UNIVERSIDAD NACIONAL
SANTIAGO ANTÚNEZ DE MAYOLO
FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL
INGENIERÍA DE SISTEMAS E INFORMÁTICA

"GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS DE LA UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, 2017"

TESIS
PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS E INFORMÁTICA

PRESENTADO POR:

Bach. Roberto Elías BRITO RODRÍGUEZ

ASESOR

Ing° Luis Ruperto Alvarado Cáceres

HUARAZ – PERÚ
2019

DEDICATORIAS

Dedico estas líneas de investigación, primero a Dios por haberme brindado salud, por darme la familia que tengo y por un día más de vida.

A mis queridos padres: Elías y Enedina que con mucho esmero inspiraron en mis los sentimientos más puros de amor al trabajo. A mi hermana Mariza, porque con su ejemplo y comprensión ha alentado mi esfuerzo, y a una persona muy especial en mi vida, Almendra que con paciencia y amor alienta mi superación

A todos los que alguna vez perdieron algo: la salud, la libertad, la ilusión, o a alguien especial, pero que a pesar de todo siguen luchando en la vida.

A mis docentes, en especial a mi asesor, que han sido una guía e inspiración profesional.

A mis amigos, porque a pesar de las circunstancias adversas siempre están ahí.

Roberto Brito R.

AGRADECIMIENTOS

Quiero agradecer de manera especial y sincera al magíster Luis Alvarado Cáceres por acceder y aceptar realizar esta tesis bajo su orientación, su soporte y confianza en mis conocimientos y habilidades. Su vasta experiencia ha permitido guiar mis capacidades, para el desarrollo de mi formación profesional.

Agradecer al Mg. Eddy Jesús Montañez Muñoz, que, con sus principios enmarcados en su formación y rigor, ha determinado y guiado un buen trabajo de investigación. Al Lic. Carlos Alva Jauregui por su motivación y su gran contribución a la tesis.

A mi alma mater la Universidad Nacional Santiago Antúnez de Mayolo y a todos los catedráticos de la escuela profesional de Ingeniería de Sistemas e Informática por contribuir con mi formación profesional.

También quiero expresar mi más sincero agradecimiento al Mg. Erick Giovani Flores Chacón, por su importante asesoría en el perfeccionamiento de esta tesis. Quiero destacar, por encima de todo su visión sistémica para revisar el trabajo de investigación

PRESENTACIÓN

Señores miembros del Jurado, en cumplimiento con el Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniería de Sistemas e Informática, de la Facultad de Ciencias, de la Universidad Nacional Santiago Antúnez de Mayolo, presento ante ustedes la tesis, titulada *"Gestión de Incidentes de la Seguridad de la Información en la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo, 2017"*. este trabajo de investigación para optar por el título profesional, ha sido desarrollado en la Facultad de Ciencias buscando establecer los controles de seguridad a través del diseño de un modelo de Gestión de Incidentes de Seguridad de la Información, basado en el estándar ISO/IEC 27000. Estos controles buscan garantizar la confidencialidad, integridad y disponibilidad de la información y la utilización de los recursos tecnológicos de manera óptima a través de normas de seguridad y protocolos de atención de incidentes de seguridad.

La seguridad de información en la Facultad de Ciencias es un lineamiento de política nacional como lo describe el Plan de Desarrollo de la Sociedad de la Información en el Perú, este documento establece la necesidad de promover una administración pública de calidad orientada a la población, y la necesidad de contar con una Estrategia Nacional de Seguridad de la Información, con el objetivo de controlar los Incidentes de Seguridad de la Información en los recursos de información y recursos informáticos valiosos para el estado.

El modelo planteado de Gestión de Incidentes de la Seguridad de la Información nos permitirá controlar de manera eficaz los riesgos y vulnerabilidades encontrados en los activos de información de la facultad de ciencias, a partir de los reportes y registros se determinaran los procedimientos para la eliminación y control exitoso de los incidentes, esto nos permitirá salvaguardar los recursos informáticos y activos de información, teniendo como base metodológica la familia ISO/IEC 27000 y la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 que describe claramente el contenido de las etapas en que se estructura el proceso de preparación, planificación, diseño y ejecución de los instrumentos de control.

En el trabajo de investigación se realizó el diagnóstico actual de la seguridad de la información, para determinar los riesgos inherentes de los activos de información, la valoración de los controles y los riesgos residuales; todo esto nos permitió generar instrumentos de análisis. Se estudiaron y analizaron los riesgos y vulnerabilidades identificados en los activos de información y recursos tecnológicos de las oficinas de la facultad, con el fin de establecer los controles de seguridad en la Facultad de Ciencias, estos controles están orientados al diseño de políticas y normas de seguridad de la información, para reducir los incidentes informáticos, cumplir con la legislación vigente de protección de datos y servicios administrativos de la sociedad de la información, transacción electrónica, propiedad intelectual y en general aquella relacionada con la seguridad de la información valiosa para la Facultad de Ciencias.

HOJA DE VISTO BUENO

Ing. Eddy Jesús Montañez Muñoz
Presidente

Ing. Erick Flores Chacón
Secretario

Ing. Luis Ruperto Alvarado Cáceres
Vocal

RESUMEN

El presente trabajo de investigación, tiene como objetivo principal establecer controles de seguridad de la información en la Facultad de Ciencias, empleando un modelo de gestión de incidentes basada en la norma ISO/IEC 27000, sobre el análisis de las condiciones actuales de seguridad de la información.

Para realizar un análisis exhaustivo de las condiciones de seguridad de la información y la realidad problemática en la Facultad de Ciencias se logró el compromiso de las autoridades para brindar las facilidades de acceso a la información y a los procesos y procedimientos en la institución, esto, no solo por ser un punto contemplado en el estándar ISO/IEC 27000, sino por el acceso que se requiere para realizar el análisis de los activos de información y la planificación sinérgica de todas las áreas de la facultad en favor del Proyecto de investigación, ello nos permitió sentar las bases del trabajo de investigación.

Sentadas las bases del trabajo de investigación se iniciaron los trabajos de recopilación de datos y el análisis de los problemas relacionados con los incidentes de seguridad de los activos de información, ejecutar la auditoría interna o análisis GAP, y con esto, definir los requerimientos del trabajo de investigación, además de ello se aplicó una metodología de evaluación de riesgos apropiada para la facultad, según las necesidades y criterios de aceptación de riesgos.

Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente, pero el estándar ISO 27000 no impone ninguna, aunque especifica que la metodología empleada debe ser coherente con la complejidad y los niveles de protección, para ello, se realizó el inventario de activos y consecutivamente se identificaron las amenazas y vulnerabilidades inherentes a cada activo de información para rastrear los impactos que podrían ocasionar una pérdida de la confidencialidad, la integridad y la disponibilidad en los activos de información.

Para realizar un análisis de la seguridad de la información más exacto en la Facultad de Ciencias se utilizaron herramientas que nos permitieron evaluar los impactos y la posibilidad de que se produzcan, los fallos de seguridad de la información se analizaron en función a las amenazas, vulnerabilidades y los controles no implantados, de esta manera evaluar con exactitud los niveles de riesgo para determinar si este es aceptable o requiere tratamiento, todo ello usando los criterios de aceptación de riesgos establecidos por la norma ISO/IEC 27001.

Para Finalizar se realizó una selección de controles de la Norma ISO 27000, estos controles delimitaron la declaración de aplicabilidad y el sustento de su selección, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento de los incidentes de la seguridad de la información producidos en la Facultad de Ciencias.

ABSTRACT

The present research work is based on the application of the ISO / IEC 27000 standard and analysis of the current conditions of the science faculty for the management of information security incidents to achieve the administrator of the optimal way the resources of Information and computer resources.

For an exhaustive analysis of the problematic reality in the faculty of sciences, the foundations were laid down on which a project of this type is initiated, such as the clear and determined support of the institution's management, not only because it is a point contemplated in The standard required, but rather because of the access required to perform the information assets analysis and the synergistic planning of all areas of the institution. This allowed us to define the scope of the incident management system and the security policy that included the General framework and safety objectives in the faculty of science, having legal and contractual requirements regarding information security. All this is reflected in the statement of the problem, the hypothesis and the objectives drawn by the research work.

It began with the analysis of the problems related to the security of the information assets, the internal audit or GAP analysis to meet the requirements of the research work, in addition an appropriate risk assessment methodology was defined for the institution, according to The need and risk acceptance criteria, there are many internationally accepted risk assessment

methodologies, but the standard does not impose any but specifies that the methodology used should be consistent with the complexity and levels of protection, in this research work was taken As a reference the Magerit version 3.0 methodology, for this the inventory of assets was carried out and the threats and vulnerabilities inherent to each information asset were identified in order to identify the impacts that could lead to a loss of confidentiality, integrity and availability in each one of one The assets.

In order to make a more specialized analysis, the impacts and the realistic possibility of their occurrence, the security failure based on the threats and vulnerabilities, the impacts associated with these assets, and the controls currently in place were evaluated, thus estimating the Levels of risk to determine if the risk is acceptable or requires treatment using the risk acceptance criteria established by ISO / IEC 27001.

Finally, the controls for a declaration of applicability were called SOA Statement of Applicability which is a list of all the selected controls and the reason for their selection, in short, a summary of the decisions taken regarding the treatment of the incidents of the Security of information produced in the Faculty of Sciences.

ÍNDICE GENERAL

CAPÍTULO I

GENERALIDADES

En un mundo globalizado donde se viene desarrollando la cuarta revolución industrial, la información ha adquirido vital importancia, este activo se ha convertido en el más valioso activo para los gobiernos e industrias en el mundo, la cantidad de información generada por las actividades públicas y privadas proporcionan grandes conjuntos de datos, requeridos por nuevos servicios. Según estima la International Data Corporation - ICD (International Data Corporation, 2018) hoy los datos trascendentes se incrementan un 50 % al año, y se duplican cada dos años. El informe del Foro Económico Mundial (FORO ECONÓMICO MUNDIAL , 2017) declaró que los datos constituyen una nueva clase de activo económico, que sustentan las bases de datos y las redes de telecomunicaciones, que se han convertido en un servicio público como las redes sanitarias y las redes eléctricas. Los servicios de información, los sistemas de información y los servicios informáticos que existen, son factores esenciales para el desarrollo económico y social en el mundo, por ello es imprescindible gestionar de manera adecuada los incidentes de seguridad de la información.

1.1. REALIDAD PROBLEMÁTICA

La seguridad de la información es un lineamiento de Política Nacional como lo describe el “Plan de Desarrollo de la Sociedad de la Información en el Perú” –“La Agenda Digital Peruana 2.0” (Jaime Reyes Miranda, Juan Pacheco Romaní, 2005) que establecen la necesidad de promover una administración pública de calidad orientada a la población, y la necesidad de contar con una Estrategia Nacional de Seguridad Informática, con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente con los recursos informáticos y afectar la información valiosa para las instituciones públicas.

En la Universidad Nacional Santiago Antúnez de Mayolo estos sistemas de información, bases de datos y las redes de telecomunicaciones sirven para alcanzar un servicio con las mismas oportunidades de acceso de información y una democratización digital que contribuye con la necesidad de originar una administración pública de calidad, pero es importante recordar que todos estos activos informáticos y activos de información se encuentren expuestos a riesgos e incidentes que amenazan la seguridad, y el normal funcionamiento de los sistemas de información que dan soporte a las actividades económicas, productivas y administrativas de la institución.

Es importante entender el valor económico de la información y realizar políticas de gobierno en la Facultad de Ciencias para el tratamiento y protección de estos activos y de los sistemas de información que son

susceptibles a ataques e intrusión procedentes de una amplia diversidad de fuentes, incluyendo fraudes, simulaciones, espionaje, sabotaje, deterioro, vandalismo, incendios o inundaciones; también fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios los cuales se están volviendo cada vez más comunes, ambiciosos y sofisticados, es por ello que a lo largo de esta investigación se entenderán los aspectos necesarios a considerar para poder controlar los Incidentes de la Seguridad de la Información en la Facultad de Ciencias de la UNASAM, se abarcarán actividades desde los primeros pasos a realizar como la contextualización de la realidad en la facultad, teniendo en cuenta la definición de una serie de criterios y análisis de la organización, así también se realizará la idónea evaluación y tratamiento de riesgos para brindar los lineamientos adecuados para asegurar los activos de información en la Facultad de Ciencias.

Por ello la Facultad de Ciencias de la Universidad Santiago Antúnez de Mayolo como ente de administración pública que genera información valiosa para la Oficina General de Estudios de la UNASAM, debe ser capaz de manejar y utilizar los recursos tecnológicos bajo políticas de seguridad, ya que esto asegurará que la Universidad tenga la capacidad para controlar y minimizar los efectos negativos que puedan verse reflejados en los datos e información importante que se genera, como actas, notas académicas, silabus, resoluciones de grados y títulos,

resoluciones de sustentación de tesis, oficios y activos informáticos importantes para el normal desarrollo de sus actividades, por ello es importante establecer controles a los repositorios de información y mitigar el uso inapropiado y desorganizado de los recursos informáticos ya que esto genera que los recursos informáticos sean infectados con malware y sufran un deterioro acelerado y una inadecuada utilización por parte de los usuarios, convirtiéndose en herramientas ineficientes para el normal desarrollo de las actividades, además de ello es importante mitigar problemas de acceso no autorizado a información valiosa y documentos de gran interés institucional, todos los usuarios tienen acceso a los archivadores que contienen documentación importante para la Facultad de Ciencias, esto genera la perdida de documentos de interés o maltrato de los mismos, generando la denegación de servicio por perdida de documentos y ausencia de respaldos digitales, por otro lado es importante delimitar el acceso no autorizado a sistemas administrativos que generan divulgación de información sensible, instalación de software hostil que genera desaparición de información, lentitud en los sistemas informáticos, saturación del sistema y mal funcionamiento de los programas de uso administrativo en la facultad. Por todo lo descrito es necesario controlar los incidentes de seguridad de la información, de manera estandarizada a través de un modelo de Gestión de Incidentes de Seguridad de la Información (SGISI), según el estándar internacional ISO/IEC 27000, con el propósito de proteger los activos de información, y de esta manera dar

un tratamiento a los riesgos e incidentes de información presentes en los procesos y actividades de nuestra facultad.

Esto se logra implementando un conjunto de controles, como políticas de seguridad de la información, buenas prácticas en seguridad de la información, procedimientos normalizados, generación de estructuras organizativas y delimitación de funciones de software y hardware.

Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, para asegurar que cumplan los objetivos específicos de eliminación de incidentes de seguridad, todo esto bajo el contexto de la coyuntura presupuestaria que atraviesa el sector público, que nos obliga a optimizar los recursos informáticos y activos de información, buscando permanentemente la mayor calidad, eficacia y eficiencia en la administración de los mismos, ya que sabemos que la información es un valioso activo, por ello controlar los incidentes que afecten su probidad dependerá del buen funcionamiento de una organización, mantener su integridad, confidencialidad y disponibilidad es esencial para alcanzar los objetivos planteados y se definan los requerimientos necesarios para el desarrollo e implementación de futuros Sistemas Informáticos, seguros y bajo políticas de seguridad que precisen claramente los protocolos y estándares de seguridad a cumplir.

1.2. ENUNCIADO DEL PROBLEMA

¿De qué manera con la Gestión de Incidentes, se establecerán los Controles de Seguridad de la Información en la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo?

1.3. HIPÓTESIS

1.3.1. HIPÓTESIS GENERAL

Con la Gestión de Incidentes se establecerán los Controles de Seguridad de la Información en la Facultad de Ciencias de la UNASAM.

1.3.2. HIPÓTESIS ESPECÍFICAS

A. Con el diagnóstico y análisis GAP se determinará la brecha de seguridad de la información en la Facultad de Ciencias.

B. Con el diagnóstico de los riesgos inherentes se determinará el impacto y los niveles de riesgo de los activos de información de la Facultad de Ciencias.

C. Con el análisis de valoración de los controles de seguridad de la información se determinará el desplazamiento del mapa de riesgo.

1.4. OBJETIVOS

1.4.1. Objetivo General

Diseñar la Gestión de Incidentes para establecer los controles de Seguridad de la Información en la Facultad de Ciencias de la UNASAM.

1.4.2. Objetivos Específicos

D. Elaborar el diagnóstico y análisis GAP para determinar la brecha de seguridad de la información en la Facultad de Ciencias.

E. Elaborar el diagnóstico de los riesgos inherentes para determinar el impacto y los niveles de riesgo de los activos de información de la Facultad de Ciencias.

F. Elaborar el análisis de valoración de los controles de seguridad de la información para determinar el desplazamiento del mapa de riesgo.

1.5. JUSTIFICACIÓN

El desarrollo de la investigación se justifica en la búsqueda de la aplicación de metodologías y teorías de Seguridad de la Información para lograr establecer un modelo de Gestión de Incidentes de Seguridad de la Información para controlar, los sucesos críticos que afectan los activos de información y recursos informáticos de la Facultad de Ciencias de la UNASAM, surgen las necesidades de la estandarización de metodologías y modelos de análisis en términos de SGSI. Es decir, se tiene que abandonar la aplicación de técnicas y buenas prácticas en forma empírica a favor de un proceso formal y disciplinado, que esté definido por reglas, que resulte predecible y provea una adecuada integridad, disponibilidad y confidencialidad de los datos del stakeholders, además es necesario hacer un estudio sobre el desarrollo de los SGISI para dar solución a la naturaleza caótica de la información dentro de la Facultad de Ciencias.

De acuerdo con los objetivos de la investigación, el resultado nos permitirá encontrar soluciones concretas para controlar los incidentes que atentan la seguridad de la información y activos informáticos en la Facultad de Ciencias, de esta manera ampliar, complementar o modificar los conocimientos teóricos de acuerdo a la realidad contextual del problema.

1.5.1. JUSTIFICACIÓN ECONÓMICA

Desde el punto de vista económico, el proyecto de investigación, es justificada porque busca:

A. En términos claves, orientar a la modernización de la Seguridad de la Información de la Facultad de Ciencias a través de establecer los controles para reducir los costos administrativos de mantenimiento y corrección de datos.

B. Orientar a la Facultad de Ciencias a decidir donde gastar y cuanto gastar en mantenimiento de las TIC, teniendo en consideración los reportes de incidentes a base de los controles de seguridad de la institución. Así como establecer nuevas fuentes de prevención para reducir gastos.

C. Desde el ámbito de investigación, el estudio es viable en términos económicos, ya que se realizará un estudio de campo, donde primará la recopilación de información sobre procesos que manejan datos importantes para la Facultad de Ciencias, teniendo en cuenta los fenómenos que podrían afectar estos activos hasta llegar a la fase de desarrollo de los controles de seguridad.

1.5.2. JUSTIFICACIÓN OPERATIVA

Desde el punto de vista operativo, es justificada porque busca:

A. Mejorar la gestión de los servicios informáticos en la institución en términos de seguridad a través de la elaboración de controles.

B. Orientar el desarrollo de los proyectos TIC en la institución para la constitución del gobierno electrónico con los protocolos y controles de seguridad de la información promovido por el estado.

C. Orientar las actividades informáticas de la Facultad en el marco del plan Nacional al 2021 y sus actualizaciones del Estado.

D. Lograr que la relación Facultad– Estudiante – Docente – Ciudadano, sea directa, transparente, segura y más exigente en términos de tiempo, dado que las tecnologías de información permitan que cada stakeholders participe activa, cercana e inmediatamente en la construcción de los controles de seguridad a través de las políticas de seguridad de la información.

E. Permitirá que la revolución digital que plantea un reto a la capacidad de respuesta gubernamental ante la creciente demanda estudiantil sea más segura, productiva y duradera. Debido a que el estudiante pasivo es un concepto pasado. Por ende, la administración de la información en la Facultad de Ciencias tendrá que enfrentar nuevas formas de participación académica en la toma decisiones y deberá tener listos los canales para darles un seguimiento exitoso.

1.5.3. JUSTIFICACIÓN TECNOLÓGICA

Desde el punto de vista Tecnológico, es justificada porque busca:

A. Establecer controles para el desarrollo de software, ser un enlace y concordancia entre las tecnologías estructuradas y tecnologías de objetos para el desarrollo de proyectos de software referidos a la seguridad de la información y seguridad de las tecnologías de información en la Facultad de Ciencias.

B. Incrementar sustancialmente la infraestructura de control de seguridad de las tecnologías de información de la institución.

C. Analizar las últimas tecnologías en control de seguridad de la información que han permitido que más personas y empresas accedan a tener sistemas controlados y seguros con menores costos

1.5.4. JUSTIFICACIÓN SOCIAL

Desde el punto de vista Social, es justificada porque busca:

A. Concientizar a la comunidad santiaguina, a la población profesional y a los alumnos de la Facultad de Ciencias sobre la influencia que tiene la Gestión de Incidentes de Seguridad de la Información para brindar servicios de calidad en términos de controles de seguridad, con confidencialidad, integridad, disponibilidad de información a la sociedad y así de esta manera mejorar la imagen institucional.

1.5.5. JUSTIFICACIÓN NORMATIVA

Desde el punto de vista normativo, se justifica con los siguientes lineamientos:

A. El presente proyecto tiene su justificación normativa en la ISO/IEC 27001, un estándar de seguridad de la información, publicado como estándar internacional en octubre de 2005 por International ISO (*"Organization for Standardization")* y por la comisión IEC (*"International Electrotechnical Commission")*.

B. Norma Técnica Peruana, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI".

C. Implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008e, mediante Resolución Ministerial N.º 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008".

i. Uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014, Resolución Ministerial N° 004-2016-PCM.

1.6. LIMITACIONES Y ALCANCE

Las limitaciones que se presentan en el presente trabajo de investigación se originan por el escaso recurso económico, para implementar los controles de seguridad, esto desencadena una serie de limitaciones como:

- Ausencia de capacitación constante en temas referidos al conocimiento de las normas técnicas de protección de datos.
- Inadecuado manejo de los controles por parte del personal administrativo en los procesos que involucren información sensible.
- La no disposición de recursos tecnológicos para la protección de datos.

El alcance del trabajo de investigación, está orientado a cubrir las fases de análisis, diseño y desarrollo de controles de seguridad, en las oficinas que generan información valiosa para la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo, oficinas como, decanatura, direcciones de escuela, jefaturas de departamento, archivo (donde se encuentra el acervo documentario de la facultad) y el centro de cómputo de la facultad, donde se concentran la mayor cantidad de activos informáticos. Por lo tanto, el proceso de clasificación de activos de información y valoración de riesgos solo se realizará para las oficinas mencionadas.

1.7. VIABILIDAD

El trabajo de investigación se sustenta en elaborar un modelo de gestión para establecer los controles de seguridad bajo el análisis de viabilidad técnica a través de buscar una solución metodológica, que se adapte a nuestras necesidades de procesos y a las limitaciones existentes. Enmarcamos la viabilidad técnica en factores que garanticen la solución del problema plantado en el proyecto de investigación, factores como la eficacia, que busca satisfacer los requisitos del usuario, o la usabilidad de las normas y políticas propuestas que van a depender de la fiabilidad de resolver cualquier incidente o alguna probabilidad de riesgo de seguridad que atente la información, y finalmente la eficiencia que busca la capacidad del modelo de gestión de incidentes de cumplir su objetivo con el mínimo consumo de recursos necesario.

1.8. DESCRIPCIÓN Y SUSTENTACIÓN DE LA SOLUCIÓN

Para controlar de manera apropiada los incidentes de seguridad de información se determinará y establecerá las fases de gestión de incidentes de seguridad de la información de la facultad, que describirán las actividades involucradas en el ciclo de vida de la gestión de riesgos, además de ello se determinara los objetivos y las actividades post incidente, se elaborará herramientas para la categorización de los incidentes, los procedimientos de reporte y los protocolos de atención de incidentes. Un manual técnico de normas y lineamientos de políticas de

seguridad de la información, que definan los procedimientos, obligaciones y responsabilidades de todos los usuarios que tengan acceso a información de la institución de acuerdo a los objetivos y controles definidos en la norma ISO/IEC 27001:2013. Para tal fin se describen, fundamentalmente, herramientas de análisis y diseño, sus diagramas, especificación, y criterios de aplicación de las mismas. Como complemento se describirán las metodologías de desarrollo del sistema que utilizan dichas herramientas, ciclos de vida asociados y discusión sobre el proceso de desarrollo de los controles de incidentes de seguridad de la información, más adecuados para las diferentes aplicaciones. A continuación, establecemos un método para estructurar, planificar y controlar el proceso de nuestro proyecto de investigación.

1.8.1 Análisis de Requerimientos

Se realizaron observaciones sobre la realidad problemática para comprender las exigencias técnicas para la solución del problema. Estas observaciones están formadas por las especificaciones de los requerimientos técnicos, externos e internos del modelo basado en el conocimiento y análisis del problema especificados en el diseño lógico. Del resultado del análisis en esta etapa obtendremos un documento de los requerimientos, un análisis del modelo (modelo conceptual) y un instrumento de viabilidad.

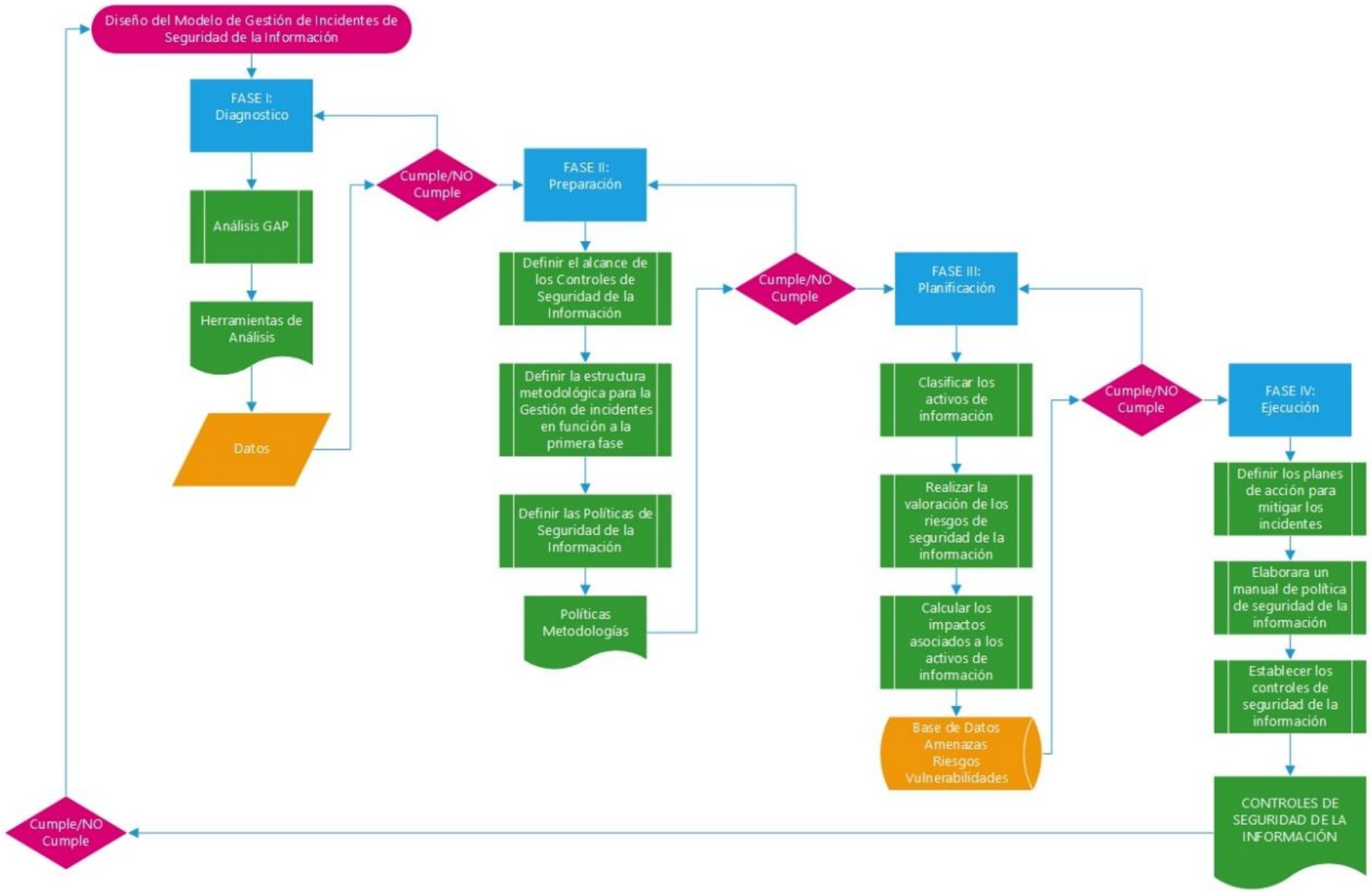
1.8.2 El Diseño

Corresponde al esbozo de las diferentes etapas que se delimitaron para el diseño del modelo de gestión de incidentes de seguridad de la información, las cuales poseen una serie de actividades cuya ejecución permite alcanzar los objetivos específicos que se han establecido para el logro del objetivo general del presente trabajo de investigación.

El diseño muestra la trazabilidad del modelo de gestión de incidentes de la información y su descripción funcional y una descripción física en la que se especifica punto a punto cada uno de sus componentes. En este proceso de diseño debe salir toda la especificación modular del sistema y la descripción detallada de cómo debe ser, desde el punto de vista holístico.

A continuación, se describen las fases de acuerdo a la Norma ISO/IEC 27000

Figura N° 1.1. Modelo De Planeación Estratégica



A. Fase de Diagnóstico

En esta fase se identificó el nivel de madurez inicial de la Facultad, tomando como punto de referencia el modelo de seguridad de la información que formula la norma ISO/IEC 27001:2014. También en esta fase de recolección y análisis de información, se utilizaron mecanismos y herramientas como el diligenciamiento de cuestionarios y análisis de informes anteriores, con el objetivo de determinar el nivel de cumplimiento de los dominios de la norma ISO/IEC 27001:2014. Se evaluó la documentación existente, el MOF y el ROF de la institución, que establecen los procedimientos y el tratamiento de la información de los usuarios como alumnos, docentes y administrativos de la institución y los roles y funciones asociados a la seguridad de la información.

B. Fase de Preparación

En esta fase se determinaron las actividades que se desarrollaron para instaurar el modelo de Gestión de Incidentes de Seguridad de la Información en la Facultad de Ciencias, es importante mencionar que se analizaron detalladamente la información del contexto problemático de la institución, de acuerdo a los requerimientos establecidos en la norma ISO/IEC 27001:2014. Este análisis determinó la realidad contextual externa e interna de la institución, que actividades son influyentes para la implementación del Modelo de Gestión de Incidentes de

Seguridad de la Información. También es importante mencionar que en esta etapa se definieron el alcance de los controles de seguridad, en el cual se establece los límites y la aplicabilidad del Modelo de Gestión de Incidentes de Seguridad de la Información, definir la política de seguridad de la información y definir la estructura organizacional de la institución que contiene los roles y responsabilidad pertinentes a la seguridad de la información.

C. Fase de planificación

En esta fase se realizaron actividades para identificar detalladamente los activos de información y activos informáticos en la Facultad, su clasificación de acuerdo a su criticidad y el nivel de protección, todo ello para realizar la valoración de riesgos de seguridad de la información de acuerdo al alcance del SGSI., es importante mencionar que se definieron los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos. Para determinar la selección de los controles de seguridad, se tomaron como referencia los objetivos de control y los controles establecidos en la norma ISO/IEC 27001, de esta manera se elaboró la declaración de aplicabilidad, que define y detalla los objetivos de control y controles seleccionados para el nivel de cumplimiento.

D. Fase de Ejecución

En esta fase se establecieron los planes de acción para mitigar los incidentes de seguridad de la información a través de la elaboración de los lineamientos institucionales de política de seguridad de la información, que corresponde a una directriz que contiene los procedimientos y lineamientos que se implementaran en la Facultad de Ciencias con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información y finalmente establecer los procedimiento para ejecutar los controles de seguridad informática. El desarrollo de las fases que se plantearon en esta metodología para el Modelo de Gestión de Incidentes de la Seguridad de la información para Facultad de Ciencias, se encuentra descritas y desarrolladas en los próximos capítulos.

1.8.3 Implantación del Modelo

En esta etapa se considerará la construcción del Modelo de Gestión de Incidentes de Activos Informáticos y Activos de Información para certificar el cumplimiento de controles que nos garanticen la seguridad de la información en la Facultad de Ciencias, todo ello integrando los componentes y módulos descritos en la fase de diseño.

1.8.4 Retroalimentación

Este proceso de control que nos permite revisar el flujo de trabajo de las fases de implementación y sus salidas finales con el fin de establecer mecanismos de mejora continua en la implementación de los controles de seguridad nos permitirá establecer con exactitud la implementación de actividades requeridas para proteger los activos de información basados en la gestión de riesgos.

Consiste entonces en la puesta en marcha del modelo de mejorar continua con el fin de implementar el sistema de gestión de incidentes iniciando sus actividades, y contrastando su funcionamiento.

Al final este proceso garantizará el correcto cumplimiento de los dominios ISO 27001 y conducirá el resultado de madurez.

CAPITULO II

MARCO TEÓRICO

2.1. ANTECEDENTES

2.1.1. Internacionales

- **Nicasio (2015)**, en su tesis *Diseño e Implementación de un Sistema de Gestión de Calidad en Seguridad de la Informacion SGSI,* Universidad Nacional Autónoma de México - México DF - México, El trabajo de investigación está basado en el área de seguridad de la información, que hoy en día es una de las principales e importantes áreas en instituciones tanto públicas como privadas. El área de seguridad se encarga de vigilar, monitorear el comportamiento de los sistemas, resguardar los activos y pasivos informáticos que se manejan, por ende, si estos sufren algún incidente o afectación ya sea física o lógica se estaría poniendo en juego la competitividad, la estabilidad, la continuidad de la empresa y en un caso extremo su permanencia en el mundo empresarial, por perdidas de información, tiempo y recursos financieros, que es vital para una empresa. Existen varias alternativas para darle solución a lo anterior, sin embargo, se sugiere por la experiencia adquirida del autor la implantación de un Sistema de Gestión de la Seguridad de la Información – SGSI, por ser un sistema más amplio e integral e implantar

soluciones completas a la seguridad de la empresa y por seguir asegurando la continuidad y su correcta operación cotidiana.

Análisis.- Este trabajo de investigación describe claramente el proceso de Diseño e Implementación de un Sistema de Gestión de la Seguridad, pero por motivos de ética profesional e integridad de la información se omitieron datos precisos del análisis y diagnóstico de la empresa y de sus activos informáticos pero se esboza claramente las metodologías utilizadas ordenadas bajo fases de evaluación, estrategia, implantación, verificación, mantenimiento y mejora, además de ello describe el plan de trabajo realizado para crear mecanismos de administración y control de cambios, la metodología utilizada es respaldada por un proceso formal que asegura su entendimiento a cada uno de los responsables de llevar a la práctica dicho proceso y a los lectores interesados en documentarse sobre la metodología utilizada para la implementación de un SGSI, finalmente realiza un análisis de resultados a partir del informe de vulnerabilidades y los reportes de evidencia, del estado de los servicios y el detalle técnico de cada uno de los activos.

- **Ripoll (2012)**, en su estudio *"Seguridad en los Sistemas de Información (SSI)"*, Universidad Politécnica de Valencia – Valencia – España, el tesista logró el siguiente objetivo: proporcionar apuntes y el material de apoyo de la asignatura de "Seguridad en los Sistemas Informáticos" que se imparte en la Escuela Técnica Superior de Ingeniería Informática de la Universidad Politécnica de Valencia. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: estos apuntes se han elaborado con la intención de servir de apoyo a la impartición de las clases. Puede que algunos temas o conceptos no se expliquen con la extensión y detalle necesarios; siendo necesario consultar otras fuentes para completar la formación.

  Análisis. - El presente estudio nos sirve de apoyo para unificar nuestras ideas respecto al sistema de gestión de seguridad de la información aportando de esta manera con conceptos y definiciones claras y precisas, ya que se muestran detalladamente.

- **Pallas (2009)**, en su tesis de maestría *Metodología de Implantación de un SGSI en un Grupo Jerárquico,* Universidad de la Republica-Montevideo-Uruguay, Los sistemas de gestión y de información están muy arraigados en los procesos productivos, industriales, de servicios, gubernamentales y casi cualquier sector activo de la sociedad. Esta dependencia de los sistemas de

información en general, requiere dotar de seguridad a los mismos para preservar la calidad de los servicios y velar por la eficacia y eficiencia de los procesos de negocio y el valor de sus activos. Ya no es suficiente con establecer controles en forma aislada ni ad hoc, tampoco es suficiente actuar de modo meramente reactivo y defensivo, se requiere de un sistema de gestión de seguridad de la información (SGSI) y un accionar proactivo. Si consideramos un grupo empresarial, donde dos o más empresas se integran verticalmente, el desafío de gestionar la seguridad de una manera conveniente es aún mayor. Existen diferentes estándares que se desarrollaron para gestionar la seguridad de la información, algunos más generales, algunos centrados en la gestión de riesgos (serie ISO/IEC 27.000), y otros incluso tendientes a desarrollar un modelo de madurez de la seguridad de la información (por ejemplo, ISM3); sin embargo, en la especificación de las mismos no se afronta su aplicación a un grupo empresarial, lo cual requiere consideraciones adicionales. En este trabajo, se analizan diferentes enfoques de estos estándares, con el fin de proponer una metodología de implementación, gestión y mejora de un SGSI en un grupo empresarial jerárquico. Se presentan además diferentes alternativas estratégicas y se discute sobre su conveniencia o no. Se analizan diferentes métodos conocidos de análisis y gestión

de riesgos. Algunos de ellos promovidos por los gobiernos y/o industria de países de vanguardia y trayectoria reconocida en la seguridad de la información que han tenido gran aceptación. Se promueve un enfoque sistémico y pragmático, no dogmático, en pro de una metodología eficaz y sostenible, primando un criterio de conveniencia costo-beneficio. Se enfatiza la necesidad de su orientación y adecuación a los reales requerimientos de seguridad del negocio. Se presenta una metodología adecuada a un grupo empresarial, que busca integrar lo mejor de cada uno de los enfoques analizados; se incluye una propuesta de organigrama de Seguridad que compatibiliza la jerarquía estructural del grupo y las necesidades de un SGSI.

Adicionalmente se incursiona en la aplicación de técnicas de grafos para la valoración de activos; se formaliza el concepto en términos de propiedades y algoritmia de grafos, y se define con una visión propia del tema, un algoritmo para el ajuste contemplando valoraciones cualitativas y cuantitativas y dependencias parciales y/o totales entre activos. También se describen características y funcionalidades deseables de una herramienta de software de apoyo a la metodología. Finalmente se analiza la aplicación de la metodología a un Caso de Estudio, en particular, un 'Internet Service Provider' (ISP) integrado verticalmente con una 'TelCo' (empresa de Telecomunicaciones).

En el mismo se analizan las particularidades del caso de estudio: los estándares y recomendaciones internacionales específicos, el modelo organizacional aplicable al negocio, datos estadísticos, y la seguridad requerida para este sector de la industria.

Análisis.- El trabajo de investigación presenta una propuesta metodológica bajo dos enfoques, por un lado trata de gestionar los desafíos y particularidades de ataques innovadores que no resuelve la familia ISO/IEC 27000, pero que deben de ser tenidos en cuenta al momento de implantar y gestionar un SGSI y así se afrontan en la metodología que se define, posteriormente se presenta concretamente una metodología basada en la ISO 27000 con el fin de alinearla con la serie ISO/IEC 27005, fundamentalmente con un enfoque sistémico, considerando las necesidades del negocio y la estructura empresarial planteada. Se realiza un análisis y evaluación de riesgos para definir la estrategia e identificarlos, hacer su respectiva evaluación y estimación, todo ello se plasma en la declaración de aplicabilidad para implementar los estándares y procedimientos de seguridad, los controles y la continuidad del negocio, para finalmente plasmar los alcances y límites de las políticas de seguridad.

- **Álvarez (2010)**, en su tesis magistral de *"Seguridad en informática (Auditoría de Sistemas)"*, Universidad Iberoamericana – México D.F – México, el tesista logró el siguiente objetivo: Proponer

lineamientos que se deben tomar en cuenta en cuanto a la seguridad informática, así como también ver la importancia de realizar auditoría de sistemas en las organizaciones. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades.

Análisis. - Como bien se menciona en la teoría nuestro proyecto realizara el uso de las normas ISO 27000 y en base al proyecto indicado tomaremos los lineamientos que debemos tener en cuenta para realizar la seguridad informática de los activos ya que es de vital importancia para la institución.

2.1.2. Nacionales

- **Gómez (2012)**, en su tesis *Implantación de los Procesos de Gestión de Incidentes y Gestión de Problemas Según ITIL V3.0 en el Área de Tecnologías de Información de una Entidad Financiera,* desarrollado en la Pontificia Universidad Católica del Perú – Lima –Perú, Establece que en la actualidad, muchas áreas de sistemas de las empresas no tienen una adecuada gestión de incidentes o de problemas de los sistemas de información empresariales en sus ambientes productivos, es por ello que, muchas veces el personal de soporte de sistemas que atiende estos eventos, no tiene definido el proceso de escalamiento o los tiempos de atención en que deben ser atendidos según la prioridad del mismo. Muchas veces el servicio de Tecnologías de Información llega a recuperarse, pero no se logra investigar y descubrir las causas raíz de los problemas o peor aún, se tienen incidentes que no son resueltos en realidad. Todo esto repercute en la imagen y la capacidad del personal de TI, así como en la continuidad del negocio. Es por ello, que tomando en cuenta esta necesidad en el área de Tecnologías de Información de las empresas, se desarrolla el proyecto de tesis, para poder tener procesos definidos de gestión de incidentes y de problemas con una visión de organización para la atención de estos eventos. Para el análisis de los procesos anteriormente mencionados, la

presente tesis se basará en las mejores prácticas recomendadas por el marco referencial de ITIL. En la presente tesis se analiza la problemática actual del área de Tecnología de Información de una entidad financiera mostrando una solución alineada a los lineamientos estratégicos del negocio. Asimismo, se muestran los resultados mes a mes de los procesos implantados para poder obtener conclusiones y proponer mejoras futuras.

Análisis. - El trabajo de investigación se fundamenta en la definición de mejora de procesos bajo los parámetros generales de ITIL que tiene como objetivo proporcionar a las organizaciones las habilidades para diseñar, desarrollar e implementar la gestión de servicios como un acto estratégico, así como para pensar y actuar de una manera estratégica. Asimismo, formula las directrices y guías a seguir en la gestión dentro del modelo de ciclo de vida del servicio, se realiza un diseño de la gestión de incidentes para la optimización de procesos, roles e indicadores además de ello se hace el diseño de la gestión de problemas, el plan de despliegue se establecen los siguientes procesos: planeación y soporte en la transición, gestión de cambios, gestión de activos de servicio y de configuraciones, gestión de liberaciones e implementación, validación del servicio y pruebas, evaluación y gestión del conocimiento, para finalmente establecer

roles que mejoren la seguridad de la información y se garanticen la operatividad de los servicios.

- **Camacho y Ramos (2010)**, en su tesis “Metodología táctica para la implantación de sistemas de información basado en métrica y COBIT”, Universidad Nacional Mayor de San Marcos – Lima - Perú, los tesistas lograron el siguiente objetivo: Elaborar una metodología a nivel táctico, orientada a satisfacer las necesidades gerenciales y/o de jefe de proyectos a fin de implementar sistemas de información. Tipo: Descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: El proceso de puesta en marcha de un sistema de información será realizado con mayor fluidez y ordenamiento. Con el previo análisis de las metodologías existentes, se ha logrado obtener un producto capaz de mantener estándares de auditoria. La simplicidad que refleja permitirá realizar el proceso de toma de decisiones gerenciales de una manera eficaz y eficiente.

  Análisis. - En base a este proyecto nos apoyaremos en el uso adecuado de las metodologías para el desarrollo del presente, la cual nos permita tener un control de los estándares aplicados y usados para así llevarlos a cabo en la Facultad de Ciencias exponiendo este plan para la toma de decisiones de la alta gerencia.

- **Villena M. (2011)**, en su tesis “Sistema de Gestión de Seguridad de Información para una institución financiera”, Pontificia Universidad Católica del Perú – Lima – Perú, el tesista logra el siguiente objetivo: establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado modelo de sistema de gestión de seguridad de información (SGSI) en una institución financiera en el Perú. Tipo: aplicado. Nivel: experimental. Diseño: aplicativo. Conclusión: Para implantar una adecuada gestión de seguridad de información en una institución financiera, el primer paso es obtener el apoyo y soporte de la alta gerencia, haciéndolos participes activos de lo que significa mantener adecuadamente protegida la información de la institución financiera.

  Nos apoyamos en este proyecto para realizar la parte logística del proyecto como es el de realizar la entrevista personal a los trabajadores de dicha área, para así tener acceso a los activos de la institución y de esta manera haciéndolos participes del proyecto a realizar.

  Análisis. - Este proyecto nos brinda las pautas a seguir para realizar una adecuada gestión de la seguridad de la información, basándola en nuestra institución ya que en este caso estamos hablando de una institución estatal en la cual vamos a hacer

partícipes a los colaboradores para que nos permitan el acceso a los activos.

- **Ampuero (2011)**, en su tesis “Diseño de un SGSI para una compañía de seguros”, Pontificia Universidad Católica del Perú – Lima – Perú, logra el siguiente objetivo: utilizar estándares y buenas prácticas reconocidos mundialmente para poder desarrollar cada una de las etapas del diseño del Sistema de Gestión de Seguridad de Información (SGSI) y así poder tener una base que se pueda implementar en cualquier compañía de seguros. Tipo: aplicado. Nivel: experimental. Diseño: aplicado. En la actualidad, con el desarrollo de la tecnología, la información ha tomado mayor fuerza en las empresas, convirtiéndose en la mayoría de los casos en el activo más importante que tienen. Es por esta razón que tienen la obligación de proteger aquella información que es importante para ellas y que tiene relación ya sea con el negocio o con los clientes.

  Análisis. - Este proyecto nos brinda el conocimiento de cómo realizar el diseño y gestión de la seguridad de la información ya que es muy importante su aplicación y/o desarrollo en las instituciones tanto públicas y privadas.

- **Espinoza (2013)**, en su tesis “Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización

de productos de consumo masivo", Pontificia Universidad Católica del Perú – Lima – Perú, logra el siguiente objetivo: tomar en cuenta los aspectos más importantes de la norma ISO/IEC 27001:2005, a partir de los cuales se buscará poder desarrollar cada una de las etapas del diseño de un sistema de gestión de seguridad de información. Tipo: aplicado. Nivel: experimental. Diseño: aplicado. Conclusión: En los últimos 20 años la información se ha convertido en un activo muy importante y crucial dentro de las organizaciones, es por ello que tiene la necesidad de protegerla si es que la información tiene relación ya sea con el negocio o con sus clientes.

2.1.3. Locales

- **Mory, (2014)**, en su tesis *"Diagnóstico y Diseño de un Sistema de Gestión de Seguridad de Información aplicado a la empresa HM Contratistas S.A."* El tesista tiene como objetivo principal Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) siguiendo las normas internacionales ISO/IEC 27001:2005 en la empresa HM CONTRATISTAS S.A. de la ciudad de Huaraz, ya que a partir de su realidad problemática tiene el fin de proteger sus activos de información ante las amenazas a las cuales están expuestos, cumpliendo con los objetivos específicos de dicho proyecto. El autor realizo el diseño un Sistema de Gestión de Seguridad de Información (SGSI) según el estándar internacional

ISO/IEC 27001:2005 en dicha constructora así de esta manera dando y/o exponiendo los controles adecuados para proteger sus activos de información ante las amenazas a las cuales están expuestos, dándole un tratamiento adecuado a los riesgos de información presentes en los procesos más importantes de la empresa. Este proyecto de tesis aporta al nuestro en la manera de identificar y evaluar los riesgos en base a la familia de la norma ISO 27000 el cual nos permitirá, a la institución, gestionar la seguridad de la información que maneja, de manera que se pueda cumplir con la preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Carrión (2014)**, en su informe del programa de titulación *Diagnóstico y Propuesta de Mejora para la Gestión de Riesgos Basado en la ISO/IEC 27002:2008 Para la Oficina General de Estudios UNASAM*, desarrollado en la Universidad Nacional Santiago Antúnez de Mayolo – Huaraz – Perú, describe que actualmente la información es un valioso recurso, que posee cualquier organización. Pero la información está expuesta a riesgos y amenazas que atentan contra su integridad. La Oficina General de Estudios, maneja información de importancia para la comunidad universitaria, es por ello que el objetivo del proyecto es hacer un diagnóstico de la gestión de riesgos para ayudar a la mejora de los procesos académicos que desarrollan dentro de

esta oficina (manejo de información). Para el diagnóstico de la gestión de riesgo, se basa en la norma ISO/IEC 27002:2008 y a su vez en la metodología MAGERIT, todo ello con el fin de poder identificar y minimizar los riesgos y amenazas a los que está expuesta la información, y también para poder establecer controles, no sólo dentro de la oficina, sino también con miras a educar al usuario. El nivel de riesgo a los que están expuestos los activos de la Oficina General de Estudios es alto, pero aprovechando el potencial humano con el que cuenta se puede contrarrestar todo ello y tomando las políticas y los controles adecuados estará preparado ante cualquier incidencia futura.

Análisis. – En el trabajo de investigación realizado además de realizar un análisis de las técnicas y procedimientos basados en la norma ISO/IEC 27002, se hace una descripción del modelo de negocio, el análisis de la situación actual, el organigrama funcional y estratégico, la evaluación instalada para identificar los requerimientos de seguridad con el fin de realizar un informe de diagnóstico y medidas de mejoramiento, finalmente se establecen los controles de seguridad, una descripción del diseño funcional de la solución y el plan de monitoreo y evaluación.

- **Armas y Pérez (2018)**, en su tesis "*Desarrollo de un Sistema de Gestion de Seguridad de la Información para Minimizar Riesgos*

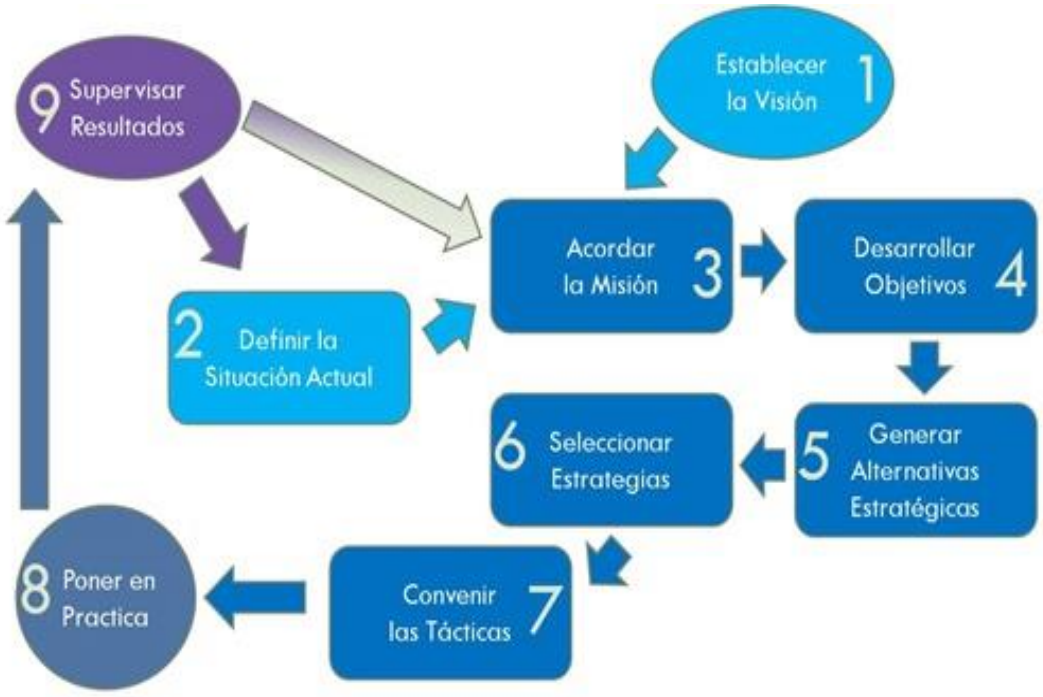
en los activos de información en la Sub Gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia 2016", Universidad Nacional Santiago Antúnez de Mayolo – Huaraz - Perú, los tesistas lograron desarrollar un sistema de gestión de seguridad de la información para la sub gerencia de informática y telecomunicaciones de la municipalidad distrital de independencia utilizando la norma ISO/IEC 2700 y a su vez utilizaron las herramientas que brinda MAGERIT con el fin de identificar y mitigar los riesgos y amenazas logrando el documento de aplicabilidad.

2.2. TEORÍAS QUE SUSTENTAN EL TRABAJO

2.2.1. Plan estratégico de tecnología de información

El plan estratégico de tecnología de información es un conjunto de definiciones tecnológicas e iniciativas de TI que deben soportar la visión, misión y estrategias que la institución, tiene para un horizonte de tiempo definido, la razón de ser de las tecnologías de información es la información misma y por ende ambas perspectivas (información y tecnología) deben estar alineadas y contar con mecanismos para facilitar este alineamiento.

Figura N° 2.1. Modelo De Planeación Estratégica



Fuente: Elaboración Propia

El plan estratégico de TI, debe servir de herramienta para acompañar a la alta dirección en la programación de inversiones en iniciativas de TI por cada paso estratégico realizado en el negocio, conocer el impacto de las iniciativas de tecnología en la institución, tener una idea clara del beneficio tangible e intangible a obtener y una aproximación de los costos y plazos para cada iniciativa. Para responder a todos estos requerimientos y confeccionar el plan para un Sistema de Gestión de la Seguridad de la Información, utilizare la Metodología de Oficina Nacional de Gobierno Electrónico e Informática – ONGEI, cual contiene las mejores prácticas públicas con respecto al uso de tecnología de información en el Perú.

2.2.2. Sistema de Gestión de la Seguridad de la Información

Un Sistema de Gestión de la Seguridad de la Información (SGSI) (en inglés: Information Security Management System, ISMS) es, como el nombre lo sugiere, un conjunto de políticas de administración de la seguridad de la información. El término es utilizado principalmente por la ISO/IEC 27001, aunque no es la única normativa que utiliza este término o concepto.

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. Como todo proceso de gestión, un SGSI debe seguir siendo eficiente durante un largo tiempo adaptándose a los cambios internos de la organización, así como los externos del entorno.

2.2.3. Normas ISO/IEC 27000:2013

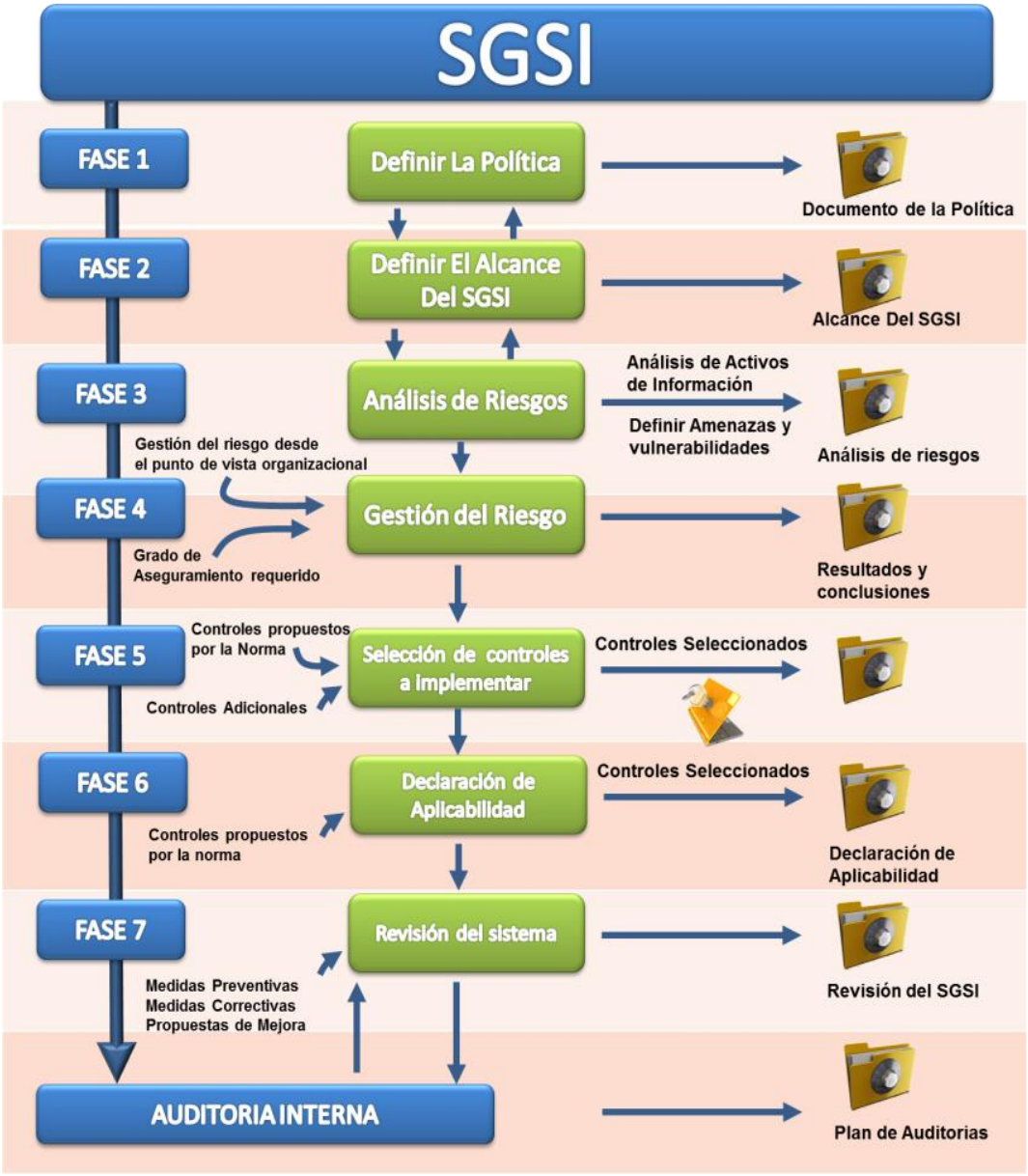
La adecuada gestión de la seguridad de la información hace necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización. La familia de normas ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission),

que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

2.2.4. ISO/IEC 27001:2005

Es el estándar principal de la serie y contiene los requisitos para el desarrollo de un Sistema de Gestión de Seguridad de la Información. Se basó en la BS 7799- 2:2002 (no vigente). Los SGSI se certifican actualmente contra este estándar por auditores externos a las organizaciones. Este estándar internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización. [ISO 27001] Este estándar internacional fomenta que sus usuarios enfaticen la importancia de [ISO 27001], entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información, implementar y operar controles para manejar los riesgos de la seguridad de la información, monitorear y revisar el desempeño y la efectividad del SGSI y finalmente el mejoramiento continuo en base a la medición del objetivo.

Figura N° 2.2 Fases de la implementación ISO/IEC 27000



El estándar adopta el modelo PDCA o también conocido como el "Ciclo de Deming", presenta lo siguiente para cada etapa [ISO 27001]: Primero Planear (establecer el SGSI): Establecer la política, objetivos, procesos y procedimientos para el SGSI relevantes para manejar el

riesgo y mejorar la seguridad de la información, para entregar resultados en concordancia con las políticas y objetivos generales de la organización, segundo Hacer (implementar y operar el SGSI) Implementar y operar la política, controles, procesos y procedimientos para el SGSI, tercero Chequear (monitorear y revisar el SGSI): Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas del SGSI y cuarto Reportar los resultados a la gerencia para su revisión.

Figura 2.3. Ciclo de Deming

Fuente: Elaboración propia

2.2.5. Norma técnica peruana NTP

Desde la Perspectiva de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI). El objetivo del plan de desarrollo de la Sociedad de la Información en el Perú es “Acercar la administración

del estado y sus procesos a la ciudadanía y a las empresas en general, proveyendo servicios de calidad, accesibles, seguros, transparentes y oportunos, a través del uso intensivo de las TIC". Se refiere precisamente al desarrollo del gobierno electrónico en el Perú, que viene a ser la aplicación de las TIC's para lograr la interacción de la sociedad con el sector público y determinar su organización. Desde la perspectiva del Ministerio de Transportes y Comunicaciones del Perú (MTC), el gobierno electrónico consiste en todas aquellas iniciativas que implican el uso de las tic en la gestión inter organizacional del estado e incluye la definición, coordinación, implementación y desarrollo de las políticas públicas, teniendo en cuenta que el gobierno electrónico es mucho más que tecnología cuando se define como el aprovechamiento de esta, para refundar las relaciones internas y externas del estado.

Desde la perspectiva de la Facultad de Ciencias, todas estas definiciones deben ser consideradas, si bien algunas de ellas ya se vienen utilizado, es importante que se fortalezcan mediante la tecnología y sus políticas/normas. Porque la disponibilidad de información de manera oportuna trasparente y la mejora de la eficiencia del trabajo interno son aspectos donde los sistemas de información juegan un papel importante para la Sociedad de la información.

2.3. DEFINICIÓN DE TÉRMINOS

2.3.1 Activo

Algo que tenga valor para lo organización. [ISO 13335]

2.3.2 Control

Herramienta de la gestión del riesgo, incluido: políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. [ISO 27002]

2.3.3 Pauta

Descripción que aclara que es lo que se debe hacer y cómo se hace, con el fin de alcanzar los objetivos planteados en las políticas. [ISO 13335]

2.3.4 Instalaciones de proceso de información

Sistemas de información, servicio o infraestructura, o locaciones físicas que los almacena. [ISO 27002]

2.3.5 Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas. [ISO 27002]

2.3.6 Evento de seguridad de información

Es una ocurrencia identificada de un sistema, servicio, o red el cual indica una posible brecha de la política de seguridad de información o

fallas de las salvaguardias o una situación desconocida que puede ser relevante para la seguridad. [ISO 18044]

2.3.7 Aceptación de riesgo

Decisión de aceptar el riesgo. [ISO 73]

2.3.8 Incidente de seguridad de información

Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información. [ISO 18044]

2.3.9 Política

Dirección general y formal expresada por la gerencia. [ISO 73] Terceros Persona que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión. [ISO 73]

2.3.10 Amenaza

Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización. [ISO 13335]

2.3.11 Vulnerabilidad

Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas. [ISO 13335]

2.3.12 Riesgo

Combinación de la probabilidad de un evento y sus consecuencias. [ISO 73]

2.3.13 Análisis del riesgo

Uso sistemático de la información para identificar fuentes y estimar el riesgo. [ISO 73]

2.3.14 Valoración del riesgo

Proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este. [ISO 73]

2.3.15 Tratamiento de riesgo

Proceso de selección e implementación de medidas para modificar el riesgo. [ISO 73]

2.3.16 Evaluación de riesgo

Proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo. [ISO 73]

2.3.17 Gestión de riesgo

Actividades coordinadas para dirigir y controlar una organización considerando el riesgo. Gestión del riesgo incluye típicamente evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo. [ISO 73]

2.3.18 Riesgo residual

El riesgo remanente después del tratamiento del riesgo. [ISO 73]

2.3.19 Disponibilidad

La propiedad de estar disponible y utilizable cuando lo requiera una entidad autorizada. [ISO 13335]

2.3.20 Confidencialidad

La propiedad que esa información esté disponible y no sea divulgada a personas, entidades o procesos no-autorizados. [ISO 13335]

2.3.21 Integridad

La integridad es la garantía de que los datos sean correctos y de la completitud de la información. [TUPIA 2010]

2.3.22 Audibilidad

Garantía de que en todo momento es posible identificar el origen (autor) de la transacción / operación, la fecha de realización y los medios empleados para la misma. [TUPIA 2010]

2.3.23 Enunciado de aplicabilidad

Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización. [ISO 27001]

CAPITULO III

MATERIALES Y MÉTODOS

3.1. MATERIALES

3.1.1. Recursos Utilizados.

En este caso es prioritario elaborar un estudio de los recursos disponibles, para lo cual podemos contar con una serie de herramientas para determinar con exactitud los materiales utilizados, en este caso elaboramos cuadros de recursos disponibles y no disponibles, es muy importante determinar el medio de distribución de los recursos.

El inventario de materiales disponibles, en este caso, nos ayudó a conocer con qué medios contamos para realizar el proyecto de investigación, además de ello es importante determinar la disponibilidad de recursos públicos utilizados para el trabajo de investigación. El resultado de este análisis será útil para determinar con que materiales se contó durante el proyecto de investigación y conocer el contexto y la influencia del entorno.

Personal disponible

Cuadro N° 3.1: Cuadro de Personal Disponible

PERSONAL DISPONIBLE	
CARGO	**NOMBRE**
Autor del Proyecto	Brito Rodríguez, Roberto Elías
Asesor	Alvarado Cáceres Luis

Fuente: Elaboración propia

Materiales disponibles

Cuadro N° 3.2: Cuadro de Materiales Disponibles

MATERIALES		
Bienes de Consumo	**Unidad**	**Cantidad**
Lapiceros tinta seca	Caja	1.00
Papel Bond A4	Paquete	1.00
Anillo Espiralador	Caja	1.00
Mica para Anillado	Caja	1.00
Archivador	Unidad	5.00
Bandeja Portapapeles	Unidad	3.00
Binder Clip	Caja	1.00
Borrador Caucho	Unidad	1.00
Cartulina Dúplex	Paquete	2.00
Libreta de Campo	Unidad	2.00
Plumones para Pizarra	Caja	1.00

Fuente: Elaboración propia

Equipos disponibles

Cuadro N° 3.3: Cuadro de Equipos Disponibles

EQUIPOS		
Bienes de Inversión	**Unidad**	**Cantidad**
Modem inalambrico	Unidad	1.00
Computadora personal	Unidad	.00
Laptop	Unidad	1.00
Impresora	Unidad	1.00
Grapa	Unidad	1.00
Espiraladora	Unidad	1.00
Perforador	Unidad	1.00
Rotuladora	Unidad	1.00
Tablet	Unidad	1.00
UPS	Unidad	1.00

Fuente: Elaboración propia

Servicios.

Cuadro N° 3.4: Cuadro de Servicios Disponibles

SERVICIOS		
Servicio	**Unidad**	**USO**
WINDOWS 10	12 meses	PERMANENTE
MS Project Professional 2013	12 meses	TEMPORAL
Bizagi Process Modeler	12 meses	TEMPORAL
Internet	06 meses	PERMANENTE
Biblioteca	12 meses	TEMPORAL
Teleconferencia	03 meses	TEMPORAL
Capacitación Online	02 meses	TEMPORAL

Fuente: Elaboración propia

3.1.2. Recursos gestionados

Es importante mencionar y describir los recursos gestionados para detallar los materiales, equipos y servicios utilizados en su totalidad en la investigación y así tener una visión más clara de los recursos utilizados durante el proceso de investigación.

Cuadro N° 3.5: Cuadro de Materiales No Disponibles

MATERIALES			
Bienes de Consumo	**Unidad**	**Cantidad**	**Costo Soles**
Tóner	Global	2.00	50.00
Papel	Millar	2.00	40.00
Post-it	Caja	3.00	15.00
CD	Pack	1.00	12.00
DVD	Pack	1.00	20.00
Correctores	Unidad	2.00	3.00
Folders	Pack	1.00	10.00
COSTO TOTAL			**S/.150.00**

Fuente: Elaboración propia

Equipos gestionados

Cuadro N° 3.6: Cuadro de Equipos No Disponibles

EQUIPOS			
Bienes de Inversión	**Unidad**	**Cantidad**	**Costo Soles**
Multímetro	Unidad	1.00	60.00
Pack Destornillador	Unidad	1.00	30.00
Modem Inalámbrico	Unidad	1.00	50.00
Pizarra	Unidad	1.00	60.00
Video Cámaras	Unidad	1.00	800.00
Cámaras Fotográficas	Unidad	1.00	400.00
COSTO TOTAL			**S/.1400.00**

Fuente: Elaboración propia

Servicios gestionados

Cuadro N° 3.7: Cuadro de Servicios No Disponibles

SERVICIOS			
Servicio	**Unidad**	**Cantidad**	**Costo Soles**
Internet Inalámbrico	Meses	6.00	180.00
Seguro de riesgo	Unidad	1.00	200.00
Capacitación	Global	2.00	800.00
Empastado	Unidad	10.00	20.00
Telefonía Móvil	Meses	6.00	200.00
Movilidad	Meses	6.00	300.00
Plastificación	Unidad	9.00	30.00
Estadía Capacitación	Meses	2.00	400.00
COSTO TOTAL			**S/.2130.00**

Fuente: Elaboración propia

3.1.3. Locales gestionados

Se utilizaron los siguientes locales:

- Laboratorios de la Facultad de Ciencias
- Oficinas de la Facultad de Ciencias de la UNASAM.
- Biblioteca de la Facultad de Ciencias
- Oficina de la Escuela Profesional de Ingeniería de Sistemas e Informática.

3.1.4. Presupuesto

Se elabora en función de los recursos no disponibles.

Cuadro N° 3.8: Cuadro del Presupuesto Total

PRESUPUESTO	
Costo de Recursos no Disponibles	**Costo Soles**
Costo del Personal	4000.00
Costo de los Materiales	150.00
Costo de los Equipos	1400.00
Costo de los Servicios	2130.00
COSTO TOTAL	**S/.7680.00**

Fuente: Elaboración propia

3.1.5. Población y Muestra

Población

La población en la cual se aplicó los instrumentos de recolección de datos está conformada por el personal administrativo responsable de la seguridad de los activos de información y activos informáticos de la facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo, a continuación, se muestra el personal que conforma la población en la tabla N° 3.9

Cuadro N° 3.9: Población

POBLACIÓN TOTAL PERSONAL ADMINISTRATIVO RESPONSABLE DE LA SEGURIDAD DE LA INFORMACION EN LA FACULTAD DE CIENCIAS		
	Población	**N°**
A	Decano de la Facultad de Ciencias	1
B	Secretario Del Consejo de facultad	2
C	Jefe de Departamento Académico de Sistemas	3
D	Secretaria de Escuelas	4
E	Secretaria de Decanatura	5
F	Secretaria de Departamentos Académicos	6
G	Bibliotecario de la Facultad	7
H	Jefe del Centro de Computo	8
I	Encargado del Centro de Computo	9
J	Practicante – Encargado de Archivos	10
	TOTAL	10

Fuente: Elaboración propia

Hay que tener en cuenta que el personal administrativo está siendo considerado como usuarios directos de la gestión de incidentes de seguridad de la información y responsables de la información sensible que se maneja, por ello es importante y determinante aplicar herramientas de recolección de datos para procesar información precisa para la investigación.

Muestra

Teniendo en cuenta la población, para la presente investigación, la muestra será igual a la población, ya que la población objetivo está delimitada a un solo grupo de estudio, en el cual están involucrados el personal administrativo responsable del manejo y resguardo de los activos informáticos e información valiosa en la Facultad de Ciencias.

Unidad de análisis

Personal administrativo que es responsable del resguardo de los activos informáticos y activos de información sensibles para la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo, el objetivo de contar con la información de este personal es analizar la situación actual de la gestión de los activos informáticos y activos de información y presentar la declaración de aplicabilidad del sistema de gestión de incidentes de la seguridad de la información en la Facultad de Ciencias, 2017".

3.2. MÉTODOS

3.2.1. Tipo de investigación

A. **De acuerdo a la orientación.-** El presente trabajo de investigación es de tipo aplicada, porque busca la aplicación o utilización de los conocimientos obtenidos durante el desarrollo y se empleó conocimientos relacionados con este instrumento teórico y metodológico, la cual está basada en el desarrollo de un modelo de gestión de incidentes para la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo, para minimizar los incidentes de seguridad de la información en los activos informáticos y de información en la institución.

B. **De acuerdo a la técnica de contrastación. -** Es descriptiva ya que los datos son obtenidos directamente de la realidad y situación actual de la Facultad de Ciencias sin que estos sean manipulados por los investigadores

3.2.2. Definición de variables

Variable independiente (Vi) = Gestión de Incidentes.

Variable dependiente (Vd) = Seguridad de la Información en la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo.

3.2.3. Operacionalización de variables

Tabla N° 3.10 *Matriz de Operacionalización de variables*

TITULO	ENUNCIADO DEL PROBLEMA	HIPÓTESIS	OBJETIVO	VARIABLES	Tipo de Variable	Definición Conceptual	Dimensiones
"GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE CIENCIAS DE LA UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, 2017"	¿DE QUE MANERA CON LA GESTIÓN DE INCIDENTES SE ESTABLECERÁN LOS CONTROLES DE SEGURIDAD DE LA INFORMACION EN LA FACULTAD DE CIENCIAS DE LA UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, 2017?	**GENERAL** Con la Gestión de Incidentes se establecerán los controles de Seguridad de la Información en la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo.	**GENERAL** Diseñar un Modelo de Gestión de Incidentes para establecer los controles de Seguridad de la Información en la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo.	**V1: Gestión de incidentes**	**Independiente**	La Gestión de Incidentes tiene como objetivo resolver de manera rápida y eficaz, cualquier incidente que atente la seguridad de la información y que cause una interrupción en el servicio tecnológico e informático.	riesgos
		ESPECÍFICOS **A.** Con el diagnostico y analisis GAP se determinara la brecha de seguridad de la información en la Facultad de Ciencias.	**ESPECÍFICOS** **A.** Elaborar el diagnóstico y analisis GAP para determinar la brecha de seguridad de la información en la Facultad de Ciencias.				impactos
		B. Con el diagnostico de los riesgos inherentes se determinara el impacto y los niveles de riesgo de los activos de información en la facultad de ciencias.	**B.** Elaborar el diagnostico de los riesgos inherentes para determinar el impacto y los niveles de riesgo de los activos de información de la Facultad de Ciencias.				
		C. Con el analisis de la valoracion de los controles de seguridad de la informacion se determinara el desplazamiento del mapa de riesgo.	**C.** Elaborar el analisis de valoracion de los controles de seguridad de la información para determinar el desplazamiento del mapa de riesgo.	**V2: Seguridad de la información en la Facultad de Ciencias de la UNASAM**	**Dependiente**	Conjunto de políticas, estándares y controles que se implementan en la organización con la finalidad de asegurar la preservación de la información y servicios informáticos	Confiabilidad de la información
							Integridad de la información
							Disponibilidad de la información

Fuente: Elaboración propia

3.2.4. Diseño de la investigación

Diseño general

Descriptivo, considerando el tipo y nivel de la investigación, el diseño general de la investigación es descriptivo porque se analizó la realidad problemática y se logró comprender de forma íntegra el presente.

Bibliográfico, en la primera etapa del proceso investigativo que proporciona el conocimiento de las investigaciones ya existentes, de un modo sistemático, a través de una amplia búsqueda de: información, conocimientos y técnicas sobre los modelos de gestión de incidentes de la seguridad de la información.

Diseño Metodológico

Para el diseño metodológico es necesario adoptar un enfoque basado en procesos que permita establecer, implementar, operar, hacer seguimiento, mantener y mejorar el modelo de gestión de incidentes de la seguridad de la información.

Según la norma ISO 9001 puede aplicarse a todos los procesos la metodología conocida como “Planificar – Hacer – Verificar – Actuar (PHVA),

3.3. TÉCNICAS DE PROCESAMIENTO DE INFORMACIÓN

Según Tamayo (2009) las técnicas de recolección de datos son las distintas formas o maneras de obtener la información, estas pueden ser la observación directa, la encuesta en sus dos modalidades (entrevista o cuestionario), el análisis documental y el análisis de contenido. Los instrumentos son los medios materiales que se emplean para recoger y almacenar la información, estos pueden ser fichas, formatos de cuestionarios, guías de entrevista, grabadores, escalas de actitudes u

opinión. Según Reyes (2012) técnicas es el conjunto de reglas y procedimientos que permiten al investigador establecer la relación con el objeto o sujeto de la investigación. En el trabajo de investigación utilizaremos técnicas como:

3.3.1. La observación

Es el registro visual de lo que ocurre en una situación real de incidente de seguridad de la información ocurrida en la Facultad de Ciencias, clasificado y consignando los datos de acuerdo con los esquemas de la norma ISO/IEC 27001 previsto y de acuerdo al problema planteado.

3.3.2. La encuesta

Método que utilizamos para obtener información acerca de la población, a través de la entrevista (oral) y escrita (cuestionario), También, se usó de diferentes fuentes de información, tales como tesis, libros, textos, revistas, normas, etc., existentes tanto en medios físicos, electrónicos y publicados en Internet.

3.4. PROCEDIMIENTOS

3.4.1. Procedimientos según el estándar internacional ISO 27001

Según el estándar internacional ISO 27001 el submodelo de procesos define de forma sistémica el camino que se debe seguir para realizar un proyecto de análisis y gestión de riesgos e incidentes. Este submodelo es el marco de trabajo en el que se agrupan y ordenan todas las acciones que se realizan y, además, incluye todas las dificultades para conseguirlo, resumiendo, define lo siguiente: Primero, estructurar el proyecto, sirve de guía al equipo de trabajo y permite involucrar en él a los clientes, a los responsables de activos que hay que proteger y a los clientes. Segundo, definir el conjunto de productos que se ofrece. Tercero, aplicar un conjunto de técnicas para conseguir los productos de seguridad de información. Cuarto, definir las funciones y responsabilidades de las personas que ponen en marcha el proyecto.

El submodelo de procesos es capaz de formalizar las diferentes acciones, las sucesiones y la estructura en tres niveles diferentes: etapas, actividades y tareas.

- En cada etapa se agrupan diferentes actividades, establece los hitos de decisión y consigue los productos intermedios y finales.
- En cada actividad se agrupan las diferentes tareas con criterios de carácter funcional.
- En cada terea se describe el trabajo realizado en el mínimo componente del desglose y suele asignarse a un solo tipo de

puesto y de ejecutantes. Las descripciones de estos conceptos son: acciones que se deben realizar, atores, productos y documentos que se obtendrán como productos de acciones, validaciones y aprobaciones de los resultados obtenidos.

El método MAGERIT utiliza el término “unidades” para referirse a los diferentes ámbitos de la organización dentro de una entidad. El esquema explicativo es necesario para construir un proyecto de seguridad específico, ayuda por una parte a seguir el procedimiento general y por otra a adaptarlo al problema que queremos solucionar, pero siempre teniendo en cuenta la política de seguridad establecida por la organización como le solicita la norma ISO27001. El submodelo de procesos de MAGERIT dispone cuatro etapas:

Etapa 1 “Planificación de análisis y gestión de riesgos”, estableciendo las consideraciones necesarias para poder comenzar con el proyecto de análisis y gestión de riesgos, lo que permite la investigación de la oportunidad definiendo los objetivos que se cumplen y el dominio que engloba.

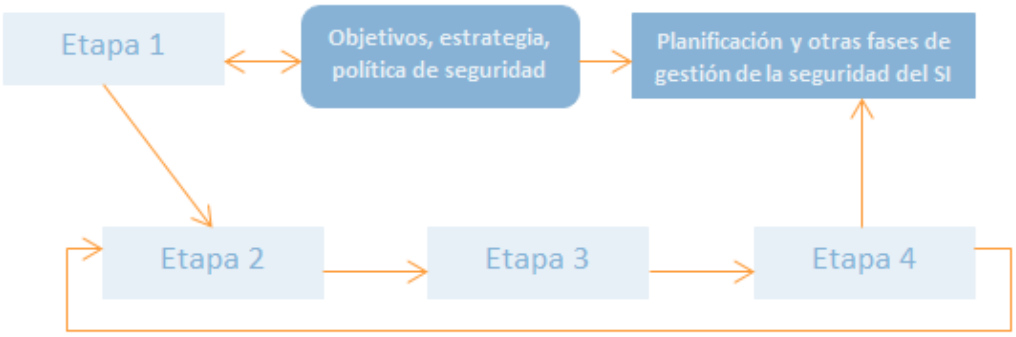
Etapa 2 “Análisis de riesgos”, facilita la identificación y valora las entidades que intervienen en el riesgo, se obtiene la evaluación de dichas áreas de dominio y, además, realiza una estimación de los diferentes riesgos.

Etapa 3 “Gestión de riesgos”, permite identificar las diferentes funciones que reducen el riesgo detectado, selecciona las medidas

necesarias para que sean aceptables las funciones existentes y las restricciones.

Etapa 4 “Selección de salvaguarda”, facilita la selección de los diferentes mecanismos que se deben implementar, además elabora una orientación del plan de implantación de los diferentes mecanismos que permitan que se salve la información importante, recoge los diferentes documentos de trabajo del proceso de análisis y gestiona los riesgos.

Gráfico N° 3.1. Etapas del Modelo Magerit



Elaboración Propia

En esta figura representamos el ciclo de etapas del proceso realizado por el método MAGERIT y conforma la fase de análisis y la gestión de riesgos dentro de la gestión de la Seguridad de los Sistemas de Seguridad de la Información ISO 27001 en cada etapa se realizan diferentes actividades, cada una con contenido específico, aunque se comparta con otras tareas más técnicas en cuanto a ejecución. Estas actividades son:

Etapa 1: Planificación de análisis y gestión de riesgos

- Oportunidad de realización: se clarifica la oportunidad de realización.
- Definición del dominio y los objetivos: se especifica el dominio de los objetivos del proyecto.
- Planificación del proyecto: se planifican las entrevistas.
- Puesta en marcha del proyecto: seleccionar criterios de evaluación y técnicas para el proyecto, asignar los recursos necesarios.

Etapa 2: Análisis de riesgos

- Recogida de información: preparar la información.
- Identificación y agrupación de activos: identificar los grupos de activos y valorarlos.
- Identificación y evaluación de amenazas: identificar y agrupar las amenazas.
- Identificación y estimación de vulnerabilidades: identificar y estimar las vulnerabilidades.
- Identificación y valoración de impactos: identificar, tipificar y valorar los impactos.
- Evaluación del riesgo: evaluar y analizar el riesgo.

Etapa 3: Gestión de riesgos

- Interpretación del riesgo: interpretar los diferentes riesgos.
- Identificación y estimación de las funciones para proteger la información: identificar las funciones de protección.
- Seleccionar las mejores funciones de protección: aplicar parámetros de selección.
- Cumplir con los objetivos marcados: determinar el cumplimiento de los objetivos.

Etapa 4: Selección de medidas de protección

- Identificar mecanismos de protección de información: identificar, estudiar e incorporar restricciones.
- Selección de mecanismos de protección: identificar los diferentes mecanismos a implantar.
- Especificación de los mecanismos de implantación: especificar los mecanismos que implantar.
- Planificar la implementación: priorizar y evaluar los mecanismos.
- Integrar los resultados: integrar los resultados.

CAPITULO IV:

ANÁLISIS

4.1. ANÁLISIS DE LA SITUACIÓN ACTUAL

La Facultad de Ciencias representa una de las 11 facultades que conforman a la UNASAM, su finalidad es la formación académica y profesional de sus estudiantes, está integrada por docentes, personal administrativo y estudiantes de pregrado; en ella se estudia carreras, según la afinidad de sus contenidos, y de acuerdo a los currículos elaborados por ellas. Está conformada por tres escuelas académico profesionales que son encargadas de la formación de los estudiantes a través de la formulación, implementación y ejecución del currículo. La Facultad de Ciencias al tener actividades y procesos importantes que evalúan la formación profesional de los estudiantes, genera información importante para el análisis del desenvolvimiento académico de los estudiantes, pero esta información generada es almacenada de manera incorrecta y con ausencia de buenas prácticas para salvaguardar la seguridad de la información.

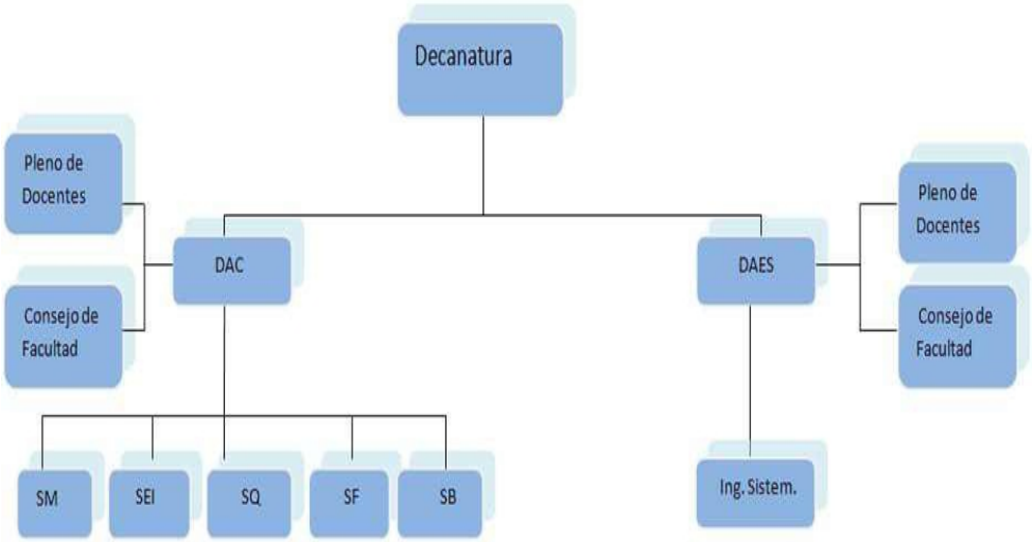
4.1.1. Historia de la institución

La Facultad de Ciencias fue creada con la Ley Universitaria N° 23733, en 1984, entró en funcionamiento el 26 de agosto de 1994, según Resolución Rectoral N° 382-94-UNASAM. desde entonces, conformada por la Escuela Profesional de Matemática y Estadística e Informática. Ya el 18 de febrero de 2004, con Resolución N° 005-

2004-UNASAM, se aprobó la creación de la carrera de Ingeniería de Sistemas e Informática.

4.1.2. Organigrama Académico

Gráfico N° 4.1. Organigrama Académico de la Facultad de Ciencias



Elaboración propia

4.1.3. Organigrama Administrativo

Gráfico N° 4.2. Organigrama Administrativo de la Facultad de Ciencias

Elaboración propia

4.1.3. Identificación de los objetivos de la institución

En la Facultad de Ciencias se identificaron los siguientes objetivos principales:

A. Salvaguardar, desarrollar, revalorar y transmitir de manera actualizada, la herencia científica, tecnológica, cultural y artística de la comunidad huaracina, peruana y de la humanidad.

B. Formar profesionales con una alta visión integral en lo científico, humanístico y tecnológico, con pleno sentido de responsabilidad social de acuerdo a las necesidades de la región.

C. Proyectar soluciones integrales a la comunidad ancashina, basados en investigaciones científicas, para promover su cambio y desarrollo.

4.1.4. Identificación de las funciones generales de la institución

En la Facultad de Ciencias se identificaron las siguientes funciones generales:

A. Formación de profesionales: esta función comprende las acciones académicas e instructivas extra curriculares que se realizan para el cumplimiento y ejecución del proceso curricular, cuyo fin final es aumentar y enriquecer de conocimiento y habilidades a los estudiantes.

B. Investigación: orientada a la producción de nuevos conocimientos y el descubrimiento de nuevos procesos innovadores para su aplicación en favor de la solución a problemas o interrogantes de carácter científico y social.

C. Extensión cultural y la proyección social: Implementar y ejecutar programas de promoción social, atención y apoyo a la solución de problemas sociales.

D. Educación continua para contribuir al desarrollo humano.

E. Administrativo: es importante ejecutar una apropiada administración de los recursos, organizada transparente y responsable de los bienes y servicios de su propiedad en beneficios y satisfacción de los estudiantes.

F. Administrar con criterios de ética, transparencia, eficacia, calidad e innovación la información generada por los docentes y estudiantes de la facultad.

G. Estimular la participación de la comunidad académica en acciones destinadas a mejorar las condiciones tecnológicas e informáticas de la facultad

H. Promover los programas de capacitación y perfeccionamiento del personal en las áreas de su competencia con la elaboración de un plan de capacitación.

4.1.5. Grupo de interés institucional

La Facultad de Ciencias interactúa con diversas entidades relacionadas al servicio público y social, así como con otros grupos de interés, como instituciones públicas y privadas, estos grupos de interés en muchos casos requieren y solicitan, el intercambian de información de manera física o digital. Los grupos de interés se

concentran fundamentalmente en entidades que requieren de profesionales y estudiantes de pre-grado. Quienes son los actores principales en brindar servicios y son los encargados del cumplimiento de las metas y objetivos de la facultad.

Entre los principales grupos de interés / actores de la Facultad de Ciencias se muestran a continuación.

Figura N° 4.3. Grupos de interés

Elaboración propia

Otros grupos de Interés / Actores que se relacionan con la Facultad de Ciencias de manera indirecta son:

- Universidades privadas.
- ONG´s.
- Instituciones educativas Públicas y Privadas.
- INEI.
- Entidades Gubernamentales.
- Otros

4.1.6. Orientación estratégica de la TIC.

La Facultad de Ciencias, no cuenta con un Plan de Desarrollo Institucional, la orientación es empírica y a base de conocimientos anteriores, cabe rescatar que esta orientación fundamenta sus estrategias en la misión y visión de la institución, este proyecto de investigación buscara brindar una orientación estratégica de manera que los servicios administrativos se desarrollen de manera eficiente, eficaz en términos de seguridad de la información, de modo que mejoramos la atención a los estudiantes y docentes de la universidad para ser una institución moderna, predecible y segura administrativamente, utilizando tecnologías de información seguras, todo ello coadyuvando a fortalecer la imagen institucional.

4.1.7. Factores Críticos de Éxito Institucional

Los factores críticos de éxito de acuerdo a Porter (1998) son aquellas variables en las que la institución puede influir a través de sus decisiones y medidas que pueden afectar, significativamente, las posiciones competitivas generales de las distintas compañías de una industria.

Para el caso de la Facultad de Ciencias por ser una institución pública, los Factores Críticos de Éxito se constituyen en las variables que pueden afectar su posición comparativa y de cumplimiento de su orientación estratégica; Misión y Visión.

A continuación, se muestra la tabla de los Factores Críticos de Éxito de la Facultad de Ciencias de la UNASAM.

Cuadro N° 4.1: Factores críticos de éxito

FACTORES CRÍTICOS DE ÉXITO - FCE	DESCRIPCIÓN DE LOS FACTORES CRÍTICOS DE ÉXITO	OBJETIVOS GENERALES DE LA FACULTAD DE CIENCIAS	CONTRIBUCIÓN POTENCIAL
Mejoramiento del acceso a la información	Implica la necesidad por parte de la Facultad de Ciencias de ofrecer al estudiante un servicio eficiente, eficaz, efectivo y oportuno en sus procesos administrativos a través de las TIC.	Brindar al estudiante un servicio rápido y oportuno, inclusivo y con carácter universal.	Mejorar y ampliar la cobertura de la seguridad de información en los servicios que las oficinas realizan. Asegurar y fortalecer la implementación de sistemas de calidad.
Fortalecimiento de la Gestión Institucional	Implica la integración, consolidación de los procesos institucionales a través de sistemas de información, a fin de lograr una gestión moderna y eficiente que responda a las demandas existentes por parte de los estudiantes y docentes en relación con la calidad de la información.	Ejercer una gestión de la información moderna, a través de sistemas de información que basen su construcción teniendo en cuenta el plan estratégico del SGSI, para contar con sistemas que manejen información segura y fiable.	Fortalecer la gestión de data de los recursos humanos. Modernizar los activos informáticos en las oficinas de la facultad de Ciencias Optimizar los procedimientos donde se maneje información valiosa para la facultad. Mejorar la infraestructura física y la gestión presupuestal.
Integridad y Transparencia administrativa	Se refiere a la imagen de la Facultad. Efectividad para detectar casos de corrupción y mal manejo de la información. Incrementar la confianza del estudiante a través de la transparencia, independencia e integridad de la información.	Generar confianza en las instituciones con las que interactúa, con intercambio de información la Facultad de Ciencias.	Fortalecer el monitoreo y control de los administradores de información.

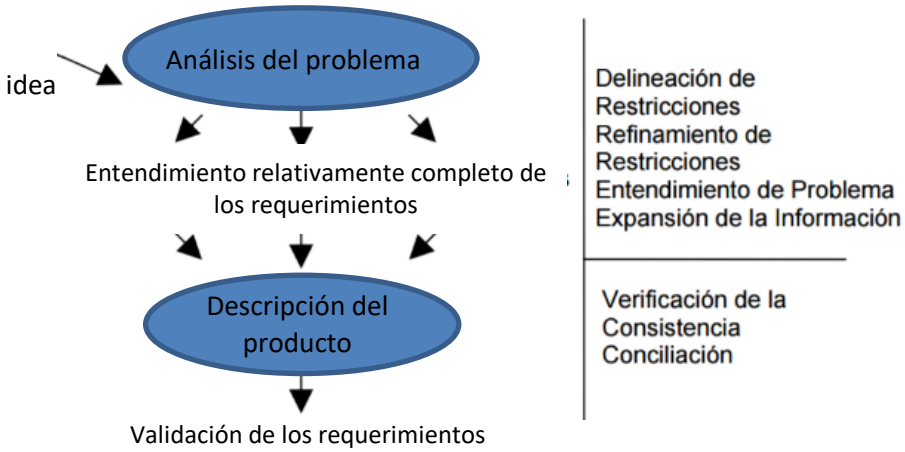
Fuente: Elaboración propia

4.2. IDENTIFICACIÓN Y DESCRIPCIÓN DE REQUERIMIENTOS

Para identificar los requerimientos se aplicaron las técnicas de ingeniería de requerimientos, con el fin de asegurar que los requerimientos obtenidos refieran las características necesarias para evitar gastos innecesarios y pérdida de tiempo al ser implementados se emplea este enfoque holístico para recoger, organizar, establecer y documentar los requerimientos del sistema; este proceso que establece y mantiene acuerdos sobre los cambios de requerimientos, entre los usuarios y el investigador busca ayudar a conocer, que controles de seguridad de la información se necesitan construir.

Para realizar un análisis completo de los requerimientos del proyecto de investigación es necesario identificar los problemas de la institución

Figura N° 4.4 Grupos de interés



Elaboración propia

4.2.1. Identificación de problemas

El principal problema en relación a la seguridad de la información que se observa en la facultad de ciencias es que no se han establecido los controles de seguridad para garantizar la disponibilidad, integridad y confidencialidad de la información, así mismo esto genera que los activos informáticos estén expuestos a riesgos e incidentes que amenazan la seguridad y el normal funcionamiento de los sistemas de información que dan soporte a las actividades de la institución.

A demás se identificaron otros problemas relacionados con la seguridad de la información.

- **P1.** No cuenta con una unidad u oficina de Informática y/o Sistemas que disponga sus propios recursos para la ejecución de metodologías que salvaguarden información valiosa para la Facultad.
- **P2.** No cuenta con un plan estratégico de tecnologías de información.
- **P3.** Infraestructura tecnológica implementada sin ningún estudio técnico.
- **P4.** Infraestructura Tecnológica - Hardware y software desfasados y/o Irregulares.

P5. Hardware (equipos de cómputo) y sus redes de comunicación (LAN) está bajo la responsabilidad de la Jefatura del Centro de Cómputo dependencia que no cuenta con presupuesto para realizar acciones preventivas y reactivas con respecto a los activos informáticos.

P6. Instrumentos Normativos de Gestión mal estructurados y desfasados.

P7. Bajo nivel de remuneración del personal.

P8. Falta de capacitaciones al personal que encargado de los recursos informáticos.

P9. Inadecuada infraestructura eléctrica para la prestación de servicios en los centros de cómputo.

P10. Desconocimiento de los problemas de seguridad de la información.

4.2.2. Análisis FODA de la Facultad de Ciencias

Para el análisis de la situación actual se revisaron los componentes internos y externos correspondientes s los servicios TIC. A nivel Interno se analizaron los procesos, infraestructura, tecnología y organización respecto a la seguridad de información en la Facultad de Ciencias.

A nivel externo se analizaron los grupos de interés o Stakeholders, sus expectativas, así como los aspectos científicos, económicos, sociales y tecnológicos que directamente podrían afectar, la pérdida de información, a la reputación institucional. Como resultado de todo este análisis, se resumieron los principales factores en una matriz FODA.

A continuación, se detallan las principales fortalezas, debilidades, oportunidades y amenazas identificadas en la Facultad de Ciencias.

Cuadro N° 4.2: Análisis FODA de la Facultad de Ciencias

FORTALEZAS	DEBILIDADES
F1. Voluntad por parte de los responsables de las oficinas para el fortalecimiento de la facultad de ciencias. F2. Personal con experiencia profesional, dispuesto a comprometerse con el logro de los objetivos de la Facultad de Ciencias. F3. Imagen como entidad con una gran reputación dentro de la provincia. F4. Haber logrado un papel direccional de servicios de formación profesional. F5. Tener capacidad para suscribir convenios con entidades públicas y privadas destinadas a actividades informáticas. F6. Relaciones inter institucionales óptimas para realizar actividades complementarias de intercambio de información. F7. Capacidad de generar recursos propios	D1. No se ha implementado adecuadamente los procesos de seguridad de la información en las actividades del personal D2. Insuficiente infraestructura e Inadecuada distribución de espacios, almacenes para bienes y equipos que contienen información valiosa para la Facultad de Ciencias. D3. Falta de estudio técnico para la adquisición de equipos informáticos. D4. Poca difusión de los programas académicos direccionados al desarrollo y capacitación del personal. D5. Bajo nivel de atención y orientación a los usuarios. D6. Predominio del estilo de dirección no participativo e inadecuado proceso de toma de decisiones.

OPORTUNIDADES	AMENAZAS
O1. Existencia de proyectos informáticos formulados por docentes y estudiantes, que pueden incorporarse e implementarse para mejorar las operaciones dentro de la Facultad de Ciencias. O2. Posee escuelas profesionales que desarrollan estudios para la automatización de procesos y obtener datos e información de forma eficaz y eficiente. O3. Convenio estratégico con el organismo rector de gobierno electrónico - ONGEI. O4. Existencia de convenios de desarrollo digital que posibilita la ejecución de programas sociales (Alfabetización Digital) mediante convenios de cooperación. O5. Existencia de proyectos en materia de seguridad de la información a través de la implementación de la fibra óptica. O6. Acceder a las políticas nacionales y normas técnicas para la implementación de sistemas informáticos certificados y sistemas legitimados.	A1. Procesos y procedimientos establecidos parcialmente, que en su mayoría se generan en base a la experiencia y no en políticas definidas. A1. Desarticulación entre los niveles de gobierno. Ausencia y falta de coordinación entre Autoridades administrativas, docentes y estudiantes. A2. Ausencia de políticas de seguridad de la información. A3. Carencia de un Sistema de Gestión de la Seguridad de la Información. A4. Bajo nivel de la calidad de los servicios en la mayoría de las oficinas de la facultad de ciencias, debido a la ausencia de herramientas de gestión y equipos tecnológicos. A5. Ausencia de grupos de trabajo, comunidades académicas y círculos de investigación que focalicen sus esfuerzos en resolver problemas vinculados con el desarrollo e implementación de proyectos informáticos que solucionen problemas como la seguridad e integridad de la información. A6. Deterioro progresivo de los patrimonios informáticos. A7. Perdida de información y tiempo al ejercer funciones administrativas.

Fuente: Elaboración propia

4.2.3. Análisis GAP para la identificación de la brecha

A. Se realizo el análisis GAP bajo tres pilares de análisis: procesos, tecnología y de potencial humano, de esta manera se presentarán los resultados con los criterios de cumplimiento establecidos en la norma ISO 27001- 2:2014 por la organización internacional de estándares ISO, específicamente en los aspectos y mejores prácticas que deberían tener las organizaciones para tratar los temas de seguridad de la información.

B. Se realizo el levantamiento de información para posteriormente hacer el análisis de cumplimiento e identificar las diferencias con respecto a los controles y objetivos de control que se encuentran distribuidos en los dominios de la ISO 27001- 2:2014.

C. Posteriormente se definieron los indicadores adecuados para medir la gestión de incidentes de la seguridad de la información

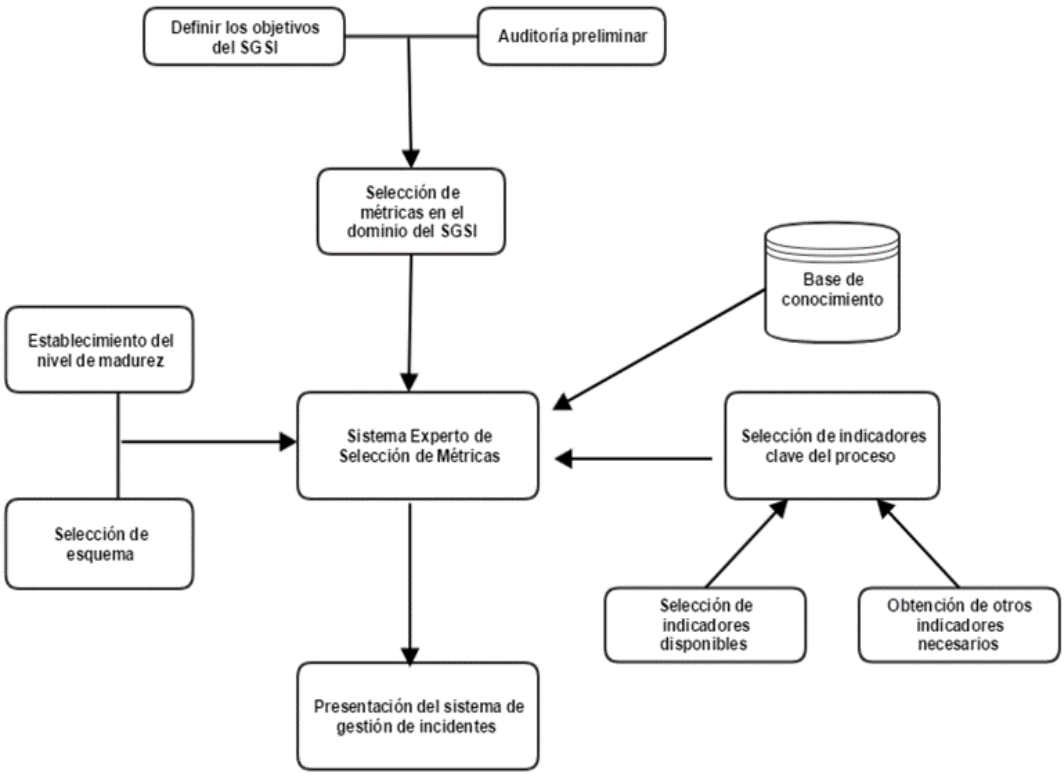
D. Una vez definidos los indicadores se realizó el análisis de la información e informe de resultados de evaluación y diagnóstico, bajo la norma ISO/IEC 27001-2:2014.

E. A continuación, se determinaron las amenazas potenciales, para determinar la probabilidad de que una amenaza propicie la materialización de un riesgo de seguridad de la información a través de la explotación de una vulnerabilidad. Se determino cuál es el impacto de la materialización del riesgo para la Facultad de

Ciencias, en términos financieros, de la operación y de la imagen institucional.

F. Se identificaron los controles necesarios para llevar a cabo el tratamiento de los riesgos, minimizar, transferir o evitar los riesgos identificados y priorizados.

Figura N° 4.5. Procesos que involucran el análisis GAP



Elaboración propia

4.3. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

4.3.1. Evaluación y Análisis GAP

La evaluación y análisis GAP en el que contrastamos los controles y las políticas de seguridad de la Facultad de Ciencias actualmente, frente a la norma ISO 27000, nos mostró la realidad contra el estado esperado o ideal. Las diferencias entre estas situaciones delimitaran las brechas de seguridad de la información, que con los controles implantados se eliminaran.

El análisis entre el estado actual y el estado ideal bajo estándares y bunas prácticas, lleva a la identificación de los posibles riesgos a los que está expuesta la institución y que son posibles incidentes que se clasifican según la criticidad y el impacto que pueden generar.

Con este análisis podremos estratificar la Facultad de Ciencias permitiéndonos identificar de forma general, el nivel de complejidad que le puede significar a la facultad la implementación de su Modelo de Gestión de Incidentes de Seguridad de la Información.

Este enfoque permite adquirir datos referentes a percepciones e instituir prioridades de mejora de los incidentes de seguridad de la información, realizando un análisis de las diferencias entre unas y otras, para las diferentes características del servicio, en lo que llamamos Análisis GAP. Con esto, los planes de mejora (CONTROLES) originados por la información proveniente de la revisión del incidente, pueden clasificarse de modo que los recursos

sean utilizados más eficientemente en la consecución de mejoras significativas.

Para hacer este análisis, se tomó como instrumento la estratificación del modelo actual de seguridad de la información, para la estrategia de TI, estos definen tres tipos de medida: bajo, medio y alto, cuyo valor se consigue al evaluar los siguientes factores: primero, el valor del presupuesto de funcionamiento, segundo, la infraestructura asociada al total de computadores, y tercero, los servicios ofrecidos en línea y la capacidad del área de sistemas. Finalmente, para poder estratificar a la Facultad de Ciencias, se utilizó el siguiente formato, el cual muestra las respuestas que fueron seleccionadas de acuerdo a la información proveída por los responsables de los activos informáticos y responsables de cada oficina de la institución que maneja información vital, su respectivo puntaje asignado a cada una de ellas, puntajes que fueron sumados para así obtener el valor de estratificación de la institución.

Cuadro N° 4.3 Análisis GAP

Parámetros de Evaluación	Opciones de Respuesta	Puntos	Observación
Presupuesto	Menos de S/ 3000 mensuales	1	
	S/3000 < X < S/5000	2	
	Más de S/ 5000 mensuales	3	
N° total de computadoras	Menos de 20 computadoras	1	
	20 < X < 50	2	
	Más de 50 computadoras	3	
N° de servidores	1 < X < 5	1	
	5 < X < 10	2	
	Más de 10 servidores	3	
N° de personal vinculados con la tecnología	Menos de 5 empleados	1	
	5 < X < 20	2	
	Más de 20 empleados	3	
Función técnica del área de sistemas	No existe el área de informática y de sistemas	1	
	Área enfocada a la operación del día, que cumple labores reactivas	2	
	Área que planea y desarrolla proyectos nuevos e innovadores	3	
Existe autonomía administrativa y económica en el área de sistemas	No existe autonomía	1	
	Existe autonomía administrativa	2	
	Existe autonomía administrativa y económica	3	
Existencia y objeto de la WAN	WAN publica solo para correos y navegar	1	
	WAN publica con servicios ofrecidos al cliente	2	
	La existencia de una WAN privada	3	
Transaccionalidad en la WEB	Solo ofrece servicios de consulta	1	
	Transaccionalidad local, generación de servicios con una BD y APP	2	
	BD, APP y Transaccionalidad con otras entidades externas	3	
Desarrollo de software	No se desarrolla software	1	
	Si se desarrolla para algunos procesos internos	2	
	Si se desarrolla software para necesidades internas y externas	3	

Para lograr puntuar y definir el nivel de estratificación es importante determinar los puntajes independientes obtenidos por cada parámetro de evaluación, la suma de los puntajes de las respuestas en el caso de la Facultad de Ciencias es igual a 17 puntos.

De acuerdo al nivel de estratificación de la Facultad de Ciencias, se determina según el análisis, los rangos de valoración.

Cuadro N° 4.4 Rango de puntaje total del análisis GAP

	RANGO DE PUNTOS	ESTRATO
1	Menor a 9 puntos	**Bajo**
2	Entre 10 y 18 puntos	**Medio**
3	Mayor a 18 puntos	**Alto**

Fuente: Elaboración propia

Estos rangos de valoración nos permiten determinar el esfuerzo que implicara para la implementación del Sistema de Gestión de Incidentes de Seguridad de la Información, ya que nos encontramos en un estrato MEDIO que conlleva a mejorar los parámetros bajos (Rojos).

4.3.2. Análisis de Brecha – Áreas de Control Herramienta ISO 27001

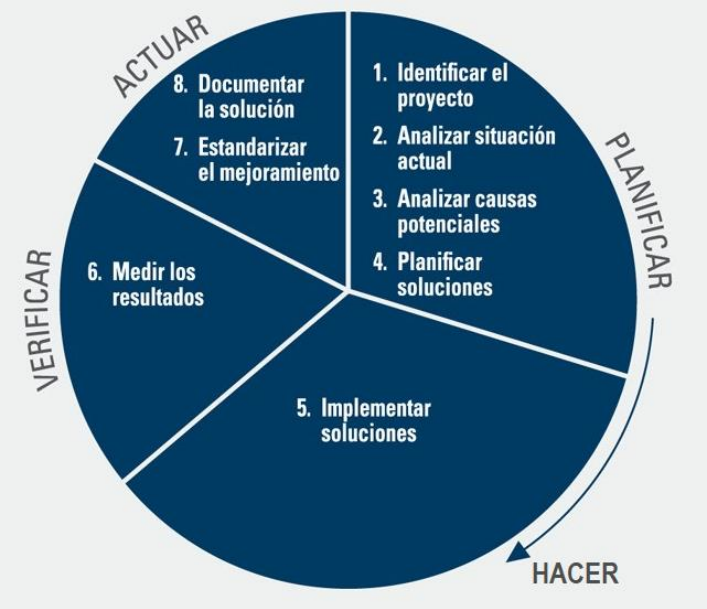
Es importante utilizar la herramienta de análisis de brecha de la ISO 27001 para concluir que el nivel de cumplimiento de los requisitos está en un 40%, el requisito mínimo de madurez de una entidad para lograr una gestión medible en establecimientos de control de seguridad de la información debe ser igual o superior a 70%, el análisis obtenido de acuerdo a cada área nos mostrará que controles establecer en la facultad de ciencias.

CAPITULO V

DISEÑO DE LA SOLUCIÓN

El diseño de la solución se realiza tomando como metodología el Ciclo de Deming, que es establecido por la ISO/IEC 27000 como esquema de arquitectura y construcción de un SGSI, a continuación, detallamos cada una de estas etapas para el diseño de la solución planteada.

Cuadro N° 5.1 Ciclo de Deming



Fuente: Elaboración Propia

Para identificar el proyecto es importante conocer el contexto de la Facultad de Ciencias, ello implica conocer y entender la organización, su contexto, sus fortalezas, debilidades, oportunidades y amenazas, para comprender cuales son las necesidades y expectativas de las partes interesadas o stakholder, esto determinará el alcance del proyecto de investigación. El liderazgo y compromiso de la alta dirección en la Facultad de Ciencias, es importante para

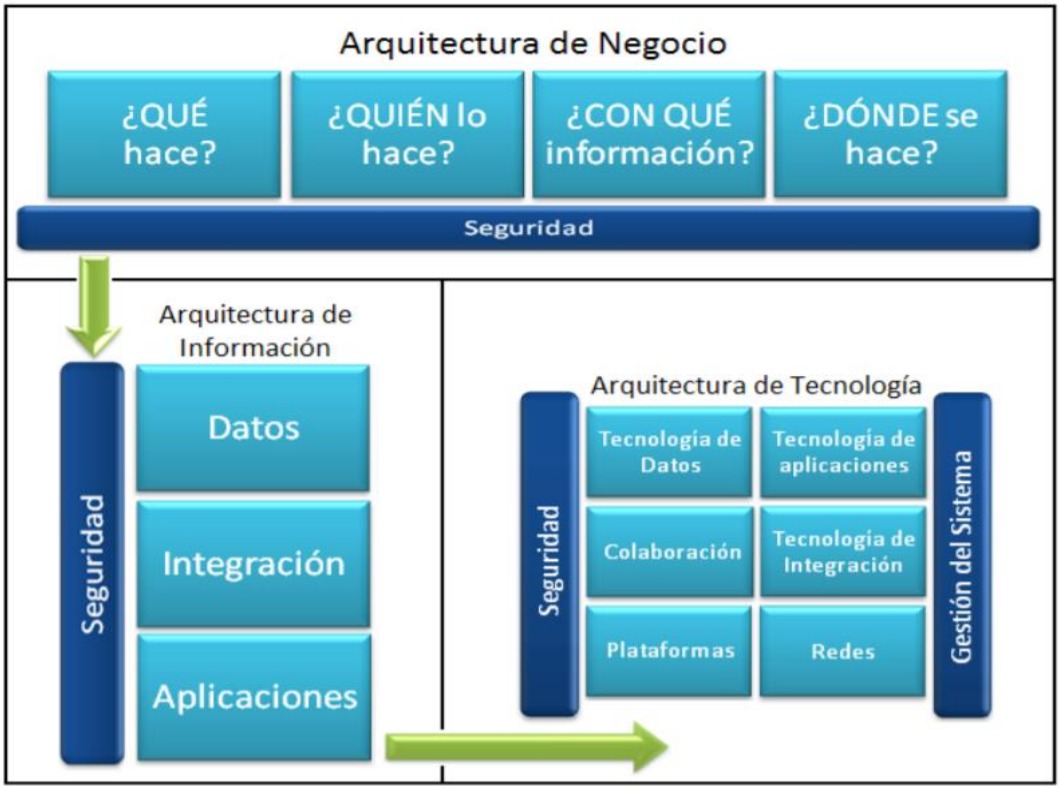
determinar la Política de Seguridad de la Información y determinar los roles, las responsabilidades y nombrar a los encargados de la seguridad en la facultad. La planificación incluye un marco general y los objetivos de seguridad de la información dentro de las oficinas de la facultad para abordar los riesgos y oportunidades estratégicas de la gestión de incidentes. Definir una metodología de evaluación del riesgo apropiada e identificar las amenazas en relación al soporte con que se cuenta, los recursos humanos, los recursos informáticos, las vías de comunicación y los procedimientos documentados es de vital importancia. Implementar soluciones estableciendo las operaciones a través del control y planeación operacional con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades. Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles para la evaluación de riesgos y tratamientos de riesgos de la seguridad de la información. Para medir los resultados la Facultad de Ciencias deberá ejecutar procedimientos de monitorización y revisión para detectar a tiempo los errores en los resultados generados por el procesamiento de la información; identificar brechas e incidentes de seguridad; detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores; determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas, este monitoreo y medición nos permitirá hacer el análisis y evaluación que nos permitirán realizar periódicamente las auditorías internas revisadas periódicamente por la alta

dirección para garantizar que el alcance definido sea el adecuado y que las mejoras en el proceso sean evidentes a través de acciones correctivas y mejora continua esto nos permitirá documentar la solución y estandarizar el mejoramiento.

5.1. Arquitectura Tecnológica de la Solución

La arquitectura de seguridad de información en la Facultad de Ciencias es parte de la arquitectura de servicio, la facultad posee muchas arquitecturas como la arquitectura del negocio, la arquitectura de información, la arquitectura tecnológica y la arquitectura de seguridad que es trasversal a las demás.

Cuadro 5.2 Diseño de la Arquitectura Tecnologica del negocio



Elaboración Propia

Dentro de la arquitectura del negocio solo nos centraremos a analizar la arquitectura de seguridad de la información. Para analizar la seguridad de las arquitecturas del negocio, es importante hacerse las siguientes preguntas ¿Qué hace? ¿Quién lo hace? ¿Con qué lo hace? ¿Dónde se hace? Estas preguntas nos permitirán definir el diseño conceptual que define la operación del negocio, bajo dos arquitecturas principales, primero, la arquitectura de información que es la encargada del estudio, análisis, organización, disposición y estructuración de la información en espacios de información, y de la selección y presentación de los datos en los sistemas de información interactivos y no interactivos para la integración en aplicaciones. Y la segunda, la arquitectura de tecnología, que define la gestión de los sistemas a través de las tecnologías de datos, la tecnología de aplicaciones, la tecnología de integración, redes, plataformas y colaboración.

5.2. Diseño de la Funcionalidad de la Solución

Cuadro N° 5.3: Descripción de las fases de la arquitectura ISO 27000

FASE	MÉTODO	ALCANCE
Fase I	Conocimientos y contextualización de los procesos	1. Se debe realizar un levantamiento detallado de la información necesaria para entender los procesos críticos y las falencias de control de la Facultad de Ciencias. 2. Se debe realizar un estudio detallado del flujo de actividades del proceso académico y la infraestructura con el propósito de identificar cada uno de los elementos que interactúan, la plataforma tecnológica que lo soporta (software y hardware).

		3. Identificar el estado actual del proceso a nivel de Seguridad de la Información usando marcos de referencia de normas internacionales actuales. 4. Revisión y análisis de la documentación actual: es importante poder definir la estrategia para el alcance del modelo de gestión de incidentes, por ello es importante la revisión de los diferentes planes (Plan Estratégico PETIC, Plan Desarrollo, Planes de Acción, Manual GEL, SGC).
Fase II	Gobierno de Seguridad de la Información	1. Actualización del análisis GAP basado en la ISO 27001 del año 2017, a la actualidad de la institución y los requerimientos de la norma ISO 27002:2013. 2. Desarrollar una propuesta para el gobierno de seguridad de la información para la facultad de ciencias, de acuerdo a los cambios y las necesidades actuales de la organización. 3. Definir la gestión de métricas de seguridad la información en base a la norma ISO 27004. 4. Definición de Políticas de seguridad de la información, para brindar cumplimiento a los requerimientos del estándar ISO 27001:2013 y la norma ISO 27002:2013. 5. Definir y construir el Manual de seguridad de la información. 6. Definición del proceso de seguridad de la información, y su adopción y definición en el SGSI.
Fase III	Gestión de Seguridad de la Información	1. Revisión y actualización de la gestión de activos, considerando los cambios actuales de la organización. 2. Revisión y actualización de la gestión de riesgos de la organización en base a proyectos desarrollados en el año 2016, considerando los cambios de la organización para el año 2017. 3. Análisis de la gestión de los controles de seguridad de la información de acuerdo a los requerimientos de la norma ISO 27001:2013/27002. 4. Definir el Plan de Tratamiento de Riesgos de Seguridad de la información para la facultad de ciencias. 5. Definición de la arquitectura de seguridad informática de acuerdo a los criterios del plan de tratamiento de riesgos.

Fase IV	Tecnología y Seguridad de la Información	1. Resumen Ejecutivo: Que especifique la situación actual y las recomendaciones respectivas (Profundizar sobre como la entidad puede mejorar para incrementar el nivel de prevención y control de fugas de información). 2. Informe detallado de hallazgos, que contenga como mínimo: identificación de activos críticos, tipificación y distribución de activos de la información, los medios de almacenamiento de activos de la información y protecciones existentes, los medios utilizados para el intercambio de información entre dependencias internas y con terceros y protecciones existentes sobre el mismo si las hubo. 3. Informe detallado sobre los hallazgos generados de las pruebas de vulnerabilidades, las cuales deben estar organizadas por su nivel de criticidad, con sus respectivas recomendaciones para elevar los niveles de protección. 4. Informe sobre las pruebas de Hacking ético con los siguientes alcances: Vulnerabilidades identificadas, Numero CVE de cada una, clasificación, evidencia de los ataques exitosos y fallidos, plan de acción para su remediación, detalle de las soluciones propuestas, resultados para el mapa de riesgos.
Fase V	Implementación Practica.	1. Definir las actividades necesarias para dar aplicación a las políticas, procedimientos y controles definidos en el SGSI y realizar el “Plan para la implementación”, el cual debe incluir el programa de implementación detallando las actividades y los tiempos en que se deben implementar, de acuerdo con las prioridades para atender los riesgos asociados según su valoración. 2. Identificar, si hay lugar a ello, los recursos tecnológicos requeridos para garantizar la adecuada aplicación de una política particular. 3. Elaborar la documentación, formatos y procedimientos requeridos para la administración del sistema de seguridad de la información y la aplicación de las políticas. 4. Definir indicadores adecuados para medir la gestión de la seguridad de la información. 5. Definir los procesos críticos que soportan el servicio, la prioridad de cada uno de estos servicios, los tiempos estimados de recuperación y los máximos tolerables de interrupción de los servicios, mediante un análisis BIA adecuado a las necesidades.

Fase VI	Capacitación y Concientización.	1. Definición del alcance del plan de concientización y entrenamiento con respecto a las políticas, estándares y procedimientos de la seguridad de información desarrollada. 2. Generación de una cultura de Seguridad de la información dentro de la organización enmarcada dentro de una mejora continua.

Fuente: Elaboración propia

5.3. Diseño de la funcionalidad de la solución

5.3.1. ISO 27000 Fundamentos

Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Con el fin de mejorar la calidad de los servicios informáticos en la Facultad de Ciencias se pretende aplicar el presente Sistema de Incidentes de Seguridad de la Información a los procesos, recursos informáticos y tecnológicas de las oficinas de la facultad, con el fin de establecer políticas para gestionar adecuadamente la seguridad de la información para ser aplicada y cumplida por todos los responsables de las oficinas en estudio, además se realiza el estudio de los incidentes para realizar la políticas de seguridad.

5.3.2. ISO 27001 - Especificaciones de un SGSI

Definir una política de seguridad que incluya el marco general y los objetivos de seguridad de la información de la organización; considere requerimientos legales o contractuales relativos a la seguridad de la

información; esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI; establezca los criterios con los que se va a evaluar el riesgo; esté aprobada por la dirección.

5.3.3. Políticas del Sistema de Gestión

La Facultad de Ciencias pretende que la información manejada por la entidad en sus diferentes áreas y oficinas; se encuentre debidamente protegida de los incidentes de seguridad de la información, con el fin de preservar y salvaguardar la confidencialidad, disponibilidad e integridad de la información, ya que es una entidad pública.

5.3.4. ISO 27002 - Código de buenas prácticas

El código de buenas prácticas establece los controles; que deben ser elegidos en base a una evaluación de riesgos de los activos más importantes de la Facultad de Ciencias. Al contrario de lo que muchos gestores piensan, la ISO 27002 se puede utilizar para apoyar la implantación del SGSI en cualquier tipo de organización, centrando sus directrices en la gestión de activos.

5.3.5. Metodología de Evaluación de Riesgo

La metodología que se utilizó nos permite puntualmente analizar el impacto de los incidentes de seguridad de la información, buscando gestionar los riesgos a través de la identificación de las amenazas y

las vulnerabilidades, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas. Para el proyecto se eligió la metodología MAGERIT; para el análisis y gestión de los riesgos, a continuación, se describen las fases de aplicación.

- Fase de Identificación de los Activos.
- Fase de Valoración de los Activos.
- Fase de Identificación de las Dependencias de los Activos.
- Fase de Identificación de Amenazas y Vulnerabilidades.
- Fase de Valorización de Amenazas.
- Fase de Determinación de los Niveles de Riesgo.
- Fase de Determinación del Impacto Potencial.
- Fase de Determinación del Riesgo Potencial.

CAPITULO VI

CONSTRUCCIÓN DE LA SOLUCIÓN

6.1. Construcción

6.1.1. Alcance e identificación de activos

La identificación de los activos de información se realizó de acuerdo al alcance del proyecto, el cual solo contempla los procesos donde se maneja información crítica, por lo tanto, únicamente se identificaron los activos de información que son administrados y utilizados por las oficinas que manejan información vital para la Facultad de Ciencias, estas oficinas que manejan información importante fueron elegidas de acuerdo a la importancia jerárquica de la institución, como la decanatura, las direcciones de escuela, las jefaturas de departamento, los laboratorios de cómputo y las oficinas administrativas de las escuelas profesionales, los cuales fueron el insumo para el proceso de valoración de riesgos de los activos de información.

A continuación, describimos los criterios tomados para proteger la información de acuerdo a la importancia para los usuarios, la infraestructura tecnológica, la información asociada al personal, los procesos y las actividades desarrolladas por la Facultad de Ciencias.

INFORMACION A PROTEGER

Información asociada a nuestros clientes

Es toda la información relacionada con los usuarios de la Facultad de Ciencias de la UNASAM.

1. Alumnos de pregrado.
2. Alumnos de educación continua - especialización.
3. Egresados.

Información asociada a nuestra infraestructura tecnológica

1. Laboratorios
2. Red de comunicaciones

Información asociada a nuestro personal

1. Autoridades.
2. Docentes.
3. Jefes de Practica.
4. Personal administrativo no docente.

Información asociada a nuestras operaciones y actividades

1. Actividades académicas.
2. Actividades administrativas.
3. Actividades de investigación.
4. Actividades de disposición y control.

Información asociada a los servicios que presta la institución

1. Servicios académicos
2. Servicios administrativos
3. Servicios de investigación

6.1.2. Metodología de valoración de riesgos.

Es importante definir los pasos para el desarrollo de las actividades vinculadas con la identificación y clasificación de los activos de información del proceso y la pertinente valoración de los riesgos, para ello se utilizó Magerit, de acuerdo a esta metodología en los sistemas de información existen dos componentes esenciales, la primera, es la información que se maneja dentro del activo y la segunda, los objetivos que cumplen, estos componentes esenciales, que posteriormente marcan los requisitos de seguridad para el análisis de los activos y su respectiva valoración.

A continuación, se hace un análisis de los tipos de activos de información en la Facultad de Ciencias, además se detalla una descripción y su respectiva tipificación que nos permitirá asociarlas a los criterios de identificación de activos.

Cuadro N° 6.1: Tipos de activos de información

TIPO DE ACTIVO	CÓDIGO	DESCRIPCIÓN
Servicios	A1	Contempla los servicios prestados por la Facultad de Ciencias en la Universidad.
Datos/ Información	A2	Resoluciones, constancias, certificados, datos de gestión interna, credenciales, datos de validación de credenciales, datos de control de acceso, registro de actividades.
Software	A3	Programas, aplicativos, desarrollados, software base, sistema de información,
Equipos informáticos	A4	Hardware. Medios materiales, físicos, destinados a soportar directa o

		indirectamente los servicios que presta la organización.
Personal	A5	Personal administrativo relacionadas con los sistemas de información, personal que maneja información y tiene acceso a ello.
Redes de comunicaciones	A6	Servicios de comunicaciones contratados a terceros; medios de transporte que llevan datos de un sitio a otro.
Soporte de información	A7	Dispositivos físicos que permiten almacenar información de forma permanente.
Equipamiento auxiliar	A8	Otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.
Instalaciones	A9	Lugares donde se hospedan los sistemas de información y comunicaciones e información valiosa para la entidad.

Fuente: elaboración propia

A continuación, relacionamos el inventario descrito anteriormente con los activos de información que se identificaron en la Facultad de Ciencias.

Cuadro N° 6.2: Inventario de activos de información

Nombre del Activo	Descripción del activo	Tipo de activo	Contenedor
Centro de cómputo G-301	Primer laboratorio, donde se prestan servicios de cómputo a los miembros de la comunidad académica de la Facultad de Ciencias.	A9	Facultad de Ciencias
Centro de cómputo G-302	Segundo laboratorio, donde se prestan servicios de cómputo a los miembros de la comunidad académica de la Facultad de Ciencias.	A9	Facultad de Ciencias

Centro de cómputo G-303	Tercer laboratorio, donde se prestan servicios de cómputo a los miembros de la comunidad académica de la Facultad de Ciencias.	A9	Facultad de Ciencias
Oficina del departamento de sistemas e informática	Lugar donde se prestan los servicios de trámites administrativos y se hace la recepción y almacenan todos los documentos	A9	Facultad de Ciencias
Oficina del departamento de matemática	Lugar donde se prestan los servicios de trámites administrativos y se hace la recepción y almacenan todos los documentos.	A9	Facultad de Ciencias
Oficina del departamento de estadística e informática	Lugar donde se prestan los servicios de trámites administrativos y se hace la recepción y almacenan todos los documentos.	A9	Facultad de Ciencias
Decanatura	Lugar donde se prestan los servicios de trámites administrativos y se hace la recepción y almacenan todos los documentos.	A9	Facultad de Ciencias
Almacén	Lugar donde almacenan oficios, resoluciones, informes, silabus y todo el acervo documentario de la Facultad de Ciencias.	A9	Facultad de Ciencias
Redes LAN 1	Red de los laboratorios G-301.	A6	Laboratorios de Computo
Redes LAN 2	Red de los laboratorios G-302.	A6	L.C.
Redes LAN 3	Red de los laboratorios G-303.	A6	L.C.
Red WAN	Red WAN de la facultad.	A6	Facultad de Ciencias
Red WIFI	Red Wifi utilizada por los equipos móviles y portátiles para acceder a	A6	

	los recursos de la red interna de la institución.		Facultad de Ciencias
Dispositivos de red	Equipos y dispositivos de red activos (switch, router).	A6	Decanatura
Computadores Administrador 1	Equipo utilizado para los servicios administrativos.	A4	Secretaría de Decanatura
Computadores Administrador 2	Equipo utilizado para los servicios administrativos.	A4	Oficina del departamento Académico de Sistemas
Computadores Administrador 3	Equipo utilizado para los servicios administrativos.	A4	Oficina de la Escuela profesional de sistemas
Computadores Administrador 4	Equipo utilizado para los servicios administrativos.	A4	Oficina de la Escuela profesional de estadística
Computadores de escritorio usuarios	Computadores de escritorio asignados a los colaboradores de la entidad.	A4	Oficinas Administrativas
Portátiles	Portátiles utilizados para fines y objetivos de la institución.	A4	Decanatura
Impresoras	Impresoras asignadas a las distintas oficinas de la facultad.	A8	Oficinas Administrativas
Software ofimático	Software que es utilizado en las oficinas de la Facultad de Ciencias.	A3	Oficinas Administrativas
Sistemas de bases de datos	Contenedor de datos e información almacenada, ordenada y disponible para ser procesado o consultado.	A3	Oficinas Administrativas
Antivirus	Antivirus utilizado en las portátiles y computadores de la Facultad de Ciencias.	A3	Laboratorios de cómputo, Oficinas

SIGA WEB	Sistema de Gestión Administrativa de la Universidad.	A3	Oficinas Administrativas
Sistema de Gestión documentaria	Sistema utilizado para la gestión documentaria.	A3	Oficinas Administrativas
Página WEB	Página web de la institución.	A3	Servidor Externo a la F.C.
Correos electrónicos	Correos corporativos y personales utilizados para la comunicación de la institución.	A3	Servidor Externo a la F.C.
Datos de autenticación	Usuario y Contraseña que utilizan los usuarios para ingresar a los recursos tecnológicos y aplicaciones.	A2	Laboratorios de Cómputo y Oficinas Administrativas
Log de evento de seguridad	Log que contiene los registros de los eventos de seguridad y de los eventos de administración sobre las aplicaciones.	A2	Laboratorios de Cómputo y Oficinas Administrativas
Registro de incidentes de seguridad	Registro de incidentes de seguridad reportados por la herramienta de mesa de ayuda.	A2	Jefe de los Laboratorios de Cómputo
Manuales de seguridad	Corresponde a los documentos, manuales y procedimientos relacionadas con la administración de la información y activos informáticos.	A7	Decanatura de la Facultad de Ciencias
Documentos	Registro de todos los documentos importantes para la institución, además de información valiosa para auditorias y controles futuros.	A7	Decanatura de la Facultad de Ciencias

Fuente: Elaboración propia

6.1.3. Valoración de activos de información

Al tener definidos e identificados los activos de información se valoró el grado de importancia y criticidad, para esto, se evaluó el grado de perdida que le puede generar a la Facultad de Ciencias en aspectos, financieros, legales y de imagen, en el ámbito financiero el criterio de valoración más utilizado actualmente es el precio de adquisición o coste del activo y su costo de mantenimiento, no solo por el análisis contable que hace la universidad sino también en el marco de contabilidad pública y de modernización del estado, sin embargo, existe una gran variedad de bases de valoración que, en mayor o menor medida, podrían resultar aplicables a los activos públicos, entre las que destacan son la valoración legal, que tiene como criterio de valoración el control y sanciones impuestas por la normatividad vigente de la facultad, el decreto legislativo de transparencia y acceso a la información pública y finalmente de imagen que están relacionados con las políticas de gobierno electrónico y la repercusión que puede tener la pérdida de confianza con actores externos o grupos de interés como la sociedad civil, la Superintendencia Nacional de Educación Superior Universitaria, universidades, entidades gubernamentales y el sector privado. En cada caso que al materializarse una amenaza se analizará el grado en que afecte su disponibilidad, integridad o confidencialidad. Para tal efecto, se utilizaron los siguientes criterios para realizar la respectiva valoración.

Tabla 6.3: Valoración de activos de información

ASPECTO	Criterio de valoracion	Criterio de valoración	Valor a asignar
FINANCIERO	Pérdidas económicas para la institución (porcentaje calculado sobre el costo de mantenimiento)	menor o igual a 0.25%	1
		mayor a 0.25% y menor o igual a 5%	2
		mayor a 5% y menor o igual a 20%	3
		mayor a 20% y menor o igual a 50%	4
		mayor al 50%	5
LEGAL	Incumplimiento de normatividad y legislación	No tiene repercucion frente a normatividad y contratos	1
		Genera llamados de atencion por parte de los entes de control	2
		Genera posibles sanciones menores por parte de los entes de control y reclamos por parte de terceros	3
		Genera sanciones ecónomicas por parte de los entes de control y demandas de terceros	4
		Genera sanciones mayores por parte de entes de control, cancelacion de contratos, suspensión de cargos y proceso administrativo.	5
IMAGEN	Afectación de la imagen de la institución	Conocido solo de manera interna en la institución pero no de interés publico	1
		Atención de algunas partes interesadas a nivel local que potencialmente puedan afectar a la institución	2
		Media atención de las partes interesadas a nivel local y regional.	3
		Alta atencion de las partes interesadas a nivel regional y nacional	4
		Conocimiento general a nivel nacional e internacional	5

Fuente: Elaboración propia

Para determinar la criticidad del activo se formularon las preguntas de acuerdo a las incidencias que pueden tener dentro de cada factor,

esto nos permitirá evaluar de forma ordenada y haciendo el análisis por cada criterio de valoración.

Tablas 6.4: Preguntas para determinar la criticidad del activo

Factores	Criterios	Pregunta
DISPONIBILIDAD	Financiero	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar pérdidas económicas para la institución?
	Legal	¿Si el activo o la información que se gestiona a través de él no están disponibles puede generar sanciones legales de entes de control o demandas de terceros?
	Imagen	¿Si el activo o la información que se gestiona a través de él no están disponibles puede afectar la imagen de la institución?
INTEGRIDAD	Financiero	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar pérdidas económicas para la institución?
	Legal	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede generar sanciones de entes de control?
	Imagen	¿Si el activo o la información que se gestiona a través de él son alterados sin autorización puede afectar la imagen de la institución?
CONFIDENCIALIDAD	Financiero	¿Su divulgación no autorizada puede relevar información sensible de la institución requerida para la toma de decisiones estratégicas y financieras?
	Legal	¿Su divulgación no autorizada puede afectar el cumplimiento de regulaciones impartidas por entes de control o puede generar demandas de terceros?
	Imagen	¿Su divulgación no autorizada puede afectar la imagen de la institución?

Fuente: Elaboración propia

6.1.4. Análisis de los niveles de criticidad

Para mejorar el aspecto operacional en la Facultad de Ciencias en cuanto a la seguridad de la información está asociado con los tres

aspectos de seguridad, confidencialidad, integridad y disponibilidad, que nos sirven para determinar el nivel de riesgo según los criterios de valoración, en nuestro caso hemos realizado el análisis de criticidad en base a la información obtenida de las interrogantes de acuerdo a las incidencias, desde el elemento más crítico hasta el menos crítico del total del universo analizado, diferenciando cuatro zonas de clasificación: la primera, alta criticidad que de acuerdo al rango es mayor o igual a 4, la segunda, mediana criticidad, que se encuentra entre el rango mayor a 2 y menor a 4, la tercera, baja criticidad y un último nivel de no aplicación. Al ser reconocidas estas zonas, es más sencillo diseñar una estrategia, para realizar estudios o proyectos que mejoren la confiabilidad operacional, la integridad de los datos y la disponibilidad de los sistemas que soportan las principales actividades de la Facultad de Ciencias, iniciando las acciones de control en el conjunto de procesos que sean parte de la zona de alta criticidad. Los criterios para analizar la criticidad, están ligados a la normativa de seguridad, costos de operación y mantenimiento, tiempo de reparación e imagen proyectada principalmente.

Estos criterios se relacionan con una ecuación matemática de ponderación y promedio donde se redondea al número superior, en Excel esta fórmula estaría expresada de la siguiente manera [=REDONDEAR.MAS(PROMEDIO(RANGO);0)] que genera

puntuación para cada elemento evaluado. La lista generada, es producto del trabajo analítico que permite instituir prioridades, y distribuir el esfuerzo que garantice el éxito maximizando la rentabilidad en la Facultad de Ciencias.

Para poder determinar con exactitud los niveles de criticidad del activo se valoró en la siguiente tabla:

Tabla 6.5: Nivel de criticidad de los activos de información

CRITERIO DE EVALUACIÓN	Rango de criticidad 0 a 5	Nivel de criticidad
La gestión del activo compromete en un alto grado la integridad y/o confidencialidad y/o disponibilidad de la información de la institución.	>= 4	**Alto**
La gestión del activo compromete en un nivel medio la integridad y/o confidencialidad y/o disponibilidad de la información.	> 2 y < 4	**Medio**
La gestión del activo compromete en un nivel bajo la integridad y/o confidencialidad y/o disponibilidad de la información de la institución.	> 0 y <=2	**Bajo**
La gestión del activo no compromete la integridad, confidencialidad y disponibilidad de la información de la institución.	Igual a 0	**No aplica**

Fuente: Elaboración propia

De acuerdo a la metodología planteada la siguiente valoración del nivel de criticidad de los activos de información y activos informáticos de la facultad de ciencias nos proporciona información relevante para hacer un esquema del sistema de gestión de incidentes y elegir con mayor exactitud los controles a implantar.

Tabla 6.6: Valoración del nivel de criticidad de los activos de información y activos informáticos

N°	Nombre del activo	VALORACIÓN DEL NIVEL DE CRITICIDAD DEL ACTIVO DE INFORMACIÓN													
		Confidencialidad			Integridad			Disponibilidad			Confidencialidad	Integridad	Disponibilidad	VALOR TOTAL	NIVEL DE CRITICIDAD
		Financiero	Legal	Imagen	Financiero	Legal	Imagen	Financiero	Legal	Imagen					
1	Centro de cómputo G-301	5	4	4	5	4	3	5	4	4	4	4	4	5	ALTO
2	Centro de cómputo G-302	5	4	3	5	4	3	5	4	4	4	4	4	5	ALTO
3	Centro de cómputo G-303	5	4	3	5	4	3	5	5	4	4	4	5	5	ALTO
4	Oficina del departamento de sistemas e informática	3	3	1	3	3	3	3	3	2	2	3	3	3	MEDIO
5	Oficina del departamento de matemática	4	5	3	4	4	3	4	4	3	4	4	4	4	ALTO
6	Oficina del departamento de estadística e informática	4	4	3	4	4	3	3	4	4	4	4	4	4	ALTO
7	Decanatura	3	2	1	3	2	3	3	3	2	2	3	3	3	MEDIO
8	Almacén	1	1	0	1	0	0	1	1	0	1	1	1	1	BAJO
9	Redes LAN 1	4	3	2	4	3	2	4	4	2	4	4	4	4	ALTO
10	Redes LAN 2	4	4	4	4	4	3	4	3	4	4	4	4	4	ALTO
11	Redes LAN 3	4	4	3	4	3	5	4	3	5	4	4	4	4	ALTO
12	Red WAN	1	2	0	1	1	0	0	2	1	1	1	1	1	BAJO
13	Red WIFI	3	2	3	3	2	3	4	3	2	3	3	3	3	MEDIO

14	Dispositivos de red	3	3	2	3	3	2	2	1	3	3	3	2	**3**	**MEDIO**
15	Computadores Administrador 1	4	3	1	4	3	1	2	1	2	4	4	2	**3**	**MEDIO**
16	Computadores Administrador 2	4	3	4	3	3	3	4	4	4	4	3	4	**4**	**ALTO**
17	Computadores Administrador 3	4	3	2	3	2	3	3	3	3	3	3	3	**3**	**MEDIO**
18	Computadores Administrador 4	5	4	5	5	4	5	5	5	5	5	5	5	**5**	**ALTO**
19	Computadores de escritorio usuarios	4	3	4	5	4	5	4	5	5	4	5	5	**5**	**ALTO**
20	Portátiles	3	3	3	2	2	2	3	3	3	3	2	3	**3**	**MEDIO**
21	Impresoras	4	5	3	5	4	5	5	5	5	4	5	5	**5**	**ALTO**
22	Software ofimático	5	3	4	5	5	4	5	5	5	4	5	5	**5**	**ALTO**
23	Sistemas de bases de datos	4	4	4	4	3	4	3	4	4	4	4	4	**4**	**ALTO**
24	Antivirus	1	1	1	1	0	1	1	1	0	1	1	1	**1**	**BAJO**
25	SIGA WEB	4	2	3	2	1	2	3	3	3	3	2	3	**3**	**MEDIO**
26	Sistema de Gestión documentaria	3	3	3	4	2	3	4	3	2	3	3	3	**3**	**MEDIO**
27	Página WEB	2	2	2	1	3	1	1	2	2	2	2	2	**2**	**BAJO**
28	Correos electrónicos	3	4	4	5	4	4	4	5	4	4	4	4	**5**	**ALTO**
29	Datos de autenticación	4	5	5	5	5	5	4	5	5	5	5	5	**5**	**ALTO**
30	Log de evento de seguridad	3	3	3	4	2	3	3	2	3	3	3	3	**3**	**MEDIO**
31	Registro de incidentes de seguridad	1	1	1	1	2	2	3	1	1	1	2	2	**2**	**BAJO**
32	Manuales de seguridad	2	4	3	3	3	3	4	2	3	3	3	3	**3**	**MEDIO**
33	Documentos	5	5	5	4	4	4	4	3	2	5	4	3	**4**	**ALTO**

Fuente: Elaboración propia

Tabla 6.7: Nivel de criticidad de los activos de Información

VALORACIÓN DEL NIVEL DE CRITICIDAD DEL ACTIVO DE INFORMACIÓN																
N°	Nombre del activo	Confidencialidad			Integridad			Disponibilidad			Confidencialidad	Integridad	Disponibilidad	PROMEDIO	VALOR SUPERIOR TOTAL	NIVEL DE CRITICIDAD
		Financiero	Legal	Imagen	Financiero	Legal	Imagen	Financiero	Legal	Imagen						
A1	Centro de computo G-301	5	4	4	5	4	3	5	4	4	5	4	5	4.667	5	ALTO
A2	Centro de computo G-302	5	4	3	5	4	3	5	4	4	4	4	5	4.333	5	ALTO
A3	Centro de computo G-303	5	4	3	5	4	3	5	5	4	4	4	5	4.333	5	ALTO
A4	Oficina del departamento de sistemas e informá	3	3	1	3	3	1	3	3	1	3	3	3	3	3	MEDIO
A5	Oficina del departamento de matemática	4	5	3	4	4	3	4	4	3	4	4	4	4	4	ALTO
A6	Oficina del departamento de estadística e inforn	4	4	3	4	4	3	3	4	4	4	4	4	4	4	ALTO
A7	Decanatura	3	2	1	3	2	3	3	3	2	2	3	3	2.667	3	MEDIO
A8	Almacén	1	1	0	1	0	0	1	1	0	1	1	1	1	1	BAJO
A9	Redes LAN 1	4	3	2	4	3	2	4	4	2	3	3	4	3.333	4	ALTO
A10	Redes LAN 2	4	4	4	4	4	3	4	3	4	4	4	4	4	4	ALTO
A11	Redes LAN 3	4	4	3	4	3	5	4	3	5	4	4	4	4	4	ALTO
A12	Red WAN	1	2	0	1	1	0	0	2	1	1	1	1	1	1	BAJO
A13	Red WIFI	3	2	3	3	2	3	4	3	2	3	3	3	3	3	MEDIO
A14	Dispositivos de red	3	3	2	3	3	2	2	1	3	3	3	2	2.667	3	MEDIO
A15	Computadores Administrador 1	4	3	1	4	3	1	2	1	2	3	3	2	2.667	3	MEDIO
A16	Computadores Administrador 2	4	3	4	3	3	3	4	4	4	4	3	4	3.667	4	ALTO
A17	Computadores Administrador 3	4	3	2	3	2	3	3	3	3	3	3	3	3	3	MEDIO
A18	Computadores Administrador 4	5	4	5	5	4	5	5	5	5	5	5	5	5	5	ALTO
A19	Computadores de escritorio usuarios	4	3	4	5	4	5	4	5	5	4	5	5	4.667	5	ALTO
A20	Portátiles	3	3	3	2	2	2	3	3	3	3	2	3	2.667	3	MEDIO
A21	Impresoras	4	5	3	5	4	5	5	5	5	4	5	5	4.667	5	ALTO
A22	Software ofimático	5	3	4	5	5	4	5	5	5	4	5	5	4.667	5	ALTO
A23	Sistemas de bases de datos	4	4	4	4	3	4	3	4	4	4	4	4	4	4	ALTO
A24	Antivirus	1	1	1	1	0	1	1	1	0	1	1	1	1	1	BAJO
A25	SIGA WEB	4	2	3	2	1	2	3	3	3	3	2	3	2.667	3	MEDIO
A26	Sistema de Gestión documentaria	3	3	3	4	2	3	4	3	2	3	3	3	3	3	MEDIO
A27	Página WEB	2	2	2	1	3	1	1	2	2	2	2	2	2	2	BAJO
A28	Correos electrónicos	3	4	4	5	4	4	4	5	4	4	5	5	4.667	5	ALTO
A29	Datos de autenticación	4	5	5	5	5	5	4	5	5	5	5	5	5	5	ALTO
A30	Log de evento de seguridad	3	3	3	4	2	3	3	2	3	3	3	3	3	3	MEDIO
A31	Registro de incidentes de seguridad	1	1	1	1	2	2	3	1	1	1	2	2	1.667	2	BAJO
A32	Manuales de seguridad	2	4	3	3	3	3	4	2	3	3	3	3	3	3	MEDIO
A33	Documentos	5	5	5	4	4	4	4	3	2	5	4	3	4	4	ALTO

Elaboración Propia

Es importante ejecutar el análisis de riesgos de los activos informáticos y activos de información, para ello se siguieron las recomendaciones metodológicas de la NTP/ISO 27001-2014 de establecer los activos para la valoración de riesgos, para ello se seleccionó los activos de información con nivel de criticidad Alto y Medio, estos fueron agrupados para realizar la valoración de riesgos en vez de hacerlo sobre el activo, de acuerdo a lo anterior, los activos fueron agrupados en contenedores para el proceso de valoración de riesgos:

Tabla 6.8: Activos seleccionados para la valoración de riesgos

ACTIVO DE INFORMACIÓN	NIVEL DE CRITICIDAD	CONTENEDOR /ACTIVO SELECCIONADO PARA LA VALORACIÓN DE RIESGOS
Área administrativa	**Alto**	Área administrativa de la institución.
Computadoras de los administrativos	**Alto**	
Centro de computo G-301	**Alto**	Computadoras
Centro de computo G-302	**Alto**	
Centro de computo G-303	**Alto**	
Oficina del departamento de sistemas e informática	**Medio**	Informacion documentaria
Oficina del departamento de matemática	**Alto**	
Oficina del departamento de estadística e informática	**Alto**	
Decanatura	**Medio**	
Computadores Administrador 1	**Medio**	Base de datos
Computadores Administrador 2	**Alto**	
Computadores Administrador 3	**Medio**	
Computadores Administrador 4	**Alto**	
Computadores de escritorio usuarios	**Alto**	
Portátiles	**Medio**	

Impresoras	**Alto**	Hardware
Dispositivos de red	**Medio**	
Redes LAN 1	**Alto**	Red LAN
Redes LAN 2	**Alto**	
Redes LAN 3	**Alto**	
Red WIFI	**Medio**	
Software ofimático	**Alto**	Plataformas informáticas
Sistemas de bases de datos	**Alto**	
SIGA WEB	**Medio**	
Sistema de Gestión documentaria	**Medio**	
Correos electrónicos	**Alto**	
Datos de autenticación	**Alto**	
Log de evento de seguridad	**Medio**	
Manuales de seguridad	**Medio**	
Documentos	**Alto**	

Fuente: Elaboración propia

6.1.5. Valoración de riesgos en los activos de información

Se realizo la estimación de los riesgos que están expuestos los activos de información y activos informáticos que se identificaron, para ello, se desarrolló las siguientes actividades:

- Primero, se identificaron los riesgos.
- Segundo, se realizó el análisis del riesgo inherente.
- Tercero, se elaboró la matriz de riesgo inherente.
- Cuarto, se hizo la valoración de controles.
- Quinto, se determinó los riesgos residuales.
- Sexto, se elaboró una matriz de riesgo residual.

Según la revista tecnológica ESPOL (Solarte, 2015) Los riesgos informáticos son problemas potenciales, que pueden afectar a los

sistemas de información o a los equipos de cómputo. Si no se tienen las medidas adecuadas para salvaguardar los datos y la información, dichos riesgos se pueden presentar por las vulnerabilidades y amenazas en cualquier momento.

De acuerdo a la definición es importante identificar las vulnerabilidades y amenazas, analizar que agentes los generan, identificar si es un agente de amenaza y el nivel de un resultado inesperado.

Tabla 6.9: Identificación de riesgos

IDENTIFICACIÓN DE RIESGOS	Dimensiones		
	C	I	D
Abuso de privilegios de acceso Acceso no autorizado	X X	X X	
Auditorias débiles			X
Cambio de privilegios sin autorización	X	X	X
Denegación de servicio			X
Divulgación o robo de información de autentificación Divulgación no autorizada de información	X X		
Errores del administrador	X	X	X
Instalación de software no autorizado		X	X
Interceptación no autorizada de información en tránsito Manipulación de la configuración	X X		
Modificación sin autorización Pérdida o robo de información	 X	X 	 X
Suplantación de identidad de usuarios	X	X	
Uso inadecuado de sistemas para generar fraudes	X	X	
Uso inadecuado de sistemas que generan interrupción		X	X

Fuente: Elaboración propia

6.1.6. Identificación de amenazas

Es importante inspeccionar las amenazas a las que se enfrentan nuestros sistemas, los potenciales atacantes que violan nuestros limitados protocolos de seguridad no siempre son atacantes especializados como los *crackers*, o *hackers*, sin embargo, esto es producto de los mitos creados por los medios de comunicación ya que, en realidad, la enorme mayoría de problemas e incidentes de seguridad vienen dados por atacantes internos de la universidad. En instituciones como nuestra facultad, estos atacantes suelen ser los propios estudiantes, rara vez el personal administrativo encargado de velar por los activos informáticos y de información, así como usuarios externos a la facultad que aprovechan la habitualmente mala protección de los sistemas y la facilidad para acceder a ellos y conseguir así información personal y clasificada. Los conocimientos de estos estudiantes en materias de sistemas operativos, redes o seguridad informática suelen ser concretos y muchas veces limitado. Por ello, es importante inferir que las amenazas como actos intencionados contra nuestro sistema de administración de información muchos de los problemas pueden ser ocasionados por accidentes, desde un personal que derrama una bebida sobre una terminal hasta un estudiante que tropieza con el cable de alimentación de un servidor y lo desconecta de la línea eléctrica, pasando por temas como el borrado accidental de datos o los errores de

programación. Por supuesto, tampoco tenemos que reducirnos a los accesos no autorizados al sistema, las amenazas con programas espías como los Spywre que son códigos maliciosos cuyo principal objetivo es recoger información sobre las actividades de un usuario, o los famosos virus troyanos que son pequeños programas de código malicioso, que de diferentes maneras se alojan en los computadores con el propósito de permitir el acceso no autorizado a un atacante, y otros tipos de ataques como los Phishing, Spam, Botnets que según los datos de la encuesta anual de seguridad del FBI, los virus informáticos siguen siendo la principal fuente de perdida financiera en las organizaciones, seguido por los impactos derivados del acceso no autorizado a los sistemas, el robo de información de propiedad industrial, y la perdida de computadoras personales o elementos de computación móvil, estas causas generan más del 74% del total de las pérdidas financieras, en nuestra realidad, las amenazas provienen de factores humanos, accidentales o errores, falla en los procedimientos y fallas en los sistemas de procesamiento de la información. Es por ello que se identificaron las amenazas y fueron seleccionados para la valoración de riesgos, para facilitar esta labor de identificación, se elaboró la siguiente lista que contiene los riesgos más usuales de seguridad que en términos generales pueden afectar la confidencialidad, disponibilidad e integridad de la información en la facultad.

Tabla 6.10: Amenazas que afectan los activos de información

AMENAZAS	ACTIVOS DE TECNOLOGÍA QUE PUEDEN SER AFECTADOS	
Acceso no autorizado	Area administrativa Bases de datos Cuarto de redes Laboratorios de computo	Servidores Correos electronicos Almacen de acervo documentario SIGA WEB
Ataques externos e internos de hacking	Bases de datos Equipos de seguridad Servidores Correos	RED LAN RED WIFI SIGA WEB RED WAN
Cambio de privilegios sin autorización	Bases de datos Directorios autorizados	Servidores de bases de datos Servidores de administración
Desastres naturales	Almacen de acervo documentario Cuarto de redes	Laboratorios de computo Computadoras de la red administrativa
Divulgacion de informacion de autentificación	Bases de datos Directorio del personal autorizado	Informacion confidencial y personal Password y usuarios
Error de los administradores	Area administrativa Bases de datos Cuartos de redes Laboratorios de computo	Servidores Correos electronicos Almacen de acervo documentario SIGA WEB
Instalación de software no autorizado	Portatiles Bases de datos	Computadoras de la red administrativa Impresoras
Interrupción no autorizada de informacion en transito	RED LAN Red WAN	Correos electronicos Servidores
Interrupción en los servicios	Bases de datos RED LAN	Servidores RED WAN
Modificación sin autorización	Bases de datos Directorios autorizados	Password y usuarios Informacion confidencial y personal
Robo de equipos	Servidores Equipos informáticos	Laboratorios de computo cuarto de redes
Robo de información	Almacen de acervo documentario Base de datos	Correos electronicos Servidores
Suplantacion de identidad de usuarios	Correos electronicos	Password y usuarios
Uso inadecuado de sistemas para generar fraudes	Base de datos Equipos informáticos	Servidores Correos electronicos
Uso inadecuado de sistemas para generar interrupción	Base de datos Equipos informáticos RED LAN	Servidores Correos electronicos RED WAN
Abuso de privilegios	Equipos de computo Red administrativa Portatiles	Computadoras de la red administrativa RED LAN RED WAN

Fuente: Elaboración propia

El siguiente análisis muestran las vulnerabilidades vinculadas a las amenazas identificadas que guardan relación con las características de los activos de información y sus contenedores:

Tabla 6.11: Vulnerabilidades que afectan los activos de información

AMENAZAS	VULNERABILIDADES	
Acceso no autorizado	Inadecuada Administración de Seguridad	Falta de seguridad de los puertos de red
	Ausencia de una configuración segura de la red	Políticas no aplicada o no existencia de segurida
	Ausencia o Inadecuada plataforma de Seguridad Perimetral	Contraseñas no seguras
	Inadecuada Administración o Asignación de roles y permisos	Configuración incorrecta de las cuentas de usuario
Ataques externos e internos de hacking	Inadecuada administracion de seguridad	Ausencia de una configuración segura de la red
	Ausencia o Inadecuada plataforma de Seguridad Perimetral	Falla de seguridad en los componentes de red
Cambio de privilegios sin autorización	Contraseñas no seguras	Inadecuada Administración de Seguridad
	Inadecuada Administración o Asignación de roles y permisos	Políticas no aplicada o no existencia de segurida
Desastres naturales	Ausencia de un sistema de continuidad de negocio	Ubicación física del centro de cómputo
	Ubicación física de los equipos	Políticas no aplicada o no existencia de seguridad físic
Divulgacion de informacion de autentificación	Inadecuada Administración de Seguridad	Contraseñas no seguras
	Inadecuada Administración o Asignación de roles y permisos	Políticas no aplicada o no existencia de seguridad
Error de los administradores	Ausencia de capacitación permanente	Desmotivación personal
	Ausencia o inadecuado procedimiento de control de cambios	Manual de procedimientos
Instalación de software no autorizado	Políticas no aplicada o no existencia de seguridad	Inadecuada Administración o Asignación de roles y permisos
Interrupción no autorizada de informacion en transito	Políticas no aplicada o no existencia de seguridad	Inadecuado mecanismo de cifrado
Interrupción en los servicios	Inadecuada Configuración y Capacidad de los ambientes	Ausencia o inadecuado procedimiento de control de cambios
	Falta de mantenimiento de equipos	
Modificación sin autorización	Políticas no aplicada o no existencia de seguridad	Inadecuada Administración o Asignación de roles y permisos
	Inadecuado mecanismo de cifrado	
Robo de equipos	Políticas no aplicada o no existencia de seguridad	Inadecuado inventario de activos físicos
	Ausencia o inadecuada plataforma de seguridad fisica	Ubicación física de los equipos
Robo de información	Inadecuada Administración de Seguridad	Ausencia o Inadecuada plataforma de Seguridad Perimetral
	Inadecuada Administración o Asignación de roles y permisos	Inexistencia de Logs de eventos de seguridad
Suplantacion de identidad de usuarios	Contraseñas no seguras	Cuentas de usuario sin auditar
Uso inadecuado de sistemas para generar fraudes	Inadecuada Administración de Seguridad	Inexistencia de Logs de eventos de seguridad
	Cuentas de usuarios sin auditar	Inadecuada Administración o Asignación de roles y permisos
Uso inadecuado de sistemas para generar interrupción	Inadecuada Administración de Seguridad	Inexistencia de Logs de eventos de seguridad
	Cuentas de usuarios sin auditar	Inadecuada Administración o Asignación de roles y permisos
	Políticas no aplicada o no existencia de seguridad	
Abuso de privilegios	Cuentas de usuario sin auditar	Contraseñas no seguras
	Inexistencia de Logs de eventos de seguridad	Inadecuada Administración o Asignación de roles y permiso
	Políticas no aplicada o no existencia de seguridad	

Fuente: Elaboración propia

6.1.7. Análisis de riesgo inherente

A través de un exhaustivo análisis de los riesgos que se presentan en los activos de información se establecieron la probabilidad de ocurrencia de los riesgos y el impacto que puedan causar en los activos de información y activos informáticos, con el objetivo de lograr identificar los niveles de riesgo inherente, el cual, nos permitirá definir el nivel de riesgo inherente a la actividad, sin tener en consideración las medidas y controles de seguridad que actualmente existen en la Facultad de Ciencias para mitigar o minimizar los riesgos.

Para determinar la probabilidad de ocurrencia de una amenaza sobre cada uno de los activos, se utilizó los criterios de valoración que toman una referencia cronológica de ocurrencia, que van desde una vez al año hasta más de una vez al mes, divididos en 5 tipos de ocurrencia como raro, bajo (improbable), media (posible), alta (probable) y muy alta probabilidad y su respectivo valor cualitativo, teniendo estos componentes se puede cuantificar de manera más exacta el riesgo intrínseco de cada actividad.

Tabla 6.12: Valoración de probabilidad de ocurrencia

Probabilidad de ocurrencia	Valor Cualitativo	Valor Asignado
Una vez cada año	Raro	1
Una vez cada seis (6) meses	Baja (Improbable)	2
Una vez cada tres (3) meses	Media (Posible)	3
Una vez cada mes	Alta (Probable)	4
Más de una vez al mes	Muy Alta	5

Fuente: Elaboración propia

Es importante determinar e identificar el nivel del impacto que pueden tener las pérdidas de confidencialidad, integridad y disponibilidad sobre la información y los activos informáticos. Los siguientes criterios de valoración que generan impactos cuantitativos que afectan los porcentajes de utilidad o recursos financieros en la institución y los impactos cualitativos que afectan la imagen y la seguridad de la institución.

Estos criterios de valoración para el análisis de los impactos se clasifican en 5 tipos que son descritos desde insignificantes, menor, moderado, mayor y catastrófico cada uno de los criterios obedece a un análisis de porcentaje de perdida financiera y pérdida de confianza en la institución por parte de los usuarios.

Tabla 6.13: Valoración del impacto cualitativo y cuantitativo

IMPACTO	Impacto cuantitativo (Porcentaje sobre utilidad	Impacto cualitativo (uno o más factores)	Valor
Insignificante	Genera pérdidas financieras pequeñas no significativas. (Perdida Menor o igual a 0.25%)	• No afecta la seguridad de la información de la facultad de ciencias. • No afecta la imagen de la facultad de ciencias ante las partes interesadas. • Genera reprocesos insignificantes. • La información se puede recuperar rápidamente con la misma calidad.	1
Menor	Genera pérdidas financieras menores no significativas. (Perdida Mayor a 0.25% y menor o igual a 5%)	• No afecta la seguridad de la información de la facultad de ciencias. • Afecta en menor grado la imagen de la facultad de ciencias ante las partes interesadas. • Genera reprocesos menores. • La información se puede recuperar en un tiempo moderado con la misma calidad.	2
Moderado	Genera pérdidas financieras moderadas. (Mayor a 5% y menor o igual a 20%)	• Afecta en menor grado la seguridad de la información de la facultad de ciencias. • Afecta medianamente la imagen de la facultad de ciencias ante las partes interesadas. • Genera reprocesos moderados. • La información se puede recuperar pero no con la misma calidad	3
Mayor	Genera pérdidas financieras mayores. (Perdida mayor o igual a 20% y menor a 50%)	• Afecta en mayor grado la seguridad de la información de la facultad de ciencias. • Afecta altamente la imagen de la facultad de ciencias ante las partes interesadas. • Genera reprocesos mayores. • Es difícil recuperar la información	4
Catastrófico	Genera pérdidas financieras críticas. (Perdidas Mayores a 50%)	• Afectar seriamente la seguridad de la información de la facultad de ciencias. • Afecta gravemente la imagen de la facultad de ciencias ante las partes interesadas • Puede generar pérdida masiva de clientes. • Genera alto nivel de reprocesos. • Es difícil y costoso recuperar la información. • Afecta la continuidad del negocio	5

Fuente: Elaboración propia

Para calcular el nivel de riesgo inherente tenemos que calcular también el valor de la probabilidad multiplicada por el valor del impacto. Para empezar a clasificar el riesgo inherente o residual es importante saber el nivel de riesgo, a continuación, se utilizaron los siguientes criterios de valoración que determinan el tipo de riesgo y la acción requerida en cada uno de los 5 tipos de riesgo.

Tabla 6.14: Valoración de riesgos

TIPO DE RIESGO	VALOR NIVEL DE RIESGO	ACCIÓN REQUERIDA
Riesgo Extremo	Nivel Riesgo mayor o igual a 15 puntos	Requiere acciones inmediatas que permitan reducir y compartir el riesgo, transferirlo o incluso evitarlo
Riesgo Alto	Nivel Riesgo mayor o igual a 10 y menor a 15 puntos	Requieren atención urgente e implementar medidas para reducir el nivel del riesgo
Riesgo Medio	Nivel Riesgo mayor o igual a 5 y menor a 10 puntos	Requiere de medidas prontas y adecuadas que permitan disminuir el riesgo a nivel bajo o inusual
Riesgo Bajo	Nivel Riesgo mayor o igual a 3 y menor a 5 puntos	El riesgo se mitiga con actividades propias y por medio de algunas medidas preventivas para reducir el riesgo
Riesgo Inusual	Nivel Riesgo Menor a 3 puntos	Se puede aceptar el riesgo sin necesidad de tomar otras medidas de control diferentes a las existentes.

Fuente: Elaboración propia

La tabla de valoración de riesgos nos permitirá realizar un análisis exhaustivo de los riesgos inherentes, su respectiva valoración del impacto producido en la disponibilidad, integridad y confidencialidad a través de los 5 criterios de impacto cuantitativo, ello nos permitirá determinar la estimación del riesgo que a su vez determinará la probabilidad de impacto en los activos de información de la Facultad de Ciencias.

Tabla 6.15: Estimación del riesgo por niveles

CODIGO	RIESGOS	VALORACIÓN DEL IMPACTO			PROBABILIDAD	ESTIMACIÓN DEL RIESGO			NIVEL DE RIESGO
		D	I	C		D	I	C	
R1	Acceso no autorizado		Mayor	Catastrófico	Alta		Riesgo Extremo	Riesgo Extremo	Riesgo Extremo
R2	Ataques externos / internos	Mayor		Mayor	Alta	Riesgo Extremo		Riesgo Extremo	Riesgo Extremo
R3	Cambio de privilegios sin autorización	Moderado	Moderado	Moderado	Alta	Riesgo Alto	Riesgo Alto	Riesgo Alto	Riesgo Alto
R4	Desastres naturales	Mayor			Raro	Riesgo Bajo			Riesgo Bajo
R5	Divulgación de información de autenticación			Moderado	Media			Riesgo Medio	Riesgo Medio
R6	Error del administrador	Moderado			Alta	Riesgo Alto			Riesgo Alto
R7	Instalación de software no autorizado		Menor		Media		Riesgo Medio		Riesgo Medio
R8	Interceptación no autorizada de información en tránsito		Mayor	Mayor	Alta		Riesgo Extremo	Riesgo Extremo	Riesgo Extremo
R9	Interrupción en los servicios	Moderado			Media	Riesgo Medio			Riesgo Medio
R10	Modificación sin autorización		Moderado		Media		Riesgo Medio		Riesgo Medio
R11	Robo de equipos	Moderado			Media	Riesgo Medio			Riesgo Medio
R12	Robo de información	Mayor		Mayor	Media	Riesgo Alto		Riesgo Alto	Riesgo Alto
R13	Suplantación de identidad de usuarios			Moderado	Baja			Riesgo Medio	Riesgo Medio
R14	Uso inadecuado de sistemas para generar fraudes			Mayor	Baja			Riesgo Medio	Riesgo Medio
R15	Uso inadecuado de sistemas que generan interrupción	Mayor			Baja	Riesgo Medio			Riesgo Medio
R16	Abuso de privilegios		Mayor	Mayor	Alta		Riesgo Extremo	Riesgo Extremo	Riesgo Extremo

Fuente: Elaboración propia

6.1.8. Riesgos inherentes de Tecnología por tipo de riesgo

A continuación, se clasifican los activos de información de acuerdo al nivel de riesgo, desde los más sensibles hasta los que no requieren de controles, esto nos permitirá ordenar y priorizar decisiones en la administración y órganos de gobierno sobre el tratamiento de estos activos y sus respectivos controles de seguridad.

A partir de este análisis podemos determinar las implicaciones estratégicas, financieras, operacionales y de imagen para abordar los riesgos de manera estructurada y efectiva para su control, esto nos permitirá adquirir capacidades de recuperación de TI y gestionar los incidentes, recordemos que el riesgo que emana de una estrategia inefectiva se encuentra entre las principales amenazas que una institución con activos de información tan sensibles como la Facultad de Ciencias enfrenta, pero la metodología usada incluye el ciclo de Deming o mejora continua, esto nos permitirá hacer una retroalimentación optima y así ir mejorando la gestión de incidentes de seguridad de la información.

Con la información facilitada cada actividad en los servicios de la Facultad y cada activo de información tiene que tener la capacidad de recuperación ante disrupciones y cortes. La institución debe tener estándares de capacidad de recuperación de manera que las

inversiones en capacidad de recuperación se dirijan a la tecnología que respalde sus procesos de negocio más críticos o activos con niveles de riesgo crítico. La prueba de la recuperación, especialmente para la tecnología crítica, tiene que ser rigurosa y tiene que verificar que los planes de recuperación funcionarán.

Tabla 6:16: Riesgos inherentes

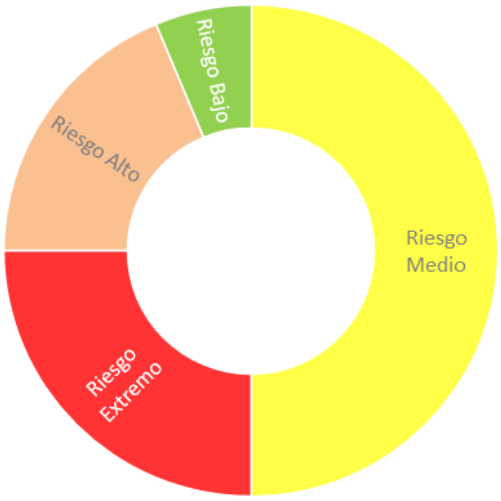
CODIGO	RIESGOS	ACTIVOS	PROBABILIDAD	IMPACTO	PROBABILIDAD X IMPACTO	NIVEL DE RIESGO
R1	Acceso no autorizado	Area administración Bases de datos Cuartos de Red Directorio de usuarios Equipos de seguridad Correos electronicos Oficinas de la facultad Almacen de acervo documentario Laboratorios de computo	4. ALTA	5. CATASTROFICO	20	RIESGO EXTREMO
R2	Ataques externos e internos	Bases de datos Equipos de computo Servidores SIGA WEB	4. ALTA	4. MAYOR	16	RIESGO EXTREMO
R3	Interceptación no autorizada de información en tránsito Interceptación no autorizada de	Red WAN Red LAN Correos electronicos	4. ALTA	4. MAYOR	16	RIESGO EXTREMO
R4	Abuso de privilegios	Oficinas de la facultad Correos electronicos Almacen de acervo documentario Bases de datos Directorio de Usuarios	4. ALTA	4. MAYOR	16	RIESGO EXTREMO
R5	Cambio de privilegios sin autorización	Almacen de acervo documentario Directorio de usuarios Correos electronicos	4. ALTA	3. MODERADO	12	RIESGO ALTO
R6	Error del administrador	Bases de datos Red LAN y Red WAN Servidores SIGA WEB Laboratorios de computo Almacen de acervo documentario	4. ALTA	3. MODERADO	12	RIESGO ALTO
R7	Robo de información	Bases de datos SIGA WEB Correos electronicos Almacen de acervo documentario	3. MEDIA	4. MAYOR	12	RIESGO ALTO
R8	Divulgacion de información	Bases de datos SIGA WEB Correos electronicos	3. MEDIA	3. MODERADO	9	RIESGO MEDIO
R9	Interrupción en los servicios	SIGA WEB Servidores Plataformas implementadas Infrmación administrativa	3. MEDIA	3. MODERADO	9	RIESGO MEDIO
R10	Modificación sin autorización	Bases de datos Directorio de usuarios Laboratorios de computo Plataformas implementadas	3. MEDIA	3. MODERADO	9	RIESGO MEDIO
R11	Robo de equipos	Laboratorios de computo Cuartos de Red Serviidores	3. MEDIA	3. MODERADO	9	RIESGO MEDIO
R12	Uso inadecuado de sistemas para generar fraudes	Bases de datos SIGA WEB Correos electronicos	2.BAJA	4. MAYOR	8	RIESGO MEDIO
R13	Uso inadecuado de sistemas que generan interrupción	Bases de datos Plataformas implementadas SIGA WEB Servidores	2.BAJA	4. MAYOR	8	RIESGO MEDIO
R14	Instalación de software no autorizado	Laboratorios de computo Portatiles Computadoras administrativas	3. MEDIA	2. INUSUAL	6	RIESGO MEDIO
R15	Suplantación de identidad de usuarios	Directorio de usuarios Laboratorios de computo Correos electronicos	2.BAJA	3. MODERADO	6	RIESGO MEDIO
R16	Desastres naturales	Laboratorios de computo Servidores Cuartos de Red	2. BAJO	2. INUSUAL	4	RIESGO BAJO

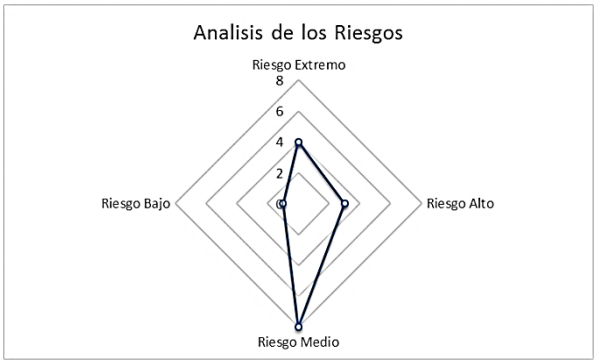
Fuente: Elaboración propia

A continuación, hacemos un análisis de los porcentajes de los niveles de riesgo y la concentración del riesgo inherente asociado a los activos de información de la Facultad de Ciencias.

Gráfico6.1: Porcentajes de los niveles de riesgo

NIVEL DE RIESGO	ACTIVOS	PORCENTAJE
Riesgo Extremo	4	25 %
Riesgo Alto	3	19 %
Riesgo Medio	8	50 %
Riesgo Bajo	1	6 %
Total	**16**	**100 %**





Fuente: Elaboración propia

6.1.1. Mapa de calor

Es importante utilizar una herramienta de análisis como el mapa de calor que nos permitirá en este caso, representar de manera gráfica las zonas donde se localizan los riesgos de acuerdo al impacto y la probabilidad, estas áreas se encuentran ubicadas de acuerdo a la cercanía del origen. Cada zona dentro del mapa de calor pertenece a un tipo de riesgo, el cual describe el tratamiento de los riesgos asociados. A continuación, se muestra el mapa de calor que se elaboró para determinar y establecer la ubicación de los riesgos inherentes.

Cuadro 6.1: Mapa de calor respecto al impacto

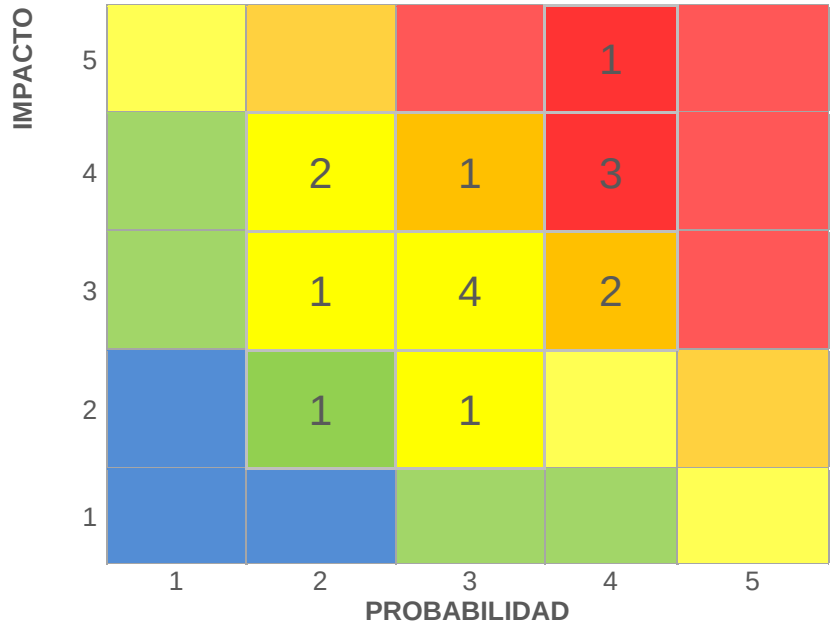
IMPACTO	Riesgo Inusual	Riesgo Bajo	Riesgo Medio	Riesgo Alto	Riesgo Extremo
5	Zona de riesgo medio 5 Puntos Reducir el riesgo a niveles mas bajos	Zona de riesgo alto 10 Puntos Evitar - Gestionar el riesgo	Zona de riesgo extremo 15 Puntos Evitar - Gestionar riesgo Requiere acción inmediata	Zona de riesgo extremo 20 Puntos Evitar - Gestionar riesgo Requiere acción inmediata	Zona de riesgo extremo 25 Puntos Evitar - Gestionar riesgo Requiere acción inmediata
4	Zona de riesgo bajo 4 Puntos Administrar el riesgo	Zona de riesgo medio 8 Puntos Reducir el riesgo a niveles mas bajos	Zona de riesgo alto 12 Puntos Evitar - Gestionar el riesgo	Zona de riesgo extremo 16 Puntos Evitar - Gestionar riesgo Requiere acción inmediata	Zona de riesgo extremo 20 Puntos Evitar - Gestionar riesgo Requiere acción inmediata
3	Zona de riesgo bajo 3 Puntos Administrar el riesgo	Zona de riesgo medio 6 Puntos Reducir el riesgo a niveles mas bajos	Zona de riesgo medio 9 Puntos Reducir el riesgo a niveles mas bajos	Zona de riesgo alto 12 Puntos Evitar - Gestionar el riesgo	Zona de riesgo extremo 15 Puntos Evitar - Gestionar riesgo Requiere acción inmediata
2	Zona de riesgo inusual 2 Puntos Asumir el riesgo	Zona de riesgo bajo 4 Puntos Administrar el riesgo	Zona de riesgo medio 6 Puntos Reducir el riesgo a niveles mas bajos	Zona de riesgo medio 8 Puntos Reducir el riesgo a niveles mas bajos	Zona de riesgo alto 10 Puntos Evitar - Gestionar el riesgo
1	Zona de riesgo inusual 1 Puntos Asumir el riesgo	Zona de riesgo inusual 2 Puntos Asumir el riesgo	Zona de riesgo bajo 3 Puntos Administrar el riesgo	Zona de riesgo bajo 4 Puntos Administrar el riesgo	Zona de riesgo medio 5 Puntos Reducir el riesgo a niveles mas bajos
	1	2	3	4	5
	PROBABILIDAD				

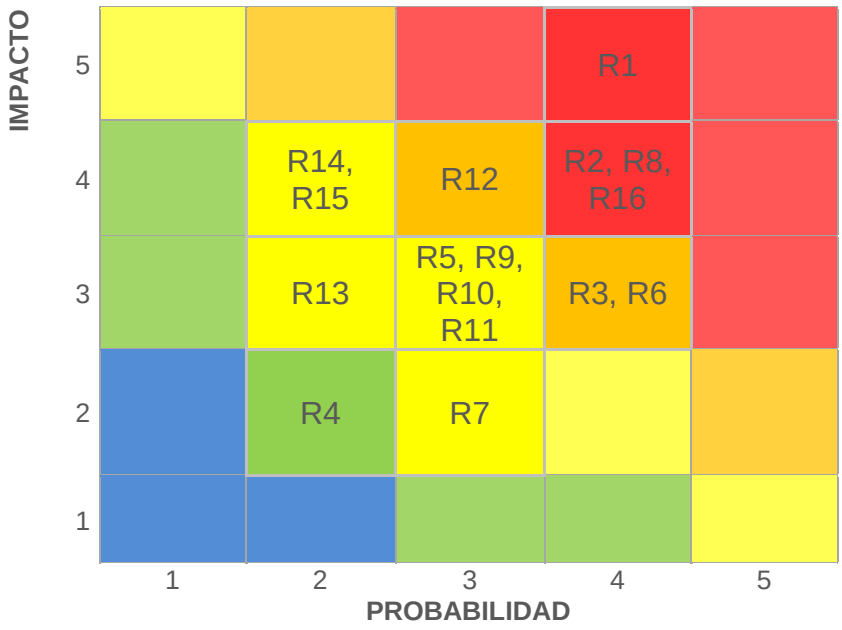
Fuente: Elaboración propia

6.1.2. Mapa de riesgo inherente

El siguiente cuadro muestra el resumen de la estratificación y zonificación de los riesgos inherentes en los activos de información y activos informáticos de la Facultad de Ciencias.

Cuadro 6.2: Estratificación de los mapas de calor





Fuente: Elaboración propia

6.2. VALORACIÓN DE LOS CONTROLES DE SEGURIDAD

6.2.1. Valoración de controles de seguridad en la Facultad de Ciencias

Teniendo la matriz de riesgo inherente se analizó y valoró los controles de incidencias, con el fin de determinar el nivel de posible desplazamiento que estos pudieran generar sobre el mapa de calor de riesgo, lo cual establece, el mapa de calor del riesgo residual. Es importante que para establecer con certeza el control implementado se utilizó como guía la metodología de riesgos propuesta por el estándar ISO 27001, el cual establece valorar los siguientes aspectos, caracteres del control, a los cuales se les asigna un peso que es resultado del porcentaje sobre un total de 1/100 puntos.

Tabla 6.17: Valoración de controles de seguridad

ASPECTOS A EVALUAR	OPCIONES DE RESPUESTA	PESO
Afecta impacto o probabilidad. Permite establecer el movimiento que genera sobre la matriz, si sobre el eje X (probabilidad) o sobre el eje Y (impacto)	Impacto	
	Probabilidad	
Categoria de control	Control preventivo	20
	Control Detectivo	15
	Control Correctivo	5
Herramientas para ejercer el control	SI	15
	NO	0
Están definidos los responsables de la ejecución del control y del seguimiento	SI	15
	NO	0
La frecuencia de la ejecución del control y seguimiento es adecuada	SI	20
	NO	0
El tiempo que lleva el control ha demostrado ser efectivo	SI	20
	NO	0
Está documentado los pasos para el manejo del control	SI	10
	NO	0

Fuente: Elaboración propia

Tabla 6.17: Análisis de valoración de riesgos y amenazas

Riesgos/Amenaza	Descripción del Control	Tipo de Control	Categoría	Existe una herramienta para el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada	El tiempo que lleva el control ha demostrado ser efectivo	Esta docuemntado los pasos para el manejo del control	PUNTAJE TOTAL
R1. Acceso no autorizado	Se cuenta con un sistema de control de acceso para ingresar a las áreas seguras y camaras de vigilancia	Probabilidad	Preventivo	SI	NO	SI	SI	NO	75
			20	15	0	20	20	0	
	Existe un sistema de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	El acceso de los usuarios a los recursos tecnológicos tiene control de los encargados	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	Probabilidad	Preventivo	SI	NO	NO	NO	NO	35
			20	15	0	0	0	0	
	Se cuenta con un esquema de privilegios sobre los documentos importantes para la institución	Probabilidad	Preventivo	SI	NO	NO	NO	NO	35
			20	15	0	0	0	0	
R2. Ataques externos / internos (hacking no ético)	Existe una plataforma de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	SI	SI	SI	SI	NO	90
			20	15	15	20	20	0	
R3. Cambio de privilegios sin autorización	Se cuenta con un procedimiento formal de control de cambios	Impacto	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	
R4. Desastres naturales	Area encargada de los desastres naturales como terremotos, inundaciones, Incendios, etc	Impacto	Correctivo	SI	SI	NO	NO	SI	45
			5	15	15	0	0	10	
	Simulacros de evaluación	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	
R5. Divulgación de información de autenticación	Se tiene implementada la politica de contraseñas y ususarios	Probabilidad	Preventivo	SI	NO	SI	SI	NO	75
			20	15	0	20	20	0	
R6. Error del administrador	Se cuenta con un procedimiento formal de control de cambios	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	

Riesgos/Amenaza	Descripción del Control	Tipo de Control	Categoría	Existe una herramienta para el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada	El tiempo que lleva el control ha demostrado ser efectivo	Esta docuemntado los pasos para el manejo del control	PUNTAJE TOTAL
R7. Instalación de software no autorizado	Se tiene implementada la política para restringir la instalación de software por parte de los usuarios	Probabilidad	Preventivo	SI	NO	SI	SI	NO	75
			20	15	0	20	20	0	
R8. Interceptación no autorizada de información en	Los canales de comunicación utilizan protocolos de encriptación para la transmisión de datos	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
R9. Interrupción en los servicios	Se cuenta con una plataforma de servicios	Impacto	Correctivo	SI	SI	NO	SI	NO	55
			5	15	15	0	20	0	
	Se cuenta con un procedimiento formal de control de cambios	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	
	Centro de procedimientos de control de desastres naturales	Impacto	Correctivo	SI	SI	NO	NO	SI	45
			5	15	15	0	0	10	
R10. Modificación sin autorización	El acceso de los usuarios al los recursos tecnológicos se controla a través del directorio activo	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	Probabilidad	Preventivo	SI	NO	NO	NO	NO	35
			20	15	0	0	0	0	
	Se cuenta con un esquema de privilegios sobre los documentos importantes para la institución	Probabilidad	Preventivo	SI	NO	SI	NO	NO	55
			20	15	0	20	0	0	
R11. Robo de equipos	Se cuenta con un sistema de control de acceso para ingresar a las áreas seguras y camaras de vigilancia	Probabilidad	Preventivo	SI	SI	SI	SI	SI	100
			20	15	15	20	20	10	
	Existe guardias de seguridad que revisan los equipos que entran y salen	Probabilidad	Preventivo	SI	SI	SI	NO	SI	80
			20	15	15	20	0	10	
	Existe algun convenio de seguridad	Impacto	Correctivo	SI	SI	SI	SI	SI	85
			5	15	15	20	20	10	

Fuente: elaboración propia

Riesgos/Amenaza	Descripción del Control	Tipo de Control	Categoría	Existe una herramienta para el control	Están definidos los responsables de la ejecución del control y del seguimiento	La frecuencia de la ejecución del control y seguimiento es adecuada	El tiempo que lleva el control ha demostrado ser efectivo	Esta docuemntado los pasos para el manejo del control	PUNTAJE TOTAL
R12. Robo de información	Existe una plataforma de seguridad perimetral en alta disponibilidad	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
	Existe un esquema de permisos y procedimientos de seguridad impementados en los sistemas de información	Probabilidad	Preventivo	SI	SI	SI	NO	NO	70
			20	15	15	20	0	0	
R13. Suplantación de identidad de usuarios	Se cuenta con un sistema de control de acceso para ingresar a las áreas seguras y camaras de vigilancia	Probabilidad	Preventivo	SI	SI	SI	SI	SI	100
			20	15	15	20	20	10	
R14. Uso inadecuado de sistemas para generar fraudes	Los programas de haking etico cuentan con un esquema de autentificación y seguimiento de auditoria	Probabilidad	Preventivo	SI	NO	SI	NO	NO	55
			20	15	0	20	0	0	
R15. Uso inadecuado de sistemas que generan interrupción	Se cuenta con procedimientos para auditar los sistemas de información utilizados en la institución	Impacto	Correctivo	SI	SI	NO	SI	NO	55
			5	15	15	0	20	0	
	Se cuenta con los protocolos para el control de incidentes	Impacto	Correctivo	SI	SI	NO	NO	SI	45
			5	15	15	0	0	10	
R16. Abuso de privilegios	Se cuenta con auditorias de privilegios	Probabilidad	Preventivo	SI	SI	NO	NO	NO	50
			20	15	15	0	0	0	
	Los sistemas de información son sometidos a auditorias y protocolos de seguridad	Probabilidad	Preventivo	SI	SI	NO	NO	SI	60
			20	15	15	0	0	10	
	Se auditan los esquemas de privilegios y utilizacion de información	Impacto	Correctivo	SI	SI	NO	NO	NO	35
			5	15	15	0	0	0	

Fuente: Elaboración propia

6.2.2. Monitoreo del Desplazamiento del Mapa de Calor

El monitoreo del desplazamiento cabe precisar que es después de realizar un análisis sobre los aspectos característicos o cualidades del control, por ello se procedió a establecer el nivel de desplazamiento que generará la aplicación de los controles dentro de la matriz de riesgo de acuerdo a su certidumbre.

Tabla.6.18: Criterios para el control de disminución de probabilidad de impacto

Valores de Calificación del Control	Control de disminución - Probabilidad o Impacto	
	Niveles a disminuir en la probabilidad	Niveles a disminuir en el impacto
Entre 0 - 50 puntos	0	0
Entre 51 - 75 puntos	1	1
Entre 76 - 100 puntos	2	2

Fuente: Elaboración propia

Es importante analizar el nivel de desplazamiento que surge la aplicación del control, además de ello nos permite determinar el riesgo residual.

En la siguiente matriz se muestra el sistema de la valoración que se realizó para determinar el nivel de desplazamiento en el mapa de riesgos en base a los controles establecidos.

Tabla 6.19: Desplazamiento del mapa de riesgo

			DESPLAZAMIENTO MAPA DE RIESGO										
			INHERENTE			DISMINUCIÓN				RESIDUAL		
Riesgos/Amenaza	Descripción del Control	PUNTAJE TOTAL	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	Probabilidad	Total de controles	Impacto	Total de controles	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO
R1. Acceso no autorizado	Se cuenta con un sistema de control de acceso para ingresar a las áreas seguras y camaras de vigilancia	75	4	5	RIESGO EXTREMO	1	3	0	0	1	5	RIESGO MEDIO
	Existe un sistema de seguridad perimetral en alta disponibilidad	70				0		0				
	El acceso de los usuarios a los recursos tecnológicos tiene control de los encargados	70				1		0				
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	35				0		0				
	Se cuenta con un esquema de privilegios sobre los documentos importantes para la institución	35				1		0				
R2. Ataques externos / internos (hacking)	Existe una plataforma de seguridad perimetral en alta disponibilidad	90	4	4	RIESGO EXTREMO	2	2	0	0	2	4	RIESGO MEDIO
R3. Cambio de privilegios sin autorización	Se cuenta con un procedimiento formal de control de cambios	60	4	3	RIESGO EXTREMO	1	1	0	0	3	3	RIESGO MEDIO
R4. Desastres naturales	Area encargada de los desastres naturales como terremotos, inundaciones, Incendios, etc	45	4	4	RIESGO EXTREMO	1	1	0	0	3	3	RIESGO MEDIO
	Simulacros de evaluación	60				0		1				
R5. Divulgación de información de autenticación	Se tiene implementada la politica de contraseñas y ususarios	75	3	3	RIESGO ALTO	1	1	0	0	2	3	RIESGO MEDIO
R6. Error del administrador	Se cuenta con un procedimiento formal de control de cambios	60	4	3	RIESGO ALTO	1	1	0	0	3	3	RIESGO MEDIO
R7. Instalación de software no autorizado	Se tiene implementada la política para restringir la instalación de software por parte de los usuarios	75	3	4	RIESGO ALTO					3	4	RIESGO ALTO
R8. Interceptación no autorizada de información	Los canales de comunicación utilizan protocolos de encriptación para la transmisión de datos	70	3	3	RIESGO MEDIO	1	1	1	1	2	2	RIESGO BAJO
R9. Interrupción en los servicios	Se cuenta con una plataforma de servicios	55	3	3	RIESGO MEDIO		1	1	1	2	2	RIESGO BAJO
	Se cuenta con un procedimiento formal de control de cambios	60										
	Centro de procedimientos de control de desastres naturales	45				1						
R10. Modificación sin autorización	El acceso de los usuarios al los recursos tecnológicos se controla a través del directorio activo	70	3	3	RIESGO MEDIO	1	2		2	1	1	RIESGO RESIDUAL
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	35										
	Se cuenta con un esquema de privilegios sobre los documentos importantes para la institución	55				1		2				
R11. Robo de equipos	Se cuenta con un sistema de control de acceso para ingresar a las áreas seguras y camaras de vigilancia	100	3	3	RIESGO MEDIO		2		2	1	1	RIESGO RESIDUAL
	Existe guardias de seguridad que revisan los equipos que entran y salen	80				1		1				
	Existe algun convenio de seguridad	85				1		1				
R12. Robo de información	Existe una plataforma de seguridad perimetral en alta disponibilidad	70	3	3	RIESGO MEDIO		1		1	2	2	RIESGO BAJO
	Existe un esquema de permisos y procedimientos de seguridad impementados en los sistemas de información	70				1		1				
R13. Suplantación de identidad de usuarios	Se cuenta con un sistema de control de acceso para ingresar a las áreas seguras y camaras de vigilancia	100	3	3	RIESGO MEDIO							RIESGO MEDIO
R14. Uso inadecuado de sistemas para generar fraudes	Los programas de haking etico cuentan con un esquema de autentificación y seguimiento de auditoria	55	3	3	RIESGO MEDIO					3	3	RIESGO MEDIO
R15. Uso inadecuado de sistemas que generan interrupción	Se cuenta con procedimientos para auditar los sistemas de información utilizados en la institución	55	3	2	RIESGO MEDIO		1			2	2	RIESGO BAJO
	Se cuenta con los protocolos para el control de incidentes	45				1						
R16. Abuso de privilegios	Se cuenta con auditorias de privilegios	50	3	3	RIESGO MEDIO	1	1		1	2	2	RIESGO BAJO
	Los sistemas de información son sometidos a auditorias y protocolos de seguridad	60										
	Se auditan los esquemas de privilegios y utilizacion de información	35						1				

Elaboración Propia

CAPITULO VII

IMPLEMENTACIÓN

7.1. Monitoreo y evaluación de la solución

7.1.1. Políticas de seguridad de la información

Se realizaron las directrices donde se señalan y especifican las políticas Seguridad de la Información, que contienen las normas y los lineamientos que normaran la seguridad de la información en la Facultad de Ciencias de la Universidad Santiago Antúnez de Mayolo, además de ello delimita los compromisos, responsabilidades, obligaciones y deberes de todo el personal administrativo y docente, además de los estudiantes y terceros que tengan acceso a la información de la institución.

Es importante mencionar que el correcto cumplimiento de las políticas de seguridad de la información por los involucrados en el manejo de información sensible de la facultad, permitirá reducir los riesgos, es por ello que, para alcanzar este objetivo, es imperante que el Sistema de Gestión de Seguridad de la Información y las políticas de gestión de incidentes sean impulsada por el consejo de facultad, para su aprobación e implementación.

Es significativo difundir en toda la Facultad de Ciencias la importancia de los objetivos, los propósitos y las formas

adecuadas para la implementación de las políticas de seguridad de la información antes de su implantación arbitraria, buscando estratégicamente que los responsables de cada oficina entiendan que las políticas ayudaran a proteger la integridad, confidencialidad y disponibilidad de la información de la institución. Todo este proceso es de vital importancia para que el personal administrativo y docente no vean estas políticas como reglas que están direccionadas a la restricción de sus labores sino por el contrario, lo que se busca con una adecuada difusión y socialización es conseguir que todos los actores involucrados en la seguridad de la información de la Facultad de Ciencias acepten estas nomas para evitar que sus labores se compliquen con los riesgos asociados a la perdida de información. A continuación, se detalla el resumen del anexo a de la norma ISO 27001 que describe la política general de la seguridad de la información.

RESUMEN ANEXO A NORMA ISO 27001:2013

A5. Política general de seguridad de la información

A6. Organización de seguridad de la información

A7. Seguridad de los recursos humanos

A8. Gestión de activos

A9. Control de accesos

A10. Criptografía

A11. Seguridad física y del entorno

A12. Seguridad de las operaciones

A13. Seguridad de las comunicaciones

A14. Adquisición, desarrollo y Mantenimiento de sistemas

A15. Relaciones con los proveedores

A16. Gestión de incidentes de seguridad de la información

A17. seguridad de la información en la continuidad del negocio

A18. cumplimiento de requisitos legales y contractuales

Las Políticas de Seguridad de la Información definidas en el manual presentado en el anexo, son de obligatorio cumplimiento por todos los involucrados en el manejo de información importante para la Facultad de Ciencias.

7.1.2. Gestión de Incidentes de Seguridad

Gestionar los incidentes de seguridad de la información en la Facultad de Ciencias tiene como principal objetivo proveer un mecanismo estructurado en base a las políticas de seguridad de la información desarrolladas que permitirán negociar de manera adecuada los incidentes de seguridad que afectan la disponibilidad, integridad y confidencialidad de la información.

En base a los controles establecidos en la Facultad de Ciencias se han desarrollado procedimientos para actuar de manera correcta cuando se desarrolle un incidente de seguridad de la información, este deberá ser analizado, registrado y finalmente debe de ser reportado al encargado de la oficina del centro de cómputo quien se encargará de clasificar y tipificar dicho evento,

Esta dependencia administrativa de la Facultad de Ciencias será quien ocupará el rol de soporte técnico ante incidentes, para determinar si el incidente corresponde a un incidente o fenómeno de seguridad de la información o está relacionado con fallos o carencias de la infraestructura tecnológica.

Es importante mencionar que la oficina del centro de cómputo de la Facultad de Ciencias deberá tener en constante capacitación al personal técnico, para poder realizar el análisis y la clasificación de manera correcta, de esta manera se asegurará el correcto escalamiento de los incidentes en caso de ser necesario.

La clasificación de incidentes deberá ser de acuerdo a su tipo o naturaleza: técnico, humano o procedimental

7.1.3. Evaluación de los incidentes de seguridad

Esta etapa de evaluación de los incidentes de seguridad se debe realizar según la respuesta a la prioridad dentro de la Facultad de Ciencias, de acuerdo a su “prioridad” el cual se expresa como la multiplicación del impacto por su urgencia. Es importante mencionar que el nivel de prioridad se basa esencialmente en dos parámetros, el primero al número de usuarios que afecta y segundo, el tiempo máximo de demora para la resolución del mismo. Una vez analizado los dos parámetros de impacto es importante determinar una escala para determinar su urgencia, esto nos permitirá reducir los tiempos de atención y minimizar los procesos afectados en la Facultad de Ciencias

Finalmente es imprescindible analizar 3 aspectos esenciales como elementos que nos permitirán resolver las incidencias de manera más ágil, el primero elemento, son los recursos necesarios para resolver los problemas técnicos, el segundo, el tiempo para dar una solución y el tercer elemento es saber qué servicios son más críticos que otros, de acuerdo a esta escala, podremos saber cuándo dar una solución oportuna a servicios muy críticos o servicios poco críticos, de acuerdo a lo anterior se propone el siguiente método

Este pequeño método propuesto para valorar la prioridad de los incidentes de seguridad de la información en la Facultad de

Ciencias, consiste en elaborar una matriz doble de tres entradas donde se medirán los niveles de impacto por urgencia. De acuerdo a la herramienta grafica el eje X medirá el nivel de impacto que estará definido por los siguientes estados: Poco crítico (1), crítico (2), altamente crítico (3). Y el eje Y que definirá la urgencia está definido por los siguientes estados: No urgente (1), urgente (2), muy urgente (3)

Tabla 7.1: Criterio de prioridad del Incidente

URGENCIA		IMPACTO		
		1	2	3
	1	1	2	3
	2	2	4	6
	3	3	6	9

Elaboracion Propia

Esta matriz determinará los estados de urgencia de acuerdo a la multiplicación de los estados de urgencia por impacto, cuanto mayor sea el resultado del producto será mayor el nivel de prioridad para su atención, esto también estará ligada a la concurrencia de las incidencias presentadas.

7.1.4. Identificación de Incidentes de Seguridad de la Información.

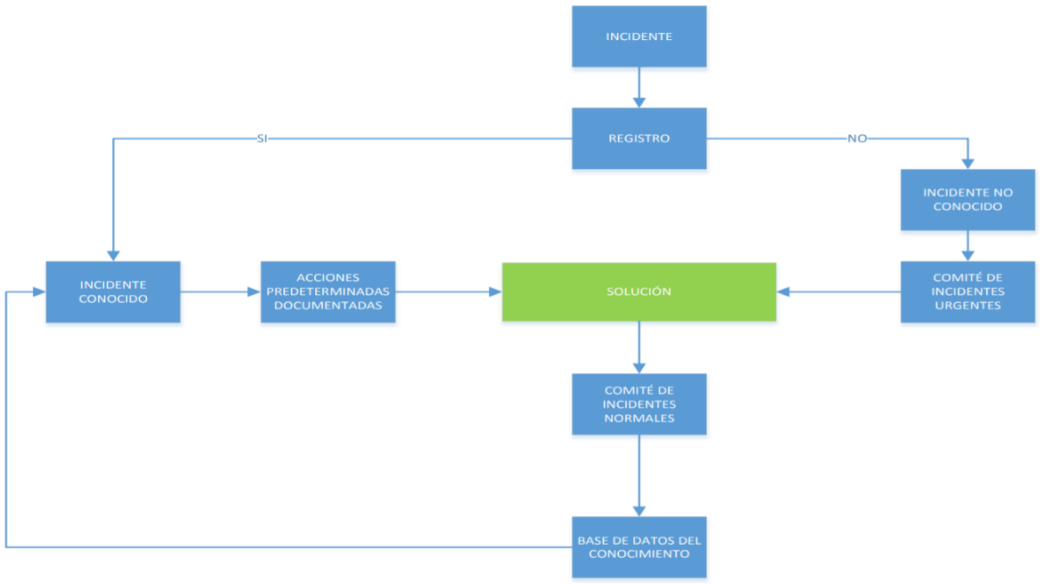
Para identificar un incidente de seguridad de la información en la Facultad de Ciencias es importante recibir inicialmente un reporte por los medios estipulados al encargado del centro de cómputo, vía llamada celular, correo electrónico, o en su defecto es rastreado por medio de logs anormales durante pruebas de rutina o monitoreo de los equipos informáticos, fallas en servicios, alertas en los sistemas administrativos de seguridad (antivirus, IDS, IPs), o fenómenos como robos o destrucción de activos de información. Para que el encargado del centro de cómputo pueda establecer si es un incidente de seguridad de la información se requiere previamente haber establecido un estado inicial del funcionamiento de la infraestructura tecnológica, esto nos ayudara a realizar posteriormente una verificación de las distintas fuentes que distorsionan el normal funcionamiento de los flujos de información. Además, es sumamente necesario realizar una evaluación que nos permita conocer los sistemas afectados, la información comprometida, la criticidad de los activos de información y la infraestructura afectada, para desplegar el plan de mitigación y eliminar las posibles causas que originan estos incidentes. Cabe precisar que es un punto importante en este procedimiento aislar e incomunicar los sistemas afectados, para bloquear conexiones externas, y detener de raíz las posibles causas, adicionalmente se realizara un registro de eventos para un análisis

forense si se requiriera más adelante, estos procedimientos deberán respetar el manejo de custodia y tratar discretamente los aspectos legales que pudieran surgir durante este proceso.

7.1.5. Acciones correctivas y preventivas ante incidentes

Es importante llevar acciones preventivas y correctivas ante los incidentes de seguridad de la información, a continuación, se definieron los siguientes procedimientos, donde un incidente no conocido pasa por una serie de pasos con el fin de darle una solución, documentándolo para que la próxima vez que se presente, se tengan las herramientas para contenerlo o eliminarlo con mayor rapidez y reduciendo el impacto que pueda generar.

Gráfico 7.1: Diagrama de flujo para la atención de un incidente



Elaboracion Propia

Dentro de la Facultad de Ciencias se definirá un comité encargado de analizar los incidentes de seguridad para que los integrantes del consejo de facultad puedan tomar las decisiones que mejoren los procedimientos correctivos y preventivos. Es de suma importancia concretar acciones preventivas y correctivas que permitan erradicar los incidentes conocidos, o los incidentes que son concurrentes. Para ello este comité tendrá que elevar informes donde se describan las acciones de finalización de la revisión del incidente, las pruebas realizadas que avalen que la solución planteada sea efectiva, de lo contrario el comité debe evaluar otras posibles soluciones para atacar los eventos e incidentes de raíz. Los incidentes que amenacen la seguridad de la información y que puedan generar un alto impacto, ya sea por el número de usuarios afectados o porque se han visto incluidos sistemas o servicios críticos para la Facultad de Ciencias, deberán ser tratados de acuerdo a los protocolos de respuesta urgente, propuestos por el comité de incidentes, que tendrán documentados una serie de protocolos técnicos para la eliminación de los incidentes conocidos. Es importante describir que cuando se presentan los incidentes no conocidos estos deben pasar por el comité para realizar una serie de pasos que involucran la búsqueda de la recuperación del servicio y la contención del impacto que pueda ocasionar de la manera más rápida, esta solución deberá ser documentada y registrada, para que así el comité de incidentes lo analice y catalogue como un incidente conocido, registrando el procedimiento de solución en la base de datos

del conocimiento y permitiendo aplicar la solución a los incidentes igualmente clasificados o catalogados. El proceso planteado permite de igual forma realizar un mejoramiento en la base de datos del conocimiento cada vez que se solicite o cada vez que el incidente presente conmutaciones. Al registrar el incidente y compararlo con la base de datos de incidentes conocidos, un incidente puede plantearse por sí mismo o como combinación de uno o más incidentes. Una vez se registra el incidente, los comités verificarán si se tienen información del mismo y si existe ya una solución temporal o definitiva conocida. Si el incidente comunicado tiene una solución temporal o definitiva, es un incidente conocido. El grupo de respuesta a incidentes de seguridad puede ponerse en contacto con el usuario para ofrecerle dicha solución. Incidente normal: Estos incidentes también tienen un procedimiento establecido, pero requieren de valoración y autorización del comité. A su vez, los incidentes de esta categoría se pueden dividir en menores, significativos y mayores. Es el principal. Incidentes Estándar: Son incidentes ya establecidos, pre-autorizados por el comité y para los cuales ya existe un procedimiento definido.

7.1.6. Plan de mejoramiento continuo ante los incidentes de seguridad

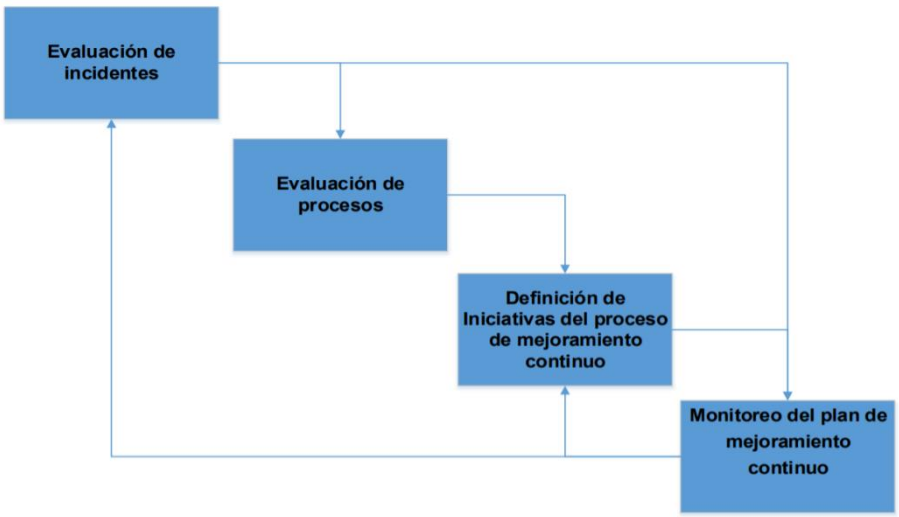
Basados en la norma ISO/IEC 27000 se propone que el plan de mejoramiento continuo de los incidentes tenga los siguientes procesos, se define de la siguiente manera:

- **Evaluación de incidentes:** Evaluar la gestión de incidentes de seguridad de la información regularmente. Esto incluye la identificación de áreas o servicios en que no se cumplen los niveles de seguridad propuestos, y las conversaciones regulares con las áreas del negocio para asegurar que los niveles de seguridad propuestos sean cónsonos con sus incidentes.
- **Evaluación de Procesos:** Evaluar los procesos de gestión de incidentes de seguridad de la información regularmente. Esto implica identificación de áreas o servicios en que no se cumple con las metas de KPI propuestas por la Facultad, así como comparativas, auditorías, evaluaciones de madurez y revisiones de procesos. Se debe evaluar constantemente las políticas, la gestión de incidentes, la clasificación de incidentes y todos los procesos que van ligados.
- **Definición de Iniciativas del proceso de mejoramiento continuo:** Definir iniciativas específicas con el fin de mejorar la seguridad de la información y los procesos involucrados, partiendo de los resultados de evaluaciones de la seguridad de la información y lo procesos. Las iniciativas resultantes son internas y propiciadas

por el grupo de respuesta a incidentes de seguridad de la información, o iniciativas que requieren la cooperación de las demás áreas o terceros expertos en el tema. Se deben proponer planes, proyectos, soluciones que ayuden a mejorar los procesos apuntando al mejoramiento continuo de la gestión de incidentes y la organización en general, buscando proteger los activos de la información.

- **Monitoreo del plan de mejoramiento continuo:** "Verificar si las iniciativas de mejora se implementan de acuerdo con lo planificado, e introducir medidas correctivas, de ser necesario. Verificar si los objetivos propuestos con el sistema de gestión de incidentes de seguridad de la información se están cumpliendo". (ITIL Perfeccionamiento Continuo del Servicio - CSI, 2015)

Gráfico 7.2: Estructura del proceso de mejoramiento ante un incidente



Elaboración propia

CAPITULO VIII

RESULTADOS

Los Resultados obtenidos al finalizar la investigación post aplicación de los instrumentos de análisis y herramientas de procesamiento e identificación de Amenazas, vulnerabilidades, Riesgos y posibles impactos, se pudo evidenciar lo siguiente, que, con la Gestión de Incidencias de Seguridad de la Información podemos establecer los controles de seguridad de la información para la Facultad de Ciencias de la UNASAM.

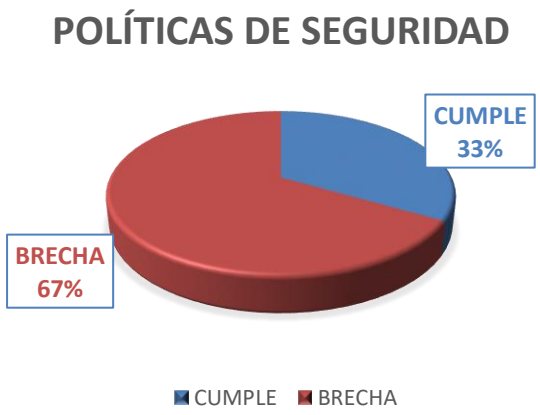
Los resultados van acorde al planteamiento de nuestros objetivos específicos los cuales se sustentan a continuación:

I. RESULTADO 1

De acuerdo a lo planteado en nuestro primer objetivo donde se plantea elaborar el diagnóstico y análisis GAP para determinar la brecha de seguridad de la información en la Facultad de Ciencias.

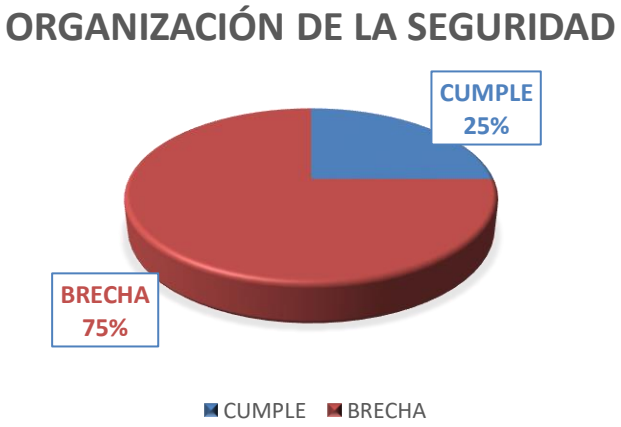
Este diagnóstico se realizó determinando la situación actual de la Facultad de Ciencias en términos de seguridad de la información, en el Anexo 01 se detalla lo siguiente

- A nivel de Políticas de Seguridad, la brecha y nivel de cumplimiento es el siguiente:



Estos valores porcentuales reflejan la no existencia de políticas de seguridad, normatividad vigente, procedimientos, responsables de la seguridad de la información y los controles para verificar la efectividad de los mismos.

- El nivel de cumplimiento en la organización de la seguridad de la información es el siguiente:



Estos valores porcentuales reflejan la no existencia de roles y responsabilidades definidos, nivel de organización en las áreas de la facultad para gestionar la seguridad de la información, el nivel bajo de formación en temas vinculados a la seguridad la información.

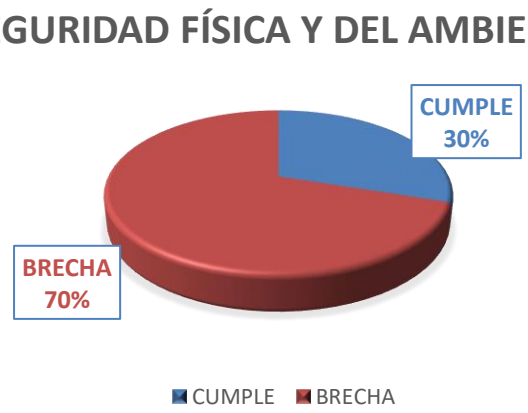
- El nivel de Administración de Activos para la seguridad de la información es el siguiente:

Estos valores porcentuales reflejan una administración parcial de los activos de información, ya que algunas áreas poseen un inventario de los datos y equipos que poseen, otras las omiten y no disponen de una clasificación de las mismas.

- El nivel de Seguridad del RR.HH. para la seguridad de la información es el siguiente:

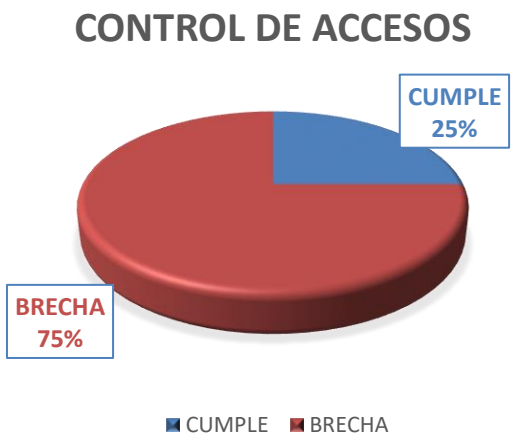
Estos valores porcentuales reflejan la no existencia de controles de seguridad para el recurso humano dentro de la Facultad de Ciencias.

- El nivel de Seguridad Física y del Ambiente. para la seguridad de la información es el siguiente:



- El nivel de Gestión de comunicaciones y operaciones para la seguridad de la información es el siguiente:

- El nivel de control de accesos para la seguridad de la información es el siguiente:



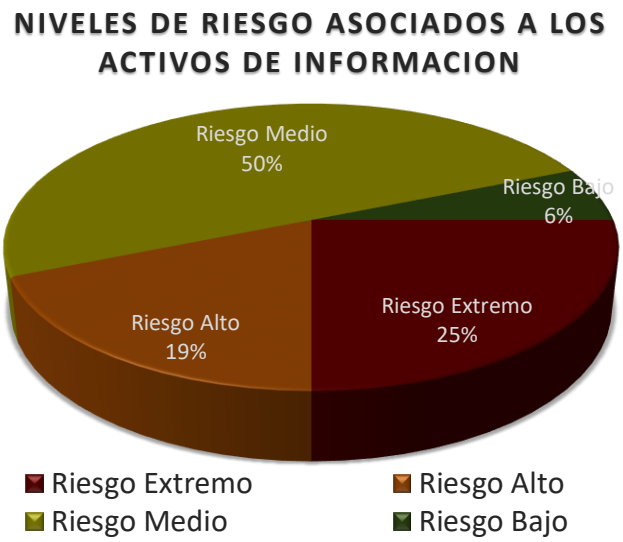
- El nivel de Desarrollo y mantenimiento de los sistemas para la seguridad de la información es el siguiente:

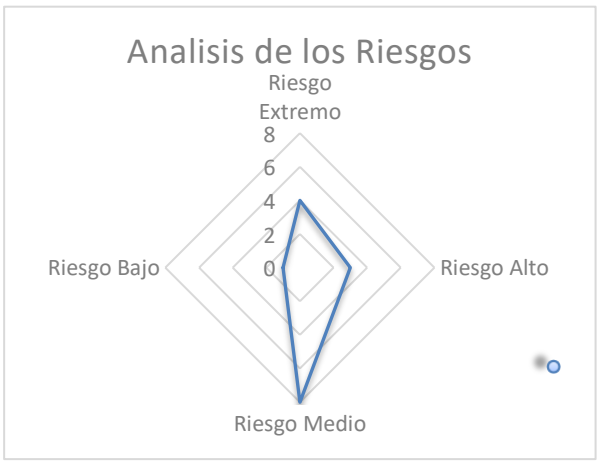
- El nivel de Administración de Incidentes de los sistemas para la seguridad de la información es el siguiente:

- El nivel de Continuidad del Negocio de los sistemas para la seguridad de la información es el siguiente:

II. RESULTADO 2

En el segundo objetivo específico nos propusimos elaborar el diagnóstico de los riesgos inherentes para determinar el impacto y los niveles de riesgo de los activos de información de la Facultad de Ciencias. En el Anexo 02 se detallan los niveles de riesgos asociados a cada grupo activos de información. A continuación, se detallan los resultados en términos de porcentaje obtenidos al aplicar las herramientas de análisis de riesgos para determinar los niveles de riesgo y los impactos asociados a estos.

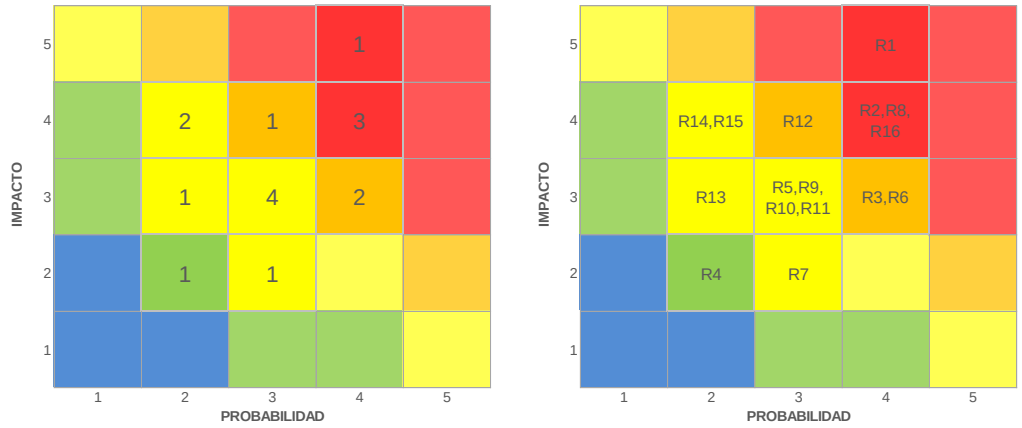




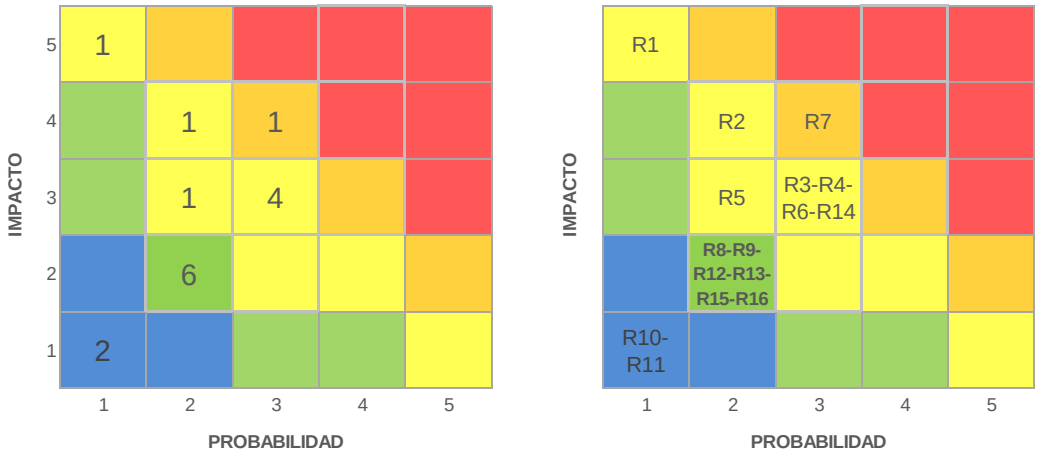
III. RESULTADO 3

En el tercer objetivo nos propusimos elaborar el análisis de valoración de los controles de seguridad de la información para determinar el desplazamiento del mapa de riesgo. En el Anexo 03 se detalla el nivel de desplazamiento del mapa de calor. A continuación, se puntualiza los resultados esperados al aplicar las herramientas de análisis propuestos en la Norma ISO 27000.

MAPA DE CALOR DEL RIESGO INICIAL



MAPA DE CALOR DEL RISGO FINAL



La figura muestra el comportamiento que sufren los riesgos al establecer controles de seguridad, vemos que parte de los riesgos que estaban en la zona extrema, que correspondían a riesgos que requerían acciones inmediatas de tratamiento orientadas a reducir, compartir el riesgo, transferirlo o incluso evitarlo ahora sean riesgos medios.

CAPÍTULO IX

DISCUSIÓN DE RESULTADOS

El proyecto tuvo como fin demostrar que a través de la Gestión de Incidentes de la Seguridad de la Información se podría establecer los controles de seguridad en la Facultad de Ciencias, habiendo estructurado el proceso de identificación de las áreas susceptibles para incidir en los controles y sabiendo que activos informáticos requieren de controles de seguridad se desarrolló los controles que nos permitirán medir la efectividad de los controles. Esta disminución permitió que todos los riesgos extremos se movieran a otras zonas del mapa de calor. Los controles identificados y valorados para el riesgo R1 - Acceso no autorizado, permitieron que este riesgo se moviera de la zona extrema a una de las zonas de riesgo medio. Esta reducción fue una de las más efectivas en el mapa de calor, a pesar de la reducción del nivel de este riesgo, el mismo quedo es una zona de riesgo medio que requiere de medidas adecuadas que permitan seguir disminuyendo el riesgo a un nivel bajo o inusual.

El Riesgos R2 - Ataques externos / internos (hacking no ético), paso de la zona extrema a la zona de riesgo medio, debido a una disminución en su nivel de riesgo generada por los controles identificados. Este riesgo requiere de acciones prontas y adecuadas para reducir el riesgo a niveles más bajos.

Los Riesgo R8 - Interceptación no autorizada de información en tránsito y R16 - Abuso de privilegios, que estaban en la zona extrema, solo tuvieron una reducción del 25% generada por sus respectivos controles, quedando en la zona riesgo alto que requiere de una atención y medidas urgentes para reducir el nivel del riesgo.

Los controles valorados para el riesgo R11 - Robo de equipos, generaron el mayor nivel desplazamiento en el mapa de calor, permitiendo que este riesgo pasara de la zona media a la zona más baja de riesgo inusual. Este riesgo se asume y no necesita tratamiento. El riesgo Robo de información pasó de la zona de riesgo alta a la zona de riesgo media, debido a que los controles valorados generaron una disminución media. Este riesgo al quedar en una zona de riesgo medio requiere de medidas adecuadas que permitan disminuir el riesgo a nivel bajo o inusual.

Los Cambio de privilegios sin autorización y Error del administrador, solo tuvieron una disminución mínima de acuerdo a la valoración de los respectivos controles, lo cual, genero una disminución de un solo punto sobre el eje de la probabilidad. A pesar de que estos riesgos pasaron de la zona de riesgo alto a la de riesgo medio, requieren de acciones para seguir reduciendo el riesgo a niveles más bajos. La Divulgación de información de autenticación y Uso inadecuado de sistemas que generan interrupción, tuvieron una disminución en su nivel de riesgo, permanecieron en la zona media del mapa de calor. Estos riesgos

requieren de medidas para seguir reduciendo el riesgo a niveles más bajos.

A pesar de la disminución que los controles genero sobre el Desastres naturales, este permaneció en la zona de riesgo bajo, donde se requieren de algunas medidas preventivas para reducir el riesgo.

Después de elaborar el mapa de riegos inherente del proceso de tecnología, se establecieron los planes de tratamiento orientados a mitigar los riesgos, con el objetivo de preservar las características de confidencialidad, integridad y disponibilidad de la información que se gestiona a través de los activos seleccionados para el proceso de valoración de riesgos.

CONCLUSIONES

Habiendo finalizado la investigación se ha podido llegar a las siguientes conclusiones, primero, es importante la gestión de incidentes de seguridad de la información para administrar de manera eficaz los sucesos críticos que afectan los activos de información y recursos informáticos de la facultad de ciencias de la UNASAM. Segundo, que los controles establecidos en base al desarrollo de una metodología estructurada generan que los riesgos asociados a los activos de información se reduzcan de manera considerable. Tercero, que método para clasificar y evaluar los incidentes de seguridad de la información que actualmente se presentan o los que se pueden presentar, partiendo de un método estándar conocido como la ISO 27000. Cuarto es importante utilizar herramientas que permitirán al investigador ver y gestionar sus incidentes de seguridad en todo momento y hacer un seguimiento continuo siempre bajo normas certificadas en las mejores prácticas ISO 2700, así se tendrá toda la trazabilidad del incidente desde el momento en el que inicia hasta que se resuelve. Finalmente se propone conformar los comités de atención a los incidentes de seguridad de la información, este comité de incidentes sería el responsable del análisis y aprobación de las soluciones de seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

- Amutio A., y Candau, J. (2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid, España. Extraído dehttp://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.U_GmSsWSz94.
- Information Systems Audit and Control Association. (2008). Alineando COBIT® 4.1, ITIL® V3 e ISO/IEC 27002 en beneficio de la empresa.
- Information Systems Audit and Control Association (2012). Control Objectives for Information and Related Technologies.
- Instituto Nacional de Estadística e Informática [INEI]. Guía Teórico Practica para la Elaboración de Planes Estratégicos de Tecnologías de Información. Extraído de http://www.ongei.gob.pe/publica/metodologias/5162.pdf.
- International Organization for Standardization ISO/IEC 27001. (2005). Information technology - Security techniques - Information security management systems - Requirements.
- International Organization for Standardization ISO/IEC 27002. (2005). Information technology - Security techniques - Code of practice for information security management.
- International Organization for Standardization ISO/IEC 27003. (2010). Information technology - Security techniques - Information security management systems implementation guidance.
- International Organization for Standardization ISO/IEC 27005. (2008). Information technology - Security techniques - Information security risk management.
- International Organization for Standardization ISO/IEC Guide 73. (2002). Risk management - Vocabulary - Guidelines for use in standards.

- International Organization for Standardization ISO/IEC TR 18044. (2004). Information technology - Security techniques - Information security incident management.
- International Organization for Standardization. ISO/IEC 13335-1. (2004). Information technology – Security technique - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.
- International User Group. (2012). International Register of ISMS Certificates. Consulta: 13 de septiembre de 2012. Extraído de http://www.iso27001certificates.com/
- Ley N° 29733. Congreso de la República del Perú. 03 de julio del 2011.
- Norma Técnica Peruana ISO/IEC 7001. (2008). EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información" en todas las entidades integrantes del Sistema Nacional de Informática. Extraído de http://bvirtual.indecopi.gob.pe/normas/isoiec27001.pdf
- Romero R., y Noriega, S. (2009). Factores Críticos de Éxito: Una Estrategia de Competitividad. Culcyt. Extraído de http://erevistas.uacj.mx/ojs/index.php/culcyt/article/view/340/322
- Tupia, M. (2010). Administración de la Seguridad de Información. Lima: Tupia Consultores y Auditores S.A.C.
- UNIT - ISO/IEC 27001. (2005). “Tecnología de la información– Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información”. Extraído de http://www.unit.org.uy/iso27000/iso27001.php.

ANEXOS

ANEXO 01

ANÁLISIS GAP DIAGNÓSTICO DE LA BRECHA EN LA FACULTAD DE CIENCIAS

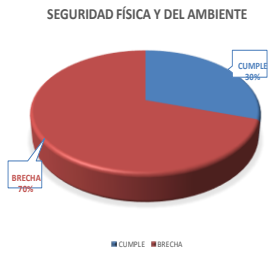
HERRAMIENTA DE DIAGNÓSTICO DE ANALISIS DE BRECHA						
ANALISIS GAP						
POLÍTICAS DE SEGURIDAD		TEST - ENTREVISTA	Pto.	VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Existen documento(s) de políticas de seguridad de los SI	FALSO	0	6	SI	NO
2	Existe normativa relativa a la seguridad de los SI	FALSO	0			
3	Existen procedimientos relativos a la seguridad de SI	VERDADERO	1			
4	Existe un responsable de las políticas, normas y procedimientos	VERDADERO	1			
5	Existen mecanismos para la comunicación a los usuarios de las normas	FALSO	0			
6	Existen controles regulares para verificar la efectividad de las políticas	FALSO	0			
RANGO DEL 0 AL 06		CALIFICACION TOTAL	2		33.33	66.67
ORGANIZACIÓN DE LA SEGURIDAD		TEST- ENTREVISTA	Pto.	VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Existen roles y responsabilidades definidos para las personas implicadas en la seguridad	VERDADERO	1	8	SI	NO
2	Existe un responsable encargado de evaluar la adquisición y cambios de SI	FALSO	0			
3	La Dirección y las áreas de la Organización participa en temas de seguridad	FALSO	0			
4	Existen condiciones contractuales de seguridad con terceros y outsourcing	VERDADERO	1			
5	Existen criterios de seguridad en el manejo de terceras partes	FALSO	0			
6	Existen programas de formación en seguridad para los empleados, clientes y terceros	FALSO	0			
7	Existe un acuerdo de confidencialidad de la información que se accesa.	FALSO	0			
8	Se revisa la organización de la seguridad periódicamente por una empresa externa	FALSO	0			
RANGO DEL 0 A 08		CALIFICACION TOTAL	2		25	75.00
ADMINISTRACION DE ACTIVOS		TEST - ENTREVISTA	Pto.	VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Existen un inventario de activos actualizado	VERDADERO	1	6	SI	NO
2	El Inventario contiene activos de datos, software, equipos y servicios	FALSO	0			
3	Se dispone de una clasificación de la información según la criticidad de la misma	FALSO	0			
4	Existe un responsable de los activos	VERDADERO	1			
5	Existen procedimientos para clasificar la información	VERDADERO	1			
6	Existen procedimientos de etiquetado de la información	FALSO	0			
RANGO DEL 0 A 06		CALIFICACION TOTAL	3		50.00	50.00
ADMINISTRACIÓN DE ACTIVOS		TEST - ENTREVISTA	Pto.	VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Se tienen definidas responsabilidades y roles de seguridad	FALSO	0	9	SI	NO
2	Se tiene en cuenta la seguridad en la selección y baja del personal	VERDADERO	1			
3	Se plasman las condiciones de confidencialidad y responsabilidades en los contratos	FALSO	0			
4	Se imparte la formación adecuada de seguridad y tratamiento de activos	FALSO	0			
5	Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad	FALSO	0			
6	Se recogen los datos de los incidentes de forma detallada	VERDADERO	1			
7	Informan los usuarios de las vulnerabilidades observadas o sospechadas	VERDADERO	1			
8	Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades	FALSO	0			
9	Existe un proceso disciplinario de la seguridad de la información	FALSO	0			
RANGO DEL 0 A 09		CALIFICACION TOTAL	3		33.33	66.67

HERRAMIENTA DE DIAGNÓSTICO DE ANALISIS DE BRECHA

ANALISIS GAP

	SEGURIDAD DE LOS RRHH	TEST - ENTREVISTA	Pto.		VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Existe perímetro de seguridad física(una pared, puerta con llave).	VERDADERO	1				
2	Existen controles de entrada para protegerse frente al acceso de personal no autorizado	VERDADERO	1				
3	Un área segura ha de estar cerrada, aislada y protegida de eventos naturales	VERDADERO	1				
4	En las áreas seguras existen controles adicionales al personal propio y ajeno	FALSO	0				
5	Las áreas de carga y expedición están aisladas de las áreas de SI	VERDADERO	1				
6	La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.	FALSO	0	11	SI	NO	
7	Existen protecciones frente a fallos en la alimentación eléctrica	FALSO	0				
8	Existe seguridad en el cableado frente a daños e intercepciones	VERDADERO	1				
9	Se asegura la disponibilidad e integridad de todos los equipos	FALSO	0				
10	Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente	FALSO	0				
11	Se incluye la seguridad en equipos moviles	FALSO	0				
	RANGO DEL 0 A 11	CALIFICACION TOTAL	5		45.45	54.55	

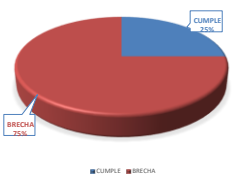
	SEGURIDAD FÍSICA Y DEL AMBIENTE	TEST	Pto.		VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Todos los procedimientos operativos identificados en la política de seguridad se encuentran documentados	FALSO	0				
2	Estan establecidas responsabilidades para controlar los cambios en equipos	VERDADERO	1				
3	Estan establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad	FALSO	0				
4	Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas	FALSO	0				
5	Existe una separación de los entornos de desarrollo y producción	VERDADERO	1				
6	Existen contratistas externos para la gestión de los Sistemas de Información	FALSO	0				
7	Existe un plan de acopio de la información para asegurar la adecuada capacidad de proceso y de almacenamiento de la informaación	FALSO	0				
8	Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones	FALSO	0				
9	Controles contra software maligno	VERDADERO	1				
10	Realizar copias de backup de la información esencial para la facultad	VERDADERO	1				
11	Existen logs para las actividades realizadas por los operadores y administradores	FALSO	0				
12	Existen logs de los fallos detectados	FALSO	0	23	SI	NO	
13	Existen rastro de auditoría	FALSO	0				
14	Existe algún control en las redes	VERDADERO	1				
15	Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)	FALSO	0				
16	Eliminación de los medios informáticos. Pueden disponer de información sensible	FALSO	0				
17	Existe seguridad de la documentación de los Sistemas	VERDADERO	1				
18	Existen acuerdos para intercambio de información y software	FALSO	0				
19	Existen medidas de seguridad de los medios en el tránsito de la información	FALSO	0				
20	Existen medidas de seguridad en las transacciones electrónicas en la facultad.	FALSO	0				
21	Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada	FALSO	0				
22	Existen medidas de seguridad en las transacciones en linea	FALSO	0				
23	Se monitorean las actividades relacionadas a la seguridad	FALSO	0				
	RANGO DEL 0 A 23	CALIFICACION TOTAL	6		30.00	70.00	



HERRAMIENTA DE DIAGNÓSTICO DE ANALISIS DE BRECHA

ANALISIS GAP

GESTIÓN DE COMUNICACIONES Y OPERACIONES		TEST	Pto.	VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Existe una política de control de accesos	FALSO	0	23	SI / NO	
2	Existe un procedimiento formal de registro y baja de accesos	VERDADERO	1			
3	Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario	FALSO	0			
4	Existe una gestión de los password de usuarios	FALSO	0			
5	Existe una revisión de los derechos de acceso de los usuarios	FALSO	0			
6	Existe el uso del password	FALSO	0			
7	Se protege el acceso de los equipos desatendidos	VERDADERO	1			
8	Existen políticas de limpieza en el puesto de trabajo	VERDADERO	1			
9	Existe una política de uso de los servicios de red	FALSO	0			
10	Se asegura la ruta (path) desde el terminal al servicio	FALSO	0			
11	Existe una autenticación de usuarios en conexiones externas	FALSO	0			
12	Existe una autenticación de los nodos	FALSO	0			
13	Existe un control de la conexión de redes	FALSO	0			
14	Existe un control del routing de las redes	VERDADERO	1			
15	Existe una identificación única de usuario y una automática de terminales	FALSO	0			
16	Existen procedimientos de log-on al terminal	FALSO	0			
17	Se ha incorporado medidas de seguridad a la computación móvil	FALSO	0			
18	Está controlado el teletrabajo por la organización	FALSO	0			
RANGO DEL 0 A 23		CALIFICACION TOTAL	4		25.00 / 75.00	

CONTROL DE ACCESOS		TEST	Pto.	VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Se asegura que la seguridad está implantada en los Sistemas de Información	FALSO	0	8	SI / NO	
2	Existe seguridad en las aplicaciones	VERDADERO	1			
3	Existen controles criptográficos.	FALSO	0			
4	Existe seguridad en los ficheros de los sistemas	FALSO	0			
5	Existe seguridad en los procesos de desarrollo, testing y soporte	VERDADERO	1			
6	Existen controles de seguridad para los resultados de los sistemas	FALSO	0			
7	Existe la gestión de los cambios en los SO.	FALSO	0			
8	Se controlan las vulnerabilidades de los equipos	FALSO	0			
RANGO DEL 0 A 08		CALIFICACION TOTAL	2		25.00 / 75.00	

DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS		TEST	Pto.	VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Se comunican los eventos de seguridad	VERDADERO	1	5	SI / NO	
2	Se comunican los debilidadesde seguridad	VERDADERO	1			
3	Existe definidas las responsabilidades antes un incidente.	FALSO	0			
4	Existe un procedimiento formal de respuesta	FALSO	0			
5	Existe la gestión de incidentes	FALSO	0			
RANGO DEL 0 A 05		CALIFICACION TOTAL	2		40.00 / 60.00	

ADMINISTRACIÓN DE INCIDENTES		TEST	Pto.	VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Existen procesos para la gestión de la continuidad.	VERDADERO	1	5	SI / NO	
2	Existe un plan de continuidad del negocio y análisis de impacto	VERDADERO	1			
3	Existe un diseño, redacción e implantación de planes de continuidad	FALSO	0			
4	Existe un marco de planificación para la continuidad del negocio	FALSO	0			
5	Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.	FALSO	0			
RANGO DEL 0 A 05		CALIFICACION TOTAL	2		40.00 / 60.00	

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		TEST	Pto.	VALOR PORCENTUAL		GRAFICO PORCENTUAL
1	Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas	FALSO	0	5	SI / NO	
2	Existe el resguardo de la propiedad intelectual	VERDADERO	1			
3	Existe el resguardo de los registros de la organización	VERDADERO	1			
4	Existe una revisión de la política de seguridad y de la conformidad técnica	FALSO	0			
5	Existen consideraciones sobre las auditorías de los sistemas	FALSO	0			
RANGO DEL 0 A 05		CALIFICACION TOTAL	2		40.00 / 60.00	

ANEXO 02

HERRAMIENTA PARA DETERMINAR LOS NIVELES DE RIESGO Y LOS IMPACTOS ASOCIADOS A ESTOS.

”

CODIGO	RIESGOS	ACTIVOS	PROBABILIDAD	IMPACTO	PROBABILIDAD X IMPACTO	NIVEL DE RIESGO
R1	Acceso no autorizado	Area administración Bases de datos Cuartos de Red Directorio de usuarios Equipos de seguridad Correos electronicos Oficinas de la facultad Almacen de acervo documentario Laboratorios de computo	4. ALTA	5. CATASTROFICO	20	RIESGO EXTREMO
R2	Ataques externos e internos	Bases de datos Equipos de computo Servidores SIGA WEB	4. ALTA	4. MAYOR	16	RIESGO EXTREMO
R3	Interceptación no autorizada de información en tránsito Interceptación no autorizada de	Red WAN Red LAN Correos electronicos	4. ALTA	4. MAYOR	16	RIESGO EXTREMO
R4	Abuso de privilegios	Oficinas de la facultad Correos electronicos Almacen de acervo documentario Bases de datos Directorio de Usuarios	4. ALTA	4. MAYOR	16	RIESGO EXTREMO
R5	Cambio de privilegios sin autorización	Almacen de acervo documentario Directorio de usuarios Correos electronicos	4. ALTA	3. MODERADO	12	RIESGO ALTO
R6	Error del administrador	Bases de datos Red LAN y Red WAN Servidores SIGA WEB Laboratorios de computo Almacen de acervo documentario	4. ALTA	3. MODERADO	12	RIESGO ALTO
R7	Robo de información	Bases de datos SIGA WEB Correos electronicos Almacen de acervo documentario	3. MEDIA	4. MAYOR	12	RIESGO ALTO
R8	Divulgacion de información	Bases de datos SIGA WEB Correos electronicos	3. MEDIA	3. MODERADO	9	RIESGO MEDIO
R9	Interrupción en los servicios	SIGA WEB Servidores Plataformas implementadas Infrmación administrativa	3. MEDIA	3. MODERADO	9	RIESGO MEDIO
R10	Modificación sin autorización	Bases de datos Directorio de usuarios Laboratorios de computo Plataformas implementadas	3. MEDIA	3. MODERADO	9	RIESGO MEDIO
R11	Robo de equipos	Laboratorios de computo Cuartos de Red Serviidores	3. MEDIA	3. MODERADO	9	RIESGO MEDIO
R12	Uso inadecuado de sistemas para generar fraudes	Bases de datos SIGA WEB Correos electronicos	2.BAJA	4. MAYOR	8	RIESGO MEDIO
R13	Uso inadecuado de sistemas que generan interrupción	Bases de datos Plataformas implementadas SIGA WEB Servidores	2.BAJA	4. MAYOR	8	RIESGO MEDIO
R14	Instalación de software no autorizado	Laboratorios de computo Portatiles Computadoras administrativas	3. MEDIA	2. INUSUAL	6	RIESGO MEDIO
R15	Suplantación de identidad de usuarios	Directorio de usuarios Laboratorios de computo Correos electronicos	2.BAJA	3. MODERADO	6	RIESGO MEDIO
R16	Desastres naturales	Laboratorios de computo Servidores Cuartos de Red	2. BAJO	2. INUSUAL	4	RIESGO BAJO

ANEXO 03

NIVEL DE DESPLAZAMIENTO DEL MAPA DE CALOR

DESPLAZAMIENTO MAPA DE RIESGO

			INHERENTE			DISMINUCIÓN				RESIDUAL						
Riesgos/Amenaza	Descripción del Control	PUNTAJE TOTAL	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	Probabilidad	Total de controles	Impacto	Total de controles	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	ANALISIS DE DISMINUCION PORCENTUAL	%		DISMINUCION
R1. Acceso no autorizado	Se cuenta con un sistema de control de acceso para ingresar a las áreas seguras y camaras de vigilancia	75	4	5	RIESGO EXTREMO	1	3	0	0	1	5	RIESGO MEDIO	20	5	25%	75%
	Existe un sistema de seguridad perimetral en alta disponibilidad	70				1		0								
	El acceso de los usuarios a los recursos tecnológicos tiene control de los encargados	70				1		0								
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	35				0		0								
	Se cuenta con un esquema de privilegios sobre los documentos importantes para la institución	35				0		0								
R2. Ataques externos / internos (hacking)	Existe una plataforma de seguridad perimetral en alta disponibilidad	90	4	4	RIESGO EXTREMO	2	2	0	0	2	4	RIESGO MEDIO	16	8	50%	50%
R3. Cambio de privilegios sin autorización	Se cuenta con un procedimiento formal de control de cambios	60	4	3	RIESGO EXTREMO	1	1	0	0	3	3	RIESGO MEDIO	12	9	75%	25%
R4. Desastres naturales	Area encargada de los desastres naturales como terremotos, inundaciones, Incendios, etc	45	4	4	RIESGO EXTREMO	0	1	0	0	3	3	RIESGO MEDIO	16	6	38%	63%
	Simulacros de evaluación	60				1		1								
R5. Divulgación de información de autenticación	Se tiene implementada la politica de contraseñas y ususarios	75	3	3	RIESGO ALTO	1	1	0	0	2	3	RIESGO MEDIO	6	6	100%	0%
R6. Error del administrador	Se cuenta con un procedimiento formal de control de cambios	60	4	3	RIESGO ALTO	1	1	0	0	3	3	RIESGO MEDIO	7	6	86%	14%
R7. Instalación de software no autorizado	Se tiene implementada la política para restringir la instalación de software por parte de los usuarios	75	3	4	RIESGO ALTO	1	1			2	4	RIESGO MEDIO	12	6	50%	50%
R8. Interceptación no autorizada de información	Los canales de comunicación utilizan protocolos de encriptación para la transmisión de datos	70	3	3	RIESGO MEDIO	1	1	1	1	2	2	RIESGO BAJO	6	4	67%	33%
R9. Interrupción en los servicios	Se cuenta con una plataforma de servicios	55	3	3	RIESGO MEDIO	1	2			1	3	RIESGO BAJO	9	3	33%	67%
	Se cuenta con un procedimiento formal de control de cambios	60				1										
	Centro de procedimientos de control de desastres naturales	45														
R10. Modificación sin autorización	El acceso de los usuarios al los recursos tecnológicos se controla a través del directorio activo	70	3	3	RIESGO MEDIO	1	2	1	2	1	1	RIESGO RESIDUAL	9	2	22%	78%
	Las aplicaciones cuentan con esquemas de seguridad basado en roles y permisos	35														
	Se cuenta con un esquema de privilegios sobre los documentos importantes para la institución	55				1		1								
R11. Robo de equipos	Se cuenta con un sistema de control de acceso para ingresar a las áreas seguras y camaras de vigilancia	100	4	4	RIESGO MEDIO	2	3		2	1	2	RIESGO RESIDUAL	8	2	25%	75%
	Existe guardias de seguridad que revisan los equipos que entran y salen	80				1		2								
	Existe algun convenio de seguridad	40				0										
R12. Robo de información	Existe una plataforma de seguridad perimetral en alta disponibilidad	70	3	3	RIESGO MEDIO	1	2		1	1	2	RIESGO RESIDUAL	9	2	22%	78%
	Existe un esquema de permisos y procedimientos de seguridad impementados en los sistemas de información	70				1		1								
R13. Suplantación de identidad de usuarios	Se cuenta con un sistema de control de acceso para ingresar a las áreas seguras y camaras de vigilancia	100	4	3	RIESGO MEDIO	2	2	1	1	2	2	RIESGO RESIDUAL	12	4	33%	67%
R14. Uso inadecuado de sistemas para generar fraudes	Los programas de haking etico cuentan con un esquema de autentificación y seguimiento de auditoria	55	4	3	RIESGO MEDIO	1	1	1	1	3	2	RIESGO MEDIO	7	6	86%	14%
R15. Uso inadecuado de sistemas que generan interrupción	Se cuenta con procedimientos para auditar los sistemas de información utilizados en la institución	55	3	2	RIESGO MEDIO		1			2	2	RIESGO BAJO	5	4	80%	20%
	Se cuenta con los protocolos para el control de incidentes	45				1										
R16. Abuso de privilegios	Se cuenta con auditorias de privilegios	50	3	3	RIESGO MEDIO	1	2	1	1	1	2	RIESGO RESIDUAL	9	2	22%	78%
	Los sistemas de información son sometidos a auditorias y protocolos de seguridad	60				1										
	Se auditan los esquemas de privilegios y utilizacion de información	35														

TIPO DE RIESGO	VALOR NIVEL DE RIESGO
Riesgo Extremo	Nivel Riesgo mayor o igual a 15 puntos
Riesgo Alto	Nivel Riesgo mayor o igual a 10 y menor a 15 puntos
Riesgo Medio	Nivel Riesgo mayor o igual a 5 y menor a 10 puntos
Riesgo Bajo	Nivel Riesgo mayor o igual a 3 y menor a 5 puntos
Riesgo Inusual	Nivel Riesgo Menor a 3 puntos

Valores de Calificación del Control	Control de disminución - Probabilidad o Impacto Niveles a disminuir en la probabilidad
Entre 0 - 50 puntos	0
Entre 51 - 75 puntos	1
Entre 76 - 100 puntos	2

ANEXO 04

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA EL BUEN USO DEL HARDWARE

Esta política se refiere al buen uso que debemos darles a los equipos de Cómputo de la facultad de ciencias de la UNASAM

1.- POLÍTICAS DE SEGURIDAD PARA EQUIPOS DE COMPUTO

1.1. Los equipos de Cómputo sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implementado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

1.2. Los equipos sólo deben usarse para actividades académicas de investigación y actividades inherentes a la formación profesional y no para otros fines, tales como juegos y pasatiempos.

1.3. Debe respetarse y no modificar la configuración de hardware y software establecida por el departamento de sistemas.

1.4. No se permite, comer o beber mientras se esté usando un equipo.

1.5. Deben protegerse los equipos de riesgos del ambiente (por ejemplo, polvo, radiación solar y agua).

1.6. Para el uso de los equipos de cómputo deben usarse estabilizadores de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpidas (UPS).

1.7. Cualquier falla en las computadoras o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o no disponibilidad de los servicios.

1.8. Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

1.9. No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de los centros de cómputo se requiere una autorización escrita.

1.10. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

1.11. Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas y además deben configurar el protector de pantalla 62 para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad.

1.12. No está permitido conectar a la RED computadores portátiles (laptops) de terceros y en caso de ser necesario se debe solicitar la autorización correspondiente y notificar al encargado del centro de cómputo.

1.13. Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN.

1.14. A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la facultad de ciencias está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

1.15. Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al encargado del centro de cómputo y poner el equipo en cuarentena hasta que el problema sea resuelto.

1.16. Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos a continuación.

Solo se pueden bajar archivos que sean estrictamente de trabajo.

No se permite descargar música, videos, o programas no autorizados de Internet.

No se permite hacer transferencia de archivos a través de programas de mensajería como Yahoo Messenger, Aol instant Messenger, Facebook.

No se permite descargar archivos y guardarlos localmente desde correos personales como Hotmail, Yahoo, etc.

Debe utilizarse un programa antivirus para examinar todo software que venga de fuera.

1.17. No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el encargado del centro de cómputo. 1.18. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el departamento de Sistemas. 63 1.19. Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo el software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro. 1.20. No deben usarse USB u otros medios de almacenamiento de externos en cualquier computadora a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos. 1.21. Periódicamente debe hacerse el respaldo de los datos guardados en PC’s y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. 1.22. Es responsabilidad del usuario tener toda su información dentro de una sola carpeta raíz, como Mis Documentos, para facilitar el respaldo de su información. 1.23. La información de carácter personal se deberá almacenar en una carpeta fuera de Mis Documentos y esta no formará

parte del respaldo del equipo responsabilidad del departamento de sistemas. 1.24. El conocimiento de las claves de acceso a cuentas de correo, servicios Web y servidores debe limitarse estrictamente a las personas autorizadas (departamento de sistemas y una persona más para emergencias) y en ningún caso deben revelarse a consultores, contratistas y personal temporal. 1.25. Siempre que sea posible, debe eliminarse información confidencial de las computadoras y unidades de disco duro antes de que se les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante. 1.26. Los usuarios deben ser responsables de sus impresiones y por lo tanto asegurarse de recoger sus documentos impresos y revisar que la impresora quede con suficiente papel. 1.27. Los usuarios que tengan impresoras instaladas dentro de su cubículo o en su área de trabajo (conectadas directamente a sus equipos o en Red) son responsables de encender y apagar la(s) impresora(as). 1.28. El personal que utiliza un equipo portátil que contenga información confidencial de la Fundación, no debe dejarla desatendida, sobre todo cuando esté de viaje. 1.29. Los equipos de cómputo deben apagarse por completo durante periodos largos de ausencia (juntas, reuniones, hora de comida) y por supuesto al salir de la oficina, asegurándose de apagar también el monitor.

FORMATO DE AUTORIZACIÓN PARA PUBLICACIÓN DE TESIS Y TRABAJOS DE INVESTIGACIÓN, PARA OPTAR GRADOS ACADÉMICOS Y TÍTULOS PROFESIONALES EN EL REPOSITORIO INSTITUCIONAL DIGITAL - UNASAM

Conforme al Reglamento del Repositorio Nacional de Trabajos de Investigación – RENATI.
Resolución del Consejo Directivo de SUNEDU N° 033-2016-SUNEDU/CD

1. Datos del Autor:

Apellidos y Nombres: Brito Rodriguez, Roberto Elias

Código de alumno: 052.0125.608 Teléfono: 939109097

Correo electrónico: bito110@hotmail.com DNI o Extranjería: 44476929

2. Modalidad de trabajo de investigación:

( ) Trabajo de investigación ( ) Trabajo académico

( ) Trabajo de suficiencia profesional (**X**) Tesis

3. Título profesional o grado académico:

( ) Bachiller (**X**) Título ( ) Segunda especialidad

( ) Licenciado ( ) Magister ( ) Doctor

4. Título del trabajo de investigación:

"Gestión de Incidentes de Seguridad de la Información en la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo, 2017"

5. Facultad de Ciencias

6. Escuela, Carrera o Programa: Ingeniería de Sistemas e Informática

7. Asesor:

Apellidos y Nombres: Alvarado Cáceres, Luis Ruperto Teléfono: 943975749

Correo electrónico: luisalvaradoca@hotmail.com DNI o Extranjería: 07587674

A través de este medio autorizo a la Universidad Nacional Santiago Antúnez de Mayolo, publicar el trabajo de investigación en formato digital en el Repositorio Institucional Digital, Repositorio Nacional Digital de Acceso Libre (ALICIA) y el Registro Nacional de Trabajos de Investigación (RENATI).

Asimismo, por la presente dejo constancia que los documentos entregados a la UNASAM, versión impresa y digital, son las versiones finales del trabajo sustentado y aprobado por el jurado y son de autoría del suscrito en estricto respeto de la legislación en materia de propiedad intelectual.

Firma: .....

D.N.I.: 44476929

FECHA: 10 / 03 /2020