confiabilidad	8	Daño grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	7	Daño grave
Equipamiento auxiliar	[AUX]	[UPS]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	5	Daño importante
Equipamiento auxiliar	[AUX]	[POWER]	Confiabilidad	8	Daño grave
			Integridad	9	Daño muy grave
			Autenticidad	8	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	2	Daño menor

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Equipamiento auxiliar	[AUX]	[GEN]	Confiabilidad	8	Daño grave
			Integridad	9	Daño muy grave
			Autenticidad	8	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	2	Daño menor
Equipamiento auxiliar	[AUX]	[AC]	Confiabilidad	8	Daño grave
			Integridad	8	Daño grave
			Autenticidad	8	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	2	Daño menor
Equipamiento auxiliar	[AUX]	[CABLING]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	8	Daño grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	1	Daño menor
Equipamiento auxiliar	[AUX]	[FURNITURE]	Confiabilidad	9	Daño muy grave
			Integridad	8	Daño grave
			Autenticidad	0	Irrelevante a efectos prácticos
			Disponibilidad	9	Daño muy grave
			Trazabilidad	0	Irrelevante a efectos prácticos

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Instalaciones	[L]	[SITE]	Confiabilidad	9	Daño muy grave
			Integridad	8	Daño grave
			Autenticidad	0	Irrelevante a efectos prácticos
			Disponibilidad	9	Daño muy grave
			Trazabilidad	0	Irrelevante a efectos prácticos
Instalaciones	[L]	[LOCAL]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	4	Daño importante
Instalaciones	[L]	[SHELTER]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	1	Daño menor
			Disponibilidad	9	Daño muy grave
			Trazabilidad	1	Daño menor

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Personas	[P]	[UE]	Confiabilidad	0	Irrelevante a efectos prácticos
			Integridad	0	Irrelevante a efectos prácticos
			Autenticidad	0	Irrelevante a efectos prácticos
			Disponibilidad	0	Irrelevante a efectos prácticos
			Trazabilidad	0	Irrelevante a efectos prácticos
Personas	[P]	[UI]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	5	Daño importante
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	0	Irrelevante a efectos prácticos
Personas	[P]	[OP]	Confiabilidad	9	Daño muy grave
			Integridad	9	Daño muy grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	9	Daño muy grave
			Trazabilidad	0	Irrelevante a efectos prácticos
Personas	[P]	[ADM]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	1	Daño menor

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Personas	[P]	[COM]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	1	Daño menor
Personas	[P]	[DBA]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	1	Daño menor
Personas	[P]	[SEC]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	1	Daño menor

A3 – continuación

CLASIFICACIÓN DEL ACTIVO	TIPO DE ACTIVO - MAGERIT	NOMBRE DEL ACTIVO - MAGERIT	DIMENSIÓN DE SEGURIDAD	VALOR	CRITERIO
Personas	[P]	[DES]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	1	Daño menor
Personas	[P]	[SUB]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	5	Daño importante
Personas	[P]	[PROV]	Confiabilidad	10	Daño extremadamente grave
			Integridad	10	Daño extremadamente grave
			Autenticidad	9	Daño muy grave
			Disponibilidad	10	Daño extremadamente grave
			Trazabilidad	5	Daño importante

Anexos 5 - A4 – Análisis - identificación de amenazas

Relación de amenazas por activo identificando su frecuencia e impacto									
Grupo	**Amenaza**	**Activo**	**Probabilidad**	[D]	[I]	[C]	[A]	[T]	**Vulnerabilidad**
[N] Desastres naturales	[N.1] Fuego	[HW] equipos informáticos.	1	9	5	7	6	4	Probabilidad muy baja
		[Media] soportes de información.	1	9	8	10	9	6	Probabilidad muy baja
		[AUX] equipamento auxiliar.	1	9	9	9	7	2	Probabilidad muy baja
		[L] instalaciones.	1	9	9	10	4	2	Probabilidad muy baja
	[N.2] Daños por agua	[HW] equipos informáticos.	1	9	6	7	6	4	Probabilidad muy baja
		[Media] soportes de información.	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamento auxiliar.	1	9	9	9	7	2	Probabilidad muy baja
		[L] instalaciones.	1	9	9	10	4	2	Probabilidad muy baja
	[N.*] Desastre natural	[HW] equipos informáticos.	3	9	6	7	6	4	Probabilidad media
		[Media] soportes de información.	3	9	9	10	9	6	Probabilidad media
		[AUX] equipamento auxiliar.	3	9	9	9	7	2	Probabilidad media

		[L] instalaciones.	1	9	9	10	4	2	Probabilidad muy baja

A4 – continuación

Relación de amenazas por activo identificando su frecuencia e impacto									
Grupo	**Amenaza**	**Activo**	**Probabilidad**	**[D]**	**[I]**	**[C]**	**[A]**	**[T]**	**Vulnerabilidad**
[N] Desastres naturales	[N.1] Fuego	[HW] equipos informáticos.	1	9	5	7	6	4	Probabilidad muy baja
		[Media] soportes de información.	1	9	8	10	9	6	Probabilidad muy baja
		[AUX] equipamento auxiliar.	1	9	9	9	7	2	Probabilidad muy baja
		[L] instalaciones.	1	9	9	10	4	2	Probabilidad muy baja
	[N.2] Daños por agua	[HW] equipos informáticos.	1	9	6	7	6	4	Probabilidad muy baja
		[Media] soportes de información.	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamento auxiliar.	1	9	9	9	7	2	Probabilidad muy baja
		[L] instalaciones.	1	9	9	10	4	2	Probabilidad muy baja
	[N.*] Desastre natural	[HW] equipos informáticos.	3	9	6	7	6	4	Probabilidad media
		[Media] soportes de información.	3	9	9	10	9	6	Probabilidad media
		[AUX] equipamento auxiliar.	3	9	9	9	7	2	Probabilidad media

		[L] instalaciones.	1	9	9	10	4	2	Probabilidad muy baja
[I] De origen industrial	[I.1] Fuego	[HW] equipos informáticos.	1	9	6	7	6	4	Probabilidad muy baja
		[Media] soportes de información.	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamento auxiliar.	1	9	9	9	7	2	Probabilidad muy baja
		[L] instalaciones.	1	9	9	10	4	2	Probabilidad muy baja
	[I.2] Daños por agua	[HW] equipos informáticos.	1	9	6	7	6	4	Probabilidad muy baja
		[Media] soportes de información.	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamento auxiliar.	1	9	9	9	7	2	Probabilidad muy baja
		[L] instalaciones.	1	9	9	10	4	2	Probabilidad muy baja
	[I.*] Desastres industriales	[HW] equipos informáticos.	1	9	6	7	6	4	Probabilidad muy baja
		[Media] soportes de información.	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamento auxiliar.	1	9	9	9	7	2	Probabilidad muy baja
		[L] instalaciones.	1	9	9	10	4	2	Probabilidad muy baja
	[I.3] Contaminación mecánica.	[Media] soportes de información.	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamento auxiliar.	1	9	9	9	7	2	Probabilidad muy baja

	[HW] equipos informáticos.	1	9	6	7	6	4	Probabilidad muy baja
[I.4] Contaminación electromagnética.	[Media] soportes de información.	1	9	9	10	9	6	Probabilidad muy baja
	[AUX] equipamento auxiliar.	1	9	9	9	7	2	Probabilidad muy baja
	[HW] equipos informáticos.	1	9	6	7	6	4	Probabilidad muy baja
[I.5] Avería de origen físico o lógico.	[HW] equipos informáticos (hardware)	5	9	6	7	6	4	Probabilidad muy alta
	[Media] soportes de información	3	9	9	10	9	6	Probabilidad media
	[AUX] equipamiento auxiliar	3	9	9	9	7	2	Probabilidad media
	[SW] aplicaciones (software)	5	10	8	8	8	6	Probabilidad muy alta
[I.6] Corte del suministro eléctrico	[HW] equipos informáticos.	3	9	6	7	6	4	Probabilidad media
	[Media] soportes de información (electrónicos)	3	9	9	10	9	6	Probabilidad media
	[AUX] equipamiento auxiliar	3	9	9	9	7	2	Probabilidad media
[I.7] Condiciones inadecuadas de temperatura o humedad	[HW] equipos informáticos (hardware)	1	9	6	7	6	4	Probabilidad muy baja

	[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
	[AUX] equipamiento auxiliar	1	9	9	9	7	2	Probabilidad muy baja
[I.8] Fallo de servicios de comunicaciones	[COM] redes de comunicaciones (red inalámbrica, intranet, internet)	3	9	7	8	8	5	Probabilidad media
[I.9] Interrupción de otros servicios y suministros esenciales	[AUX] equipamiento auxiliar	3	9	9	9	7	2	Probabilidad media
[I.10] Degradación de los soportes de almacenamiento de la información	[Media] soportes de información	2	9	9	10	9	6	Probabilidad baja
[I.11] Emanaciones electromagnéticas	[HW] equipos informáticos (hardware)	1	9	6	7	6	4	Probabilidad muy baja
	[Media] media	1	9	9	10	9	6	Probabilidad muy baja
	[AUX] equipamiento auxiliar	1	9	9	9	7	2	Probabilidad muy baja
	[L] instalaciones	1	9	9	10	4	2	Probabilidad muy baja

A4 – continuación

Grupo	Amenaza	Activo	Probabilidad	[D]	[I]	[C]	[A]	[T]	Vulnerabilidad
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios.	[D] datos / información	4	10	8	8	8	7	Probabilidad alta
		[S] servicios	3	8	7	7	7	5	Probabilidad media
		[SW] aplicaciones (software)	2	10	8	8	8	6	Probabilidad baja
		[Media] soportes de información	3	9	9	10	9	6	Probabilidad media
		[keys] claves criptográficas	1						Probabilidad muy baja
	[E.2] Errores del administrador	[D] datos / información	2	10	8	8	8	7	Probabilidad baja
		[keys] claves criptográficas	1	10	10	10	10	10	Probabilidad muy baja
		[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (software)	1	10	8	8	8	6	Probabilidad muy baja
		[HW] equipos informáticos (hardware)	1	9	6	7	6	4	Probabilidad muy baja
		[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
		[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja

	[E.3] Errores de monitorización (log)	[D.log] registros de actividad	1	10	8	8	8	7	Probabilidad muy baja
	[E.4] Errores de configuración	[D.conf] datos de configuración	2	10	8	8	8	7	Probabilidad baja
	[E.7] Deficiencias en la organización	[P] personal	4						Probabilidad alta
	[E.8] Difusión de software dañino	[SW] aplicaciones (software)	2	10	8	8	8	6	Probabilidad baja
	[E.9] Errores de [re-]encaminamiento	[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones	1	10	8	8	8	6	Probabilidad muy baja
		[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
	[E.10] Errores de secuencia	[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (software)	1	10	8	8	8	6	Probabilidad muy baja
		[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
	[E.15] Alteración accidental de la información	[D] datos / información	3	10	8	8	8	7	Probabilidad media
		[keys] claves criptográficas	1	10	10	10	10	10	Probabilidad muy baja
		[S] servicios	3	8	7	7	7	5	Probabilidad media
		[SW] aplicaciones (SW)	1	10	8	8	8	6	Probabilidad muy baja
		[COM] comunicaciones (tránsito)	1	9	7	8	8	5	Probabilidad muy baja

		[Media] soportes de información	2	9	9	10	9	6	Probabilidad baja
		[L] instalaciones	1	9	9	10	4	2	Probabilidad muy baja
	[E.18] Destrucción de información	[D] datos / información	3	10	8	8	8	7	Probabilidad media
		[keys] claves criptográficas	1	10	10	10	10	10	Probabilidad muy baja
		[S] servicios	2	8	7	7	7	5	Probabilidad baja
		[SW] aplicaciones (SW)	1	10	8	8	8	6	Probabilidad muy baja
		[COM] comunicaciones (tránsito)	1	9	7	8	8	5	Probabilidad muy baja
		[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
		[L] instalaciones	1	9	9	10	4	2	Probabilidad muy baja
	[E.19] Fugas de información	[D] datos / información	1	10	8	8	8	7	Probabilidad muy baja
		[keys] claves criptográficas	1	10	10	10	10	10	Probabilidad muy baja
		[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (SW)	1	10	8	8	8	6	Probabilidad muy baja
		[COM] comunicaciones (tránsito)	1	9	7	8	8	5	Probabilidad muy baja
		[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
		[L] instalaciones	1	9	9	10	4	2	Probabilidad muy baja
		[P] personal (revelación)	2	9	9	9	8	2	Probabilidad baja

	[E.20] Vulnerabilidades de los programas (software)	[SW] aplicaciones (software)	4	10	8	8	8	6	Probabilidad alta
	[E.21] Errores de mantenimiento / actualización de programas (software)	[SW] aplicaciones (software)	2	10	8	8	8	6	Probabilidad baja
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[HW] equipos informáticos (hardware)	2	9	6	7	6	4	Probabilidad baja
		[Media] soportes electrónicos	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamiento auxiliar	3	9	9	9	7	2	Probabilidad media
	[E.24] Caída del sistema por agotamiento de recursos	[S] servicios	2	8	7	7	7	5	Probabilidad baja
		[HW] equipos informáticos (hardware)	1	9	6	7	6	4	Probabilidad muy baja
		[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
	[E.25] Pérdida de equipos-Robo	[HW] equipos informáticos (hardware)	1	9	6	7	6	4	Probabilidad muy baja
		[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamiento auxiliar	1	9	9	9	7	2	Probabilidad muy baja
	[E.28] Indisponibilidad del personal	[P] personal interno	3	9	9	9	8	2	Probabilidad media

A4 – continuación

Relación de amenazas por activo identificando su frecuencia e impacto									
Grupo	**Amenaza**	**Activo**	**Probabilidad**	[D]	[I]	[C]	[A]	[T]	**Vulnerabilidad**
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)	[D.log] registros de actividad	1	10	8	8	8	7	Probabilidad muy baja
	[A.4] Manipulación de la configuración	[D.log] registros de actividad	1	10	8	8	8	7	Probabilidad muy baja
	[A.5] Suplantación de la identidad del usuario	[D] datos / información	1	10	8	8	8	7	Probabilidad muy baja
		[keys] claves criptográficas	1	10	10	10	10	10	Probabilidad muy baja
		[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (software)	1	10	8	8	8	6	Probabilidad muy baja
		[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
	[A.6] Abuso de privilegios de acceso	[D] datos / información	1	10	8	8	8	7	Probabilidad muy baja
		[keys] claves criptográficas	1	10	10	10	10	10	Probabilidad muy baja
		[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (software)	1	10	8	8	8	6	Probabilidad muy baja

		[HW] equipos informáticos (hardware)	1	9	6	7	6	4	Probabilidad muy baja
		[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
	[A.7] Uso no previsto	[S] servicios	5	8	7	7	7	5	Probabilidad muy alta
		[SW] aplicaciones (software)	4	10	8	8	8	6	Probabilidad alta
		[HW] equipos informáticos (hardware)	5	9	6	7	6	4	Probabilidad muy alta
		[COM] redes de comunicaciones	5	9	7	8	8	5	Probabilidad muy alta
		[Media] soportes de información	5	9	9	10	9	6	Probabilidad muy alta
		[AUX] equipamiento auxiliar	4	9	9	9	7	2	Probabilidad alta
		[L] instalaciones	3	9	9	10	4	2	Probabilidad media
	[A.8] Difusión de software dañino	[SW] aplicaciones (software)	1	10	8	8	8	6	Probabilidad muy baja
	[A.9] [Re-]encaminamiento de mensajes	[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (software)	1	10	8	8	8	6	Probabilidad muy baja
		[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
	[A.10] Alteración de secuencia	[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (software)	1	10	8	8	8	6	Probabilidad muy baja
		[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja

	[A.11] Acceso no autorizado	[D] datos / información	1	10	8	8	8	7	Probabilidad muy baja
		[keys] claves criptográficas	1	10	10	10	10	10	Probabilidad muy baja
		[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (software)	1	10	8	8	8	6	Probabilidad muy baja
		[HW] equipos informáticos (hardware)	1	9	6	7	6	4	Probabilidad muy baja
		[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
		[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamiento auxiliar	1	9	9	9	7	2	Probabilidad muy baja
		[L] instalaciones	1	9	9	10	4	2	Probabilidad muy baja
	A.12] Análisis de tráfico	[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
	[A.13] Repudio	[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[D.log] registros de actividad	1	10	8	8	8	7	Probabilidad muy baja
	[A.14] Interceptación de información (escucha)	[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
	[A.15] Modificación deliberada de la información	[D] datos / información	1	10	8	8	8	7	Probabilidad muy baja
		[keys] claves criptográficas	1	10	10	10	10	10	Probabilidad muy baja

		[S] servicios (acceso)	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (SW)	1	10	8	8	8	6	Probabilidad muy baja
		[COM] comunicaciones (tránsito)	1	9	7	8	8	5	Probabilidad muy baja
		[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
		[L] instalaciones	1	9	9	10	4	2	Probabilidad muy baja
	[A.18] Destrucción de información	[S] servicios (acceso)	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (SW)	1	10	8	8	8	6	Probabilidad muy baja
		[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
		[keys] claves criptográficas	1	10	10	10	10	10	Probabilidad muy baja
		[D] datos / información	1	10	8	8	8	7	Probabilidad muy baja
	[A.19] Revelación de información	[D] datos / información	1	10	8	8	8	7	Probabilidad muy baja
		[keys] claves criptográficas	1	10	10	10	10	10	Probabilidad muy baja
		[S] servicios (acceso)	1	8	7	7	7	5	Probabilidad muy baja
		[SW] aplicaciones (SW)	1	10	8	8	8	6	Probabilidad muy baja
		[COM] comunicaciones (tránsito)	1	9	7	8	8	5	Probabilidad muy baja
		[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
		[L] instalaciones	1	9	9	10	4	2	Probabilidad muy baja

	[A.22] Manipulación de programas	[SW] aplicaciones (software)	1	10	8	8	8	6	Probabilidad muy baja
	[A.23] Manipulación de los equipos	[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamiento auxiliar	1	9	9	9	7	2	Probabilidad muy baja
		[HW] equipos	1	9	6	7	6	4	Probabilidad muy baja
	A.24] Denegación de servicio	[S] servicios	1	8	7	7	7	5	Probabilidad muy baja
		[COM] redes de comunicaciones	1	9	7	8	8	5	Probabilidad muy baja
		[HW] equipos informáticos (hardware)	1	9	6	7	6	4	Probabilidad muy baja
	[A.25] Robo	[AUX] equipamiento auxiliar	1	9	9	9	7	2	Probabilidad muy baja
		[HW] equipos informáticos (hardware)	1	9	6	7	6	4	Probabilidad muy baja
		[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
	[A.26] Ataque destructivo	[HW] equipos informáticos (hardware)	1	9	6	7	6	4	Probabilidad muy baja
		[Media] soportes de información	1	9	9	10	9	6	Probabilidad muy baja
		[AUX] equipamiento auxiliar	1	9	9	9	7	2	Probabilidad muy baja
		[L] instalaciones	1	9	9	10	4	2	Probabilidad muy baja
	[A.27] Ocupación enemiga	[L] instalaciones	1	9	9	10	4	2	Probabilidad muy baja

	[A.28] Indisponibilidad del personal	[P] personal interno	1	9	9	9	8	2	Probabilidad muy baja
	[A.29] Extorsión	[P] personal interno	1	9	9	9	8	2	Probabilidad muy baja
	[A.30] Ingeniería social (picaresca)	[P] personal interno	1	9	9	9	8	2	Probabilidad muy baja

Matriz de análisis de riesgos informáticos													
Grupo	**Amenaza**	**Activo**	IMPACTO					**P**	RIESGOS				
			[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]

A5 – continuación

Grupo	**Amenaza**	**Activo**	IMPACTO					**P**	RIESGOS				
			[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]

A5 – continuación

Grupo	**Amenaza**	**Activo**	IMPACTO	**P**	RIESGOS

			[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
[E] Errores y fallos no intencionados	[E.1] Errores de los usuarios.	[D] datos / información	10	8	8	8	7	4	40	32	32	32	28
		[S] servicios	8	7	7	7	5	3	24	21	21	21	15
		[SW] aplicaciones (software)	10	8	8	8	6	2	20	16	16	16	12
		[Media] soportes de información	9	9	10	9	6	3	27	27	30	27	18
		[keys] claves criptográficas						1	0	0	0	0	0
	[E.2] Errores del administrador	[D] datos / información	10	8	8	8	7	2	20	16	16	16	14
		[keys] claves criptográficas	10	10	10	10	10	1	10	10	10	10	10
		[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (software)	10	8	8	8	6	1	10	8	8	8	6
		[HW] equipos informáticos (hardware)	9	6	7	6	4	1	9	6	7	6	4
		[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5
		[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
	[E.3] Errores de monitorización (log)	[D.log] registros de actividad	10	8	8	8	7	1	10	8	8	8	7
	[E.4] Errores de configuración	[D.conf] datos de configuración	10	8	8	8	7	2	20	16	16	16	14
	[E.7] Deficiencias en la organización	[P] personal						4	0	0	0	0	0
	[E.8] Difusión de software dañino	[SW] aplicaciones (software)	10	8	8	8	6	2	20	16	16	16	12
	[E.9] Errores de [re-	[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones	10	8	8	8	6	1	10	8	8	8	6

	]encaminamiento	[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5
	[E.10] Errores de secuencia	[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (software)	10	8	8	8	6	1	10	8	8	8	6
		[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5
	[E.15] Alteración accidental de la información	[D] datos / información	10	8	8	8	7	3	30	24	24	24	21
		[keys] claves criptográficas	10	10	10	10	10	1	10	10	10	10	10
		[S] servicios	8	7	7	7	5	3	24	21	21	21	15
		[SW] aplicaciones (SW)	10	8	8	8	6	1	10	8	8	8	6
		[COM] comunicaciones (tránsito)	9	7	8	8	5	1	9	7	8	8	5
		[Media] soportes de información	9	9	10	9	6	2	18	18	20	18	12
		[L] instalaciones	9	9	10	4	2	1	9	9	10	4	2
	[E.18] Destrucción de información	[D] datos / información	10	8	8	8	7	3	30	24	24	24	21
		[keys] claves criptográficas	10	10	10	10	10	1	10	10	10	10	10
		[S] servicios	8	7	7	7	5	2	16	14	14	14	10
		[SW] aplicaciones (SW)	10	8	8	8	6	1	10	8	8	8	6
		[COM] comunicaciones (tránsito)	9	7	8	8	5	1	9	7	8	8	5
		[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
		[L] instalaciones	9	9	10	4	2	1	9	9	10	4	2
	[E.19] Fugas de información	[D] datos / información	10	8	8	8	7	1	10	8	8	8	7
		[keys] claves criptográficas	10	10	10	10	10	1	10	10	10	10	10
		[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (SW)	10	8	8	8	6	1	10	8	8	8	6
		[COM] comunicaciones (tránsito)	9	7	8	8	5	1	9	7	8	8	5

		[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
		[L] instalaciones	9	9	10	4	2	1	9	9	10	4	2
		[P] personal (revelación)	9	9	9	8	2	2	18	18	18	16	4
	[E.20] Vulnerabilidades de los programas (software)	[SW] aplicaciones (software)	10	8	8	8	6	4	40	32	32	32	24
	[E.21] Errores de mantenimiento / actualización de programas (software)	[SW] aplicaciones (software)	10	8	8	8	6	2	20	16	16	16	12
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	[HW] equipos informáticos (hardware)	9	6	7	6	4	2	18	12	14	12	8
		[Media] soportes electrónicos	9	9	10	9	6	1	9	9	10	9	6
		[AUX] equipamiento auxiliar	9	9	9	7	2	3	27	27	27	21	6
	[E.24] Caída del sistema por agotamiento de recursos	[S] servicios	8	7	7	7	5	2	16	14	14	14	10
		[HW] equipos informáticos (hardware)	9	6	7	6	4	1	9	6	7	6	4
		[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5
	[E.25] Pérdida de equipos-Robo	[HW] equipos informáticos (hardware)	9	6	7	6	4	1	9	6	7	6	4
		[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
		[AUX] equipamiento auxiliar	9	9	9	7	2	1	9	9	9	7	2
	[E.28] Indisponibilidad del personal	[P] personal interno	9	9	9	8	2	3	27	27	27	24	6

A5 – continuación

Grupo	Amenaza	Activo	IMPACTO					P	RIESGOS				
			[D]	[I]	[C]	[A]	[T]		[D]	[I]	[C]	[A]	[T]
[A] Ataques intencionados	[A.3] Manipulación de los registros de actividad (log)	[D.log] registros de actividad	10	8	8	8	7	1	10	8	8	8	7
	[A.4] Manipulación de la configuración	[D.log] registros de actividad	10	8	8	8	7	1	10	8	8	8	7
	[A.5] Suplantación de la identidad del usuario	[D] datos / información	10	8	8	8	7	1	10	8	8	8	7
		[keys] claves criptográficas	10	10	10	10	10	1	10	10	10	10	10
		[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (software)	10	8	8	8	6	1	10	8	8	8	6
		[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5
	[A.6] Abuso de privilegios de acceso	[D] datos / información	10	8	8	8	7	1	10	8	8	8	7
		[keys] claves criptográficas	10	10	10	10	10	1	10	10	10	10	10
		[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (software)	10	8	8	8	6	1	10	8	8	8	6
		[HW] equipos informáticos (hardware)	9	6	7	6	4	1	9	6	7	6	4
		[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5

	[A.7] Uso no previsto	[S] servicios	8	7	7	7	5	5	40	35	35	35	25
		[SW] aplicaciones (software)	10	8	8	8	6	4	40	32	32	32	24
		[HW] equipos informáticos (hardware)	9	6	7	6	4	5	45	30	35	30	20
		[COM] redes de comunicaciones	9	7	8	8	5	5	45	35	40	40	25
		[Media] soportes de información	9	9	10	9	6	5	45	45	50	45	30
		[AUX] equipamiento auxiliar	9	9	9	7	2	4	36	36	36	28	8
		[L] instalaciones	9	9	10	4	2	3	27	27	30	12	6
	[A.8] Difusión de software dañino	[SW] aplicaciones (software)	10	8	8	8	6	1	10	8	8	8	6
	[A.9] [Re-]encaminamiento de mensajes	[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (software)	10	8	8	8	6	1	10	8	8	8	6
		[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5
	[A.10] Alteración de secuencia	[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (software)	10	8	8	8	6	1	10	8	8	8	6
		[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5
	[A.11] Acceso no autorizado	[D] datos / información	10	8	8	8	7	1	10	8	8	8	7
		[keys] claves criptográficas	10	10	10	10	10	1	10	10	10	10	10
		[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (software)	10	8	8	8	6	1	10	8	8	8	6
		[HW] equipos informáticos (hardware)	9	6	7	6	4	1	9	6	7	6	4
		[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5

		[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
		[AUX] equipamiento auxiliar	9	9	9	7	2	1	9	9	9	7	2
		[L] instalaciones	9	9	10	4	2	1	9	9	10	4	2
	A.12] Análisis de tráfico	[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5
	[A.13] Repudio	[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[D.log] registros de actividad	10	8	8	8	7	1	10	8	8	8	7
	[A.14] Interceptación de información (escucha)	[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5
	[A.15] Modificación deliberada de la información	[D] datos / información	10	8	8	8	7	1	10	8	8	8	7
		[keys] claves criptográficas	10	10	10	10	10	1	10	10	10	10	10
		[S] servicios (acceso)	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (SW)	10	8	8	8	6	1	10	8	8	8	6
		[COM] comunicaciones (tránsito)	9	7	8	8	5	1	9	7	8	8	5
		[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
		[L] instalaciones	9	9	10	4	2	1	9	9	10	4	2
	[A.18] Destrucción de información	[S] servicios (acceso)	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (SW)	10	8	8	8	6	1	10	8	8	8	6
		[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
		[keys] claves criptográficas	10	10	10	10	10	1	10	10	10	10	10
		[D] datos / información	10	8	8	8	7	1	10	8	8	8	7
	[A.19] Revelación de información	[D] datos / información	10	8	8	8	7	1	10	8	8	8	7
		[keys] claves criptográficas	10	10	10	10	10	1	10	10	10	10	10
		[S] servicios (acceso)	8	7	7	7	5	1	8	7	7	7	5
		[SW] aplicaciones (SW)	10	8	8	8	6	1	10	8	8	8	6

		[COM] comunicaciones (tránsito)	9	7	8	8	5	1	9	7	8	8	5
		[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
		[L] instalaciones	9	9	10	4	2	1	9	9	10	4	2
	[A.22] Manipulación de programas	[SW] aplicaciones (software)	10	8	8	8	6	1	10	8	8	8	6
	[A.23] Manipulación de los equipos	[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
		[AUX] equipamiento auxiliar	9	9	9	7	2	1	9	9	9	7	2
		[HW] equipos	9	6	7	6	4	1	9	6	7	6	4
	A.24] Denegación de servicio	[S] servicios	8	7	7	7	5	1	8	7	7	7	5
		[COM] redes de comunicaciones	9	7	8	8	5	1	9	7	8	8	5
		[HW] equipos informáticos (hardware)	9	6	7	6	4	1	9	6	7	6	4
	[A.25] Robo	[AUX] equipamiento auxiliar	9	9	9	7	2	1	9	9	9	7	2
		[HW] equipos informáticos (hardware)	9	6	7	6	4	1	9	6	7	6	4
		[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
	[A.26] Ataque destructivo	[HW] equipos informáticos (hardware)	9	6	7	6	4	1	9	6	7	6	4
		[Media] soportes de información	9	9	10	9	6	1	9	9	10	9	6
		[AUX] equipamiento auxiliar	9	9	9	7	2	1	9	9	9	7	2
		[L] instalaciones	9	9	10	4	2	1	9	9	10	4	2

	[A.27] Ocupación enemiga	[L] instalaciones	9	9	10	4	2	1	9	9	10	4	2
	[A.28] Indisponibilidad del personal	[P] personal interno	9	9	9	8	2	1	9	9	9	8	2
	[A.29] Extorsión	[P] personal interno	9	9	9	8	2	1	9	9	9	8	2
	[A.30] Ingeniería social (picaresca)	[P] personal interno	9	9	9	8	2	1	9	9	9	8	2

Anexos 7 - A6 – Salvaguardas - Matriz de Controles_27002

#	Política	#	Dominio de Control	Objetivos de Control	#	Titulo Control	Descripción del Control	APLICABILIDAD SI / NO	Evidencia Solicitada	Área Responsable Secundaria	Responsable	Revisión de la Evidencia	Obs.	Calificación
A.5.- Políticas de Seguridad de la Información														

5.0	Políticas de Seguridad de la Información	A.5.1	Directrices de la Dirección en seguridad de la información	Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes.	A.5.1.1	Políticas para la seguridad de la información	La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.	**X**		Reglamento No. 056 – política de seguridad de la información	Jefatura de infraestructura	Área de seguridad y telecomunicaciones	Conforme a lo requerido en la guía de implementación de la norma GTC-ISO/IEC 27002, actualmente la organización cuenta con una política de seguridad de la información avalada por la comisión de asuntos generales del	D	**Definido**

													consejo superior, según acta No.1504 de 2015, por lo anterior esta política ha sido avalada por el consejo superior, es esta se establece el enfoque de la universidad para la gestión y objetivos de la seguridad de la información.		

5.0	Políticas de Seguridad de la Información	A.5.1	Directrices de la Dirección en seguridad de la información	Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes.	A.5.1.2	Revisión de las Políticas para la Seguridad de la Información	La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.	**X**		Comité de seguridad, solicitud de actas, validación de seguimientos	Jefatura de infraestructura	Área de seguridad y telecomunicaciones	Actualmente no se tiene un comité de seguridad de la información y no se realiza una verificación periódica de las políticas, sin embargo, todos los cambios en cuanto a seguridad deben pasar por un comité de cambios	PNP	**Inicial**

													que actualmente tiene la dirección de sistemas, en el cual se realiza evaluación del impacto.		
A.6.- Organización de Seguridad de la Información															
6.0	Organización de la Seguridad de la Información	A.A.6.1	Organización Interna	Establecer un marco de gestión para iniciar y controlar la aplicación de seguridad de la información dentro de la	A.6.1.1	Roles y responsabilidades	Se deben definir y asignar roles y responsabilidades asociadas a la Seguridad de la información dentro de la organización.	**X**		Se realiza solicitud de los procedimientos que se realizan actualmente para la asignación de permisos,	Dirección de sistemas	Dirección de sistemas	Teniendo en cuenta el proceso y el rol que el funcionario desarrolle, se han definido una serie de permisos y respons	MD	**Definido**

				organización						cara al directorio activo y a las diferentes bases de datos.			abilidades, sin embargo, cada administrador se encarga de realizar la gestión de la seguridad teniendo en cuenta el frente en el que se encuentra, actualmente no todos los procesos de seguridad de la información se		

													encuentran documentados, por lo cual es pertinente realizar una verificación de dichos procesos para proceder con la correcta documentación de responsables y protección diaria.		

6.0	Organización de la Seguridad de la Información	A.6.1	Organización Interna	Establecer un marco de gestión para iniciar y controlar la aplicación de seguridad de la información dentro de la organización	A.6.1.2	Contacto con las autoridades	Se deben definir y mantener contactos con las autoridades relevantes	**X**		Catálogo de servicios, documentación de procesos para la gestión de la seguridad de la información.	Dirección de sistemas	Dirección de sistemas	En la actualidad se cuenta con un comité de seguimiento en el que se evalúa el alcance de los requerimientos, una plataforma en la que se encuentran la documentación de los requerimientos o incidentes que se	RD	**Gestionado**

													realizan, por lo cual, la dirección de sistemas cuenta con procesos establecidos los cuales especifican los medios y las autoridades a las que se deben contactar, sin embargo, los medios establecidos y los tiempos de respuest		

													a no se encuentran definidos en el catálogo de servicios.		
6.0	Organización de la Seguridad de la Información	A.6.1	Organización Interna	Establecer un marco de gestión para iniciar y controlar la aplicación de seguridad de la información dentro de la organización	A.6.1.3	Contacto con grupos de interés especial	Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, asi como asociaciones de profesionales.	**x**		Documentación de afiliaciones a foros, grupos etc…	Jefatura de infraestructura	Área de seguridad y telecomunicaciones	Actualmente la dirección se encuentra inscrita a diferentes grupos y estaciones de alertas para mejorar el conocimiento acerca de las mejores práctica	MD	**Gestionado**

													s, estados, adverte ncias y alertas tempran as para la gestión de la seguridad de la informa ción.		
6.0	Organización de la Seguridad de la Información	A.6.1	Organización Interna	Establecer un marco de gestión para iniciar y controlar la aplicación de seguridad de la información dentro de la	A.6.1.4	Seguridad de la Información en la Gestión de Proyectos	Se debe dirigir aspectos asociados a Seguridad de la Información en la gestión de proyectos, independientemente del tipo de proyecto.	**x**		Reglamento No. 056 – política de seguridad de la información	Dirección de sistemas	Área de seguridad y telecomunicaciones	Existen responsables para dar tratamiento a la seguridad de la información, proceso definido y documentado en la política de	D	**Optimizado**

				organización									seguridad de la universidad.		
6.0	Organización de la Seguridad de la Información	A.6.1	Organización Interna	Establecer un marco de gestión para iniciar y controlar la aplicación de seguridad de la información dentro de la organización	A.6.1.5	Segregación de Tareas	Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.	**X**		Reglamento No. 056 – política de seguridad de la información	Dirección de sistemas	Dirección de sistemas	Actualmente se encuentra especificado en la política de seguridad de la información de la universidad que, conforme al rol asignado al usuario, este tenga los permisos que le corresponden y	D	**Gestionado**

													no pueda acceder, modificar o usar activos que no le sean autorizados. Actualmente se está realizando un proceso de verificación de permisos por rol para los sistemas de información administrados por la dirección de		

													sistemas.		
6.0	Organización de la Seguridad de la Información	A.6.2	Los dispositivos móviles y el teletrabajo (Trabajo Remoto)	Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles	A.6.2.1	Política de dispositivos móviles	Se debe adoptar una política formal, y medidas de seguridad apropidas para la protección contra los riesgos debidos al uso de recursos de informática y comunicaciones móviles.	**X**		Reglamento No. 056 – política de seguridad de la información	Dirección de sistemas	Dirección de sistemas	La universidad cuenta actualmente con un proyecto de flexibilidad laboral, lo cual ha obligado a pensar en la generación de políticas de seguridad para la disponibilidad en	D	**Optimizado**

													este tipo de entornos, del mismo modo los diferentes accesos a información se encuentran delimitados por diferentes controles delimitados por la política de seguridad de la información.		

6.0	Organización de la Seguridad de la Información	A.6.2	Los dispositivos móviles y el teletrabajo (Trabajo Remoto)	Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles	A.6.2.2	Teletrabajo (Trabajo Remoto)	Se debe desarrollar e implementar una política, y procedimientos y planes operaciones de actividades de trabajo remoto.		**X**	Reglamento No. 056 – política de seguridad de la información	Dirección de sistemas	Dirección de sistemas	La universidad cuenta actualmente con un proyecto de flexibilidad laboral, el cual no se ha delimitado y tampoco se ha implementado.	PNP	**Inicial**
A.7.- Seguridad en los Recursos Humanos															

7.0	Seguridad en los Recursos Humanos	A.7.1	Antes del empleo	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.1	Selección	Se debe realizar la verificación de antecedentes de todos los candidatos al empleo, contratistas y usuarios de terceras partes de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificaci	**X**		Reglamento No. 056 – política de seguridad de la información	Dirección de sistemas Dirección de desarrollo humano	Dirección de sistemas Dirección de desarrollo humano	Teniendo en cuenta lo indicado en la política de seguridad actualmente se realiza un procedimiento para evaluar que las empresas cumplan con lo requerido, a través de las diferentes propuestas reporta	MD	**Gestionado**

							ón de la información a ser accedida, y los riesgos percibidos.						das se procede a realizar una solicitud de requerimientos en el cual se realiza solicitud de datos específicos a los contratistas incluyendo información personal de los mismos.		

7.0	Seguridad en los Recursos Humanos	A.7.1	Antes del empleo	Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.2	Términos y condiciones de la relación laboral	Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deben acordar y firmar los términos y condiciones de su contrato laboral el cual debe indicar sus responsabilidades y las de la organización en	**X**		Reglamento No. 056 – política de seguridad de la información	Dirección de desarrollo humano	Dirección de desarrollo humano Dirección de sistemas	En la actualidad se lleva un proceso en el cual intervienen los diferentes entes encargados para que se realice el proceso de contratación, este documento se avalúa por la dirección de desarrollo humano en conjunt	D	**Optimizado**

							cuanto a seguridad de la información.						o con la dirección de sistemas en cuanto a contratistas y demás entes encargados, de la misma manera funciona para la contratación de empleados.		
7.0	Seguridad en los Recursos Humanos	A.7.2	Durante del empleo	Asegurar que los empleados, contratistas y usuarios de terceras	A.7.2.1	Responsabilidades de la dirección	La dirección debe requerir a los empleados, contratistas y usuarios de	**X**		Reglamento No. 056 – política de seguridad de la información	Dirección de desarrollo humano	Dirección de desarrollo humano Dirección de sistemas	Los empleados y contratistas se encuentran informados sobre sus roles	MD	**Gestionado**

				partes sean conscientes de la amenazas y de las preocupaciones de la seguridad de la información, de sus responsabilidades y obligaciones, y estén preparados para apoyar la política de seguridad de la organiza			terceras partes que apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos por la organización.						y responsabilidades de seguridad de la información.		

				ción en el curso de su trabajo normal, y para reducir el riesgo de errores humanos											
7.0	Seguridad en los Recursos Humanos	A.7.2	Durante del empleo	Asegurar que los empleados, contratistas y usuarios de terceras partes sean conscientes de la amenazas y de las preocup	A.7.2.2	Concientización, educación y formación en seguridad de la información	Todos los empleados de la organización y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de concienci a	**X**		Entrevistas, Reglamento No. 056 – política de seguridad de la información	Dirección de sistemas	Dirección de sistemas	Actualmente se encuentra especificado en la política de seguridad, sin embargo, no se ha realizado la debida gestión al mismo.	RD	**Inicial**

				aciones de la seguridad de la información, de sus responsabilidades y obligaciones, y estén preparados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y para reducir el riesgo de			apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.								

				errores humanos											
7.0	Seguridad en los Recursos Humanos	A.7.2	Durante del empleo	Asegurar que los empleados, contratistas y usuarios de terceras partes sean conscientes de la amenazas y de las preocupaciones de la	A.7.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal para empleados que hayan perpetrado una violación a la seguridad.	**X**		Reglamento No. 056 – política de seguridad de la información	Dirección de sistemas	Dirección de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	D	**Gestionado**

				seguridad de la información, de sus responsabilidades y obligaciones, y estén preparados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y para reducir el riesgo de errores											

				humanos											
7.0	Seguridad en los Recursos Humanos	A.7.3	Finalización o cambio de la relación laboral o empleo	Asegurar que los empleados, contratistas o usuarios de terceras partes se desvinculen de una organización o cambien su relación laboral de una	A.7.3.1	Responsabilidades en la desvinculación (Término o cambio de empleo)	Se deben definir y asignar claramente las responsabilidades relativas a la desvinculación o al cambio de la relación laboral, comunicada a el empleado o usuario parte externa	**X**		Reglamento No. 056 – política de seguridad de la información	Dirección de desarrollo humano	Dirección de desarrollo humano	Procesos actualmente especificados en la política de seguridad de la universidad	D	**Optimizado**

				forma ordenada. Protegiendo los intereses de la organización .											
A.8.- Gestión de Activos de la Información															
8.0	Gestión de Activos de la Información	A.8.1	Responsabilidad por los activos de información	Implementar y mantener una adecuada protección sobre los activos de la organización.	A.8.1.1	Inventario de Activos	Todos los activos se deben identificar claramente y se debe elaborar y mantener un inventario de todos los activos importantes.	**X**		Entrevistas y solicitud de inventarios actuales	Centro De Servicios Tecnológicos Dirección De Compras Administrativas	Centro De Servicios Tecnológicos Dirección De Compras Administrativas	En el Centro De Servicios Tecnológicos en conjunto con la Dirección De Compras Administrativas, se lleva un control de todos los activos tecnológicos, sin	D	**Definido**

													embargo, se debe validar la trazabilidad de la información, teniendo en cuenta que no se tiene claridad sobre el proceso que se realiza.		
8.0	Gestión de Activos de la Información	A.8.1	Responsabilidad por los activos de información	Implementar y mantener una adecuada protección sobre los activos	A.8.1.2	Propietarios de los Activos	Toda la información y activos asociados con las instalaciones de procesamiento de información deben	**X**		Entrevistas y solicitud de inventarios actuales	Centro De Servicios Tecnológicos Dirección De Compras Administrativas	Centro De Servicios Tecnológicos Dirección De Compras Administrativas	En el Centro De Servicios Tecnológicos en conjunto con la Dirección De Compras	MD	**Gestionado**

				de la organización.			pertenecer a un dueño designado por la organización.				strativas		Administrativas, se lleva un control de todos los activos tecnológicos, sin embargo, se debe validar la trazabilidad de la información, teniendo en cuenta que no se tiene claridad sobre el proceso que se realiza. En tanto para la		

													asignación de un activo, este siempre debe estar sustentado mediante una solicitud realizada por la plataforma otrs.		
8.0	Gestión de Activos de la Información	A.8.1	Responsabilidad por los activos de información	Implementar y mantener una adecuada protección sobre los activos de la organización.	A.8.1.3	Uso aceptable de activos	Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y activos asociados	**X**		Reglamento No. 056 – política de seguridad de la información	Dirección de sistemas	Dirección de sistemas	Se puede visualizar en la política actual de seguridad de la información el grupo de reglas requerido por la	MD	**Gestionado**

							con las instalaciones de procesamiento de información.						universidad para uso aceptable de la información y de los activos que se encuentran asociados a la información .		
8.0	Gestión de Activos de la Información	A.8.1	Responsabilidad por los activos de información	Implementar y mantener una adecuada protección sobre los activos de la organización.	A.8.1.4	Devolución de activos	Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Dirección de Operaciones Dirección de sistemas	Dirección de Operaciones Dirección de sistemas	Este proceso se realiza en conjunto con otras direcciones como la dirección de operaciones, actualm	D	**Optimizado**

							cargo, al terminar de su empleo, contrato o acuerdo.						ente el usuario debe firmar la paz y salvo con lo cual se garantiza que los activos de información fueron entregados a su jefe inmediato.		
8.0	Gestión de Activos de la Información	A.8.2	Clasificación de Activos de Información	Asegurar que la información reciba un nivel de protección apropiado.	A.8.2.1	Clasificación de Información	La información se clasificará en función de su valor, los requisitos legales, sensibilid	**X**		Reglamento No. 056 – política de seguridad de la información	Dirección de sistemas	Dirección de sistemas	Teniendo en cuenta los requerimientos del negocio, se tiene actualmente	D	**Optimizado**

							ad o criticidad para la organización			y Entrevistas			clasificación y controles para la protección de la seguridad de la información, con diferentes niveles de seguridad estipulados por el comité de seguridad de la información, los cuales se pueden encontrar en la política		

													de seguridad de la universidad.		
8.0	Gestión de Activos de la Información	A.8.2	Clasificación de Activos de Información	Asegurar que la información reciba un nivel de protección apropiado.	A.8.2.2	Etiquetado de Información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo al esquema de clasificación adoptado por la organización.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Dirección de sistemas	Dirección de sistemas	Actualmente la dirección de sistemas tiene en muchos de sus procesos un etiquetado específico para la información, sin embargo, no toda la información cumple a cabalidad con	RD	**Definido**

													este objetivo.		
8.0	Gestión de Activos de la Información	A.8.2	Clasificación de Activos de Información	Asegurar que la información reciba un nivel de protección apropiado.	A.8.2.3	Manejo de Activos	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el manejo de la información de acuerdo al esquema de clasificación adoptado por la organización.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Dirección de sistemas	Dirección de sistemas	Actualmente la dirección de sistemas tiene en muchos de sus procesos un etiquetado específico para la información, sin embargo, no toda la información cumple a cabalidad con	RD	**Definido**

													este objetivo.		
8.0	Gestión de Activos de la Información	A.8.3	Manejo de Medios	Prevenir o evitar la divulgación no autorizada, modificación, borrado o destrucción de los activos e interrupción de las actividades del negocio.	A.8.3.1	Gestión de los medios removibles	Deben estar implementados procedimientos para la gestión de los medios removibles, de acuerdo a la clasificación de activos de información definidos en la organización.	**X**		Entrevistas	Dirección de sistemas	Dirección de sistemas	Actualmente la dirección de sistemas tiene implementado en sus procesos herramientas para la gestión de los diferentes medios renovables, sin embargo, teniendo en cuenta	RD	**Definido**

													que el numeral 8.2.2 y 8.2.3, no cumplen a calidad este tampoco lo hace ya que depende de la gestión de los dos anteriores.		
8.0	Gestión de Activos de la Información	A.8.3	Manejo de Medios	Prevenir o evitar la divulgación no autorizada, modificación, borrado o destrucción de	A.8.3.2	Eliminación de los medios, Disposición de los medios	Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando	**X**		Entrevistas	Dirección de sistemas	Dirección de sistemas	No existe ningún procedimiento formal para tal finalidad	RD	**Inicial**

				los activos e interrupción de las actividades del negocio.			procedimientos formales.								
8.0	Gestión de Activos de la Información	A.8.3	Manejo de Medios	Prevenir o evitar la divulgación no autorizada, modificación, borrado o destrucción de los activos e interrupción de las actividades del negocio.	A.8.3.3	Transferencia de medios físicos	Se deben implementar medidas de protección contra accesos no autorizados a los medios que contienen información sensible durante el trasporte.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	D	**Gestionado**
A.9.- Control de acceso (lógico)															

9.0	Control de Acceso (lógico)	A.9.1	Requisitos de negocio para el control de acceso	Asegurar el acceso autorizado a los usuarios e impedir el acceso no autorizado a sistemas de información.	A.9.1.1	Política de Control de Acceso	Se deben establecer, documentar y revisar una política de control de acceso basadas en los requisitos de acceso del negocio y de seguridad.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	MD	**Gestionado**
9.0	Control de Acceso (lógico)	A.9.1	Requisitos de negocio para el control de acceso	Asegurar el acceso autorizado a los usuarios e impedir el acceso no autoriza	A.9.1.2	Política sobre el uso de servicios de red	Los usuarios sólo deben disponer de acceso a la red y a los servicios de red que han sido	**X**		Reglamento No. 056 – política de seguridad de la información y	Direccion de sistemas	Direccion de sistemas	Cualquier usuario que quiera acceder a la red institucional, debe tener un usuario	MD	**Gestionado**

				do a sistemas de información.			autorizados específicamente.			Entrevistas			y clave para poder acceder, sin contar que debe configurarse el equipo para que pueda acceder. Este proceso se encuentra actualmente especificados en la política de seguridad de la universidad		

9.0	Control de Acceso (lógico)	A.9.2	Gestión de acceso de los usuarios	Asegurar el acceso autorizado a los usuarios e impedir el acceso no autorizado a sistemas de información.	A.9.2.1	Registro / cancelación de registro de usuarios	Debe existir un procedimiento formal de altas de registro y cancelación de registro para otorgar y revocar los accesos a todos los servicios y sistemas de información.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Dirección de desarrollo humano Direccion de sistemas	Dirección de desarrollo humano Direccion de sistemas	Aunque existe el protocolo, algunos usuarios son creados sin cumplir con este, sin mencionar que algunos de los elementos especificados en la guía de implementación de la norma ISO 27002 no se mencionan por lo que	RD	**Definido**

													tampoco se cumplen, al cambio de cargo no se realiza la correcta actualización de accesos.		
9.0	Control de Acceso (lógico)	A.9.2	Gestión de acceso de los usuarios	Asegurar el acceso autorizado a los usuarios e impedir el acceso no autorizado a sistemas de información.	A.9.2.2	Gestión de acceso privilegiados	Se debe restringuir y controlar la asignación y uso de privilegios.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Dirección de desarrollo humano Direccion de sistemas	Dirección de desarrollo humano Direccion de sistemas	Actualmente el acceso privilegiado se controla mediante un proceso de autorización formal a través de un proceso de solicitud	MD	**Gestionado**

													estandarizado.		
9.0	Control de Acceso (lógico)	A.9.2	Gestión de acceso de los usuarios	Asegurar el acceso autorizado a los usuarios e impedir el acceso no autorizado a sistemas de información.	A.9.2.3	Gestión de contraseñas del usuario	Se debe controlar la asignación de contraseñas mediante unproceso de gestión formal.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Dirección de desarrollo humano Direccion de sistemas	Dirección de desarrollo humano Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	MD	**Gestionado**
9.1	Control de Acceso (lógico)	A.9.2	Gestión de acceso de los usuarios	Asegurar el acceso autorizado a los usuarios e impedir el acceso no	A.9.2.4	Revisión de los derechos de acceso de los usuarios	La dirección debe establecer un proceso formal de revisión periódica de los derechos	**X**		Reglamento No. 056 – política de seguridad de la información	Dirección de desarrollo humano Direccion de sistemas	Dirección de desarrollo humano Direccion de sistemas	No se logra identificar un proceso relacionado con esta gestión	PNP	**Inexistente**

				autorizado a sistemas de información.			de acceso de los usuarios.			y Entrevistas					
9.2	Control de Acceso (lógico)	A.9.2	Gestión de acceso de los usuarios	Asegurar el acceso autorizado a los usuarios e impedir el acceso no autorizado a sistemas de información.	A.9.2.5	La eliminación o ajuste de derechos de acceso	Los derechos de acceso de todos los empleados y usuarios externos a la información y sistemas de información (procesamiento) deben ser removidos de acuerdo al termino de su empleo,	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Dirección de desarrollo humano Direccion de sistemas	Dirección de desarrollo humano Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	D	**Optimizado**

							contrato o acuerdo, o ajustes de cambios.								
9.0	Control de Acceso (lógico)	A.9.3	Responsabilidades del usuario	Los usuarios deben ser conscientes de su responsabilidad para el mantenimiento de los controles de acceso eficaces por ejemplo elegir contraseñas seguras y	A.9.3.1	Uso de Contraseñas	Se debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y uso de las contraseñas.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	D	**Optimizado**

				mantener su confidencialidad.											
9.0	Control de Acceso (lógico)	A.9.4	Control de acceso al sistema y aplicaciones	Evitar el acceso no autorizado a los sistemas y aplicaciones.	A.9.4.1	Restricción de acceso información	El acceso a las información en sistemas y aplicaciones se limitará de acuerdo con la política de control de acceso	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente existe una política que brinda acceso a las aplicaciones solamente a las personas que se encuentran autorizadas, cara al directorio activo de la universidad y a al perfil de	MD	**Gestionado**

													usuario asignado.		
9.0	Control de Acceso (lógico)	A.9.4	Control de acceso al sistema y aplicaciones	Evitar el acceso no autorizado a los sistemas y aplicaciones.	A.9.4.2	Procedimientos de conexión (Log-on) seguros	El acceso a los sitemas operativos se debe controlar mediante un proceso de conexión (log-on) seguro.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	D	**Optimizado**
9.0	Control de Acceso (lógico)	A.9.4	Control de acceso al sistema y aplicaciones	Evitar el acceso no autorizado a los sistemas y aplicaciones.	A.9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñ	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	D	**Optimizado**

							as de calidad.								
9.0	Control de Acceso (lógico)	A.9.4	Control de acceso al sistema y aplicaciones	Evitar el acceso no autorizado a los sistemas y aplicaciones.	A.9.4.4	Uso de Utilitarios (Utilities) del sistema	Se debe restringuir y controlar estrictamente el uso de programas utilitarios que pueden estár en capacidad de anular el sistema y los controles de aplicación.	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente ningún usuario puede realizar la instalación de ningún programa ya que los permisos de usuario realizan esta restricción, para este fin solamente algunos usuarios autorizados tienen	D	**Gestionado**

													permisos.		
9.0	Control de Acceso (lógico)	A.9.4	Control de acceso al sistema y aplicaciones	Evitar el acceso no autorizado a los sistemas y aplicaciones.	A.9.4.5	Control de acceso al código fuente de los programas	Se debe restringir el acceso al código fuente de los programas.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente ningún usuario puede realizar la instalación de ningún programa ya que los permisos de usuario realizan esta restricción, para este fin solamente algunos usuarios autorizados	MD	**Gestionado**

													tienen permisos.		
A.10.- Criptografía															
10.0	Criptografía	A.10.1	Controles criptográficos	Proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.	A.10.1.1	Política sobre el uso de controles criptográficos	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	**X**		Reglamento No. 056 – política de seguridad de la información	Direccion de sistemas	Direccion de sistemas	Actualmente existe la política y es implementada de acuerdo a los diferentes requerimientos que se puedan presentar.	MD	**Gestionado**
10.0	Criptografía	A.10.1	Controles criptográficos	Proteger la confidencialidad, autenticidad o integridad de la	A.10.1.2	Gestión de claves	Se debe implementar un sistema de gestión de claves para apoyar el	**X**		Reglamento No. 056 – política de seguridad de la	Direccion de sistemas	Direccion de sistemas	Actualmente existe la política y es implementada de acuerdo	MD	**Gestionado**

				información, por medios criptográficos.			uso de las técnicas criptográficas por parte de la organización.			información			a los diferentes requerimientos que se puedan presentar.		
A.11.- Seguridad Física y Medio Ambiental															
11.0	Seguridad Física y Medio Ambiental	A.11.1	Áreas Seguras	Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones y la información de la organización.	A.11.1.1	Perímetro de seguridad física	Se deben utilizar perímetros de seguridad (barreras tales como paredes, puertas de entrada controladas por tarjeta o recepcionistas), para proteger las áreas que contiene	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Dirección de sistemas	Dirección de sistemas	Políticas creadas para la asignación de seguridad perimetral asignada al campus de la universidad de la sabana.	MD	**Gestionado**

							n información e instalaciones de procesamiento de información.								
11.0	Seguridad Física y Medio Ambiental	A.11.1	Áreas Seguras	Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones y la información de la organización.	A.11.1.2	Controles de acceso físico	Las áreas seguras deben estár protegidas por controles de entrada apropiados que aseguren que sólo se permite el acceso a personal autorizado.		**X**	Entrevistas	Dirección de Operaciones Dirección de sistemas	Dirección de Operaciones	Este proceso se encuentra implementado mediante control de acceso y Cámaras de vigilancia	MD	**Gestionado**

11.0	Seguridad Física y Medio Ambiental	A.11.1	Áreas Seguras	Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones y la información de la organización.	A.11.1.3	Seguridad de oficinas, recintos e instalaciones	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.		**X**	Entrevistas	Dirección de Operaciones Dirección de sistemas	Dirección de Operaciones	Este proceso se encuentra implementado mediante control de acceso y Cámaras de vigilancia	MD	**Gestionado**
11.0	Seguridad Física y Medio Ambiental	A.11.1	Áreas Seguras	Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones y	A.11.1.4	Protección contra las amenazas externas y del ambiente	Se debe diseñar y aplicar medios de protección física contra daños por incendio, inundación,		**X**	Entrevistas	Dirección de operaciones, seguridad y salud en el trabajo	Dirección de operaciones, seguridad y salud en el trabajo	En la actualidad se tiene asesoría especializada para evitar daños ambientales, explosio	D	**Optimizado**

				la información de la organización.			terremoto, explosión, disturbios civiles, y otras formas de desastre natural o provocado por el hombre						nes, disturbios civiles, administrados por las direcciones relacionadas.		
11.0	Seguridad Física y Medio Ambiental	A.11.1	Áreas Seguras	Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones y la información de la	A.11.1.5	El trabajo en las áreas seguras	Se debe diseñar y aplicar protección física y directrices para trabajar en áreas seguras.		**X**	Entrevistas	Compras y suministros	Compras y suministros	Proceso no administrado por la dirección	MD	**Gestionado**

				organización.											
11.0	Seguridad Física y Medio Ambiental	A.11.1	Áreas Seguras	Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones y la información de la organización.	A.11.1.6	Áreas de acceso público, de entrega y de carga	Se deben controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las intalaciones, y si es posible, aislarlas de las instalaciones de procesam		**X**	Entrevistas	Compras y suministros	Compras y suministros	Proceso no administrado por la dirección	RD	**Gestionado**

							iento de la información para evitar el acceso no autorizado.								
11.0	Seguridad Física y Medio Ambiental	A.11.2	Seguridad del Equipo	Prevenir pérdida, hurto o el compromiso de los activos así como la interrupción de las actividades de la organización.	A.11.2.1	Ubicación y protección del equipamiento	El equipamiento se debe ubicar o proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.	**X**		Verificación de espacios físicos y entrevistas	Direccion de sistemas	Direccion de sistemas	El control se encuentra actualmente implementado y ajustado a los requerimientos de la norma.	MD	**Gestionado**

11.0	Seguridad Física y Medio Ambiental	A.11.2	Seguridad del Equipo	Prevenir pérdida, hurto o el compromiso de los activos así como la interrupción de las actividades de la organización.	A.11.2.2	Elementos de soporte	Se debe proteger el equipamiento contra posibles fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte.	**X**		Entrevistas	Direccion de Operaciones Direccion de sistemas	Terceros	Para algunos casos la dirección de sistemas se encarga de brindar soporte y de realizar procesos de gestión, sin embargo, algunos de estos dependen de la dirección de operaciones y no de la dirección de sistemas por lo	MD	**Definido**

													que se realiza un trabajo conjunto para el suministro de información y la debida gestión de los posibles incidentes.		
11.0	Seguridad Física y Medio Ambiental	A.11.2	Seguridad del Equipo	Prevenir pérdida, hurto o el compromiso de los activos así como la interrupción de las actividades de la	A.11.2.3	Seguridad en el cableado	Se debe proteger contra intercepción o daños en el cableado de energía y de telecomunicaciones que transporta datos o	**X**		Entrevistas	Direccion de sistemas	Terceros	Actualmente la infraestructura de la red cableada cumple con el control indicado en la norma	MD	**Gestionado**

				organización.			brinda soporte a servicios de información.								
11.0	Seguridad Física y Medio Ambiental	A.11.2	Seguridad del Equipo	Prevenir pérdida, hurto o el compromiso de los activos así como la interrupción de las actividades de la organización.	A.11.2.4	Mantenimiento del equipamiento	El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad o integridad.	**X**		Entrevistas	Direccion de sistemas	Jefatura de servicios tecnológicos	Actualmente se realiza gestión reactiva ya que se realiza con base a la solicitud de incidencia que se pueda presentar o reportar.	RD	**Repetible**
11.0	Seguridad Física y Medio Ambiental	A.11.2	Seguridad del Equipo	Prevenir pérdida, hurto o el compromiso de	A.11.2.5	Eliminación / Retiro de Activos	El equipamiento, la información o el software	**X**		Entrevistas	Direccion de sistemas	Jefatura de servicios tecnológicos	El control actualmente se ejecuta con	D	**Optimizado**

				los activos así como la interrupción de las actividades de la organización.			no se deben reritar del local de la organización sin previa autorización.						forme a lo sugerido en la guía de implementación		
11.0	Seguridad Física y Medio Ambiental	A.11.2	Seguridad del Equipo	Prevenir pérdida, hurto o el compromiso de los activos así como la interrupción de las actividades de la organización.	A.11.2.6	Seguridad del equipamiento fuera de las instalaciones de la organización	Se debe asegurar todo el equipamiento fuera de los locales de organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalacio	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente se tiene políticas y procesos para la protección de los servicios y dispositivos móviles, los cuales también se encuent	MD	**Gestionado**

							nes de la organización.						ran estipulados en la política de seguridad de la universidad.		
11.0	Seguridad Física y Medio Ambiental	A.11.2	Seguridad del Equipo	Prevenir pérdida, hurto o el compromiso de los activos así como la interrupción de las actividades de la organización.	A.11.2.7	Seguridad en la reutilización o descarte de los equipos	Todo aquel equipamiento que contenga medios de almacenamiento se debe revisar para asegurar que todos los datos sensibles y software licenciado se hayan	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	El control actualmente se ejecuta conforme a lo sugerido en la guía de implementación	MD	**Gestionado**

							removido o se haya sobrescrito o con seguridad antes de su descarte o baja.								
11.0	Seguridad Física y Medio Ambiental	A.11.2	Seguridad del Equipo	Prevenir pérdida, hurto o el compromiso de los activos así como la interrupción de las actividades de la organización.	A.11.2.8	Equipo de usuario Desatendido	Los usuarios se deben asegurar de que a los equipos desantendidos se les da protección apropiada.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	El usuario no tiene claridad sobre qué proceso debería realizar con forme a lo indicado en la guía de implementación	MD	**Definido**

11.0	Seguridad Física y Medio Ambiental	A.11.2	Seguridad del Equipo	Prevenir pérdida, hurto o el compromiso de los activos así como la interrupción de las actividades de la organización.	A.11.2.9	Política de escritorio y pantalla limpios	Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	No se encuentra ninguna política creada	PNP	**Inexistente**
A.12.- Operaciones de Seguridad															
12.0	Operaciones de Seguridad	A.12.1	Procedimientos y responsabilidad	Asegurar operaciones correcta	A.12.1.1	Documentación de los procedimientos	Los procedimientos de operación se	**X**		Reglamento No. 056 – política	Direccion de sistemas	Direccion de sistemas	En la actualidad se tiene docume	MD	**Definido**

			es operacionales	s y seguras de las instalaciones de procesamiento de información		de operación	deben documentar, mantener y poner a disposición de todos los usuarios que los necesiten.			de seguridad de la información, Entrevistas y verificación de documentación			ntación para los usuarios, sin embargo, la documentación requerida para la administración de las plataformas y de los servicios no se encuentra en algunos casos actualizada y en otros es inexistente.		
12.0	Operaciones de Seguridad	A.12.1	Procedimientos y responsabilidad	Asegurar operaciones correcta	A.12.1.2	Gestión de cambios	Se deben controlar los cambios en los	**X**		Reglamento No. 056 – política	Direccion de sistemas	Direccion de sistemas	Todos los cambios que afectan	MD	**Gestionado**

			es operacionales	s y seguras de las instalaciones de procesamiento de información			sistemas e instalaciones de procesamiento de información.			de seguridad de la información, Entrevistas y verificación de documentación			de alguna manera a la información, deben pasar por el comité de cambios de la dirección, actualmente se tiene implementado un reglamento para este tipo de gestiones.		

12.0	Operaciones de Seguridad	A.12.1	Procedimientos y responsabilidades operacionales	Asegurar operaciones correctas y seguras de las instalaciones de procesamiento de información	A.12.1.3	Gestión de capacidad, Segregación de funciones	Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso inadecuado de los activos de la organización.	**X**		Entrevistas y verificación de documentación	Direccion de sistemas	Jefatura de Sistemas de información	Actualmente existe un protocolo para la debida gestión de este requerimiento, administrado por la jefatura de sistemas de información	MD	**Gestionado**
12.0	Operaciones de Seguridad	A.12.1	Procedimientos y responsabilidades	Asegurar operaciones correctas y	A.12.1.4	Separación de las instalaciones para	Las instalaciones para desarrollo, prueba y	**X**		Entrevistas y verificación de docum	Direccion de sistemas	Direccion de sistemas	Política implementada	MD	**Gestionado**

			operacionales	seguras de las instalaciones de procesamiento de información		desarrollo, prueba y producción.	producción se deben separar para reducir los riesgos de acceso no autorizado o cambios en el sistema operacional.			entación					
12.0	Operaciones de Seguridad	A.12.2	Protección contra el malware (software malicioso)	Para asegurar que las instalaciones de procesamiento de la información y de la información están protegid	A.12.2.1	Controles contra código malicioso	Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Se tienen diferentes herramientas y metodologías para la recuperación de información, administradas	MD	**Gestionado**

				os contra el malware (sofware malicioso)			con los procedimientos adecuados para concientizar a los usuarios.						principalmente por la jefatura del centro de servicios tecnológicos, no obstante las campañas que se han realizado al respecto parecen no van a ser suficientes.		
12.0	Operaciones de Seguridad	A.12.3	Respaldos	Mantener la integridad y disponibilidad de la informa	A.12.3.1	Respaldos de la Información	Se deben hacer regularmente copias de seguridad de la informaci	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Las copias de seguridad y respaldo de informa	MD	**Definido**

				ción y de las instalaciones de procesamiento de la información.			ón y del software y probarse regularmente acorde con la política de respaldo.						ción se encuentran debidamente gestionados, implementados en diferentes prioridades de acuerdo con el nivel de gestión que se requiere, de tal manera que se asigne seguridad a cada uno de los elementos requeridos.		

12.0	Operaciones de Seguridad	A.12.4	Registro y Monitoreo	Detectar actividades de procesamiento de información no autorizadas	A.12.4.1	Registros de auditoría/eventos	Se deben elaborar registros de auditoría de las actividades de los usuarios, excepciones y eventos de seguridad de la información, y se deben mantener durante un período acordado para ayudar a futuras investigaciones y en la supervisión del control	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	El control de registro se encuentra actualmente implementado en los sistemas de información que se requieren, esto conforme a lo dispuesto en la política de seguridad de la información.	MD	**Gestionado**

							de acceso.								
12.0	Operaciones de Seguridad	A.12.4	Registro y Monitoreo	Detectar actividades de procesamiento de información no autorizadas	A.12.4.2	Protección de la información de registros (logs)	Los medios de registro y la información de registro se deben proteger contra alteraciones y accesos no autorizados.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	MD	**Gestionado**
12.0	Operaciones de Seguridad	A.12.4	Registro y Monitoreo	Detectar actividades de procesamiento	A.12.4.3	Registros del administrador y el	Se deben registrar las actividades del operador	**X**		Reglamento No. 056 – política de	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especificados en	RD	**Gestionado**

				de información no autorizadas		operador	y del administrador del sistema.			seguridad de la información y Entrevistas			la política de seguridad de la universidad		
12.0	Operaciones de Seguridad	A.12.4	Registro y Monitoreo	Detectar actividades de procesamiento de información no autorizadas	A.12.4.4	Sincronización de relojes	Los relojes de todos los sitemas de procesamiento de información pertinente dentro de una organización o dominio de seguridad deben estar sincronizados con una fuente horaria	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	MD	**Gestionado**

							precisa acordada.								
12.0	Operaciones de Seguridad	A.12.5	Control de acceso al sistema operativo	Para asegurar la integridad de los sistemas operativos	A.12.5.1	Instalación del software en los sistemas operativos	Deben existir procedimientos para controlar la instalación de software en sistemas operativos.	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Procedimiento actualmente controlado con diferentes herramientas, contenidas principalmente en los dominios.	MD	**Gestionado**

12.0	Operaciones de Seguridad	A.12.6	Gestión de la vulnerabilidad técnica	Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.	A.12.6.1	Gestión de vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información usados, se debe evaluar la exposición de la organización a estas vulnerabilidades, y se deben tomar las medidas apropiadas para abordar	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Cada uno de los administradores, tiene asignado un control de alertas de cada una de las herramientas, lo que permite que en cualquier detección de vulnerabilidad ataque o riesgo se envía un correo con la detecció	MD	**Gestionado**

							el riesgo asociado.						n encontrada, conforme a la prioridad que se asigna a esta, se toma una decisión por la jefatura de infraestructura, específicamente por el área de seguridad.		
12.0	Operaciones de Seguridad	A.12.6	Gestión de la vulnerabilidad técnica	Reducir los riesgos resultantes de la explotación de las vulnera	A.12.6.2	Restricciones a la instalación de software	Se deben establecer y aplicar normas que restrinjan a los usuarios al instalar	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente existe una política que inhabilita a los usuarios	RD	**Gestionado**

				bilidades técnicas publicadas.			software no autorizados en los equipos.						realizar instalaciones no autorizadas en las estaciones d trabajo.		
12.0	Operaciones de Seguridad	A.12.7	Consideraciones de auditoría de sistemas de información	Maximizar la eficacia del proceso de auditoría de sistemas de información y minimizar la interferencia desde y hacia éste.	A.12.7.1	Controles de auditoría de sistemas de información	Los requisitos y actividades de auditoría que involucran verificaciones sobre sistemas operacionales se deben planificar y acordar cuidadosamente para minimizar el riesgo	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente se debe realizar una planeación de dicha tarea que pasa por un flujo de aprobación para su autorización.	MD	**Gestionado**

							de interrupciones en los procesos del negocio.								
A.13.- Seguridad en las Comunicaciones															
13.0	Seguridad en las Comunicaciones	A.13.1	Gestión de la seguridad de la red	Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.	A.13.1.1	Controles de Red	Las redes se deben gestionar y controlar adecuadamente, para protegerlas contra amenazas, y mantener la seguridad de los sistemas, incluyendo la información en tránsito.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Área de seguridad y telecomunicaciones	Procesos actualmente especificados en la política de seguridad de la universidad	RD	**Gestionado**

13.0	Seguridad en las Comunicaciones	A.13.1	Gestión de la seguridad de la red	Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.	A.13.1.2	Seguridad de los servicios de red	Las características de la seguridad, los niveles del servicio, y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en cualquier acuerdo de servicios de red.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Área de seguridad y telecomunicaciones	Procesos actualmente especificados en la política de seguridad de la universidad	MD	**Gestionado**
13.0	Seguridad en las Comunicaciones	A.13.1	Gestión de la seguridad de la red	Asegurar la protección de la información en las	A.13.1.3	Separación en las redes	Los grupos de servicio de información, usuarios	**X**		Reglamento No. 056 – política de segurid	Direccion de sistemas	Área de seguridad y telecomunicaciones	Procesos actualmente especificados en la	MD	**Gestionado**

				redes y la protección de la infraestructura de soporte.			y sistemas de información se deben separar en redes.			ad de la información y Entrevistas			política de seguridad de la universidad		
13.0	Seguridad en las Comunicaciones	A.13.2	Intercambio de Información	Mantener la seguridad de la información y del software intercambiado dentro de una organización y con cualquier otra entidad externa.	A.13.2.1	Políticas y procedimientos del intercambio de información	Se deben implementar políticas formales de intercambio, procedimientos y controles para proteger el intercambio de información a través del uso de cualquier tipo de recurso de	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente se tienen diferentes procesos, políticas y controles para la protección de la información. sin embargo, parte de esos elementos no se encuentran con su debida	RD	**Definido**

							comunicación.						documentación		
13.0	Seguridad en las Comunicaciones	A.13.2	Intercambio de Información	Mantener la seguridad de la información y del software intercambiado dentro de una organización y con cualquier otra entidad externa.	A.13.2.2	Acuerdos de intercambio	Se deben establecer acuerdos para el intercambio de información y de sofware entre la organización y partes externas.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Área de seguridad y telecomunicaciones	Procesos actualmente especificados en la política de seguridad de la universidad	MD	**Optimizado**
13.0	Seguridad en las Comuni	A.13.2	Intercambio de Información	Mantener la seguridad de la informa	A.13.2.3	Mensajería electrónica	La información involucrada en la	**X**		Reglamento No. 056 – política	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especific	MD	**Gestionado**

	caciones			ción y del software interca mbiado dentro de una organización y con cualquier otra entidad externa.			mensajería electrónica se debe proteger apropiadamente.			de seguridad de la información y Entrevistas			ados en la política de seguridad de la universidad		
13.0	Seguridad en las Comunicaciones	A.13.2	Intercambio de Información	Mantener la seguridad de la información y del software interca mbiado dentro de una organización y con cualquie	A.13.2.4	Los acuerdos de confidencialidad o de no divulgación	Se deben identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas Dirección de desarrollo humano	Direccion de sistemas Dirección de desarrollo humman o	Procesos actualmente especificados en la política de seguridad de la universidad	MD	**Gestionado**

				r otra entidad externa.			protección de información de la organización.								
A.14.- Adquisición, desarrollo y mantenimiento de sistemas de información															
14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.1	Requisitos de Seguridad de los Sistemas de Información	Garantizar que la seguridad es parte integral de los sistemas de información. Esto incluye, los requisitos de seguridad específicos para los sistemas de	A.14.1.1	Análisis y especificación de requisitos de seguridad	Las declaraciones de los requisitos del negocio para nuevos sistemas de información, o las mejoras a los existentes, deben especificar los requisitos para controles de	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente se maneja un flujo de aprobación, en el cual se entregan diferentes formatos y matrices con los requerimientos a suplir.	MD	**Gestionado**

				información que proporcionan servicios hacia redes públicas			seguridad.								
14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.1	Requisitos de Seguridad de los Sistemas de Información	Garantizar que la seguridad es parte integral de los sistemas de información. Esto incluye, los requisitos de seguridad específicos para los sistema	A.14.1.2	Asegurar servicios de aplicaciones en las redes públicas	la información involucrada en el Servicio de Aplicaciones que transita por redes públicas debe ser protegida ante actividades fraudolentas, disputas contractuales, y su divulgaci	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	MD	**Gestionado**

				s de información que proporcionan servicios hacia redes públicas			ón o modificación no autorizada.								
14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.1	Requisitos de Seguridad de los Sistemas de Información	Garantizar que la seguridad es parte integral de los sistemas de información. Esto incluye, los requisitos de seguridad específicos para los	A.14.1.3	Transacciones en línea (Protección en la trasferencia de Servicios)	La información implicada en transacciones en línea se debe proteger para prevenir la transmisión incompleta, la omisión de envío, la alteración no	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Procesos actualmente especificados en la política de seguridad de la universidad	RD	**Gestionado**

				sistemas de información que proporcionan servicios hacia redes públicas			autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.								
14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.2	Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software y la información del sistema de aplicaciones.	A.14.2.1	Política de Desarrollo Seguro	Se deben establecer normas o reglas básicas para desarrollo seguro de software y sistemas. Lo anterior aplica a todos los desarroll	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente existen protocolos para el desarrollo de software y de sistemas, para los desarrolladores al interior	MD	**Gestionado**

							os dentro de la organización						de la dirección.		
14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.2	Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software y la información del sistema de aplicaciones.	A.14.2.2	Procedimientos de control de cambios	La implementación de los cambios se debe controlar estrictamente mediante el uso de procedimientos formales de control de cambios.	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente se tiene un comité para la gestión y control de cambios, del mismo modo estos cambios deben cumplir con un protocolo para su ejecución.	MD	**Gestionado**

14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.2	Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software y la información del sistema de aplicaciones.	A.14.2.3	Revisión técnica de las aplicaciones después cambios del sistema operativo	Cuando se cambien los sistemas operativos, se deben revisar y poner a prueba las aplicaciones críticas del negocio para segurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Todos los administradores de plataformas y personal involucrado se involucran en el cambio a realizar y se maneja un documento de pruebas, en el cual se verifica el antes y el después del cambio realizado.	MD	**Gestionado**

14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.2	Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software y la información del sistema de aplicaciones.	A.14.2.4	Restricciones en los cambios a los paquetes de software	Se debe desalentar la realización de modificaciones a los paquetes de sofware, que se deben limitar a los cambios necesarios, y todo los cambios se deben controlar estrictamente.	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Para realizar cualquier cambio se debe tener una solicitud inicialmente se realiza la evaluación del cambio en un seguimiento de incidencias y requerimientos, posteriormente de no haber ninguna otra alternativa se procede a	MD	**Gestionado**

													realizar el cambio el cual pasa por un proceso de documentación antes de su desarrollo.		
14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.2	Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software y la información del sistema de aplicaciones.	A.14.2.5	Procedimientos de desarrollo de sistemas	Se deben establecer procedimientos de desarrollo seguro, los cuales deben ser documentados, mantenidos y aplicados a cualquier sistema de	**x**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Actualmente se maneja un flujo de aprobación, en el cual se entregan diferentes formatos y matrices con los requerimientos	MD	**Definido**

							información que implique desarrollo.						a suplir por el desarrollo del sistema.		
14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.2	Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software y la información del sistema de aplicaciones.	A.14.2.6	Desarrollo de un entorno Seguro	Se deben establecer y proteger adecuadamente un entorno seguro para el desarrollo del sistema y los esfuerzos de integración que cubre todo el ciclo de vida del desarrollo de sistemas.	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Se tienen establecidos procesos para el desarrollo seguro con el fin de proteger adecuadamente los ambientes de desarrollo.	MD	**Gestionado**

14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.2	Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software y la información del sistema de aplicaciones.	A.14.2.7	Desarrollo externo de software	El desarrollo de software contratado externamente debe ser supervisado y la organización debe monitorear esto.	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Se tienen establecidos procesos para el desarrollo seguro con el fin de proteger adecuadamente los ambientes de desarrollo.	MD	**Gestionado**
14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.2	Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software y la información del sistema de aplicaciones.	A.14.2.8	Pruebas de Seguridad	Se deben realizar pruebas de Seguridad funcionales durante el desarrollo del software.	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Cada uno de los programas servicios que no se encuentran en el ambiente de producción,	D	**Optimizado**

													pasan al menos por tres pruebas antes de salir a producción, sin contar que el desarrollador debe realizar un documento con cada una de las pruebas realizadas de la funcionalidad.		
14.0	Adquisición, desarrollo y mantenimiento de	A.14.2	Seguridad en los procesos de desarrollo y soporte	Mantener la seguridad del software y la informa	A.14.2.9	Aceptación del sistema	Se debe establecer criterios de aceptación para los sitemas	**X**		Reglamento No. 056 – política de segurid	Direccion de sistemas	Direccion de sistemas	Se lleva a cabo un documento de pruebas que se	D	**Gestionado**

	sistemas de información			ción del sistema de aplicaciones.			de información nuevos, actualizaciones y nuevas versiones.			ad de la información y Entrevistas			deben ejecutar en un ambiente de pruebas para confirmar el correcto funcionamiento de los nuevos sistemas o las actualizaciones.		
14.0	Adquisición, desarrollo y mantenimiento de sistemas de información	A.14.3	Datos de Prueba	garantizar la protección de datos que se utiliza para las pruebas	A.14.3.1	Protección de los datos de prueba	Los datos de prueba deben ser protegidos, controlados y seleccionados cuidadosamente.	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Se debería realizar verificación ya que actualmente este control se cumple parcialmente.	RD	**Definido**

A.15.- Seguridad en relación con los proveedores															
16.0	Seguridad en relación con los proveedores	A.15.1	Seguridad en las relaciones con proveedores	Garantizar la protección de la información de la organización que sea accesible por los proveedores.	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	Se deben identificar los requisitos de seguridad de la inforamción para la mitigación de los riesgos asociados al acceso de proveedores o partes externas a la información o el procesamiento de la información de la organización para los procesos	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Estos controles se llevan a cabo en la actualidad, los proveedores solo acceden a los servicios y a la información estrictamente necesaria.	D	**Optimizado**

							de negocio, y se deben implementar controles apropiados antes de otorgar el acceso.								
16.0	Seguridad en relación con los proveedores	A.15.1	Seguridad en las relaciones con proveedores	garantizar la protección de la información de la organización que sea accesible por los proveedores.	A.15.1.2	Tener en cuenta la seguridad en los acuerdos con terceras partes	Los acuerdos con terceras partes que involucren acceso, procesamiento, comunicación o gestión de la información de la organización o de las instalacio	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Estos controles se llevan a cabo en la actualidad, los proveedores solo acceden a los servicios y a la información estrictamente	D	**Optimizado**

							nes de procesamiento de información, o el agregado de productos o servicios a las instalaciones de procesamiento de información, deben cubrir todos los requisitos de seguridad pertinentes.						necesaria.		
16.0	Seguridad en relación con los proveedores	A.15.1	Seguridad en las relaciones con proveedores	garantizar la protección de la información de la	A.15.1.3	Cadena de suministro de las TIC	Los acuerdos con los proveedores de servicios deben	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Con todos los proveedores se realiza un	MD	**Gestionado**

				organización que sea accesible por los proveedores.			incluir los requisitos de seguridad asociados al tratamiento de la información, servicios de comunicaciones y tecnología de suministro.						proceso de seguimiento en conformidad con los niveles de servicios definidos en el contrato para realizar seguimiento y revisión de los servicios adquiridos.		
16.0	Seguridad en relación con los proveedores	A.15.2	Gestión de la prestación de servicios	Mantener un nivel convenido de seguridad de la información y la prestaci	A.15.2.1	Monitoreo y revisión de los servicios de proveedores o terceras partes.	La organización debe supervisar periódicamente, revisar y auditar la entrega	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Con todos los proveedores se realiza un proceso de seguimi	MD	**Gestionado**

				ón de servicios en línea con los acuerdos con proveedores.			del servicio del proveedor.						ento en conformidad con los niveles de servicios definidos en el contrato para realizar seguimiento y revisión de los servicios adquiridos.		
16.0	Seguridad en relación con los proveedores	A.15.2	Gestión de la prestación de servicios	Mantener un nivel convenido de seguridad de la información y la prestación de servicios en	A.15.2.2	Gestión de cambios en los servicios a proveedores o terceras partes.	Los cambios a la prestación del servicio, incluyendo mantenimiento y mejora de las políticas	**X**		Entrevistas	Direccion de sistemas	Direccion de sistemas	Con todos los proveedores se realiza un proceso de seguimiento en conformidad con	MD	**Gestionado**

				línea con los acuerdos con proveedores.			existentes de la seguridad de la información, procedimientos y controles, se deben gestionar tomando en cuenta la importancia de los sitemas y procesos de negocio que impliquen una nueva valoración de riesgo.						los niveles de servicios definidos en el contrato para realizar seguimiento y revisión de los servicios adquiridos.		
A.16.- Gestión de incidentes de seguridad de información															

16.0	Gestión de incidentes de seguridad de información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación en los eventos de seguridad y debilidades.	A.16.1.1	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.	**X**		Documentación y entrevistas	Direccion de sistemas	Direccion de sistemas	Política estructurada en el catálogo de servicios de la universidad de la sabana, del mismo modo para los diferentes entornos se tienen establecidas las responsabilidades y procedimientos de gestión que asegura	MD	**Gestionado**

													n una respuesta rápida eficaz y ordenada.		
16.0	Gestión de incidentes de seguridad de información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación en los eventos de seguridad y debilidades.	A.16.1.2	Informe de eventos de seguridad de la información	Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, lo más rápidamente posible.	**X**		Documentación y entrevistas	Direccion de sistemas	Direccion de sistemas	Paca cada caso se han dispuesto diferentes canales de comunicación, entre los cuales se encuentra extensiones, correo electrónico, teléfonos corporat	MD	**Gestionado**

													ivos etc…		
16.0	Gestión de incidentes de seguridad de información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación en los eventos de seguridad y debilidades.	A.16.1.3	Informe de las debilidades de seguridad	Se deben requerir a todos los empleados, contratistas y usuarios por tercera parte, de sistemas y servicios de información, que observen e informen cualquier debilidad en la seguridad de sistemas o	**X**		Documentación y entrevistas	Direccion de sistemas	Direccion de sistemas	Paca cada caso se han dispuesto diferentes canales de comunicación y se a mencionado al interior de los contratos con terceros y comunicados para empleados que informe	MD	**Gestionado**

							servicios, observada o que se sospeche.						n cualquier debilidad o anomalía que puedan llegar a encontrar.		
16.0	Gestión de incidentes de seguridad de información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluidos los de comunicación en los eventos	A.16.1.4	Evaluación y decisión respecto a los eventos de seguridad de la información	Se debe evaluar y decidir si los eventos de seguridad de la información son clasificados como incidentes de seguridad de la información.	**X**		Documentación y entrevistas	Direccion de sistemas	Direccion de sistemas	Política estructurada en el catálogo de servicios de la universidad de la sabana, del mismo modo para los diferentes entornos se tienen	MD	**Gestionado**

				de seguridad y debilidades.									establecidas las responsabilidades y procedimientos de gestión que aseguran una respuesta rápida eficaz y ordenada.		
16.0	Gestión de incidentes de seguridad de información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información,	A.16.1.5	Respuesta a los incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos	**X**		Documentación y entrevistas	Direccion de sistemas	Direccion de sistemas	Política estructurada en el catálogo de servicios de la universidad de la sabana, del mismo modo	MD	**Gestionado**

				incluidos los de comunicación en los eventos de seguridad y debilidades.			documentados.						para los diferentes entornos se tienen establecidas las responsabilidades y procedimientos de gestión que aseguran una respuesta rápida eficaz y ordenada.		
16.0	Gestión de incidentes de seguridad de información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la	Garantizar un enfoque coherente y eficaz para la gestión de	A.16.1.6	Aprendiendo de los incidentes de seguridad de la información	Se deben implementar mecanismos para posibilitar que los tipos, volúmene	**X**		Documentación y entrevistas	Direccion de sistemas	Direccion de sistemas	Existe una documentación, de cada uno de los incidentes	MD	**Definido**

			información	incidentes de seguridad de la información, incluidos los de comunicación en los eventos de seguridad y debilidades.			s y costos de los incidentes de seguridad de la información sean cuantificados y se les haga seguimiento.						presentados y sus costos, sin embargo, esta información no es validada y no se encuentra actualizada		
16.0	Gestión de incidentes de seguridad de información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información,	A.16.1.7	Recolección de evidencia	Cuando una acción de seguimiento contra una persona u organización después de un incidente de seguridad	**X**		Documentación y entrevistas	Dirección de desarrollo humano Direccion de sistemas	Direccion de sistemas	Ante cualquier anomalía que se pueda llegar a presentar, es desarrollo humano quien se encarga de	MD	**Gestionado**

				incluidos los de comunicación en los eventos de seguridad y debilidades.			de la información involucra acciones legales (ya sea civiles o penales), la evidencia se debe recolectar, retener y presentar la forma tal de cumplir con las reglas para las evidencias establecidas en la jurisdicción.						realizar los requerimientos de información para que se pueda realizar una recolección y evaluación.		
A.17.- Seguridad de la información en Continuidad del Negocio															

17.0	Gestión de la Seguridad de la Información en Continuidad de Negocios	A.17.1	Continuidad en la seguridad de la información	Información sobre la continuidad de seguridad debe estar integrada en la gestión de la continuidad del negocio de la organización (BCM) para garantizar la protección de la información en cualquier momento y de anticipa	A.17.1.1	Información de planificación de continuidad de seguridad	La organización debe determinar sus necesidades de seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	**X**		Documentación y entrevistas	Direccion de sistemas	Direccion de sistemas	Control actualmente incluido en el proceso de gestión de continuidad del negocio, proceso que se tienen en cuenta para cada uno de los sistemas de información.	MD	**Gestionado**

				rse a los sucesos adverso s											
17.0	Gestión de la Seguridad de la Información en Continuidad de Negocios	A.17.1	Continuidad en la seguridad de la información	Información sobre la continuidad de seguridad debe estar integrada en la gestión de la continuidad del negocio de la organización (BCM) para garantizar la protecci	A.17.1.2	Desarrollo e implementación de planes de continuidad que incluyen seguridad de la información	Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información al nivel requerido y en las escalas de	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Proceso especificado en la política de seguridad de la universidad, sim embargo, no se tiene documentación respecto a algunos procesos de importancia para la gestión.	MD	**Gestionado**

				ón de la información en cualquier momento y de anticiparse a los sucesos adversos			tiempo requeridas después de la interrupción o falla de los procesos críticos del negocio.								
17.0	Gestión de la Seguridad de la Información en Continuidad de Negocios	A.17.1	Continuidad en la seguridad de la información	Información sobre la continuidad de seguridad debe estar integrada en la gestión de la continuidad del negocio de la organización (BCM)	A.17.1.3	Pruebas, mantenimiento, reevaluación y continuidade la seguridad de la información	Los planes de continuidad del negocio se deben poner a prueba y actualizar regularmente para asegurar que están actualizados y son eficaces.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Proceso especificado en la política de seguridad de la universidad.	MD	**Gestionado**

				para garantizar la protección de la información en cualquier momento y de anticiparse a los sucesos adversos											
17.0	Gestión de la Seguridad de la Información en Continuidad de Negocios	A.17.2	Redundancia (Centro procesamiendo de datos)	Asegurar la disponibilidad de instalaciones de procesamiento de información.	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	Las instalaciones de procesamiento de información deben contar con redundancia suficiente para satisfacer los requisitos	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Las instalaciones de procesamiento de información actualmente cuentan con redundancia suficiente para	MD	**Gestionado**

							de disponibilidad						satisfacer los requisitos de disponibilidad		
A.18.- Cumplimiento Regulatorio															
18.0	Cumplimiento Regulatorio	A.18.1	Revisiones de seguridad de información	Garantizar que la seguridad de la información sea implementada y opere de acuerdo con la políticas y procedimientos de la organización	A.18.1.1	Revisión independiente de la seguridad de la información	Se debe revisar el enfoque de la organización para la gestión de la Seguridad de la Información y su aplicación (Objetivos de control, controles, políticas, procedimientos, procesos, entre otros) de forma	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Proceso especificado en la política de seguridad de la universidad.	RD	**Gestionado**

							independiente y en intervalos de tiempo planificados o cuando existan cambios significativos.								
18.0	Cumplimiento Regulatorio	A.18.1	Revisiones de seguridad de información	Garantizar que la seguridad de la información sea implementada y opere de acuerdo con la políticas y procedimientos de la organización	A.18.1.2	Cumplimiento con las políticas y normas de seguridad	Los gerentes deben asegurar que todos los procedimientos de seguridad que están dentro de su área de responsabilidad se realicen correctamente para lograr el	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Proceso especificado en la política de seguridad de la universidad.	RD	**Gestionado**

							cumplimiento de las políticas y normas de seguridad.								
18.0	Cumplimiento Regulatorio	A.18.1	Revisiones de seguridad de información	Garantizar que la seguridad de la información sea implementada y opere de acuerdo con la políticas y procedimientos de la organización	A.18.1.3	Revisión del cumplomiento técnico	Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normad de seguridad de la información	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Proceso especificado en la política de seguridad de la universidad.	MD	**Gestionado**

18.0	Cumplimiento Regulatorio	A.18.2	Cumplimiento de los requisitos legales y contractuales	Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de los requisitos de seguridad.	A.18.2.1	Identificación de la legislación aplicable y los requisitos contractuales	Todos los requisitos estautarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente, y mantenerlos actualizados para cada sistema de información y para la	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Proceso especificado en la política de seguridad de la universidad.	MD	**Gestionado**

							organización.								
18.0	Cumplimiento Regulatorio	A.18.2	Cumplimiento de los requisitos legales y contractuales	Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de los requisit	A.18.2.2	Derechos de propiedad intelectual (DPI)	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales sobre el uso de material con respecto	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Proceso especificado en la política de seguridad de la universidad.	MD	**Gestionado**

				os de seguridad.			al cual puede haber derechos de propiedad intelectual, y sobre el uso de productos de software patentados.								
18.0	Cumplimiento Regulatorio	A.18.2	Cumplimiento de los requisitos legales y contractuales	Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas	A.18.2.3	Protección de la información documentada	Los registros importantes se deben proteger contra pérdida,destrucción y falsificación, de acuerdo con los requisitos estatutari	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Proceso especificado en la política de seguridad de la universidad.	MD	**Gestionado**

				con la seguridad de la información y de los requisitos de seguridad.			os, regulatorios, contractuales y del negocio.								
18.0	Cumplimiento Regulatorio	A.18.2	Cumplimiento de los requisitos legales y contractuales	Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de los	A.18.2.4	Protección de los datos y privacidad de la información personal	Se debe asegurar la protección y privacidad de los datos, como se exige en la legislación, regulaciones, y si es aplicable, cláusulas contractuales	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	Proceso especificado en la política de seguridad de la universidad y la politica de habeas data	D	**Optimizado**

				requisitos de seguridad.			pertinentes.								
18.0	Cumplimiento Regulatorio	A.18.2	Cumplimiento de los requisitos legales y contractuales	Evitar el incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relacionadas con la seguridad de la información y de los requisitos de seguridad.	A.18.2.5	Regulación de controles criptográficos	Se deben utilizar controles criptográficos que cumplan con todos los acuerdos, leyes y regulaciones pertinentes.	**X**		Reglamento No. 056 – política de seguridad de la información y Entrevistas	Direccion de sistemas	Direccion de sistemas	De conformidad con la ley se tienen diferentes herramientas que cumplen con el requerimiento de la dirección de sistemas, sin embargo, no se tiene claridad del uso actual, por lo	RD	**Repetible**

													que se debe rediseñar y documentar.		