UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

ESCUELA DE POSGRADO

TESIS

Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú

Para optar el grado académico de maestro en:

Ingeniería de Sistemas y Computación

AUTOR: **Ing. Elmer Luis ATENCIO BAZAN**

ASESOR: **Mg. Teodoro ALVARADO RIVERA**

Cerro de Pasco – Perú - 2019

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

ESCUELA DE POSGRADO

TESIS

Diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001:2014 para la dirección general de informática y estadística de la Universidad Nacional Daniel Alcides Carrión Pasco Perú

Sustentada y aprobada ante los miembros del jurado

Dr. Ángel Claudio NUÑEZ MEZA	**Dr. Tito Marcial ARIAS ARZAPALO**
PRESIDENTE	**MIEMBRO**

Mg. Percy RAMIREZ MEDRANO
MIEMBRO

DEDICATORIA:

A mi familia, por su constante apoyo para el logro de mi formación personal y formación profesional.

A mis amistades, colegas y docentes que siempre comparten el conocimiento, alegrías y tristezas.

RECONOCIMIENTO

Como autor de la presente tesis de maestría deseo expresar mis agradecimientos a todos aquellos que, de una forma u otra colaboraron al desarrollo y materialización de mis ideas.

En particular, deseo agradecer a los siguientes:

A mis padres, Julio Atencio Centeno e Isidora Bazán Guerra, por todo el apoyo moral y material brindado, así como, hacer de mí una persona de bien. A todos mis hermanos y hermanas gracias por su apoyo.

A mi esposa Verónica Vargas Valverde, por su comprensión, apoyo y ayuda incondicional. A mis hijos Matts y Max Alexander, alegrías de mi vida.

A los docentes de la escuela de Post Grado de la Undac, por compartir sus conocimientos, eternamente agradecido.

Es justo reconocer, a aquellos que en algún momento me brindaron su mano cuando la necesité. Llegue hasta todos, mi más sentido respeto, consideración y agradecimiento profundo.

RESUMEN

La presente investigación tuvo como objetivo general el Diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP-ISO/IEC 27001:2014, para mejorar la integridad, confidencialidad y disponibilidad de los activos de información en la DGIyE de la UNDAC.

La investigación realizada fue tipo aplicado con un diseño no experimental transeccional descriptivo. La población y muestra estuvo constituida por ocho trabajadores administrativos y el director de la DGIyE de la UNDAC. Se usó como técnica de recopilación de datos la observación y la encuesta, así mismo se usó el instrumento Ficha de Observación.

Para la realización del diseño del Sistema de Gestión de Seguridad de la Información se comenzó con el diagnóstico de la DGIyE de la UNDAC, procediendo luego al estudio de la organización y su contexto, se identificó los procesos críticos, se definió el alcance y las políticas de seguridad de la información, se identificó las amenazas y vulnerabilidades, se empleó la metodología MAGERIT para la gestión de riesgos y finalmente se identificaron los controles de seguridad necesarios para reducir los riesgos.

Finalmente se concluye que el Diseño de un SGSI basado en la NTP-ISO/IEC 27001:2014, mejora significativamente la integridad, confidencialidad y disponibilidad de los activos de información en la DGIyE de la UNDAC. Ya que se minimiza el nivel de riesgos al aplicar controles

Palabras clave: Sistema de Gestión de Seguridad de la Información, NTP-ISO/IEC 27001:2014.

ABSTRACT

The general objective of this research was the Design of an Information Security Management System based on the NTP-ISO / IEC 27001: 2014, to improve the integrity, confidentiality and availability of information assets in the DGIyE of the UNDAC.

The research carried out was a type applied with a non-experimental descriptive transectional design. The population and sample consisted of eight administrative workers and the director of the DGIyE of the UNDAC. Observation and survey were used as a data collection technique, and the Observation Card instrument was also used.

To carry out the design of the Information Security Management System, the diagnosis of the DGIyE of the UNDAC was started, proceeding to the study of the organization and its context, the critical processes were identified, the scope and policies were defined of information security, threats and vulnerabilities were identified, the MAGERIT methodology was used for risk management and finally the necessary security controls were identified to reduce the risks.

Finally, it is concluded that the Design of an ISMS based on the NTP-ISO / IEC 27001: 2014, significantly improves the integrity, confidentiality and availability of the information assets in the DGIyE of the UNDAC. Since the level of risks is minimized when applying controls

Keywords: Information Security Management System, NTP-ISO / IEC 27001: 2014.

INTRODUCCIÓN

El presente trabajo se basa fundamentalmente por la problemática que se pudo percibir en los procesos de tratamiento de la información, en el área de sistemas de la Dirección General de Informática y Estadística de la Universidad Nacional Daniel Alcides Carrión – Pasco - Perú.

Sin duda alguna, las Tecnologías de la Información y la Comunicación (TIC) han transformado de manera vertiginosa la vida cotidiana y social de los seres humanos, el avance de las herramientas para el procesamiento de información (equipos de cómputo, dispositivos móviles, redes wifi, etc) tanto en el aspecto físico (hardware) como lógico (software), así como el desarrollo de los mecanismos empleados para establecer comunicaciones, han generado dinamismo en los procesos productivos y de prestación de servicios, pero de igual manera han surgido riesgos de la seguridad de la información.

Paralelo con este avance tecnológico y descubrimiento de nuevos riesgos de la seguridad de la información, se ha desarrollado la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, guía de buenas prácticas en la administración de los activos de información, que se convierten en estrategias adoptadas por las organizaciones para la preservación de la confidencialidad, integridad y disponibilidad de la información.

Por lo que, la presente investigación se enfocó principalmente en identificar los riesgos de los activos de información y concientizar al personal

administrativo del área de sistemas del DGIyE de la UNDAC, a cargo del manejo de la información para preservar la confidencialidad, la integridad y la disponibilidad de la información.

Asimismo, considero el esquema de tesis propuesto por la Escuela de Postgrado de la UNDAC, considerando los siguientes capítulos:

En el Capítulo I, se detallan la identificación y determinación del problema, también se dan a conocer los objetivos generales y específicos que trazaron la investigación para su desarrollo. Dicho capítulo finaliza manifestando las limitaciones, así como la justificación de la importancia de la investigación desarrollada, basada en la hipótesis de investigación y la identificación y descripción de variables que dio inicio al presente estudio.

En el Capítulo II, considero lo relacionado al soporte teórico resaltando los antecedentes y las características de la seguridad de la información, se desarrolla atendiendo a tres dimensiones principales, las cuales son, confidencialidad entendida como la garantía del acceso a la información únicamente de los usuarios autorizados, integridad como la preservación de la información de forma completa y exacta y disponibilidad como la garantía del acceso a la información en el instante en que el usuario la necesita. El capítulo finaliza manifestando la definición de términos básicos, metodologías y tecnologías utilizadas en el desarrollo de la presente investigación.

El capítulo III definido por la metodología, se inicia con la definición de tipificación y método de investigación y diseño utilizado en el trabajo de investigación. La población y muestra establecida en el estudio como también las técnicas e instrumentos utilizados en la recolección de datos en la presente investigación.

El capítulo V Primeramente se realizó el diagnóstico inicial de la DGIyE de la UNDAC, con respecto a la NTP ISO/IEC 27001:2014 y su posibilidad de aceptación, enseguida se estudió a la organización y su contexto; se identificó el proceso crítico; se definió la política de seguridad, el alcance y se identificó al comité de seguridad de la información de la organización, luego, siguiendo la metodología de análisis y gestión de riesgos adoptada, se identificó y valoró los activos de información, se identificó las amenazas, se realizó el cálculo del impacto y del riesgo, se identificaron las medidas de control necesarias para mitigar los riesgos a un nivel aceptable y finalmente se elaboró un documento denominado declaración de aplicabilidad que contiene la justificación de qué controles del Anexo A de la NTP ISO/IEC 27001:2014 pueden ser implementados en la DGIyE de la UNDAC.

Para finalizar la investigación se describen las conclusiones y recomendaciones a fin de realizar futuras investigaciones relacionadas con el tema.

INDICE

Pág.

CAPÍTULO III

METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

CAPÍTULO I

PROBLEMA DE INVESTIGACIÓN

1.1 IDENTIFICACIÓN Y DETERMINACIÓN DEL PROBLEMA.

Es de conocimiento que la Universidad Nacional Daniel Alcides Carrión al ser una institución pública de educación superior, maneja y controla información importante para los estudiantes, docentes, comunidad y estado; por lo que la utilización de la tecnología de la información y las comunicaciones le ofrecen grandes ventajas al área de sistemas de la Dirección General de Informática y Estadística (DGIE-UNDAC) y a cualquier organización hoy en día.

La necesidad de gestionar la seguridad de la información nace de un entorno cada vez más globalizado donde las instituciones deben tomar decisiones rápidas y eficientes convirtiendo la información en uno de los activos informáticos más importantes dentro de las organizaciones llegando a tener una importancia estratégica para muchas de ellas ya

que les permite mantener una ventaja competitiva frente a otras organizaciones.

Como consecuencia de esto los cambios tecnológicos y su utilización hace que el área de sistemas de la Dirección General de Informática y Estadística, en adelante DGIyE de la UNDAC; esté sometida a riesgos y amenazas para su información, debido justamente al crecimiento de hackers, programas maliciosos e incluso usuarios internos que se les considera de mayor peligro, que afectarán directamente a la información (datos) que se transmiten a través de las redes informáticas de la institución. A pesar de su plan de seguridad que maneja el responsable de la seguridad de la DGIyE-UNDAC siempre se necesitara una evaluación técnica de la seguridad de la información.

El diseño del Sistema de Gestión de Seguridad de la Información (SGSI) se enmarca en la Norma Técnica Peruana de seguridad de sistemas de información NTP ISO/IEC 27001:2014, que especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización y persiguiendo el licenciamiento universitario de la UNDAC.

Adicionalmente, el marco legal de nuestro país obliga a las entidades públicas, pertenecientes al Sistema Nacional de Informática, el diseño e implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basándose en la norma técnica peruana (NTP) – ISO/IEC 27001:2014.

Según resolución ministerial Nº 004-2016-PCM del 08 de enero del 2016 se aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

http://busquedas.elperuano.com.pe/download/url/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1

1.2 DELIMITACIÓN DE LA INVESTIGACIÓN

El tema de investigación se delimitará al Diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP-ISO/IEC 27001:2014, para la Dirección General de Informática y Estadística (DGIyE) de la Universidad Nacional Daniel Alcides Carrión, ubicado en el distrito de Yanacancha, comprensión de la provincia y región Pasco en el año 2018.

1.3 FORMULACIÓN DEL PROBLEMA.

1.3.1 PROBLEMA GENERAL

¿El Diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP-ISO/IEC 27001:2014, mejora la integridad, confidencialidad y disponibilidad de los activos de información en la DGIyE de la UNDAC?

1.3.2 PROBLEMAS ESPECÍFICOS

1. ¿Cuáles son los documentos exigidos por la NTP-ISO/IEC 27001:2014, para diseñar el Sistema de Gestión de Seguridad de la Información en la DGIyE de la UNDAC?
2. ¿Existe una valoración de activos a proteger en la DGIyE de la Universidad Nacional Daniel Alcides Carrión?
3. ¿Qué metodología usar para el análisis y gestión de riesgos en la DGIyE de la Universidad Nacional Daniel Alcides Carrión?
4. ¿Cuál será el tratamiento de los riesgos identificados en la DGIyE de la Universidad Nacional Daniel Alcides Carrión?

1.4 FORMULACIÓN DE OBJETIVOS.

1.4.1 OBJETIVO GENERAL.

Diseñar el Sistema de Gestión de Seguridad de la Información basado en la NTP-ISO/IEC 27001:2014, para mejorar la integridad, confidencialidad y disponibilidad de los activos de información en la DGIyE de la UNDAC.

1.4.2 OBJETIVOS ESPECÍFICOS.

1. Elaborar los documentos exigidos por la NTP-ISO/IEC 27001:2014 para el diseño del sistema de gestión de seguridad de la información en la DGIyE de la Universidad Nacional Daniel Alcides Carrión.
2. Elaborar la valoración de activos de información para la DGIyE de la Universidad Nacional Daniel Alcides Carrión.

3. Aplicar la metodología MAGERIT para analizar y gestionar los riesgos de los activos de información en la DGIyE de la Universidad Nacional Daniel Alcides Carrión.
4. Elaborar la lista de controles para mitigar los riesgos de los activos de información detectados en la DGIyE de la Universidad Nacional Daniel Alcides Carrión.

1.5 JUSTIFICACIÓN DE LA INVESTIGACIÓN.

La información se ha convertido en un recurso estratégico trascendental en la UNDAC, por esta razón debe existir técnicas, procedimientos y actividades que la aseguren, además de la seguridad física que se establece en los equipos que se almacena la información, es vital la seguridad lógica, que radica en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo permita acceder a la información a personal autorizado para su manipulación o gestión. La universidad no cuenta con una metodología de gestión de seguridad clara y estructurada para reducir el riesgo de pérdida, corrupción o robo de la información.

1.6 LIMITACIONES DE LA INVESTIGACIÓN.

En la Dirección General de Informática y Estadística de la UNDAC, no se encuentra limitaciones en cuanto a la recopilación de información y se cuenta con el apoyo del director y colegas Administrativos en el desarrollo de las preguntas para el llenado de la ficha de observación, que nos permita diagnosticar el nivel de seguridad de la Información, quedo muy agradecido con cada uno de ellos.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE ESTUDIO.

2.1.1 NIVEL NACIONAL:

Título

“Diseño de un Sistema de Gestión de Seguridad de Información para Servicios Postales del Perú S.A.”

Autor:

Ing. David Arturo Aguirre Mollehuanca

Universidad:

Pontificia Universidad Católica del Perú

Resumen

Es necesario difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas.

2.1.2 NIVEL INTERNACIONAL:

Título

"Planeación y diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 - 27002"

Autor:

Ing. Buenaño Quintana, José Luis

Universidad:

Universidad Politécnica Salesiana del Ecuador

Resumen

Mediante el análisis de la situación actual de la seguridad de la información, fue posible determinar que existe la necesidad de robustecer los controles establecidos para salvaguardar los activos de información. Con la información recopilada fue posible realizar el diagrama mostrado a continuación el cual evidencia la necesidad de aplicar estándares, regulados, documentados y

difundidos. Cumplimiento de mejores prácticas seguridad informática UPS Guayaquil.

2.2. BASES TEÓRICAS - CIENTÍFICAS

Para la presente investigación tomé en cuenta las siguientes definiciones de los autores que se detallan a continuación:

2.2.1. INFORMACIÓN

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración. (Fuente: ISOTOOLS)

La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. (Fuente: IMARPE)

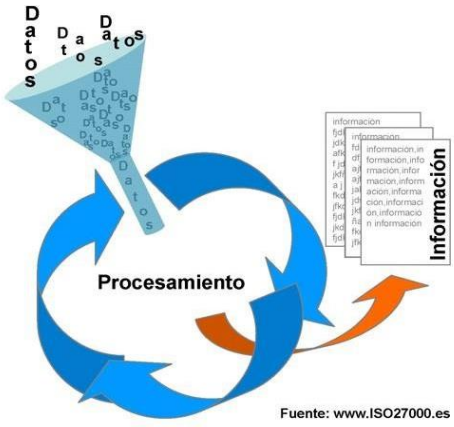


Figura 01. Proceso sistemático

2.2.2. ACTIVOS DE INFORMACIÓN

Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información.

Figura 02. Activos de información

Fuente: Ing José Manuel Poveda Ruiz- UNI-ESTE
https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-7.pdf

2.2.3. SEGURIDAD DE LA INFORMACIÓN

Seguridad de la Información es el nivel de confianza que la organización desea tener de su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información. Tiene como objetivo proteger el recurso información de una amplia gama de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el daño y, cumplir su misión y objetivos estratégicos.

La seguridad de la información se entiende como la preservación de las siguientes características:

Confidencialidad: es asegurar que la información es accesible sólo para las personas autorizadas para ello.

Integridad: es salvaguardar la exactitud y totalidad de la información en su procesamiento, transmisión y almacenamiento.

Disponibilidad: es asegurar que los usuarios autorizados tengan acceso a la información y los activos asociados cuando estos sean requeridos.

(Fuente: Wikipedia).

2.2.4. AMENAZAS y VULNERABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

2.2.4.1. VULNERABILIDADES

Junto con las amenazas, se debe estudiar las vulnerabilidades, que se definen como debilidades de seguridad asociadas con los activos de información de una organización.

- **Seguridad de los recursos humanos.** Falta de entrenamiento en seguridad, falta de mecanismos de monitoreo, políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, empleados desmotivados.

- **Control de acceso.** Segregación inapropiada de redes, falta de políticas de escritorio y pantalla limpia, políticas incorrectas de control de acceso, claves de acceso sin modificaciones.

- **Seguridad física y ambiental.** (Inadecuado control de acceso físico a oficinas, salones y edificios, ubicación en áreas propensas a inundaciones, almacenes desprotegidos, carencia de programas de sustitución de equipos, equipos mal cuidados).

- **Gestión de operaciones y comunicación.** Control de cambios inadecuados, gestión de red inadecuada, carencia de mecanismos que aseguren la emisión y recepción de mensajes, carencia de tareas segregadas, falta de protección en redes públicas de comunicación.

- **Mantenimiento, desarrollo y mantención de sistemas de información**. Protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos

procesados, falta de documentación de software, mala selección de pruebas de datos.

Una vez que se identifican las vulnerabilidades se debe evaluar la posibilidad que sean explotadas por una amenaza.

2.2.4.2. AMENAZAS

Al analizar las amenazas a las que se ve enfrentada la información podemos clasificarlas en seis categorías:

- **Sucesos de origen físico:** son todos los eventos naturales y técnicos, así mismos también eventos indirectamente causados por la intervención humana.
- **Amenazas Naturales**. Inundaciones, tsunamis, tornados, maremotos, huracanes, sismos, tormentas, incendios forestales.
- **Amenazas a Instalaciones**. Fuego, explosiones, caídas de energía, daño de agua, perdidas de acceso, fallas mecánicas.
- **Amenazas Humanas**. Huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdidas de personal clave.
- **Amenazas Tecnológicas.** Virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas de red, fallas en línea telefónica.

- **Amenazas Operacionales.** Crisis financiera, fallas en equipos, aspectos regulatorios, mala publicidad.
- **Amenazas Sociales.** Motines, protestas, sabotaje vandalismo, violencia laboral, terrorismo.

Para que una amenaza cause daño a algún activo de información tendría que explotar una o más vulnerabilidades del sistema, aplicaciones o servicios usados por la organización para ser exitosa en su intención de hacer daño.

Una vez que se establecen las distintas amenazas que pueden afectar un activo, se debe evaluar su posibilidad de ocurrencia.

2.2.5. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El SGSI es la abreviatura usada para referirse al Sistema de Gestión de la Seguridad de la Información. El SGSI ayuda a establecer las políticas, procedimientos y controles en relación a los objetivos de negocio de la organización, con objeto de mantener siempre el riesgo por debajo del nivel asumible por la propia organización.

En definitiva, con un SGSI, la organización conoce los riesgos a los que está sometida su información y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

2.2.5.1. ISO 27000

La serie de normas ISO/IEC 27000 son estándares de seguridad publicados por la Organización Internacional para la Estandarización y la Comisión Electrotécnica Internacional.

Figura 03. Familia ISO 00Figura 03. Familia ISO 27000

(Fuente: http://www.iso27000.es/download/doc_sgsi_all.pdf).

2.2.5.2. NTP ISO/IEC 27001:2014

La Norma Técnica Peruana de Seguridad de la Información (NTP-ISO/IEC 27001:2014), proporciona los requisitos necesarios para establecer, implementar mantener y mejorar continuamente un sistema de gestión de seguridad de la información.

Este sistema de gestión preserva la confidencialidad, integridad y disponibilidad de la información aplicando un

proceso de gestión de riesgos, y proporciona confianza a las partes interesadas en el sentido en que los riegos se manejan adecuadamente.

La Norma Técnica Peruana de Seguridad de la Información NTP-ISO/IEC 27001:2014, ha sido elaborada utilizando como antecedente al estándar internacional ISO/IEC 27001:2013, en donde no sólo se establecen cambios en el contenido sino también en la estructura respecto de la versión anterior (NTP-ISO/IEC 27001:2008).

Las principales modificaciones se ven reflejadas en la estructura y el contenido de los controles, donde el número total de dominios era de 11 y ahora son 14 y se reduce el número de controles de 133 a 113, todo como resultado de un proceso de fusión, exclusión e incorporación de nuevos controles de seguridad.

Además, en esta nueva versión de la 27001, se ha ampliado el tema del tratamiento de riesgos alineándolo con la ISO 31000 referida a la Gestión de Riesgos en forma genérica; es decir, a los riesgos de todo tipo (no sólo de seguridad de la información) que pueden afectar una organización.

Algo muy importante de destacar es que la ISO/IEC 27001:2013 ha sido desarrollado con base en el Anexo

SL del “Suplemento Consolidado de las Directivas ISO/IEC”, en el cual se alinean bajo una misma estructura todos los documentos relacionados con los sistemas de gestión y evitando así problemas de integración con otros marcos de referencia.

Así pues, la nueva estructura queda como sigue:

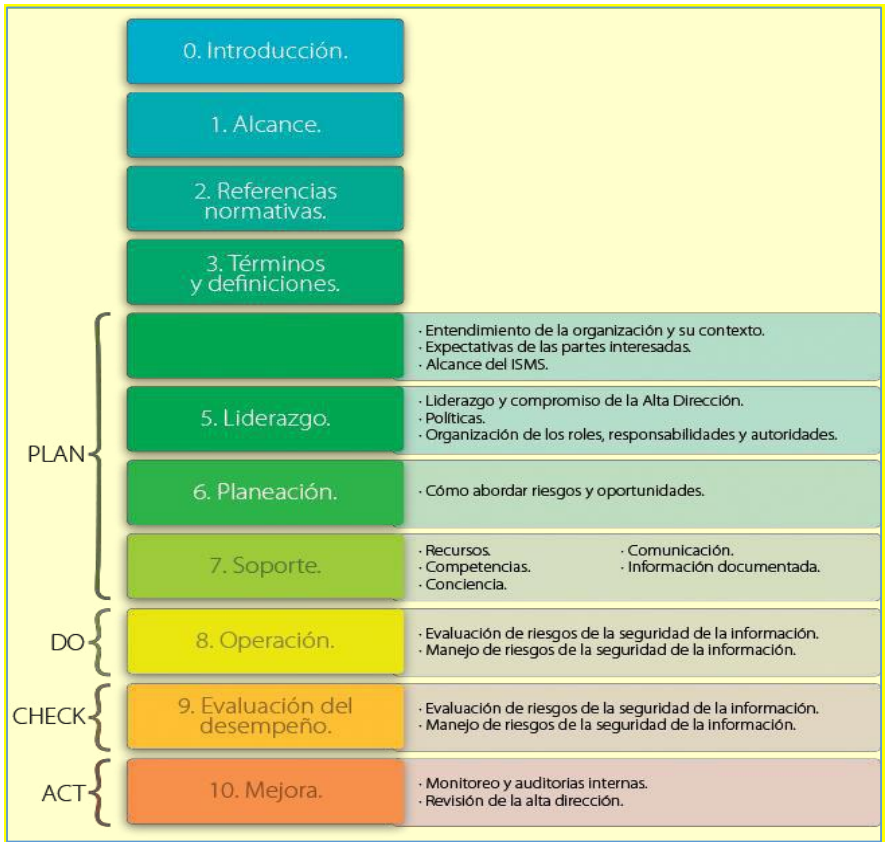


Figura 04: **Estructura del estándar ISO/IEC 27001:2013**

2.2.6. ESTRUCTURA DE LA NTP-ISO/IEC 27001:2014

En Perú contamos con la NTP-ISO/IEC 27001:2014 para garantizar tanto la confidencialidad como la integridad de la información, pero también de los sistemas que lo tratan. La NTP

ISO IEC 27001 para los Sistemas de Gestión de la Seguridad de la Información o SGSI hace posible que las organizaciones evalúen el riesgo y apliquen los controles indispensables para proceder a su mitigación o total eliminación.

La estructura de la norma queda así:

0. Introducción
1. Objeto y campo de aplicación
2. Referencias Normativas
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación
10. Mejora
11. Anexo A – Lista de controles

2.2.7. ADMINISTRACIÓN DEL SISTEMA DE GESTÓN DE SEGURIDAD DE LA INFORMACIÓN

2.2.7.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Comité de alto nivel conformado por el Rector, Autoridades de la Universidad Nacional Daniel Alcides Carrión y el Oficial de seguridad de la información

Sus funciones son:

- Aprobar las políticas de seguridad de la información.
- Aprobar las actualizaciones del SGSI
- Aprobar los planes de contingencia que permitan salvaguardar la continuidad de los procesos y operaciones críticas de la institución.
- Gestionar los recursos necesarios para contribuir con las mejoras en la seguridad de la información
- Revisar y aprobar los proyectos, planes y programas de seguridad de la información.
- Asignar roles y responsabilidades generales en materia de seguridad de la información.
- Promover y gestionar la difusión de planes y programas que permitan establecer y mantener la concientización del personal en materia de seguridad de la información
- Asegurar el cumplimiento de programas, normas y leyes vigentes en materia de seguridad de la información.
- Aprobar el entrenamiento y/o capacitaciones al personal de seguridad de la información.

2.2.7.2. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Figura responsable por velar, mantener y administrar la seguridad de los activos de información de la Universidad y que se expresa en el documento referido a Responsabilidades de la Gestión de la Seguridad.

Sus funciones entorno al SGSI son desarrolladas dentro

del equipo de seguridad interdisciplinario, donde desempeña el rol de coordinador.

2.2.7.3. EQUIPO DE SEGURIDAD INTERDISCIPLINARIO

Equipo consultivo de trabajo liderado por el oficial de seguridad de información, encargado de revisar y proponer políticas y procedimientos para la normativa.

Sus funciones son:

- Elaborar y proponer las políticas específicas del sistema de gestión de seguridad de la información.
- Evaluar, coordinar y monitorear la implementación de controles relacionados al SGSI.
- Implementación de controles específicos y evaluación de los mismos en un periodo de tiempo establecido por el Grupo interdisciplinario.
- Definir, implementar y evaluar los planes de concientización en materia de seguridad de la información.
- Comunicar al comité de seguridad, mediante el OSI, el estado de la seguridad de la información de la UNDAC en relación a la NTP-ISO 27001 2014.

2.2.8. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad identifican responsabilidades y establecen los objetivos para una protección apropiada y consistente de los activos de información de la Universidad.

2.2.9. RIESGO

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

2.2.10. GESTIÓN DE RIESGO

La gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen **la identificación**, **el análisis y la evaluación de riesgo**, para luego establecer las estrategias para su tratamiento, utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evitar el riesgo (esto es, reducir su probabilidad o impacto a 0), reducir el impacto negativo del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular mediante una decisión informada.

Algunas veces, el manejo de riesgos se centra en la contención de riesgo por causas físicas o legales (por ejemplo, desastres naturales o incendios, accidentes, muerte o demandas).

Todos los procesos de evaluación de riesgos utilizan la misma metodología. Determinar el activo a ser revisado. Identificar las amenazas, problemas o vulnerabilidades. Evaluar la probabilidad de que ocurra la amenaza y el efecto en el activo o en la organización si se realiza la amenaza (así se determina el riesgo.

Continuando se identifican controles que llevarían el efecto a un nivel aceptable.

2.2.11. CONTROL

Un “Control” es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable

Son “medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

Una clasificación generalizada de los controles puede ser:

• **Preventivos**: Reducen las vulnerabilidades.

• **Detectivos:** Descubren amenazas o escenarios previos a ellas permitiendo activar otros controles.

• **Correctivos:** Contrarrestan el impacto de la ocurrencia de una amenaza.

• **Disuasivos:** Reducen la probabilidad de ocurrencia de las amenazas.

2.2.12. METODOLOGÍA MAGERIT

MAGERIT es una metodología de análisis y gestión de riesgos de los Sistemas de Información elaborada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información, enfocada a las Administraciones Públicas. (Fuente: Wikipedia)

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

PRODUCTOS Y SERVICIOS COMPLEMENTARIOS

PILAR es una herramienta que implementa la metodología MAGERIT de análisis y gestión de riesgos, desarrollada por el Centro Criptológico Nacional (CCN) y de amplia utilización en la administración pública.

OBJETIVOS

MAGERIT persigue los siguientes objetivos:

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

Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos:

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

ORGANIZACIÓN DE LAS GUÍAS

MAGERIT versión 3 se ha estructurado en tres libros: “Método”, “Catálogo de Elementos” y “Guía de Técnicas”.

MÉTODO

El capítulo 2 presenta los conceptos informalmente. En particular se enmarcan las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.

El capítulo 3 concreta los pasos y formaliza las actividades de análisis de los riesgos.

El capítulo 4 describe opciones y criterios de tratamiento de los riesgos y formaliza las actividades de gestión de riesgos.

El capítulo 5 se centra en los proyectos de análisis de riesgos, proyectos en los que nos veremos inmersos para realizar el primer análisis de riesgos de un sistema y eventualmente cuando hay cambios sustanciales y hay que rehacer el modelo ampliamente.

El capítulo 6 formaliza las actividades de los planes de seguridad, a veces denominados planes directores o planes estratégicos.

El capítulo 7 se centra en el desarrollo de sistemas de información y cómo el análisis de riesgos sirve para gestionar la seguridad del producto final desde su concepción inicial hasta su puesta en producción, así como a la protección del propio proceso de desarrollo.

El capítulo 8 se anticipa a algunos problemas que aparecen recurrentemente cuando se realizan análisis de riesgos.

La metodología Magerit permite saber cuánto valor está en juego en las organizaciones y por ende ayuda a protegerlo. Asimismo, conocer el riesgo al que están sometidos los elementos de trabajo es, simplemente, imprescindible para poder gestionarlos. Con esta metodología, se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

2.2.13. CICLO DE MEJORA CONTINUA

La versión 2013 de la norma ISO 27001 no considera el ciclo PDCA (Plan- Do-Check-Act) como marco obligatorio para la gestión de la mejora continua del SGSI, pero en su apartado 10.2 la norma ISO 27001:2013 menciona que la organización debe mejorar continuamente la conveniencia, adecuación y efectividad del sistema de gestión de seguridad de la

información. Es decir, el ciclo PDCA está implícito en la propia estructura de la norma y es importante conocerla.

El modelo PDCA consta de un conjunto de fases, que permiten establecer un modelo comparable a lo largo del tiempo, de manera que se pueda medir el grado de mejora alcanzado:

- **Plan.** En esta fase se planifica la implantación de SGSI. Se determina el contexto de la organización, se definen los objetivos y las políticas que permitirán alcanzarlos.
- **Do.** En esta fase se implementa y pone en funcionamiento el SGSI. Se ponen en práctica las políticas y los controles que, de acuerdo al análisis de riesgos, se han seleccionado para cumplirlas. Para ello debe de disponerse de procedimientos en los que se identifique claramente quién debe hacer qué tareas, asegurando la capacitación necesaria para ello.
- **Check.** En esta fase se realiza la monitorización y revisión del SGSI. Se controla que los procesos se ejecutan de la manera prevista y que además permiten alcanzar los objetivos de la manera más eficiente.
- **Act.** En esta fase se mantiene y mejora el SGSI, definiendo y ejecutando las acciones correctivas necesarias para rectificar los fallos detectados en la anterior fase.

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS.

2.3.1. ACTIVO:

Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

2.3.2. AMENAZA:

Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

2.3.3. IMPACTO:

Consecuencia de la materialización de una amenaza.

2.3.4. RIESGO:

Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

2.3.5. VULNERABILIDAD:

Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo.

2.3.6. ATAQUE:

Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

2.3.7. DESASTRE O CONTINGENCIA:

Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la normal operación de un negocio.

2.3.8. ISO 27001

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa.

2.3.9. NTP-ISO/IEC 27001:2014

Norma técnica peruana de seguridad de la información ha sido preparada con el fin de ofrecer un modelo para establecer, implementar, operar, monitorear, mantener y mejorar un efectivo Sistema de Gestión de la Seguridad de la Información (ISMS)".

2.3.10. CONFIDENCIALIDAD

La confidencialidad se conoce como una forma de prevenir la divulgación de la información a personas o sistemas que no se encuentran autorizados.

2.3.11. INTEGRIDAD

Cuando hablamos de integridad en seguridad de la información nos referimos a cómo los datos se mantienen intactos libre de modificaciones o alteraciones por terceros, cuando una violación modifica algo en la base de datos, sea por accidente o intencionado se pierde la integridad y falla el proceso.

2.3.12. DISPONIBILIDAD

Es un pilar fundamental de la seguridad de la información, nada hacemos teniendo segura e integra nuestra información, si no va a estar disponible cuando el usuario o sistema necesite realizar una consulta.

2.3.13. GESTIÓN DE RIESGO

Es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen la identificación, el análisis y la evaluación de riesgo, para luego establecer las estrategias para su tratamiento

2.3.14. CONTROL

Un “Control” es lo que permite garantizar que cada aspecto, que se valoró con un cierto riesgo, queda cubierto y auditable

2.3.15. POLÍTICA DE SEGURIDAD:

Una “Política de Seguridad” bien planteada, diseñada, y desarrollada cubre la gran mayoría de los aspectos que hacen falta para un verdadero SGSI.

2.4. FORMULACIÓN DE HIPÓTESIS

Según Carlos Alberto Ramos Galarza, en la Revista UNIFE, plantea que no todas las investigaciones cuantitativas plantean hipótesis. El hecho de que formulamos o no hipótesis depende de un factor esencial: el alcance inicial del estudio. Las investigaciones cuantitativas que formulan hipótesis son aquellas cuyo planteamiento define que su alcance será correlacional o explicativo, o las que tienen un alcance descriptivo, pero que intentan pronosticar una cifra o un hecho.

La presente Tesis tiene un nivel de investigación descriptivo y no pronostica ningún hecho o dato por lo que no se formulará una

hipótesis

2.5. IDENTIFICACIÓN DE VARIABLES.

2.5.1. VARIABLE INDEPENDIENTE

X: Sistema de Gestión de Seguridad de la Información (SGSI) basado en la NTP-ISO/IEC 27001:2014

2.5.2. VARIABLE DEPENDIENTE

Y: Gestión de riesgos de los activos de información para la Dirección General de Informática y Estadística de la Universidad Nacional Daniel Alcides Carrión.

2.6. DEFINICIÓN OPERACIONAL DE VARIABLES E INDICADORES.

(Hernández R., 2003, pág. 143), Señala que variable “es una propiedad que puede variar y cuya variación es susceptible de medirse u observarse”, por tal razón las variables deben ser definidas de dos formas conceptual y operacionalmente.

Una definición conceptual trata la variable con otros términos, para lo cual se deben definir las variables que se utilizan y puedan ser comprobadas o contextualizadas.

Una definición operacional constituye el conjunto de procedimientos que describe las actividades que un observador debe realizar.

VARIABLES	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR
X: Sistema de Gestión de Seguridad de la Información (SGSI) basado en la NTP-ISO/IEC 27001:2014	Sirve para asegurar la confidencialidad, integridad y disponibilidad de los activos de información	Confidencialidad	Número de información divulgada
			Número de incidentes de seguridad reportados y atendidos
			Tiempo de respuesta para atender incidentes
		Disponibilidad	Porcentaje de tiempo durante el cual un sistema está disponible para el usuario
			Identificación de los activos críticos de la organización.
			Identificar los riesgos que me afectan a los procesos y activos críticos.
		Integridad	Número o porcentaje de accesos y/o cambios no autorizados a los datos de producción.
			Definición de controles en función de los riesgos detectados y las mejoras en los sistemas

Tabla 01. Variable independiente

VARIABLES	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADOR
Y: Gestión de riesgo de los activos de información en la DGIE- UNDAC.	Medidas preventivas tendientes a minimizar los riesgos vinculados con la seguridad de la información	**Alcance**	Cumple con la documentación para el SGSI
			Respuesta ante incidentes
		Análisis de riesgo	Valoración de activos
			Análisis de riesgos
			Gestión de riesgos
		Controles de seguridad	Definir políticas de seguridad
			Controles de seguridad

Tabla 02. Variable dependiente

CAPÍTULO III

METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN

La metodología adoptada en esta investigación tiene en cuenta el marco de referencia de la NTP ISO/IEC 27001:2014 que especifica, entre otros aspectos, los requerimientos y actividades que se deben desarrollar para diseñar, implementar, mantener y mejorar un sistema de gestión de seguridad de la información.

3.1. TIPO Y NIVEL DE INVESTIGACIÓN.

Por la forma como fue planteado el problema de investigación y sus objetivos, es considerada como una investigación aplicada, que implica el diseño del sistema de gestión de seguridad de la información por parte del investigador, sobre el proceso de gestión de riesgo en la DGIyE de la UNDAC, orientado a mejorar la integridad, disponibilidad

y confiabilidad de los activos de información, para lo cual se aplicará la NTP-ISO/IEC 27001:2014 y la metodología Magerit v3.0 para el análisis y gestión de riesgos.

El nivel de la presente investigación es descriptivo, porque busca identificar y describir las características fundamentales del diseño de un SGSI (teniendo como guía la NTP ISO/IEC 27001) para la Dirección General de Informática y Estadística de la UNDAC.

3.2. MÉTODOS DE INVESTIGACIÓN

Con la finalidad de abordar todos los factores que intervienen en el problema planteado, se empleó los métodos: inductivo, deductivo, análisis, síntesis y el estadístico.

3.3. DISEÑO DE INVESTIGACIÓN.

El diseño de investigación no experimental es aquel que se realiza sin manipular deliberadamente variables. Se basa fundamentalmente en la observación de fenómenos tal y como se dan en su contexto natural para después analizarlos.

la metodología utilizada fue del tipo de investigación no experimental transeccional descriptivo, porque se realizaron sin manipular deliberadamente variables, Transeccional descriptiva correlacional, por lo que se recolectaron datos en un solo momento, para lo cual se hizo una encuesta a 08 administrativos, así como Director General de la DGIyE de la UNDAC.

3.4. POBLACIÓN Y MUESTRA.

3.4.1. POBLACIÓN

En esta investigación, la población estuvo constituida por el personal de la Oficina General de Informática y Estadística de la Universidad Nacional Daniel Alcides Carrión.

3.4.2. MUESTRA

Se utilizó un muestreo de tipo no probabilístico, con juicio de experto y criterio de saturación, la cual estuvo conformado por los ocho trabajadores administrativos y el Director General de la DGIyE de la UNDAC.

3.5. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS.

Para medir las variables dependientes se utilizó la ficha de observación que se muestra en el Anexo A; y para las variables dependientes se utilizaron las encuestas, los reportes de incidencias, registros e informes, tanto del área usuaria como del analista de soporte.

3.6. TÉCNICAS DE PROCESAMIENTO Y ANÁLISIS DE DATOS

Luego del trabajo de campo y habiendo obtenido toda la información requerida se ha hecho el procesamiento de datos iniciando con la clasificación, registro, tabulación y codificación.

3.7. TRATAMIENTO ESTADÍSTICO

Para el tratamiento estadístico de los datos, se ha usado el programa Microsoft Excel, así como el SPSS versión 24, el mismo que fue considerado para la presentación de datos en tablas y gráficos

estadísticos, asimismo se usó las medidas de tendencia central y variabilidad respectivamente.

3.8. SELECCIÓN Y VALIDACIÓN DE LOS INSTRUMENTOS DE INVESTIGACIÓN

Para seleccionar los instrumentos de investigación se hizo la consulta a profesionales que conocen el tema de Seguridad de la Información como es el Sub Gerente de Racionalización y sistemas TIC del Gobierno Regional de Pasco, así como al Sub Gerente de Informática y Sistemas de la Municipalidad Provincial de Pasco. Consultados en base a la NTP ISO/IEC 27001:2014.

CAPÍTULO IV

RESULTADOS Y DISCUSIÓN

4.1. DESCRIPCIÓN DEL TRABAJO DE CAMPO.

Con el fin de alcanzar los objetivos propuestos en la tesis de investigación, para la realización del trabajo de campo se realizó el Diseño del Sistema de Gestión de Seguridad de la Información en base a la NTP ISO/IEC 27001:2014. Este sistema se basa en las directrices indicadas en la norma y en el marco del mismo se generó un análisis de evaluación de riesgos, que permitió evidenciar un nivel de brechas significativo en la DGIyE de la UNDAC, con base en el cual se establecieron políticas y controles de mejoramiento de los procesos de seguridad de la información y se definieron las declaraciones de aplicabilidad que fortalecieron todo el análisis de riesgos efectuado.

La NTP ISO/IEC 27001:2014 contempla la siguiente estructura:

1. Objeto y Campo de Aplicación
2. Referencias Normativas
3. Términos y Definiciones
4. Contexto de la Organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del desempeño
10. Mejoras

4.2 PRESENTACIÓN, ANÁLISIS E INTERPRETACIÓN DE RESULTADOS.

Se presenta los resultados de la aplicación del cuestionario dirigido al personal técnico, así como también al Director General de la Dirección General de Informática y Estadística de la UNDAC.

1. ¿Conoce las políticas de Seguridad de Información que se aplican en su área de labores?

	Antes		Después	
	f	%	f	%
Si.	1	10.0	9	90.0
No	9	90.0	1	10.0
Total	10	100.0	10	100.0

Tabla N° 5 Comparación Antes – Después acerca del conocimiento de las políticas de seguridad de información.

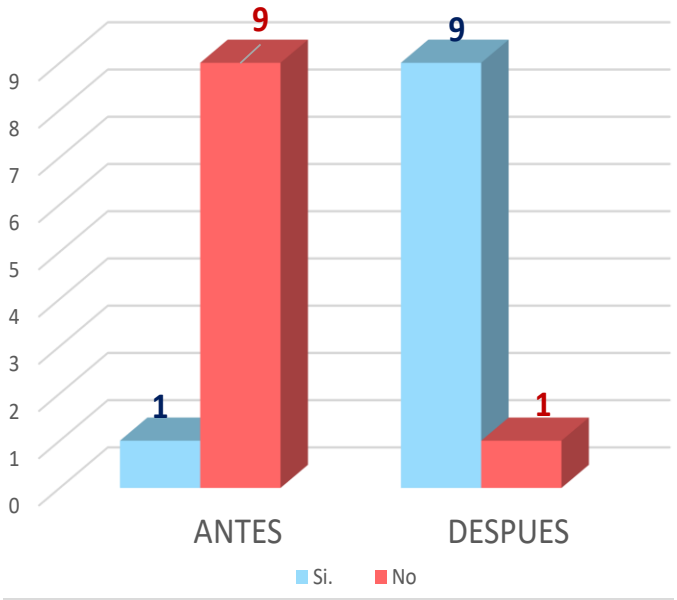


Gráfico nro. 1: conocimiento de las políticas de seguridad de información.

Interpretación: Podemos observar que la mayoría de los encuestados antes de la intervención desconocían las políticas de seguridad de la información, revertiéndose luego de la intervención.

2. ¿La DGIyE pública y comunica a todos los administrativos y partes externas un documento de política de seguridad de la información?

	Antes		Después	
	f	%	f	%
Si.	0	10.0	10	90.0
No	10	90.0	0	10.0
Total	10	100.0	10	100.0

Tabla N° 6 Comparación Antes – Después acerca que pública y comunica a todos los políticos de seguridad de información.

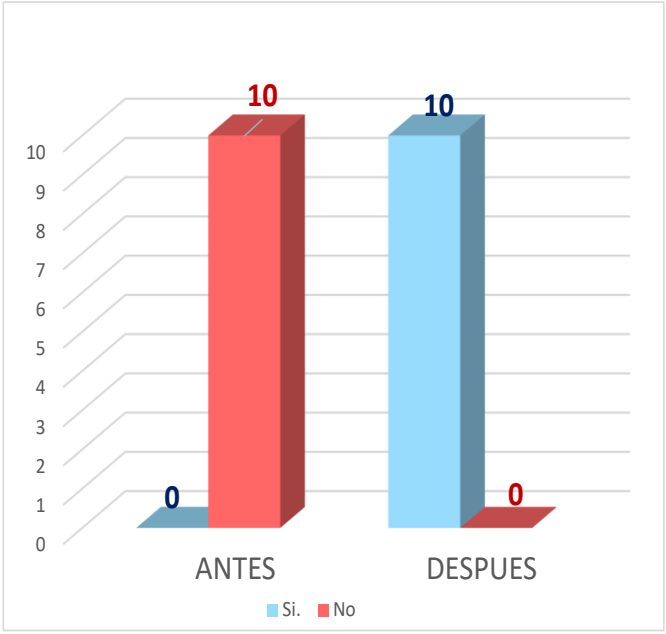


Gráfico Nro. 2: Pública y comunica las políticas de seguridad de información.

Interpretación: Podemos observar que nunca se comunicó de las políticas de seguridad de la información a los administrativos y partes externas, revertiéndose luego de la intervención.

3. ¿Los administrativos en su oficina suelen dejar documentos con información institucional que podría ser confidencial encima de su escritorio o en otro lugar de exposición para los demás?

	Antes		Después	
	f	%	f	%
Todo el tiempo	7	70.0	1	10.0
Usualmente	2	20.0	2	20.0
Pocas veces	1	10.0	4	40.0
No es Común	0	0.0	3	30.0
Total	**10**	**100**	**10**	**100**

Tabla Nro. 7 Comparación Antes – Después acerca de los administrativos suelen dejar documentos de carácter confidencial.

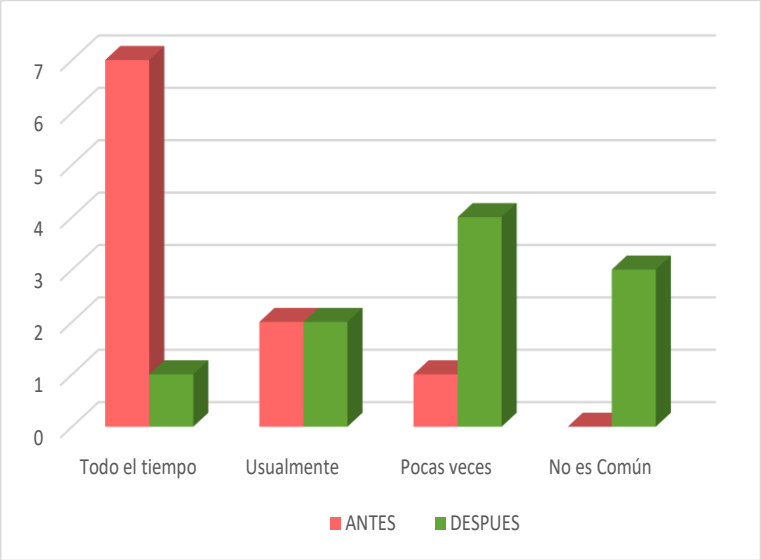


Gráfico 3: los administrativos suelen dejar documentos de carácter confidencial.

Interpretación: Podemos observar que en su mayoría opinan que los administrativos desconocen el valor de los documentos que poseen y no lo mantienen seguros, revertiéndose luego de la intervención.

4. ¿Qué sucede con los documentos de su oficina que ya no son de utilidad?

	Antes		Después	
	f	%	f	%
Se trituran	1	10.0	8	80.0
Se botan al tacho	2	20.0	0	0.0
Se almacenan en la oficina	6	60.0	2	20.0
Desconozco	1	10.0	0	0.0
Total	**10**	**100**	**10**	**100**

Tabla Nro. 8: Comparación **Antes – Después** acerca de documentos que ya no son de utilidad.

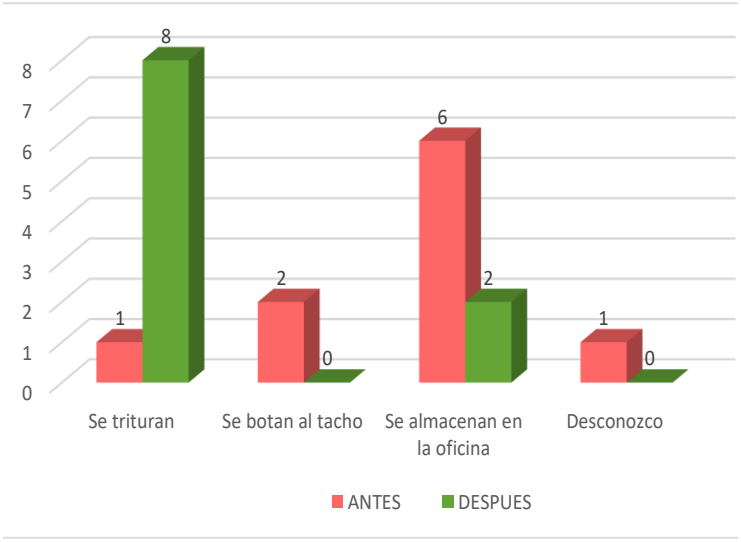


Gráfico Nro. 4: documentos que ya no son de utilidad.

Interpretación: Podemos observar que los documentos que no son de utilidad no son destruidos y son almacenados en la oficina, revertiéndose luego de la intervención

5. ¿Cuándo sale de su oficina, bloquea su computadora?

	Antes		Después	
	f	%	f	%
Siempre	2	20.0	10	100.0
A veces	6	60.0	0	0.0
Nunca	2	20.0	0	0.0
Total	**10**	**100**	**10**	**100**

Tabla Nro. 9: Comparación **Antes – Después** acerca si se bloquea el computador al salir.

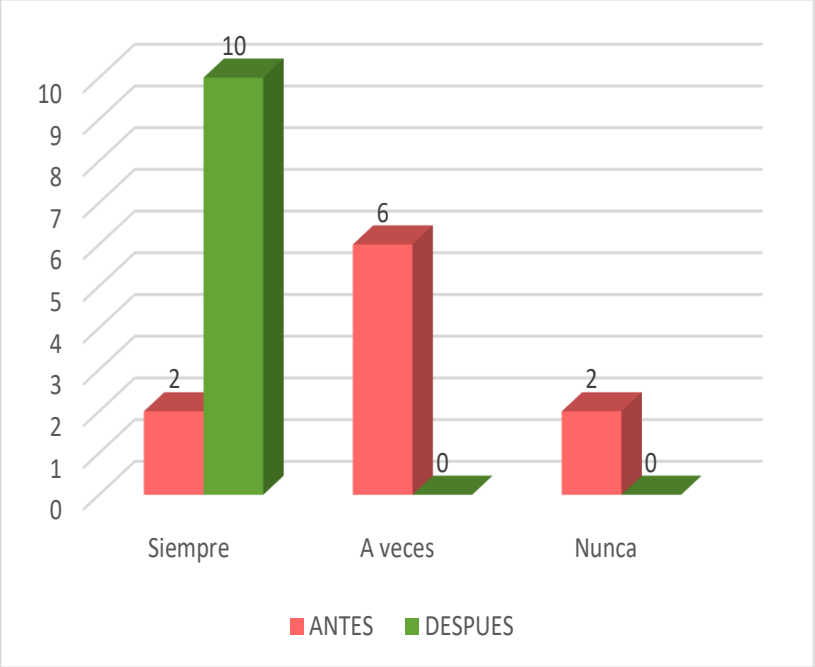


Gráfico Nro. 5: los administrativos bloquean el computador al salir.

Interpretación: Podemos observar que en su mayoría opinan que a veces bloquean su computadora cuando salen a almorzar o realizar algún trámite, revertiéndose luego de la intervención.

6. ¿Los accesos a su centro de labores son a personal autorizado?

	Antes		Después	
	f	%	f	%
Si.	1	10.0	10	100.0
No	9	90	0	0
Total	10	100.0	10	100.0

Tabla Nro. 10: Comparación **Antes – Después** acerca del acceso a su centro de labores son a personal autorizado.

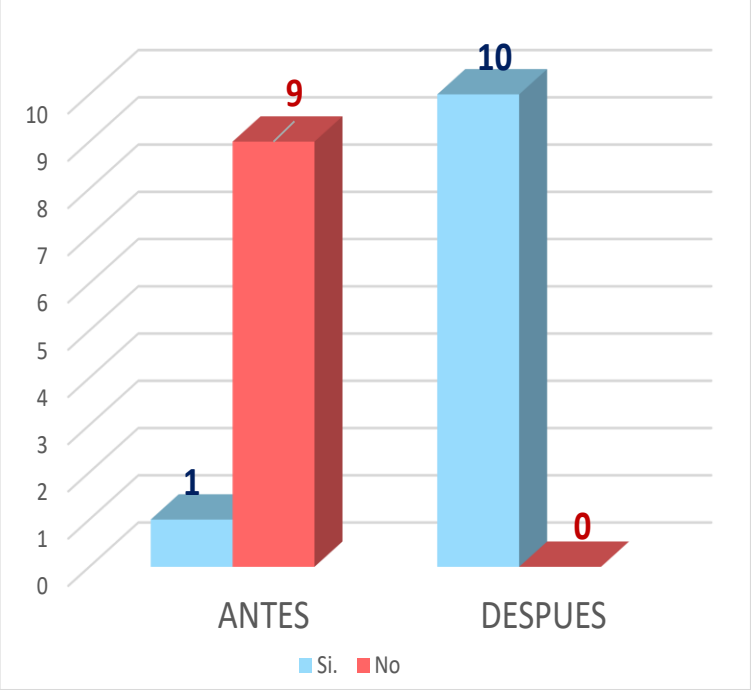


Gráfico Nro. 6: acceso a su centro de labores son a personal autorizado.

Interpretación: Los administrativos manifiestan que existen los avisos, pero esto no se cumple por no tener las condiciones necesarias.

7. ¿En la Undac existe un procedimiento para la realización de copia de seguridad?

	Antes		Después	
	f	%	f	%
Si.	3	30.0	10	100.0
No	7	70	0	0
Total	10	100.0	10	100.0

Tabla Nro. 11 Comparación **Antes – Después** acerca de procedimiento para la realización de copia de seguridad

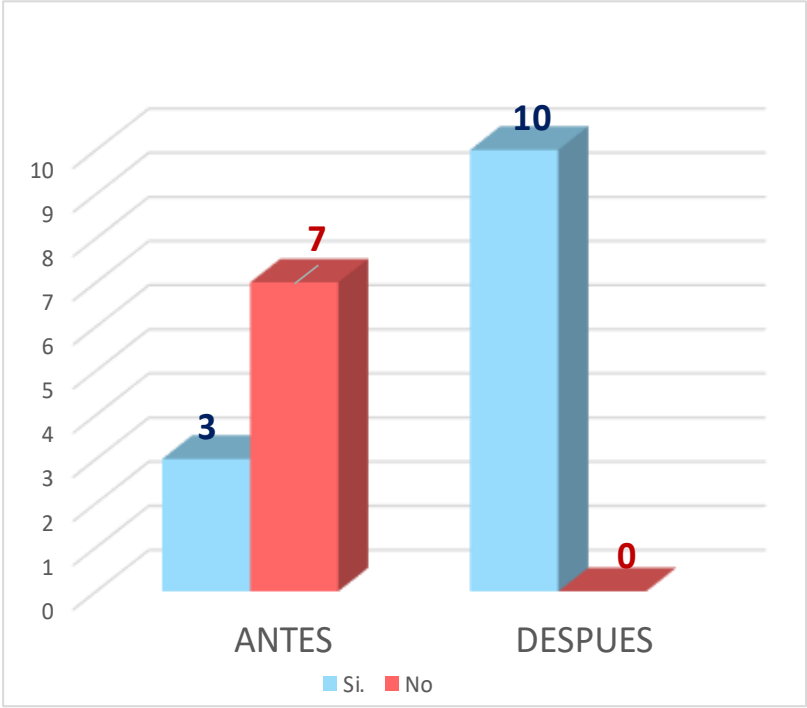


Gráfico Nro. 7: procedimiento para la realización de copia de seguridad

Interpretación: Podemos observar que en su mayoría opinan que no existen un procedimiento, pero 3 personas afirman que si, en su defecto falta hacer conocer dicho procedimiento a los demás.

8. ¿La Undac cuentan con políticas de contraseña segura? (más de 8 caracteres, contraseña alfanumérica, login diferente al password, etc.)

	Antes		Después	
	f	%	f	%
Si.	1	10.0	10	100.0
No	9	90	0	0
Total	10	100.0	10	100.0

Tabla Nro. 12: Comparación **Antes – Después** acerca de políticas de contraseña segura.

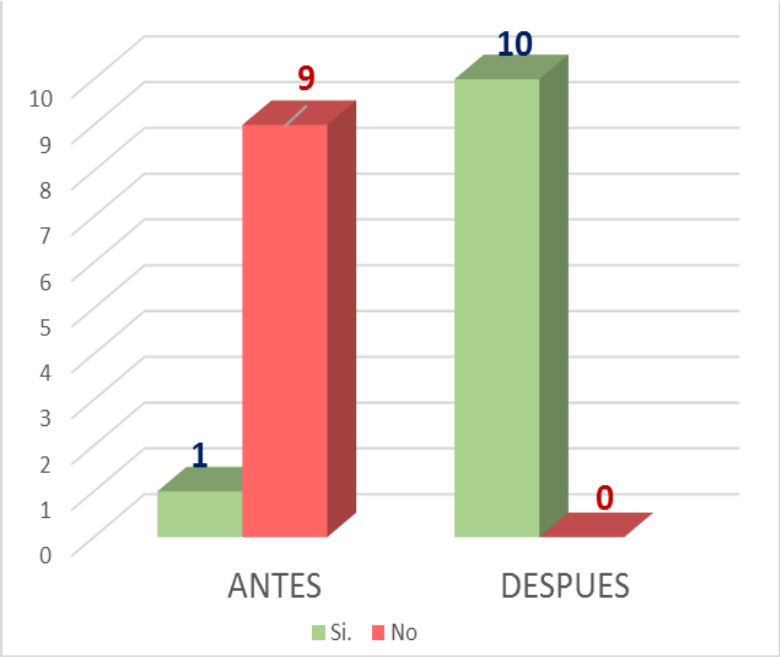


Gráfico Nro. 8: Políticas de contraseña segura

Interpretación: Podemos observar que en su mayoría no utilizan contraseñas seguras, y que una contraseña lo utilizan para vatios procesos.

9. ¿Se lleva un histórico detallado de los incidentes que se han tenido sobre la seguridad de la información?

	Antes		Después	
	f	%	f	%
Si.	2	20.0	10	100.0
No	8	80	0	0
Total	10	100.0	10	100.0

Tabla Nro. 13 Comparación **Antes – Después** acerca de histórico detallado de los incidentes.

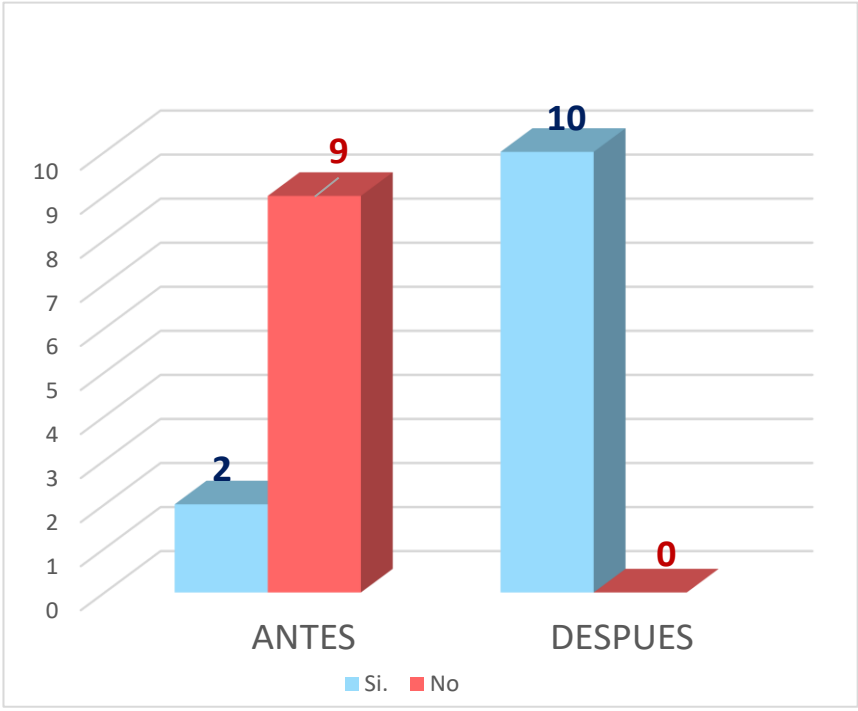


Gráfico Nro. 9: histórico detallado de los incidentes.

Interpretación: Podemos observar que los administrativos no son conscientes de la divulgación de la información, ya que no se cuenta con histórico de incidentes que se presentan, ni cómo afrontarlos.

10. ¿Existe en la Undac una metodología para la evaluación y gestión del riesgo?

	Antes		Después	
	f	%	f	%
Si.	1	10.0	10	100.0
No	9	90	0	0
Total	10	100.0	10	100.0

Tabla Nro. 14 Comparación **Antes – Después** acerca de metodología para la evaluación y gestión del riesgo.

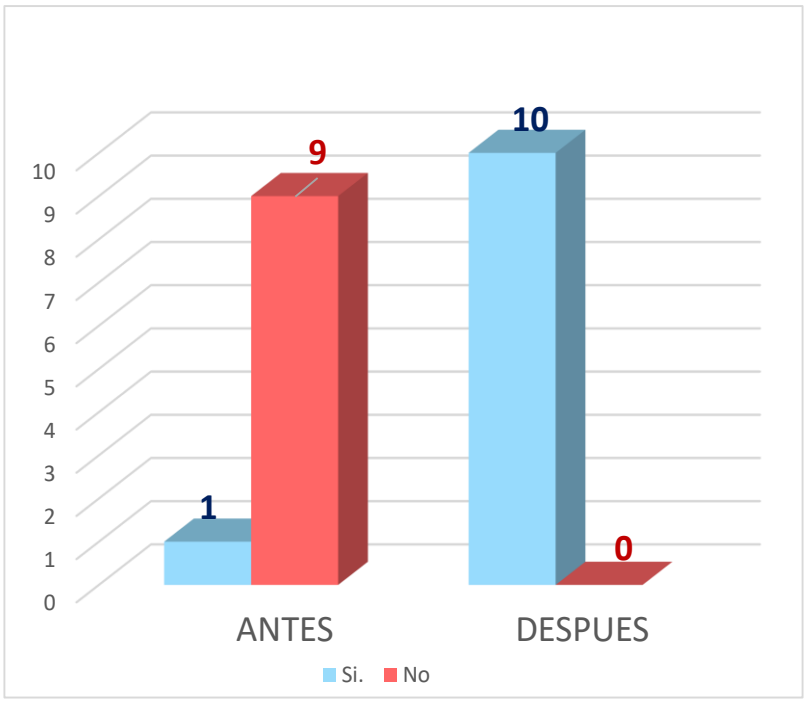


Gráfico Nro. 10: Metodología para la evaluación y gestión del riesgo.

Interpretación: En la UNDAC, no se cuenta con una metodología para la evaluación y gestión del riesgo, tampoco con un plan de contingencia para los casos que se pueda presentar.

11. ¿Todo lo relacionado con la seguridad de la información se encuentra documentado?

	Antes		Después	
	f	%	f	%
Si.	2	20.0	8	80.0
No	8	80	2	20
Total	10	100.0	10	100.0

Tabla Nro. 15 Comparación **Antes – Después** acerca de documentos de seguridad de la información.

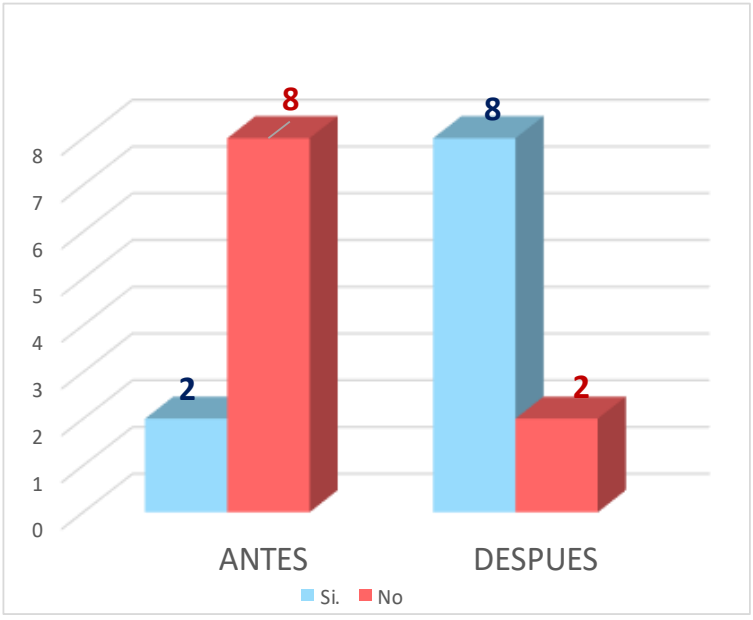


Gráfico Nro. 11: documentos de seguridad de la información.

Interpretación: Podemos observar que en su mayoría opinan que no se cuenta con estos documentos.

12. ¿Realiza copias de seguridad de su labor diaria?

	Antes		Después	
	f	%	f	%
Si.	5	50.0	10	100.0
No	5	50	0	0
Total	10	100.0	10	100.0

Tabla Nro. 16 Comparación **Antes – Después** acerca de copias de seguridad de su labor diaria

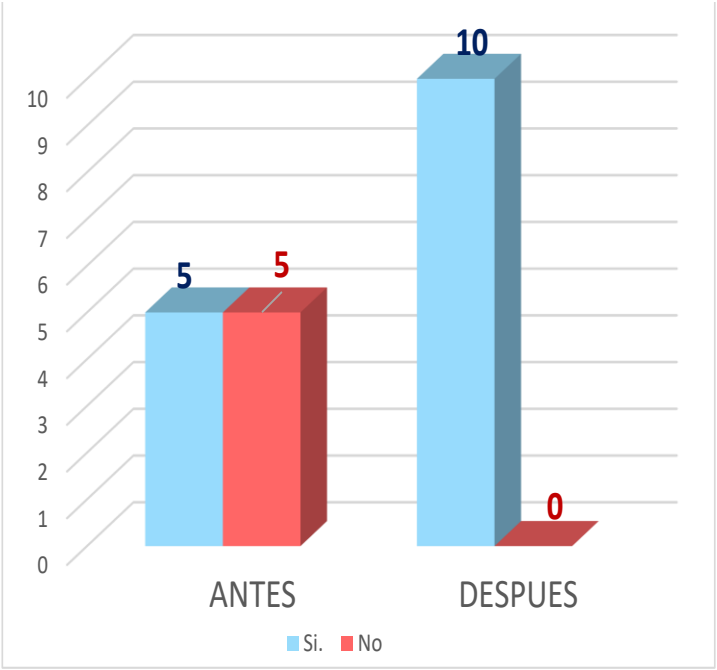


Gráfico Nro. 12: copias de seguridad de su labor diaria

Interpretación: Podemos observar que la mitad del personal administrativo de la UNDAC, realiza copias de seguridad de su trabajo, revirtiéndose después de la intervención.

4.3 PRUEBA DE HIPÓTESIS

Según Carlos Alberto Ramos Galarza, en la Revista UNIFE, plantea que no todas las investigaciones cuantitativas plantean hipótesis. El hecho de que formulamos o no hipótesis depende de un factor esencial: el alcance inicial del estudio. Las investigaciones cuantitativas que formulan hipótesis son aquellas cuyo planteamiento define que su alcance será correlacional o explicativo, o las que tienen un alcance descriptivo, pero que intentan pronosticar una cifra o un hecho.

La presente Tesis tiene un nivel de investigación descriptivo y no pronostica ningún hecho o dato por lo que no se formuló ninguna hipótesis.

4.4 DISCUSIÓN DE RESULTADOS

En esta sección de la investigación de la Tesis se da a conocer la discusión, interpretación, y explicación del resultado de la aplicación del Sistema de Gestión de Seguridad de la información en la DGIyE de la UNDAC.

El conocimiento sobre las políticas de seguridad en la Universidad era mínimo antes de la aplicación, un 9.1% de la población solo tenía referencia de algunas normas laborales en cuanto al uso de los activos de la DGIyE de la UNDAC , específicamente a las tecnologías de la información y comunicación, estas normas solo han sido mencionadas por los jefes de área o el Director, pero mas no habían sido plasmadas en un documento; ya posteriormente a la aplicación del SGSI se obtuvo que un 90,0% de la población ya tenía de conocimiento la

existencia de una política de seguridad y que en si era un documento al cual se podía consultar ya que se realizaron reuniones de capacitación para dar a conocer todas las normas inmersas en la política de seguridad.

También con la aplicación del SGSI se puedo lograr que el 70 % de los trabajadores hagan las copias de seguridad constantemente de la información que manejaban, se logró así que del total que 21 trabajadores hacían copias de seguridad.

El mayor temor de las entidades es la perdida de información sensible por parte de sus propios trabajadores, es así que antes de la solución del problema los administrativos extraviaban sus dispositivos de almacenamiento extraíbles, como consecuencia información sensible llegaba a manos desconocidas, es por eso que el 90% de los administrativos no aplicaban técnicas de cifrados para sus dispositivos, creando una vulnerabilidad de perdida de información, por lo tanto una vez aplicado la solución, el SGSI, solo decremento a un 50% la cantidad total de trabajadores que no aplicaban dicho mecanismo, es así que solo se pudo capacitar a 10 trabajadores para que puedan realizar el proceso de encriptado del dispositivo esto se entiende que 10 de ellos solo manejan información sensible de su área correspondiente.

En relación a los controles de acceso para poder acceder al computador, solo el 30% de los administrativos configuraron en sus máquinas el ingreso al sistema con usuario y contraseña, esto es que antes la inexistencia de la política de seguridad solo ese porcentaje lo

hacía por conocimiento, el resto simplemente por desinformación, ya después de haber realizado la implementación de la política de seguridad y las correspondientes capacitaciones, el 60,6% ya contaba con sus equipos seguros al momento de accederlos mediante el uso del control de acceso usando un nombre de usuario y contraseña.

También se logró que los trabajadores administrativos tomen conciencia de que tan importante es dejar bloqueado el equipo antes de salir o irse a almorzar o hacer alguna diligencia, de los cuales se logró que el 90% de ellos realizaba el bloqueo de sus equipos al retirarse, mientras que antes del diseño del sistema de gestión de seguridad de la información solo el 5 % lo hacía.

Un aspecto muy importante también fue el de haber concientizado a los trabajadores administrativos, que cada mes deberían cambiar sus contraseñas de los servicios en red utilizados, es así que los resultados nos muestran un 90% de los trabajadores administrativos lo hacían mensualmente. Así mismo esto influyo también a que los trabajadores utilicen diferentes contraseñas para diferentes servicios y no solo una contraseña general para todos los servicios, y los resultados reflejan que solo el 20% de los encuestados tomo conciencia y usaba contraseñas diferentes para cada servicio.

Las políticas de seguridad y a la aplicación de los controles de la NTP ISO/IEC 27001 2014, también ayudo a incrementar la productividad de los trabajadores por medio de la restricción de sitio web de ocio en los cuales la mayoría entretenía su tiempo laboral dejando de lados sus

actividades diarias, es así que en la encuesta se obtuvo que el 50% de los trabajadores administrativos, tenían restricción al momento de acceder a páginas distractoras como redes sociales y juegos en línea.

El acceso a los recursos conectados en red después de la implementación del SGSI, se logró que el 70% de la comunidad universitaria, accedan a la red mediante el ingreso de un nombre de usuario y contraseña, anteriormente a esto no se contaba con dicha protección.

DESARROLLO DEL PROYECTO DE INVESTIGACIÓN SGSI-UNDAC

OFICINA GENERAL DE INFORMÁTICA Y ESTADISTICA

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

DISEÑO DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA APLICACIÓN DE LA NTP-ISO/IEC 27001:2014

Código del Documento	SGSIUNDAC01
Versión	1.0
Fecha de Versión	10/07/2018
Propietario	DGIyE-UNDAC
Nivel de Confidencialidad	Alto

1. DIAGNOSTICO

En este capítulo se presentan los diagnósticos que se realizaron con el objetivo de poder tener un conocimiento inicial de la situación que presenta la DGIyE de la UNDAC frente al establecimiento de un Sistema de Gestión de Seguridad de la Información basado en la NTP-ISO/IEC 27001:2014.

1.1 Evaluación del estado inicial de la DGIyE de la UNDAC con respecto a los requisitos de la NTP-ISO/IEC 27001:2014

Para evaluar el estado inicial de la DGIyE de la UNDAC, con respecto a los requisitos de la NTP –ISO/IEC 27001:2014, se ha definido dos maneras de presentar los resultados: una descriptiva y otra cuantificable. Esta técnica se basa en calificar el estado de los requerimientos en función a una escala de Likert aplicando cinco opciones que van de menor a mayor.

CRITERIO DE CALIFICACIÓN	
No diseñado: Las actividades/métodos demuestran que no se tiene el requisito y/o no se ha bosquejado su implementación.	0%
Parcialmente diseñado: Las actividades/métodos demuestran que se tiene el requisito definido, pero este no es del todo conforme con el requisito de la NTP ISO/IEC 27001:2014.	25%
Diseñado: Los métodos son conformes con el requisito de la NTP ISO/IEC 27001:2014, pero sin evidencias de aplicación.	50%
Parcialmente implementado: Las actividades/métodos son conformes con el requisito de la NTP ISO/IEC 27001:2014, pero con pocas evidencias de aplicación.	75%
Completamente implementado: Las actividades / métodos son conformes con el requisito de la NTP ISO/IEC 27001:2014, y se cuenta con evidencias de aplicación permanentes.	100%

Tabla 17 Criterio para evaluar el estado inicial de la DGIyE de la UNDAC con respecto a los requisitos de la NTP ISO/IEC 27001:2014

Se elaboró la línea base con los capítulos y requerimientos de la norma y se realizó la evaluación de la siguiente manera:

- Se calificó cada requisito.
- De acuerdo al puntaje obtenido se colocó la evidencia/sugerencia para el cumplimiento de la NTP ISO/IEC 27001:2014.
- Para el porcentaje por capítulo, se sacó el promedio de los requisitos por capítulo.

El resultado que se obtuvo de la evaluación del estado inicial de la DGIyE de la UNDAC, respecto a los requisitos de la NTP ISO/IEC 27001:2014 se muestra en forma de tabla.

SECCIÓN	REQUERIMIENTO DE LA NTP ISO/IEC 27001:2014	ESTADO	EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE? /¿QUÉ SE TENDRÍA QUE HACER?	VALORACIÓN
4	**CONTEXTO DE LA ORGANIZACIÓN**	No Diseñado	Se sugiere realizar el análisis del contexto de la DGIyE de la UNDAC, para comprender, tanto los aspectos externos como internos, las partes interesadas y requisitos relevantes al SGSI y, elaborara y documentar el alcance del SGSI.	**6%**
4.1	**Comprender la Organización y contexto**. La organización **debe** determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este SGSI	Parcial mente diseñado	La **DGIyE de la UNDAC** posee documentos visibles de su Misión, Visión, Matriz FODA y las Estrategias. Pero no contempla de manera clara ítems de seguridad de la información. Se sugiere establecer objetivos de seguridad de la Información que estén alineados con los objetivos estratégicos.	25%
4.2	**Comprender las necesidades y expectativas de las partes interesadas.** La organización **debe** determinar las partes interesadas y los requisitos de las mismas.	No Diseñado	**Sugerencia:** Determinar las partes interesadas y comprender las necesidades y expectativas de éstas, referentes a la seguridad de la información.	0%

4.3	**Determinar el alcance del SGSI.**	No Diseñado	Sugerencia. Determinar el alcance del SGSI teniendo en consideración los aspectos referidos en 4.1, los requisitos de 4.2, documentarlo y ponerlo a disposición de las partes interesadas.	0%
4.4	**Sistema de Gestión de Seguridad de la información.** La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de esta Norma Técnica Peruana	No diseñado	Sugerencia. Establecer un plan para la mejora continua del SGSI conforme a la NTP Vigente	0%
5	**LIDERAZGO**	No Diseñado	El Titular de la Entidad, debe mostrar liderazgo y compromiso respecto al SGSI. Entonces, debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas. Por lo tanto, es necesario establecer: Una Política de Seguridad de la Información, y los Objetivos de Seguridad de la Información acorde al propósito de la organización.	3%
5.1	**Liderazgo y compromiso.** La alta dirección debe demostrar liderazgo y compromiso respecto al SGSI.	No Diseñado	El titular de la entidad debe mostrar liderazgo y compromiso	3%
5.2	**Política.**	No Diseñado	Establecer la Política de Seguridad de la Información acorde al propósito de la **DGIyE de la UNDAC**, incluir los objetivos de seguridad de la Información, mantenerla disponible y comunicada a toda la organización.	0%
5.3	**Roles, responsabilidades y autoridades organizacionales.**	No Diseñado	La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas.	0%
PUNTAJE TOTAL DE LA EVALUACIÒN DE REQUISITOS DE LA NTP ISO/IEC 27001:2014				**5%**

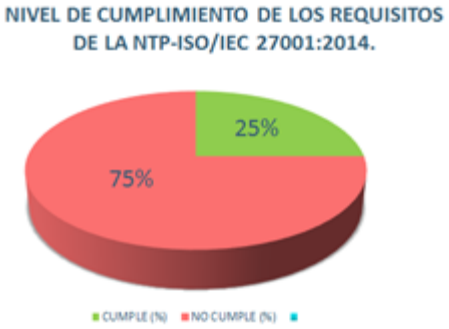


Gráfico 13 Nivel de cumplimiento de la NTP-ISO/IEC 27001:2014

Mediante este Análisis Diferencial es posible determinar que la DGIyE de la UNDAC comprende la importancia y beneficios de un SGSI y posee el liderazgo necesario para realizarlo; sin embargo, aún no se ha establecido formalmente una metodología de análisis y evaluación de riesgos informáticos y su tratamiento, así como tampoco ningún documento requerido por la NTP-ISO/IEC 27001:2014.

Resultado de la evaluación del estado inicial de la DGIyE de la UNDAC, con respecto a los requisitos de la NTP-ISO/IEC 27001:2014

Según la evaluación realizada, de un total de 100% de los requisitos de la NTP ISO/IEC 27001:2014 que se deben cumplir, la DGIyE de la UNDAC obtuvo un puntaje total de 5%, por lo que se puede determinar que la DGIyE de la UNDAC se encuentra en una etapa básica de cumplimiento de la norma (no diseñado).

El resultado anterior muestra también que la seguridad de la Información dentro de la institución no es gestionada y, que el diseño e implementación del SGSI implicará un mayor esfuerzo, y dependerá del compromiso y disponibilidad del personal de la DGIyE de la UNDAC.

Posibilidad de aceptación del SGSI y diagnóstico inicial de la seguridad de la información.

La recolección de datos se realizó mediante la encuesta que consistió en doce (12) preguntas dicotómicas para medir actitudes, opiniones y el estado básico de seguridad de información dentro de la DGIyE de la

UNDAC Esto con el fin de corroborar el estado de la seguridad de la información y la posibilidad de aceptación del diseño del SGSI.

4. CONTEXTO DE LA ORGANIZACIÓN

OFICINA GENERAL DE INFORMÁTICA Y ESTADISTICA
UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

Código del Documento	SGSIUNDAC01
Versión	1.0
Fecha de Versión	10/07/2018
Propietario	DGIyE-UNDAC
Nivel de Confidencialidad	Alto

4.1 COMPRENDER LA ORGANIZACIÓN Y SU CONTEXTO

La NTP ISO/IEC 27001:2014 menciona en el capítulo 4: Contexto de la organización, la importancia de comprender la organización y su contexto, esto es, comprender los aspectos internos y externos que son relevantes para el establecimiento del SGSI, asimismo comprender también las necesidades y expectativas de las partes interesadas y determinar el alcance de SGSI.

4.1.1 CONTEXTO EXTERNO

Por un lado, tenemos influencias como el Gobierno, las empresas públicas y privadas, la sociedad, los docentes, estudiantes, administrativos, etc. y, por otro lado, están el ingreso de las universidades nacionales y privadas al mercado regional ofreciendo programas de pregrado y postgrado en forma tradicional y a distancia; la universidad tienen que afrontar la competitividad con una formación de profesionales que puedan responder a las exigencias actuales; en otras palabras tenemos que avanzar de una visión regional a una nacional e internacional.

Para el logro de estos propósitos está la estrategia humana orientada a ser generadora de valores a través de sus

diferentes procesos como la selección, capacitación y desarrollo, compensación, gestión del desempeño, diseño de cargos, reclutamiento, entre otros; asimismo, las perspectivas de aprender algo nuevo, junto a la psicología de la capacitación para el éxito, nos permitirán romper las barreras psicológicas de carácter decisivo para todas las formas de cambio.

En este ítem se analizó los factores externos que afectan a la DGIyE de la UNDAC en el establecimiento e implementación del SGSI. Para ello se utilizó la herramienta de análisis PEST (factores Políticos - Legales, Económicos, Socio-culturales y Tecnológicos.

El resultado del análisis es la siguiente:

POLÍTICO - LEGAL	• Interés del estado por la seguridad de la información en todas las entidades públicas (la PCM a través de la ONGEI, auditorías realizadas por la Contraloría) • Evolución del e-Gobierno • Marco regulatorio sobre seguridad de la información. • Estandarización de procesos y sistemas de Gestión • Apoyo de la ONGEI para el establecimiento del SGSI
ECONÓMICO	• Poco presupuesto por parte del estado • Alto costo de consultores para establecer un SGSI
SOCIO-CULTURAL	La comprensión del contexto externo es importante para asegurarse que los objetivos e inquietudes de las partes externas se tienen en cuenta cuando se desarrollan los criterios de riesgos.
TECNOLÓGICO	• Aparición de nuevas tecnologías de información y que están siendo adaptados por el estado. • Nuevas necesidades de implementación tecnológica • Tendido de fibra óptica para mejorar la velocidad de acceso a la información • Vulnerabilidades y amenazas en la seguridad información

La comprensión del contexto externo es importante para asegurarse que los objetivos e inquietudes de las partes externas se tienen en cuenta cuando se desarrollan los criterios de riesgos.

4.1.2 CONTEXTO INTERNO

Como factores internos podemos citar, entre otros, las deficiencias académicas, falta de docentes idóneos, deserción estudiantil, falta de diálogo y tolerancia, y resistencia al cambio, entre otros.

La enseñanza universitaria en el pregrado ha tomado un sentido estrictamente profesionalizante, en la que los conocimientos prácticos desplazan a la esencial formación teórica que posibilita la investigación.

La estructura curricular privilegia los cursos obligatorios, disminuyendo el número de cursos electivos, lo que no permite a los estudiantes orientar sus preferencias profesionales y alcances en niveles de especialización aceptables.

Los planes de estudios refuerzan una tendencia a la atomización de las disciplinas profesionales, bloqueando las posibilidades de desarrollo académico que abren los estudios interdisciplinarios, modalidad en la cual se efectúan hoy en día los mayores progresos científicos.

En la curricula de las carreras universitarias no se presta mayor atención a nuestra condición de sociedad multicultural, ni a la biodiversidad que nos caracteriza, aspectos que constituyen nuestra ventaja competitiva.

El SGSI debe alinearse con la cultura, los procesos, la estructura y la estrategia de la organización.

4.1.2.1 Naturaleza de la entidad

La Universidad Nacional Daniel Alcides Carrión, abreviatura UNDAC, es la universidad pública peruana de Cerro de Pasco. Fue fundada en 1965 a iniciativa del Estado de la República del Perú. Fue reconocida como la mejor

universidad pública del centro del Perú en el año 2007 y recibió el premio Pioneros de la Minería en el 2009.

Orígenes

Inicialmente fue creada como Universidad Comunal de Pasco en 1961 y fue filial de la Universidad Comunal del Centro. El 12 de abril de 1965, tras una marcha de Cerro de Pasco a Lima que duro siete días y una presentación en el Congreso, se expidió la Ley Nª 15527, que creó la Universidad Nacional Daniel Alcides Carrión. Está ubicada en la Ciudad de Cerro de Pasco, Perú.

Estudios

La UNDAC está organizada en 11 facultades que ofrecen 33 carreras profesionales de pregrado, también cuenta con la escuela de posgrado con programas de Doctorados, Maestrías, Segundas Especializaciones y Diplomados. La ciudad universitaria se ubica en San Juan, Cerro de Pasco. Aparte tiene filiales en (Oxapampa, Paucartambo, Yanahuanca y Puerto Bermudez).

Misión

Formar profesionales competitivos, audaces, creativos, innovadores, con capacidad científica, tecnológica, humanística y multilingüe; integrando universidad- empresa – sociedad, con valores éticos para el mejoramiento de la calidad de vida en la Región Pasco, el País y el Mundo.

Visión

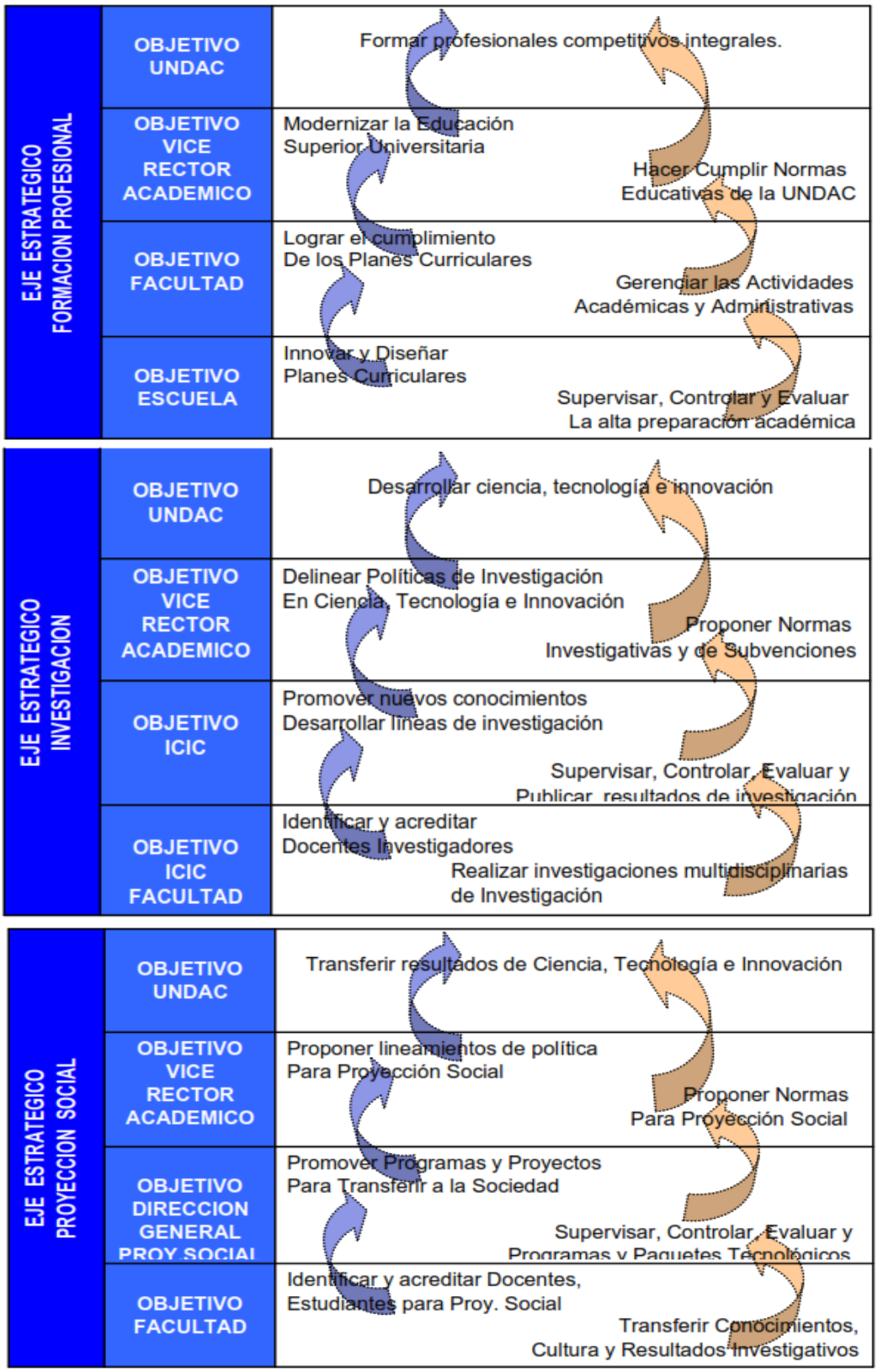
Ser universidad líder en la formación profesional, con alto nivel de responsabilidad social, que permita el desarrollo

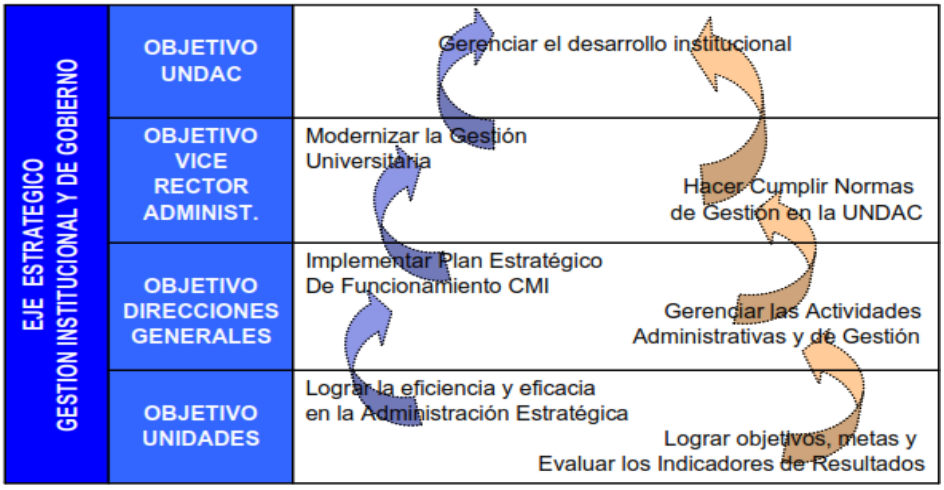
sustentable y el mejoramiento de la calidad de vida en la Región Pasco y el País.

Finalidad

La Universidad Nacional Daniel Alcides Carrión tiene los siguientes fines:

a) Preservar, acrecentar y transmitir de modo permanente la herencia científica, tecnológica, cultural y artística de la humanidad.
b) Formar profesionales de alta calidad de manera integral y con pleno sentido de responsabilidad social de acuerdo a las necesidades del país.
c) Proyectar a la comunidad sus acciones y servicios para promover el cambio y desarrollo.
d) Colaborar de modo eficaz en la afirmación de la democracia, el estado de derecho y la inclusión social.
e) Realizar y promover la investigación científica, tecnológica y humanística, la creación intelectual y artística.
f) Difundir el conocimiento universal en beneficio de la humanidad.
g) Afirmar y transmitir las diversas identidades culturales del país.
h) Promover el desarrollo humano y sostenible en el ámbito local, regional, nacional y mundial.
i) Formar personas libres en una sociedad libre.


EJE ESTRATEGICO FORMACION PROFESIONAL
OBJETIVO UNDAC
Formar profesionales competitivos integrales.
OBJETIVO VICE RECTOR ACADEMICO
Modernizar la Educación Superior Universitaria
Hacer Cumplir Normas Educativas de la UNDAC
OBJETIVO FACULTAD
Lograr el cumplimiento De los Planes Curriculares
Gerenciar las Actividades Académicas y Administrativas
OBJETIVO ESCUELA
Innovar y Diseñar Planes Curriculares
Supervisar, Controlar y Evaluar La alta preparación académica
EJE ESTRATEGICO INVESTIGACION
OBJETIVO UNDAC
Desarrollar ciencia, tecnología e innovación
OBJETIVO VICE RECTOR ACADEMICO
Delinear Políticas de Investigación En Ciencia, Tecnología e Innovación
Proponer Normas Investigativas y de Subvenciones
OBJETIVO ICIC
Promover nuevos conocimientos Desarrollar líneas de investigación
Supervisar, Controlar, Evaluar y Publicar resultados de investigación
OBJETIVO ICIC FACULTAD
Identificar y acreditar Docentes Investigadores
Realizar investigaciones multidisciplinarias de Investigación
EJE ESTRATEGICO PROYECCION SOCIAL
OBJETIVO UNDAC
Transferir resultados de Ciencia, Tecnología e Innovación
OBJETIVO VICE RECTOR ACADEMICO
Proponer lineamientos de política Para Proyección Social
Proponer Normas Para Proyección Social
OBJETIVO DIRECCION GENERAL PROY SOCIAL
Promover Programas y Proyectos Para Transferir a la Sociedad
Supervisar, Controlar, Evaluar y Programas y Paquetes Tecnológicos
OBJETIVO FACULTAD
Identificar y acreditar Docentes, Estudiantes para Proy. Social
Transferir Conocimientos, Cultura y Resultados Investigativos



Mapa de Objetivos estratégicos de la UNDAC

En la Figura 06 se muestra la estructura orgánica de la Universidad Nacional Daniel Alcides Carrión, en este organigrama se ha designado a la Dirección General de Informática y Estadística (órgano de línea) como responsable de la seguridad de información dentro de la entidad.

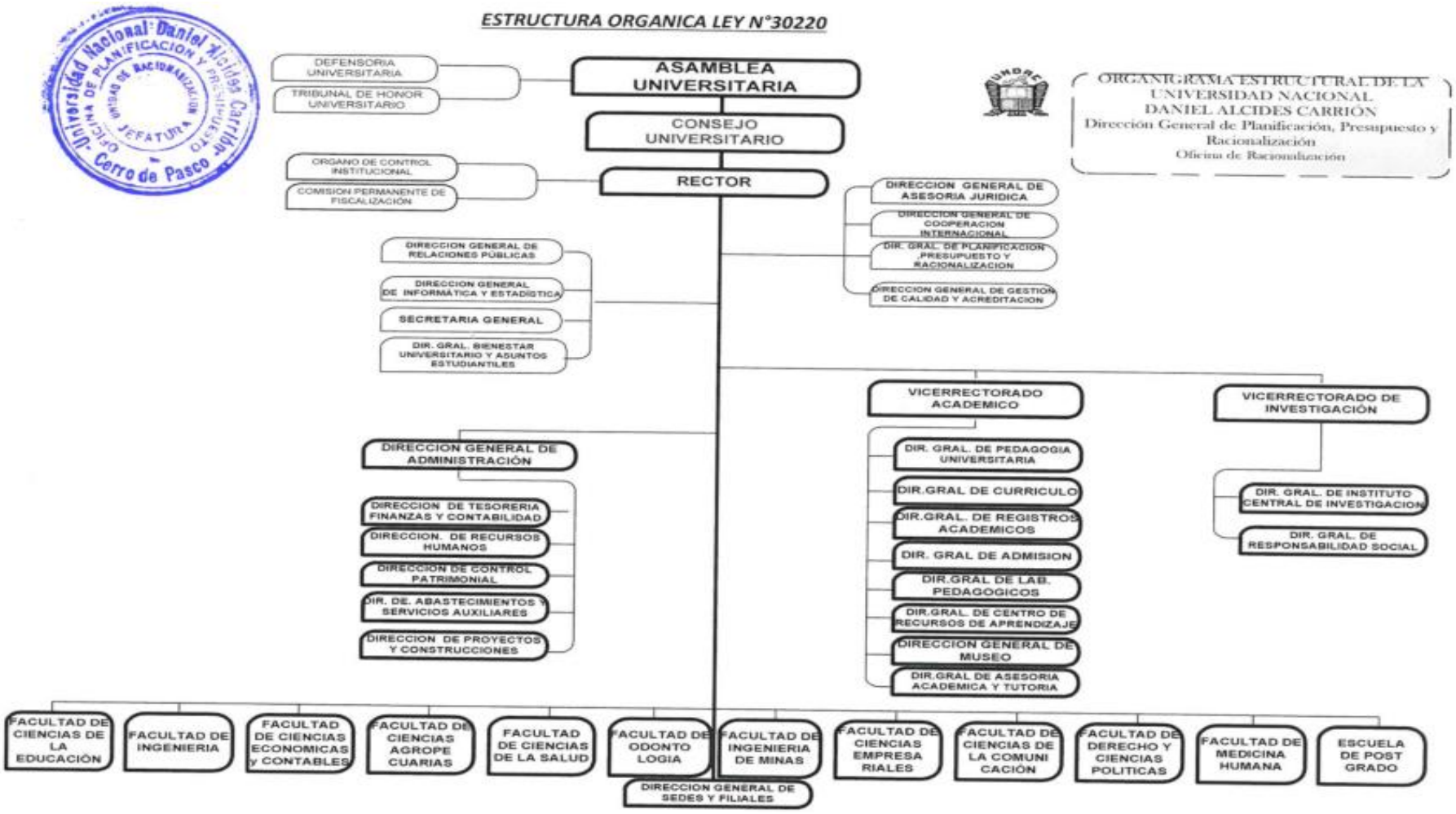


Figura 06: estructura orgánica UNDAC

DIRECCIÓN GENERAL DE INFORMÁTICA Y ESTADÍSTICA

La Dirección General de Informática y Estadística (DGIyE) de la UNDAC, es el órgano de apoyo responsable de brindar servicios de procesamiento y transmisión de la información, así como del soporte a la gestión del conocimiento, mediante la implementación de plataformas tecnológicas modernas y acorde con las exigencias institucionales, garantizando su disponibilidad, seguridad y confiabilidad de la información.

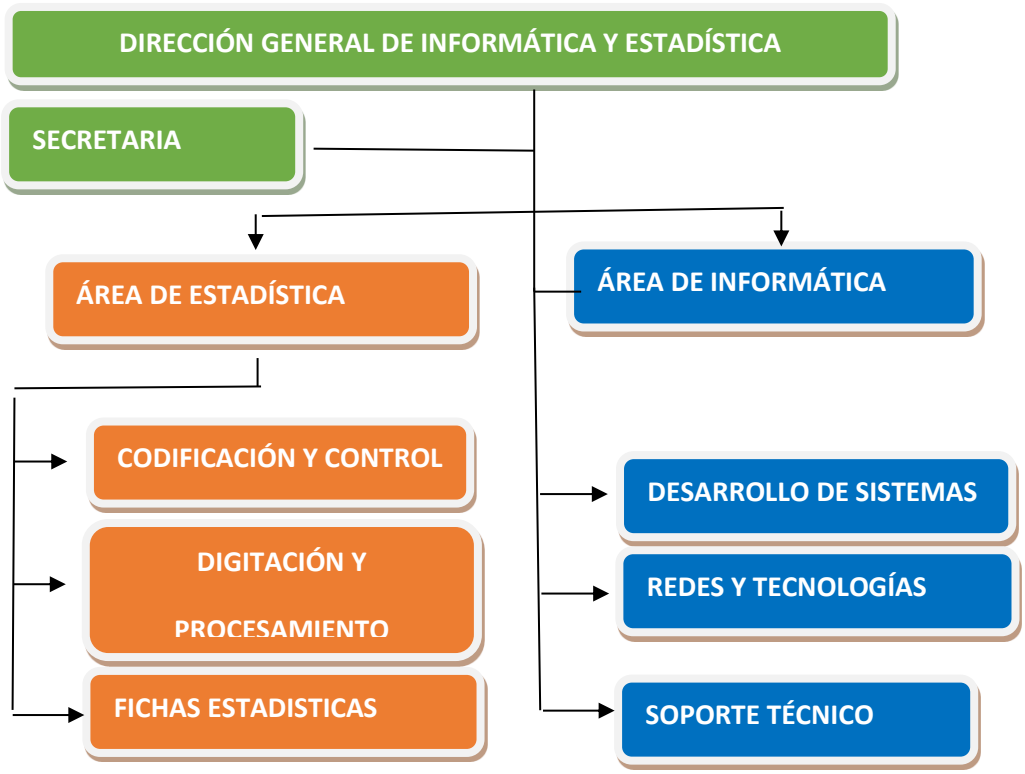


Figura 07: Estructura orgánica de la OGIyE-UNDAC

Fuente: Tesista

TECNOLOGÍA UNDAC

La Universidad Nacional Daniel Alcides Carrión no cuenta con la infraestructura tecnológica necesaria para soportar toda su estructura académica y administrativa, tanto en la sede central de Cerro de Pasco, como en las demás sedes y filial.

La fibra óptica actualmente ya se está instalando en todas las áreas de Administración Central, Posgrado, ciudad universitaria, así como también en las sedes y filiales, esperando que todas las computadoras de la universidad se logren conectar a la RED LAN UNDAC.

SISTEMAS DE INFORMACIÓN UNDAC

La Universidad Nacional Daniel Alcides Carrión, cuenta con varios sistemas de información de tipo académico, administrativo, financiero, entre otros; desarrollados por terceros y propios. Dentro de ellos se encuentran:

e-Undac 2.0: El Software de Gestión Integrada Académica UNDAC 2.0 es un sistema de información integrado que cubre la gestión de los diversos procesos académicos de la universidad, centralizando la información a través de un único sistema de software.

De esta forma la universidad cuenta con una única plataforma de software que integra los servicios existentes. Siempre salvaguardando la integridad de la información, haciendo que esta esté disponible, segura, confiable, auditable y sobre todo garantizando su confidencialidad.

Los sub módulos con que cuenta son:

- **e-Undac: Alumno**
- **e-Undac: Admisión**
- **e-Undac: Docente**
- **e-Undac: Bienestar**
- **e-Undac: Currículo**
- **e-Undac: Decano de facultad**
- **e-Undac: Egresado**
- **e-Undac: Rector**
- **e-Undac: ViceAcademico**

- **e-Undac: Matricula**
- **e-Undac: Registros académicos.**

SIUNDAC: Sistema surgido por la necesidad de controlar y manejar los procesos propios de la parte académica de la escuela de Posgrado.

SISTEMA ADMINISTRATIVO - MÓDULO ABASTECIMIENTO: El módulo de abastecimiento surge por la necesidad de realizar impresiones de los distintos tipos de documentos con que cuenta el SIAF ya que este dentro de sus opciones no cuenta con este tipo de impresiones, el módulo de abastecimiento facilita de esta manera la interacción del programa interno con la información del SIAF, dicho módulo está condicionado por las partidas presupuestales dadas por las oficinas de planificación.

SISTEMA ADMINISTRATIVO: MÓDULO DE TESORERÍA- SUB MÓDULO DE PAGADURÍA. El módulo de pagaduría surge por la necesidad de realizar impresiones de cheques y comprobantes de pago del SIAF ya que este dentro de sus opciones cuenta si con este tipo de procesos, pero el módulo de pagaduría puede hacer estas impresiones en grandes cantidades y no un documento a la vez tal como lo hace el SIAF, dicho módulo está condicionado por las partidas presupuestales.

SISTEMA ADMINISTRATIVO: MÓDULO DE TESORERÍA - SUB MÓDULO DE CAJA. El módulo de Caja permite gestionar los movimientos de dinero tanto para pago de facturas de proveedores o egresos como para el control de ingresos a través de comprobantes de egresos o recibos de caja, dicho módulo se encarga de realizar estas operaciones una por medio de una caja que se encuentra en la misma universidad llamada caja UNDAC y otra que es cobrada por el banco de la nación que esta enlazada a este sistema.

MODULO SECRETARIA GENERAL: Sistema de registros de grados y títulos de bachiller de pregrado y posgrado de la UNDAC, para su envió al registro de la SUNEDU e impresión de diplomas.

MÓDULO PLANIFICACIÓN: Este módulo contempla los procedimientos de manejo, organización, control, planificación, seguimiento y evaluación física del Plan Operativo, delineados en los objetivos a conseguir por la UNDAC durante un periodo establecido, el cual se alinea perfectamente con el Plan estratégico Institucional.

MÓDULO SIMI: Para cumplir con uno de los objetivos de la Superintendencia Nacional de Bienes Estatales, actualmente se ha desarrollado la versión 3.5 en Microsoft Visual FoxPro que lleva el nombre de “Software Inventario Mobiliario Institucional - SIMI” en donde se brindan nuevas funcionalidades.

MÓDULO CONTROL PATRIMONIAL Sirve para controlar todos los todos los Activos Depreciables y no depreciables de la UNDAC.

MÓDULO ABASTECIMIENTO: Es una herramienta de ayuda para la gestión logística, el mismo que permite administrar, registrar, controlar, elaborar, revisar y emitir información sobre adquisiciones de bienes y/o contratación de servicios y patrimonios.

MÓDULO CUENTAS POR COBRAR: Permite conocer en todo momento el estado actual de las cuentas de cada uno de los clientes y la demora en cada uno de los pagos, de modo que se puedan tomar medidas correctivas.

MÓDULO MESA DE PARTES: permite la recepción y registro de nuevos expedientes y documentos, así también la entrega de los mismos.

MÓDULO CAJA Y CAJA CHICA: El módulo de caja chica sirve para llevar el control de varias facturas que después serán pagadas con uno o más cheques.

MÓDULO PAGADURÍA: Sistema que realiza, controla y administra los pagos a los proveedores (PAGADURÍA), para la División de Contabilidad de una entidad financiera.

MÓDULO SIAF: son sistemas informáticos que automatizan los procedimientos financieros necesarios para registrar los recursos públicos recaudados y aplicarlos a la concreción de los objetivos del sector público.

MÓDULO SIGA: Herramienta informática que cuenta con una interfaz con el SIAF, es decir, nosotros podemos hacer interfaces de certificación presupuestal, de compromiso anual, compromiso mensual y devengado.

MÓDULO ESCALAFÓN: Permite organizar el ingreso y actualización de la trayectoria profesional del docente y trabajador administrado nombrado en tres tipos de legajo: activo, cesante y pensionista.

Matriz FODA

Después de analizar de los aspectos internos externos de la Universidad Nacional Daniel Alcides Carrión se elaboró la siguiente matriz FODA:

Figura 08: MATRIZ FODA DGIyE –UNDAC

4.2 COMPRENDER LAS NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

OFICINA GENERAL DE INFORMÁTICA Y ESTADISTICA

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

Código del Documento	SGSIUNDAC01
Versión	1.0
Fecha de Versión	10/07/2018
Propietario	DGIyE-UNDAC
Nivel de Confidencialidad	Alto

PROPÓSITO, ALCANCE Y USUARIOS

El propósito de este documento es comprender las necesidades y expectativas de las partes interesadas para el Sistema de Gestión de la Seguridad de la Información en la DGIyE de la UNDAC.

En este apartado se identificaron las partes interesadas externas e internas afectadas por el diseño y posterior implementación del SGSI.

4.2.1 PARTES INTERESADAS EXTERNAS

1. Gobierno (ONGEI-PCM)

La Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), es el órgano técnico especializado que depende directamente del despacho de la Presidencia del Consejo de Ministros (PCM). ONGEI, en su calidad de Ente Rector del sistema nacional de informática, se encarga de liderar los proyectos, la normatividad, y las diversas actividades que en materia de Gobierno Electrónico realiza el Estado. Entre sus actividades permanentes se encuentran las vinculadas a la normatividad informática, la seguridad de la información, el desarrollo de proyectos emblemáticos en Tecnologías de la Información y la Comunicación (TIC), brindar asesoría técnica e informática a las entidades públicas, así como, ofrecer capacitación y

difusión en temas de gobierno electrónico y la modernización y descentralización del Estado.

2. Contraloría General de la República

La Contraloría General de la República es la máxima autoridad del sistema nacional de control. Supervisa, vigila y verifica la correcta aplicación de las políticas públicas y el uso de los recursos y bienes del Estado. Para realizar con eficiencia sus funciones, cuenta con autonomía administrativa, funcional, económica y financiera.

3. La comunidad

Corresponde a los estudiantes, docentes, personal administrativo, padres de familia y grupos externos que se ven impactados por las actividades que desarrolla la DGIyE de la UNDAC.

4. Proveedores

Personas naturales o Jurídicas que prestan sus servicios a la Universidad Nacional Daniel Alcides Carrión.

4.2.2 PARTES INTERESADAS INTERNAS

1. Órganos de Gobierno

Conformado por el Consejo Universitario de la UNDAC, así como el Rector. Deben demostrar liderazgo y compromiso con la seguridad de la información, asegurando la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización y, garantizando la disponibilidad de los recursos necesarios para su implementación.

2. Órganos de alta Dirección

Conformado por el Director de la Dirección General de Informática y Estadística de la UNDAC. Debe demostrar liderazgo y compromiso respecto al sistema de gestión de la seguridad de la información, asegurando que los objetivos que se establecen son compatibles con la planeación estratégica de la organización y estableciendo una política de seguridad de la información.

3. Oficial de seguridad de la información

Es el responsable entre otros aspectos, de la seguridad de la información y continuidad tecnológica de la Entidad.

5. Estudiantes, Docentes y Administrativos de la UNDAC

Responsables de velar por la seguridad de los activos de información de la DGIyE de la UNDAC, cumplir a cabalidad con las normas y políticas de seguridad establecidas en la entidad. Además, tienen la responsabilidad del tratamiento de los datos personales de los titulares vinculados de alguna forma con la Entidad.

	Partes Interesadas	Requisitos
E x	Gobierno (ONGEI-PCM)	• Cumplimiento del marco legal y normativo de la seguridad de la información. • Alcanzar el objetivo de la política nacional de gobierno electrónico 2017-2021.
	Contraloría General de la República	• Cumplimiento de la normatividad de control interno de las entidades del estado relacionado a las tecnologías de información y comunicaciones:
	Comunidad	• Seguridad de sus datos sensibles.
	Proveedores	• Acuerdos contractuales claros en temas de seguridad de información
I n	Órganos de Gobierno	• Cumplimiento de las leyes y normatividad vigente en temas de seguridad. • Debe demostrar liderazgo y compromiso con la seguridad de la información.
	Órganos de Alta Dirección	• Supervisar las actividades y proyectos de la oficina general de Informática dela UNDAC en temas de Seguridad de la Información. • Debe demostrar liderazgo y compromiso con la seguridad de la información.
	Sub Oficial de Seguridad de la Información	• Levantamiento de no conformidades (respecto a la seguridad de información) de la auditoría presupuestal y financiera practicada a la DGIyE de la UNDAC. • Capacitar a los trabajadores en temas de seguridad de información
	Responsable de área	• Verificar la seguridad de la información antes, durante y después de la vinculación de los funcionarios y trabajadores.
	Estudiantes, Docentes, Administrativos MPH	• Conocer las normas y políticas en temas de Seguridad de la información • Velar por los activos de información de la UNDAC. • Protección de su información personal. • Disponibilidad de los servicios de la UNDAC. • Capacitación en temas de seguridad de la información

Tabla 20: Requisitos de las partes interesadas externas e internas

4.3 ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

OFICINA GENERAL DE INFORMÁTICA Y ESTADISTICA

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

ALCANCE DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Código del Documento	SGSIUNDAC01
Versión	1.0
Fecha de Versión	10/07/2018
Propietario	DGIyE-UNDAC
Nivel de Confidencialidad	Alto

1 PROPÓSITO, ALCANCE Y USUARIOS

El propósito de este documento es definir claramente el alcance y límite de la planeación del Sistema de Gestión de la Seguridad de la Información en la Dirección General de Informática de la Universidad Nacional Daniel Alcides Carrión.

Este documento es aplicable a toda la documentación y actividades relativas a la planeación del SGSI en cuestión e involucra a todos los administrativos de la Dirección General de Informática y Estadística y sus áreas de apoyo.

Los únicos usuarios autorizados a este documento son los miembros del comité de seguridad de la información y el personal autorizado de la DGIyE de la UNDAC.

1. DOCUMENTOS DE REFERENCIA

- NTP-ISO/IEC 27001:2014, cláusula 4.3.
- Documentación legal, resolución ministerial Nº 004-2016-PCM del 08 de enero del 2016 se aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014

2. DEFINICIÓN DEL ALCANCE DEL SGSI

La Dirección General de Informática y Estadística de la UNDAC, necesita establecer los límites de la planeación del SGSI con el fin de proteger sus activos informáticos que prestan el servicio a la institución. Esta fase de planeación del SGSI comprenderá las siguientes áreas:

- **Dirección General de Informática y Estadística:** Comprende el personal administrativo, sus activos informáticos y toda la infraestructura que le presta servicios de TI a la institución.

2.1 ANÁLISIS DIFERENCIAL

La norma NTP-ISO/IEC 27001:2014, requiere el cumplimiento de ciertos criterios para establecer, implementar, mantener y mejorar continuamente el Sistema de Gestión de la Seguridad de la Información (SGSI) en el contexto de una organización.

Para verificar el estado actual del cumplimiento de la NTP-ISO/IEC 27001:2014, en la Dirección General de Informática y Estadística de la UNDAC, se realiza un Análisis Diferencial de los numerales obligatorios 4 al 10 (Requisitos de la Norma NTP-ISO/IEC 27001:2014) y del Anexo A (Dominios, Objetivos de Control y Controles de Seguridad). Este análisis permite comparar las condiciones actuales con el fin de encontrar las deficiencias existentes y el nivel de cumplimiento en base al estándar y desarrollar un plan de mejoramiento de acuerdo a los objetivos de seguridad deseados.

Requisitos de la Norma NTP-ISO/IEC 27001:2014.

Para que una organización esté conforme a la norma NTP-ISO/IEC 27001:2014, no se deben excluir ninguno de los requisitos especificados en los numerales 4 al 10.

A continuación, se muestran los resultados del nivel de conformidad y cumplimiento de estos requisitos.

SECCIÓN	REQUERIMIENTO DE LA NTP ISO/IEC 27001:2014	ESTADO	EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE? /¿QUÉ SE TENDRÍA QUE HACER?	VALORACIÓN
4	**CONTEXTO DE LA ORGANIZACIÓN**	No Diseñado	Se sugiere realizar el análisis del contexto de la DGIyE de la UNDAC, para comprender, tanto los aspectos externos como internos, las partes interesadas y requisitos relevantes al SGSI y, elaborara y documentar el alcance del SGSI.	**6%**
4.1	**Comprender la Organización y contexto**. La organización **debe** determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este SGSI	Parcial mente diseñado	La **DGIyE de la UNDAC** posee documentos visibles de su Misión, Visión, Matriz FODA y las Estrategias. Pero no contempla de manera clara ítems de seguridad de la información. Se sugiere establecer objetivos de seguridad de la Información que estén alineados con los objetivos estratégicos.	25%
4.2	**Comprender las necesidades y expectativas de las partes interesadas.** La organización **debe** determinar las partes interesadas y los requisitos de las mismas.	No Diseñado	**Sugerencia:** Determinar las partes interesadas y comprender las necesidades y expectativas de éstas, referentes a la seguridad de la información.	0%
4.3	**Determinar el alcance del SGSI.**	No Diseñado	Sugerencia. Determinar el alcance del SGSI teniendo en consideración los aspectos referidos en 4.1, los requisitos de 4.2, documentarlo y ponerlo a disposición de las partes interesadas.	0%

4.4	**Sistema de Gestión de Seguridad de la información.** La organización debe establecer, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de esta Norma Técnica Peruana	No diseñado	Sugerencia. Establecer un plan para la mejora continua del SGSI conforme a la NTP Vigente	0%
5	**LIDERAZGO**	No Diseñado	El Titular de la Entidad, debe mostrar liderazgo y compromiso respecto al SGSI. Entonces, debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas. Por lo tanto, es necesario establecer: Una Política de Seguridad de la Información, y los Objetivos de Seguridad de la Información acorde al propósito de la organización.	1%
5.1	**Liderazgo y compromiso.** La alta dirección debe demostrar liderazgo y compromiso respecto al SGSI.	No Diseñado	El titular de la entidad debe mostrar liderazgo y compromiso	3%
5.2	**Política.**	No Diseñado	Establecer la Política de Seguridad de la Información acorde al propósito de la **DGIyE de la UNDAC**, incluir los objetivos de seguridad de la Información, mantenerla disponible y comunicada a toda la organización.	0%
5.3	**Roles, responsabilidades y autoridades organizacionales.**	No Diseñado	La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas.	0%
PUNTAJE TOTAL DE LA EVALUACIÓN DE REQUISITOS DE LA NTP ISO/IEC 27001:2014				**5%**

Tabla Nro. 21 Requisito de la NTP-ISO/IEC 27001:2014. CONTEXTO DE LA ORGANIZACIÓN.

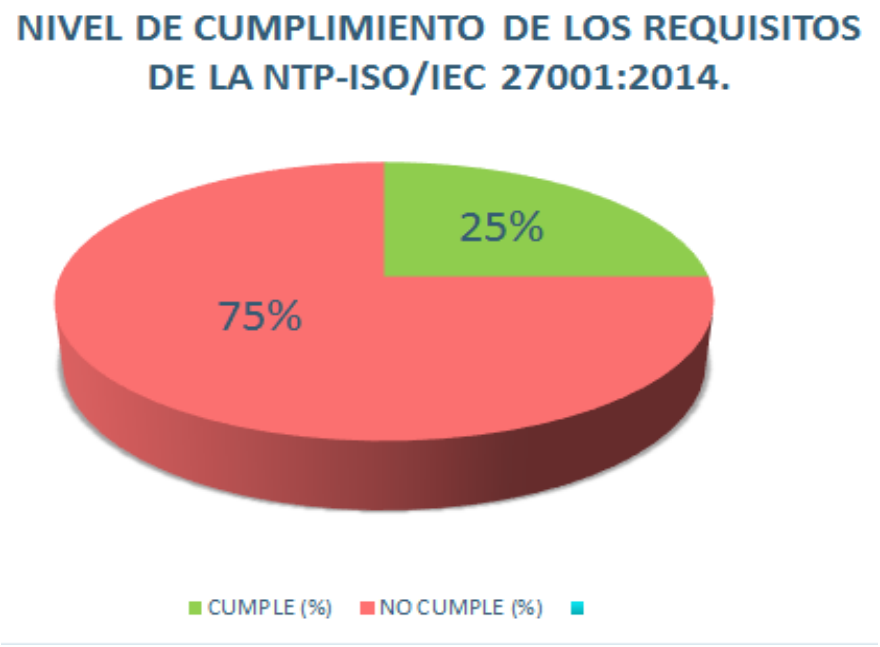


Gráfico 14 Nivel de cumplimiento de la NTP-ISO/IEC 27001:2014

Mediante este Análisis Diferencial es posible determinar que la Dirección General de informática y estadística de la UNDAC comprende la importancia y beneficios de un SGSI y posee el liderazgo necesario para realizarlo; sin embargo, aún no se ha establecido formalmente una metodología de análisis y evaluación de riesgos informáticos y su tratamiento, así como tampoco ningún documento requerido por la NTP-ISO/IEC 27001:2014. Por otra parte, se comprende la necesidad de alinear el SGSI con el proceso de desarrollo tecnológico llevado a cabo en la institución.

Código del Documento	SGSIUNDAC01
Versión	1.0
Fecha de Versión	10/07/2018
Propietario	DGIyE-UNDAC
Nivel de Confidencialidad	Alto

5.1 LIDERAZGO Y COMPROMISO

Para poner en marcha un SGSI es importante contar con el liderazgo y compromiso de la dirección, la norma contempla este epígrafe ya que el cambio de cultura que genera el proceso de implementación de un SGSI sería imposible de lograr sin la implicación constante de la alta dirección. Entre otras cosas, la alta dirección deberá demostrar su compromiso, aportando los recursos necesarios (tanto económicos como humanos), estableciendo la política y objetivos de seguridad de la información acorde a los objetivos estratégicos de la organización, comunicando la importancia de gestionar efectivamente la seguridad de la información, promoviendo la mejora continua, entre otras actividades.

Dentro de este requisito también se contempla el establecimiento de roles, responsabilidades y autoridades organizacionales para asegurar que el SGSI esté conforme a los requisitos de la NTP ISO 27001:2014 y reportar sobre el desempeño del mismo a la alta dirección.

a. Política de la seguridad de la información

En este apartado, se definió la política de seguridad de la información de la DGIyE de la UNDAC (acorde al requisito 5.2 de la NTP ISO/IEC 27001:2014). La política de seguridad será aprobada por el órgano de Gobierno y revisada anualmente.

Una vez aprobada la política de seguridad, la DGIyE de la UNDAC, comunicará esta política a toda la comunidad educativa Carrionina y a aquellos proveedores que considere necesario, además estará disponible para ser consultada por las partes interesadas.

La DGIyE de la UNDAC, en cumplimiento de nuestra misión, visión y objetivos estratégicos, y para satisfacer las necesidades de la comunidad, proveedores, y demás partes interesadas, establece la función de seguridad de la información dentro la entidad con el objetivo de:

- Proteger los activos de información de la DGIyE de la UNDAC.
  - Es Política de la DGIyE de la UNDAC asegurar que:

- La información esté protegida contra pérdidas de disponibilidad, confidencialidad e integridad.
- Se cumplan los requisitos legales y normas aplicables a la entidad respecto a la seguridad de la Información.
- Se cumplen con los requisitos de la entidad respecto a la seguridad de la información y los sistemas de información.
- Se gestionen los riesgos de seguridad de la información a través de la aplicación de una metodología, estándares y controles orientados a preservar los activos información de la entidad.
- Se fortalezca la cultura de seguridad de la información en el personal administrativo, docentes y estudiantes de la UNDAC
- Se garantice la continuidad de los servicios de la entidad.
- Cada personal administrativo es responsable de cumplir esta política y sus procedimientos según aplique a su puesto de trabajo.
- Es política de la DGIyE de la UNDAC implementar, mantener y realizar un seguimiento del SGSI.

b. Objetivos de seguridad de la información

Los objetivos del sistema de gestión de seguridad de la información son los siguientes:

- Asegurar la confidencialidad de la información de la comunidad Universitaria, almacenados en los sistemas de información de la DGIyE de la UNDAC.
- Asegurar la confidencialidad, integridad y disponibilidad de la información sensible de la DGIyE de la UNDAC.
- Maximizar la disponibilidad y calidad de los servicios prestados a la Comunidad Universitaria.
- Garantizar que nuestras operaciones y procesos actuales y futuros cumplan con la legislación y normatividad vigente en materia de seguridad de la información.
- Reducir los riesgos de seguridad de la información a un nivel aceptable para la DGIyE de la UNDAC.
- Difundir la Política de seguridad a través de cada uno de los responsables de área.
- Evaluar la efectividad del SGSI y llevar a cabo la mejora continua.

c. Requisitos legales

Cumplir con la legislación vigente en Perú es uno de los requisitos que se debe satisfacer para implantar y certificar un sistema de gestión de seguridad de la información. Su cumplimento protege a la entidad de amenazas externas e internas, además permite respetar los derechos de los estudiantes, docentes, personal administrativo y proveedores y evitará infracciones involuntarias con sus respectivos costes.

A continuación, se hace mención de algunas leyes y normas relacionadas con seguridad de la información que afectan a la DGIyE de la UNDAC.

c.1 Norma de Control Interno de las Entidades del Estado

Aprobada con Resolución de Contraloría General Nº 320-2006-CG, de fecha 30 de octubre del 2006. Según las

NORMAS BÁSICAS PARA LAS ACTIVIDADES DE CONTROL GERENCIAL, en su punto 3.10. Controles para las Tecnologías de Información y Comunicaciones (TIC) se define “La información de la entidad es provista mediante el uso de Tecnologías de la Información y Comunicaciones (TIC). Asimismo, la citada norma señala:

Disposición 01.- Los controles generales los conforman la estructura, políticas y procedimientos que se aplican a las TIC de la entidad y que contribuyen a asegurar su correcta operatividad. Los principales controles deben establecerse en:

• Sistemas de seguridad de planificación y gestión de la entidad en los cuales los controles de los sistemas de información deben aplicarse en las secciones de desarrollo, producción y soporte técnico

• Segregación de funciones:

- Controles de acceso general, es decir, seguridad física y lógica de los equipos centrales
- Continuidad en el servicio.

Disposición 02.- Para la puesta en funcionamiento de las TIC, la entidad debe diseñar controles en las siguientes etapas:

- i. Definición de los recursos
- ii. Planificación y organización
- iii. Requerimiento y salida de datos o información
- iv. Adquisición e implementación
- v. Servicios y soporte
- vi. Seguimiento y monitoreo.

Disposición 07.- Para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio. Para ello se debe elaborar, mantener y actualizar

periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia.

Disposición 08.- El programa de planificación y administración de seguridad provee el marco y establece el ciclo continuo de la administración de riesgos para las TIC, desarrollando políticas de seguridad, asignando responsabilidades y realizando el seguimiento de la correcta operación de los controles.

c2. Ley de Protección de Datos Personales

Promulgada el 2011, pero entró en aplicación el 8 de mayo de 2015. La presente Ley tiene el objeto de garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales que en ella se reconocen.

Esto quiere decir que las empresas y entidades públicas están obligadas a garantizar la protección de los datos con los que cuentan en sus sistemas informáticos evitando que terceros no autorizados accedan a ellos.

c3. Ley 30096.- Ley de Delitos Informáticos

Entró en vigencia el 23 de octubre de 2013. La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.

c4. Ley N° 30171.- Ley que modifica la Ley 30096, ley de Delitos Informáticos

Publicada en el diario Oficial el Peruano en el 10 de marzo del 2014. Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos, se modificaron los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos: Acceso ilícito, atentado a la integridad de datos informáticos, atentado a la integridad de sistemas informáticos, proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos, interceptación de datos informáticos, fraude informático, abuso de mecanismos y dispositivos informáticos.

d. Comité de la seguridad de la información

De acuerdo al requisito 5.3 Roles, responsabilidades y autoridades organizacionales de la NTP ISO/IEC 27001:2014 la alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.

Asimismo, la RM Nº 004-2016-PCM en su artículo 5 establece la creación del comité de gestión de seguridad de la información para dar cumplimiento al requisito 5.3 de la NTP ISO/IEC 27001:2014. Este comité de gestión de seguridad de la Información, estará conformado por:

1. Alta dirección o Consejo Universitario
2. Rector de la Universidad
3. El gerente de planificación y presupuesto
4. El Director de Informática y Estadística de la UNDAC;
5. El responsable de la oficina de asesoría jurídica
6. El oficial de seguridad de la información.

5.2 ROLES, RESPONSABILIDADES Y AUTORIDADES ORGANIZACIONALES

A continuación, se describen los roles y responsabilidades propuestos estos roles y responsabilidades, así como la necesidad de agregar alguna autoridad más será evaluada por la alta dirección en coordinación con el comité de seguridad de la información.

Cabe mencionar que, según la metodología, este requisito estará sometido a una mejora continua acorde a las necesidades de la DGIyE de la UNDAC.

d1. Alta dirección o Consejo Universitario.

- Aprobar la política de seguridad de la información y comunicarla a todos los trabajadores de la entidad.
- Definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.
- Promover una cultura de seguridad de la información en la entidad.

d2. Rector de la Universidad

- Proponer al Rector y Concejo Universitario la política de seguridad de la información para la Universidad.
- Hacer cumplir la política de seguridad de la información dentro de la Universidad.
- Revisar la política de seguridad de la información en intervalos planificados o cuando se produzcan cambios significativos en la normatividad de seguridad.
- Controlar el avance de la seguridad de información dentro de la DGIyE de la UNDAC.

d3. El responsable de la oficina de planificación y presupuestos

- Gestionar y coordinar los medios necesarios para la implementación, ejecución y mantenimiento del sistema de gestión de seguridad de la información.

d4. Director de Informática y Estadística de la UNDAC

- Garantizar la disponibilidad y operatividad de los sistemas de información, equipos informáticos y de comunicaciones de la Universidad.
- Establecer los mecanismos adecuados para la gestión y administración de riesgos, seguridad de la información, velar por la capacitación del personal de la entidad en lo referente a estos temas.
- Informar al Rector y Concejo Universitario sobre aspectos relacionados con el SGSI.
- Asegurar la existencia de metodologías para el tratamiento de riesgos y oportunidades, políticas de seguridad de la información, así como la existencia de los documentos exigidos por la NTP ISO/IEC 27001:2014.
- Asegurar el cumplimiento de las políticas y requerimientos de seguridad establecidos para la adquisición, diseño, desarrollo, operación, administración y mantenimiento de las TICs de la Universidad.
- Asignar las funciones, roles y responsabilidades de Seguridad, al personal administrativo a su cargo para la operación y administración de las TIC de la Universidad. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.
- Aprobar la implementación de los controles y medidas de seguridad

d5. El responsable de la oficina de asesoría jurídica

- Conocer e interpretar las leyes y normatividad vigente relacionada con seguridad de la información y bajo el contexto de la entidad.
- Evaluar el cumplimiento de las leyes y normatividad vigente en temas de seguridad de la información dentro de la entidad.

- Mantener actualizado un archivo de normas legales relacionadas con la seguridad de la información.

d6. El Oficial de seguridad de la información.

- Diseñar y coordinar la implementación de las políticas, normas y procedimientos de seguridad de la información, con la participación activa de las dependencias de la Universidad.
- Identificar los riesgos a los que se encuentran expuestos los activos de información de la DGIyE de la UNDAC y gestionar la actualización del mapa de riesgos.
- Definir los controles asociados al sistema de gestión de seguridad de la Información y evaluarlos periódicamente.
- Establecer un programa periódico de revisión de vulnerabilidades y coordinar los respectivos planes de mitigación.
- Desarrollar de forma periódica, charlas de capacitación y concientización en temas de seguridad de información para el personal de la entidad.
- Atender auditorías internas y externas de aspectos asociados a la Seguridad de Información y, facilitar la información sobre documentos de gestión de seguridad y los controles implementados.
- Reportar al Director General de Informática y Sistemas los incidentes de seguridad de la información, los resultados de las auditorias, la revisión y supervisión del SGSI.
- Asesorar en forma permanente y cercana a las distintas áreas de la institución en temas de seguridad de la Información.

5.3 POLÍTICAS DE SEGURIDAD DE LOS ACTIVOS DE LA INFORMACIÓN

5.3.1 POLÍTICA DE SEGURIDAD GENERAL

Todos los directivos y administrativos se comprometerán a mantener la información lo más segura posible. Se prohíbe la reproducción total o parcial de los documentos clasificados como confidenciales, sin la debida autorización o consentimiento del ente competente, así como el deterioro adrede de los dispositivos informáticos, software, cableado de datos, suministro eléctrico, o cualquier activo institucional.

5.3.2 POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN EN GENERAL

Se emplearán políticas y lineamientos de seguridad que fuercen a mantener la información de estudiantes, docentes y administrativos en un entorno seguro. Estas políticas estarán dirigidas a mantener los principios de la Seguridad Informática como lo son la Confidencialidad, Integridad y Disponibilidad, así como los Planes de Continuidad del Negocio y Recuperación de Desastres.

5.3.3 POLÍTICA DE SEGURIDAD A LOS SERVICIOS UNIVERSITARIOS

Para el acceso a los servicios de los sistemas de información universitarios, se solicitarán siempre las credenciales de acceso obtenidas por la Dirección General de Informática y Estadística de la UNDAC. Este será una única cuenta personal e intransferible. Si los datos de acceso son extraviados, se podrán recuperar a través del usuario del correo institucional.

5.3.4 POLÍTICA DEL DESARROLLO DE APLICACIONES

Para la contratación de software de aplicación de terceros, éste será evaluado por el personal de sistemas capacitado de la universidad para verificar si cumple con los requerimientos institucionales y de seguridad, y de acuerdo a su evaluación,

se empleará un período de pruebas no menor a 3 meses y no mayor a 6 meses.

Para el desarrollo de software de aplicación por grupos o proyectos de investigación institucionales, se verificarán que sean bajo las herramientas de desarrollo de software, multimedia o educativo con los cuales la universidad mantiene contratos de licencia. El período de evaluación y prueba cumple con las mismas condiciones del software desarrollado por terceros.

Para el software de aplicación que requiera de credenciales de acceso, éste implementará para los usuarios, conexiones seguras.

5.3.4 POLÍTICA DE LA GESTIÓN DE RIESGO

Se emplearán los mecanismos de gestión de riesgos y controles necesarios para mantener el normal funcionamiento de los procesos.

5.3.5 POLÍTICA DE LA PROTECCIÓN DE DATOS

Se implementará un sistema de protección multiniveles a los datos e información que se almacenan en las bases de datos de la institución. Se emplearán restricciones a nivel de usuario en base al rol y perfil.

5.3.6 POLÍTICA DE AUDITORÍA

Para mantener la calidad de los procesos organizativos, se harán auditorías programadas en cada una de las áreas y procesos críticos de la institución.

5.3.7 POLÍTICA DE CALIDAD

La Dirección General de Informática y Estadística se comprometerá a realizar controles y cambios en pro de mejorar continuamente sus procesos. Se realizarán evaluaciones periódicas para medir el nivel de calidad en áreas críticas y en otras donde sea necesario.

La calidad será un componente fundamental. Se cumplirán con los requerimientos de gestión para el logro de certificaciones de estándares internacionales, así como la alineación con los sistemas de calidad existentes en la institución.

5.3.8 POLÍTICA DE LOS DISPOSITIVOS TRAÍDOS POR EL USUARIO

Los funcionarios que prefieran trabajar con sus equipos de uso personal, deben estar previamente autorizados para hacerlo, el equipo se configurará de acuerdo a los lineamientos institucionales y bajo las mismas condiciones que los equipos de la institución, ya que no se aceptarán riesgos inaceptables como la propagación de software de código malicioso debido a una falla de seguridad en el equipo.

5.3.9 POLÍTICA DE DISPOSITIVOS PORTABLES

La instalación de los dispositivos portables en los equipos de la institución, serán escaneados automáticamente por la solución antivirus contratada. No se permitirá su ejecución si se detecta el código malicioso y no es removido de la unidad. Si no puede ser removido, se emitirá una alerta al ente correspondiente para su análisis.

5.3.10 POLÍTICA DE LA CREACIÓN DE USUARIOS

Los usuarios podrán acceder a los diferentes servicios utilizando un esquema de identificación único, personal e intransferible. Este será el usuario institucional y se entregará de forma automática y online en un período no máximo a las 24 horas desde el momento en el que el usuario tiene vínculo con la universidad.

5.3.11 POLÍTICA DE LA INSTALACIÓN DE SOFTWARE Y HARDWARE

Para la instalación del software y hardware, estos componentes serán únicamente instalados por el personal técnico capacitado de la institución. A cada equipo se le realizará un inventario de

hardware y la información será mantenida en una base de datos. Se realizará un chequeo de este componente cada vez que se inicie el equipo y se conecte a la red; si se detectan cambios no autorizados, quedará deshabilitado automáticamente.

5.3.12 POLÍTICA DE LA COMUNICACIÓN INSTITUCIONAL

La información y comunicación institucional será única y exclusivamente informada por medio de los correos electrónicos institucionales y no de los webs comerciales. Se realizará un escaneo con software antivirus a los documentos adjuntos tanto subidos como recibidos.

5.3.13 RESPONSABILIDAD

Cada persona administrativa de la Dirección General de Informática y Estadística velará por la seguridad de los activos informáticos que están a su disposición, así como se comprometerá a seguir los lineamientos estipulados en este documento de una manera satisfactoria y de acuerdo a las reglamentaciones contractuales.

5.3.14 PROCEDIMIENTOS EN INCIDENTES DE SEGURIDAD

Si la persona administrativa detecta que ha sido violado un procedimiento referente a las Políticas de Seguridad establecidas en este documento, deberá informarlo inmediatamente al director de la Dirección General de Informática y Estadística mediante un documento formal reportando el incidente, posibles causas y fallas que podrían haberlo generado, así como las recomendaciones y/o controles para mitigarlo.

6. PLANIFICACIÓN

OFICINA GENERAL DE INFORMÁTICA Y ESTADISTICA

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

ACCIONES PARA TRATAR LOS RIESGOS Y OPORTUNIDADES

Código del Documento	SGSIUNDAC01
Versión	1.0
Fecha de Versión	10/07/2018
Propietario	DGIyE-UNDAC
Nivel de Confidencialidad	Baja

PROPÓSITO, ALCANCE Y USUARIOS

El propósito de este documento es definir la metodología de análisis y evaluación de riesgos y evaluar el reporte de evaluación de riesgos en la Dirección General de Informática y Estadística de la UNDAC, y definir cuáles son los riesgos que tienen mayor impacto en la institución de acuerdo al estándar ISO/IEC 2001:2014.

El análisis de riesgos es aplicado a todo el alcance del Sistema de Gestión de la Seguridad de la Información incluyendo todos los activos inventariados que podrían tener un impacto en la seguridad de la información.

Los usuarios de este documento son todos aquellos docentes y/o administrativos que intervienen en el proceso de análisis y evaluación de riesgos.

1. ACCIONES PARA TRATAR RIESGOS Y OPORTUNIDADES

Las acciones para tratar riesgos y oportunidades introducen nuevos conceptos para un análisis sistemático de las amenazas y el establecimiento de acciones para abordar no solo los riesgos sino también las oportunidades que estas plantean, Resumiendo se trata de una ampliación de la perspectiva del concepto más simple de "acción preventiva" establecida en la norma anterior ISO 27001: 2005.

La identificación de los riesgos y oportunidades que afectan al contexto de la organización lo hemos visto en el apartado correspondiente de la norma Sección 4 el contexto de la organización donde se determinan en base a las necesidades y expectativas de las partes interesadas en relación a la seguridad de la información.

Esta evaluación de riesgos esta y oportunidades está en sintonía tanto con el logro los resultados esperados como con la prevención o mitigación de las consecuencias no deseadas, siempre con el objetivo final de conseguir la mejora continua. La mejora continua se consigue integrando dentro del SGSI las actividades de evaluación y medición de la efectividad de sus acciones.

2. METODOLOGÍA DE ANÁLISIS Y EVALUACIÓN DE RIESGOS Y REPORTE DE EVALUACIÓN DE RIESGOS

2.1 METODOLOGÍA MAGERIT. MAGERIT es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información elaborado por el CSAE (Consejo Superior de Administración Electrónica) que supone los beneficios evidentes de emplear las tecnologías de información, pero gestionando los riesgos inherentes a ella, donde actualmente está en su versión 3.

El objetivo principal de MAGERIT es proteger los activos informáticos en pro de ayudar al alcance de la misión de una organización de acuerdo a las Dimensiones de Seguridad propuestas:

DIMENSIÓN DE SEGURIDAD	NOMENCLATURA	DEFINICIÓN
Disponibilidad	**D**	Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
Integridad	**I**	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
Confidencialidad	**C**	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
Autenticidad	**A**	Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
Trazabilidad	**T**	Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

Tabla 22. Dimensiones de Seguridad para la Identificación y Valoración de Amenazas en MAGERIT.

Para el proceso de Gestión del Riesgo, MAGERIT contempla dos (2) grandes tareas a realizar: el Análisis de Riesgos y el Tratamiento de Riesgos. El Análisis de Riesgos pretende calificar los riesgos encontrados cuantificando sus consecuencias (análisis cuantitativo) o determinando su importancia relativa (análisis cualitativo). Este proceso de análisis conlleva la identificación de los activos, sus amenazas y los controles de seguridad propuestos, estimando así el impacto y el riesgo al que están expuestos cada uno de los activos y su repercusión en el nivel de seguridad de la información en una organización. Por su parte, el Tratamiento de Riesgos consta de las actividades que se ejecutan para modificar la situación o nivel de riesgo.

Como MAGERIT es una metodología sistemática, sigue una serie de pasos para realizar la Gestión del Riesgo, los cuales son los siguientes:

1. **Inventario de Activos:** Los activos son aquellos componentes o funcionalidades de un sistema de información que son susceptibles a ser atacados deliberada o intencionalmente con consecuencias para una organización. Son también los elementos que una organización posee para el tratamiento de la información. MAGERIT clasifica los activos en los siguientes tipos:

TIPO DE ACTIVO	NOMENCLATURA	DEFINICIÓN
Activos Esenciales	[Essential]	Son aquellos que son esenciales para la supervivencia de la organización y que su carencia o daño afectaría directamente su existencia. Generalmente desarrollan misiones críticas.
Arquitectura del Sistema	[Arch]	Son aquellos que permiten estructurar el sistema, su arquitectura interna y sus relaciones con el exterior.
Datos /Información	[D]	Es aquella información que le permite a una organización prestar sus servicios.
Claves Criptográficas	[K]	Son aquellos que permiten cifrar la información. Incluye los algoritmos de encriptación.
Servicios	[S]	Son aquellos que satisfacen las necesidades de los usuarios.

TIPO DE ACTIVO	NOMENCLATURA	DEFINICIÓN
Servicios	[S]	Son aquellos que satisfacen las necesidades de los usuarios.
Software/Aplicaciones Informáticas	[SW]	Son aquellos que procesan los datos y permiten brindar información para la prestación de servicios.
Hardware/Equipamiento Informático	[HW]	Son los medios físicos donde se depositan los datos y prestan directa o indirectamente un servicio.
Redes de Comunicaciones	[COM]	Son los medios de transporte por donde viajan los datos.
Soportes de Información	[Media]	Son los dispositivos físicos que permiten el almacenamiento temporal o permanente de la información.
Equipamiento Auxiliar	[AUX]	Son aquellos equipos que brindan soporte a los sistemas de información sin estar relacionado con los datos.
Instalaciones	[L]	Son los lugares donde se hospedan los sistemas de información y comunicaciones.
Personal	[P]	Son las personas relacionadas con los sistemas de información.

Tabla 23. Clasificación de los tipos de activos informáticos en MAGERIT.

2. **Valoración de los Activos:** Los activos que generan valor son aquellos que se necesitan proteger, y cada activo tiene una importancia mayor o menor en la organización. MAGERIT establece dos (2) tipos de valoraciones: Cualitativa que es aquella que permite calcular el valor de un activo en base al impacto que pueda tener en la organización y la Cuantitativa que estima el costo del activo (incluyendo costo de compra, de reparación, configuración, mantenimiento, etc.). Mientras que la Cualitativa permite establecer órdenes de magnitud (MA [Muy Alto], A [Alto], M [Medio], B [Bajo] y

MB [Muy Bajo]) y no genera valores numéricos, la Cuantitativa sí permite calcular el costo y/o valor monetario.

3. **Identificación y Valoración de Amenazas:** MAGERIT establece cinco (5) Dimensiones de Seguridad (D [Disponibilidad], I [Integridad], C [Confidencialidad], A [Autenticidad] y T [Trazabilidad]) donde es necesario determinar los criterios de valoración en cada dimensión. Estos valores y/o criterios son similares a los establecidos en la tabla de Valoración cualitativa de los activos informáticos en MAGERIT.

1.1. **Identificación de Amenazas:** Las amenazas son los eventos que ocurren sobre un activo que podría causarle daño a una organización. MAGERIT emplea un catálogo de amenazas posibles sobre los activos de un sistema de información, los cuales están clasificados de la siguiente manera:

TIPO DE AMENAZA	NOMENCLATURA	DEFINICIÓN
Desastres Naturales	**[N]**	Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.
De Origen Industrial	**[I]**	Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas puede darse de forma accidental o deliberada.
Errores y Fallos No Intencionados	**[E]**	Fallos no intencionales causados por las personas.
Ataques Intencionados	**[A]**	Fallos deliberados causados por las personas.

Tabla 24 Catálogo de Amenazas sobre los activos informáticos en MAGERIT

1.2. **Valoración de Amenazas**: Para establecer la valoración de las amenazas es necesario determinarla frecuencia o probabilidad de ocurrencia. En MAGERIT, las frecuencias o probabilidades se muestran a continuación:

PROBABILIDAD O FRECUENCIA	RANGO	VALOR
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semanas	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Tabla 25. Probabilidad o Frecuencia de ocurrencia de las amenazas en MAGERIT.

1.3. Impacto Potencial: Se determina el nivel de daño o impacto que tendría un activo si se llegara a materializar una amenaza determinada en cada una de sus dimensiones de seguridad.

1.4. Riesgo Potencial: El riesgo es la medida probable de daño sobre un sistema el cual es posible determinar directamente conociendo la probabilidad de ocurrencia de una amenaza sobre un activo y el impacto. Por ende, el riesgo es calculado como:

Riesgo = Probabilidad x Impacto.

A su vez, la relación de la probabilidad e impacto para determinar el riesgo de forma cualitativa se muestra en la siguiente tabla:

RIESGO		PROBABILIDAD				
		MB	B	M	A	MA
IMPACTO	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Tabla 26. Estimación cualitativa del riesgo.

4. Controles de Seguridad (Salvaguardas):

Los Controles de Seguridad o Salvaguardas son aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo, donde se deben establecer los controles para cada amenaza de cada

activo. Las salvaguardas propuestas en MAGERIT se clasifican en los siguientes:

SALVAGUARDA	NOMENCLATURA
Protecciones generales u horizontales	H
Protección de los datos / información	D
Protección de las claves criptográficas	K
Protección de los servicios	S
Protección de las aplicaciones (software)	SW
Protección de los equipos (hardware)	HW
Protección de las comunicaciones	COM
Protección en los puntos de interconexión con otros sistemas	IP
Protección de los soportes de información	MP
Protección de los elementos auxiliares	AUX
Seguridad física – Protección de las instalaciones	L
Salvaguardas relativas al personal	PS
Salvaguardas de tipo organizativo	G
Continuidad de operaciones	BC
Externalización	E
Adquisición y desarrollo	NEW

Tabla 27. Salvaguardas sobre los activos informáticos en MAGERIT.

2. **Inventario y Clasificación de Activos Informáticos.** Un activo o recurso informático está representado por los objetos físicos (hardware [routers, switches, hubs, firewalls, antenas, computadoras]), objetos abstractos (software, sistemas de información, bases de datos, sistemas operativos) e incluso el personal de trabajo y las instalaciones físicas. Dentro de los activos o recursos informáticos encontrados en la dirección general de informática y estadística se encuentran los siguientes:

RECURSO	DESCRIPCIÓN
Copias de Seguridad de los Sistemas de Información	Archivos de copias de seguridad de los diferentes Sistemas de Información, Aplicaciones y Ambientes Virtuales de Aprendizaje.
Artículos de Revistas Digitales	Artículos, investigaciones y publicaciones.
Registros de Actividad	Archivos de registros de actividad de los diferentes Sistemas de Información, Aplicaciones y Ambientes Virtuales de Aprendizaje.
Códigos Fuentes	Archivos de códigos fuentes de los diferentes Sistemas de Información propios desarrollados.
Gestión de Identidades	Gestión de las identidades, usuarios, contraseñas y privilegios de las cuentas administrativas para el uso de las computadoras institucionales.
Servicios Internos	Servicios de uso interno para docentes, estudiantes y administrativos que cuentan con datos de acceso institucionales. Software académico, Bases de Datos de Biblioteca, Gestión Documental y Atención al Usuario.
Páginas web de acceso público	Páginas, portales, ambientes virtuales de aprendizaje, sitios y aplicativos que son disponibles para el acceso público.
Software para Correo Electrónico	Software utilizado para el correo electrónico institucional.
Gestores de Bases de Datos	Administran y gestionan las bases de datos que se utilizan para soportar todo el software académico, administrativo, educativo y demás que apoyan a los demás procesos institucionales.
Software de Antivirus	Software para prevenir y eliminar el *malware* .
Sistemas Operativos	Software que administra los recursos de las computadoras de uso institucional.
Dispositivos de Respaldo	Dispositivos que almacenan la información y son útiles para la recuperación de desastres.
Firewall	Controla el tráfico entrante/saliente de la red de datos aplicando reglas de seguridad.
Servidores	Computadoras especializadas en proveer los recursos, almacenar datos y ejecutar el software y diferentes aplicaciones a través de la red.
Computadoras Portátiles de Uso Institucional	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.
Computadoras de Escritorio de Uso Institucional	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.
Escáner	Dispositivos para transformar la información en formato digital.
Impresoras	Dispositivos para la impresión en papel.
Router	Redirige el tráfico de datos de la red interna con el exterior. Permite la conexión a internet a través del ISP (Proveedor de Servicios de Internet).
Switches	Administra las VLANS el permite realizar la segmentación de la red de datos y gestionar y optimizar el ancho de banda, así como expandir la conexión de las computadoras de uso institucional.
Puntos de Acceso Inalámbricos	Amplían la cobertura de la red por medio de conexiones inalámbricas.
Red de Área Local	Permite la interconexión de las computadoras institucionales así como el acceso a los diferentes servicios. Soporta el desarrollo normal de los procesos.
Rack	Aloja los servidores, *router* , *switches* y *firewall* protegiéndolos de la humedad, golpes o uso malintencionado.
Fuente de Alimentación	Provee y regula la energía a los Servidores.
Sistema de Alimentación Ininterrumpida	Provee energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas.
Cableado Eléctrico	Provee energía eléctrica a las instalaciones y dispositivos.

Tabla 28. Activos informáticos en la DGIyE-UNDAC.

4.1 Valoración de Los Activos de Acuerdo al Impacto

Se determina la valoración de los activos de la dirección general de informática y estadística de acuerdo al tipo Cualitativo que establece MAGERIT y el impacto que tiene en la institución, de acuerdo a la siguiente escala:

IMPACTO	NOMENCLATURA	VALOR	DESCRIPCIÓN
MUY ALTO	MA	10	El daño tiene consecuencias muy graves para la organización y podrían ser irreversibles.
ALTO	A	7-9	El daño tiene consecuencias muy graves para la organización.
MEDIO	M	4-6	El daño contiene consecuencias relevantes para la organización y su operación.
BAJO	B	1-3	El daño contiene consecuencias relevantes, pero no afecta a una gran parte de la organización.
MUY BAJO	MB	0	El daño no contiene consecuencias relevantes para la organización.

Tabla 29. Valoración cualitativa de los activos informáticos en MAGERIT.

[SW] SOFTWARE

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
SW_SWP	Software de Desarrollo Propio	MA	Utilizados para el normal desarrollo de los procesos institucionales.
SW_STD	Software Estándar	MA	Utilizados para el normal desarrollo de los procesos institucionales.
SW_MAI	Software para Correo Electrónico	A	Utilizado para la comunicación de administrativos, docentes y estudiantes.
SW_DBS	Gestores de Bases de Datos	MA	Almacena toda la información de los diferentes Sistemas de Información, así como el soporte para el desarrollo normal de los procesos y tomas de decisiones. Dentro de ellos se encuentran, SQL Server 2008 R2, MySQL 5.5 y PostgreSQL.
SW_OFM	Ofimática	B	Utilizado para la ejecución de tareas.
SW_AVS	Software de Antivirus	M	Utilizado para la prevención y eliminación de software malintencionado, así como evitar la propagación de malware por la red.
SW_OPS	Sistemas Operativos	M	Administra los recursos de software y hardware de las diferentes computadoras de uso institucional.

[HW] HARDWARE

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
HW_BCK	Dispositivos de Respaldo	MA	Dispositivos que almacenan los archivos de las copias de seguridad necesarios para la recuperación en caso de desastres.
HW_FRW	Firewall	MA	Dispositivo que filtra los paquetes. Esencial para la configuración de seguridad de la red de datos.
HW_ANT	Antenas	A	Esencial para establecer los enlaces de comunicación con cada uno de los campus universitarios en otras sedes.
HW_HOS	Servidores	MA	Dispositivos esenciales para el correcto funcionamiento de los diferentes Sistemas de Información que soportan los procesos institucionales. Dentro de ellos se encuentran los Servidores de Aplicaciones, DNS, Bases de Datos, Mail y Web.
HW_PCM	Computadoras Portátiles de Uso Institucional	B	Dispositivos para la ejecución de tareas.
HW_PCP	Computadoras de Escritorio de Uso Institucional	B	Dispositivos para la ejecución de tareas.
HW_PRT	Impresoras	MB	Dispositivo para realizar impresiones en papel.
HW_ROU	Router	A	Esencial para direccionar el tráfico de datos interno y externo. A su vez, hace el papel de Gateway para dar salida a Internet.
HW_SCN	Escáner	MB	Dispositivo para digitalizar documentos.
HW_SWH	Switch	A	Esencial para direccionar el tráfico de datos interno, administración de LAN y segmentar el ancho de banda con el fin de optimizarla. Dentro de ellas se encuentran las LAN administrativa, docentes y estudiantes.
HW_WAP	Puntos de Acceso Inalámbricos	B	Dispositivos que amplían la cobertura de la red para dar acceso inalámbrico.

[COM] COMUNICACIONES

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
COM_INT	Internet	A	Esencial para tener acceso a redes externas.
COM_LAN	Red de Área Local	MA	Esencial para la transmisión de datos y dar soporte al normal funcionamiento de los servicios internos institucionales. Incluye todo el cableado estructurado.
COM_WIF	Conectividad Inalámbrica	B	Amplía la cobertura y otorga acceso inalámbrico a estos tipos de dispositivos.

[AUX] EQUIPO AUXILIAR

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
AUX_FBO	Fibra Óptica	MA	Otorga alta velocidad de transmisión en el tráfico de datos interno. Da soporte de conectividad a toda la institución.
AUX_RCK	Rack	A	Mantiene los dispositivos de red como el *router* , *switches* y servidores organizados y asegurados.
AUX_PWR	Fuente de Alimentación	MA	Esencial para el funcionamiento normal de todos los dispositivos que soportan los Sistemas de Información y procesos institucionales.
AUX_UPS	Sistema de Alimentación Ininterrumpida	A	Esencial para mantener funcionando a los dispositivos en caso de una eventual falla en el suministro eléctrico, así como también evita el daño parcial o total del hardware.
AUX_WIR	Cableado Eléctrico	MA	Cableado esencial para mantener en funcionamiento los dispositivos y el normal desarrollo de los procesos institucionales.

[L] INSTALACIONES

CÓDIGO	DESCRIPCIÓN	IMPACTO	RAZÓN
L_DGIyE	Dirección General de Informática y Estadística (DGIyE)	MA	Esencial para el normal funcionamiento de todos los Sistemas de Información que soportan los procesos institucionales.

[P] PERSONAL			
CÓDIGO	**DESCRIPCIÓN**	**IMPACTO**	**RAZÓN**
P_ADM	Administrador de Sistema	**A**	Personas encargadas de administrar los diferentes Sistemas de Información que dan soporte a los procesos institucionales y sus servicios.
P_COM	Administrador de Comunicaciones	**MA**	Personas encargadas de administrar, configurar y operar las redes de comunicación de datos que dan soporte al normal funcionamiento de los servicios internos.
P_DBA	Administrador de Bases de Datos	**MA**	Persona encargada de administrar, configurar y optimizar el rendimiento de las bases de datos que contienen los datos de los diferentes Sistemas de Información, así como velar por la seguridad de que éstos se mantengan confidenciales, disponibles e íntegros.
P_DES	Desarrolladores de Software	**M**	Personas encargadas de desarrollar y/o programar el software que se ajuste a las necesidades de la institución.

Tabla 30. Valoración cualitativa de acuerdo a los activos informáticos.

6.. Valoración de los Activos de Acuerdo a las Dimensiones de Seguridad

[D] DATOS/INFORMACIÓN

CÓDIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD			
		[D]	[I]	[C]	[A]
D_BCK	Copias de Seguridad de los Sistemas de Información	3		2	
D_CNT	Contratos		2		
D_HAC	Historial Académico		4	7	4
D_HCL	Historias Clínicas		6	7	6
D_HLB	Historial Laboral		3	2	
D_OVA	Objetos Virtuales de Aprendizaje	1			
D_PUB	Publicaciones	1			
D_RDG	Artículos de Revistas Digitales	1			
D_LOG	Registros de Actividad			2	
D_SRC	Códigos Fuentes		3	5	

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
D_BCK	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
D_CNT	[I]	2.pi1: Pudiera causar molestias a un individuo
D_HAC	[I][A][T]	4.pi2: Probablemente quebrante leyes o regulaciones
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
D_HCL	[I][A][T]	6.pi2: Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
D_HLB	[I]	3.lro: Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
D_OVA	[D]	1.pi1: Pudiera causar molestias a un individuo
D_PUB	[D]	1.pi1: Pudiera causar molestias a un individuo
D_RDG	[D]	1.pi1: Pudiera causar molestias a un individuo
D_LOG	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[T]	3.si: Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
D_SRC	[I]	3.olm: Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
	[C]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización

[S] SERVICIOS

CÓDIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
S_MAI	Correo Electrónico	3		2		
S_GID	Gestión de Identidades	5	2	2		4
S_INT	Servicios Internos	3				
S_WWW	Páginas w eb de acceso público	3				

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
S_MAI	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
S_GID	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[I]	2.pi1: Pudiera causar molestias a un individuo
	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[T]	4.crm: Dificulte la investigación o facilite la comisión de delitos
S_INT	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
S_WWW	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización

[SW] SOFTWARE

CÓDIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
SW_SWP	Software de Desarrollo Propio	3		4	7	4
SW_STD	Software Estándar	3		4	7	4
SW_MAI	Software para Correo Electrónico	5				1
SW_DBS	Gestores de Bases de Datos	7	7	7	7	
SW_OFM	Ofimática	1				
SW_AVS	Software de Antivirus			7		
SW_OPS	Sistemas Operativos	5	7			

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
SW_SWP	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	4.pi1: Probablemente afecte a un grupo de individuos
	[A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	[T]	4.crm: Dificulte la investigación o facilite la comisión de delitos
SW_STD	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
	[C]	4.pi1: Probablemente afecte a un grupo de individuos
	[A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
	[T]	4.crm: Dificulte la investigación o facilite la comisión de delitos
SW_MAI	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[T]	1.si: Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
SW_DBS	[D][I][A]	7.adm: Probablemente impediría la operación efectiva de la Organización
	[C]	7.lro: Probablemente cause un incumplimiento grave de una ley o regulación
SW_OFM	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
SW_AVS	[C]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
SW_OPS	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[I]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves

[HW] HARDWARE

CÓDIGO	DESCRIPCIÓN	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
HW_BCK	Dispositivos de Respaldo			2		3
HW_FRW	Firewall	7				
HW_ANT	Antenas	3				
HW_HOS	Servidores	5		7	7	
HW_PCM	Computadoras Portátiles de Uso Institucional	1				
HW_PCP	Computadoras de Escritorio de Uso Institucional	1				
HW_PRT	Impresoras	1				
HW_ROU	Router	5			7	
HW_SCN	Escáner	1				
HW_SWH	Switch	5			7	
HW_WAP	Puntos de Acceso Inalámbricos	1				

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
HW_BCK	[C]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización
	[T]	3.si: Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
HW_FRW	[D]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_ANT	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
HW_HOS	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[C][A]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_PCM/ HW_PCP	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización
HW_PRT/ HW_SCN	[D]	1.pi1: Pudiera causar molestias a un individuo
HW_ROU	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[T]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_SWH	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
	[T]	7.si: Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
HW_WAP	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización

[COM] COMUNICACIONES

CÓDIGO	DESCRI	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
COM_INT	Internet	3				
COM_LAN	Red de Área Local	5				
COM_WIF	Conectividad Inalámbrica	1				

CÓDIGO	DIMENSIÓN DE SEGURIDAD	DESCRIPCIÓN
COM_INT	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización
COM_LAN	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
COM_WIF	[D]	1.adm: Pudiera impedir la operación efectiva de una parte de la Organización

[AUX] EQUIPO AUXILIAR

CÓDIGO	DESCRIPCI	DIMENSIÓN DE SEGURIDAD			
		[D]	[I]	[C]	[A]
AUX_FBO	Fibra Óptica	5			
AUX_RCK	Rack	5			
AUX_PWR	Fuente de Alimentación	5			
AUX_UPS	Sistema de Alimentación	5			
AUX_WIR	Cableado Eléctrico	5			

CÓDIGO	DIMENSI	DESCRIPCIÓN
AUX_FBO	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_RCK	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_PWR	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_UPS	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
AUX_WIR	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización

[L] INSTALACIONES

CÓDIGO	DESCRIPCIÓN	DIMENSIÓN DE		
		[D]	[I]	[C]
L_SIT	Oficina de Sistemas de Información y Telemática	7		

CÓDIGO	DIMENSIÓN	DESCRIPCIÓN
L_SIT	[D]	7.adm: Probablemente impediría la operación efectiva de la Organización

[P] PERSONAL						
CÓDIGO	D	DIMENSIÓN DE SEGURIDAD				
		[D]	[I]	[C]	[A]	[T]
P_ADM	Administrador de Sistema	5				
P_COM	Administrador de Comunicaciones	5				
P_DBA	Administrador de Bases de Datos	5				
P_DES	Desarrolladores de Softw are	3				

CÓDIGO	DIMENSIÓN DE	DESCRIPCIÓN
P_ADM	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
P_COM	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
P_DBA	[D]	5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización
P_DES	[D]	3.adm: Probablemente impediría la operación efectiva de una parte de la Organización

Tabla 31. Activos de Acuerdo a las Dimensiones de Seguridad

INDICACIONES

a. Valoración de los activos

Los activos serán puntuados dependiendo de una tabla de ponderaciones en las que se evalúa la importancia para la organización:

Escala de valoración	Descripción	Valor
Muy alta	De vital importancia para los objetivos que persigue la organización	5
Alta	Altamente importante para la organización	4
Media	Importante para la organización	3
Baja	Importancia menor para el desarrollo de la organización	2
Muy baja	Irrelevante para efectos prácticos	1

Tabla N° 32 – Escala de puntuaciones de valores de los activos

b. Valoración de la degradación

Los activos serán puntuados dependiendo de una tabla de ponderaciones en las que se evalúa la confidencialidad, integridad, disponibilidad de cada uno de los activos.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

Puntuación	Disponibilidad	Integridad	Confidencialidad
5	Siempre	Extrema	Uso confidencial
4	Exenta por horas	Importante	Uso restringido
3	Exenta por 24 horas	Media	Semi restringido
2	Exenta por 48 horas	No importante	Uso interno
1	Exenta por varios días	Insignificante	Acceso público

Tabla N° 33 – Escala de puntuaciones de valores de la degradación

c. Degradación máxima

Al obtener cada uno de los puntajes asignados en la degradación, se determina el máximo valor de la degradación, dato que nos servirá para calcular el nivel de riesgo.

d. Valoración del impacto

El valor del impacto se determina por el promedio entre la degradación máxima y el valor del activo:

Impacto = (Degradación máxima + Valor del activo) / 2

e. Probabilidad

La probabilidad es la posibilidad de que se lleve a cabo una amenaza. Para la presente investigación, se determina en la siguiente escala:

Escala de valoración	Descripción	Valor
Muy alta	Nivel de probabilidad del activo es muy alta	5
Alta	Nivel de probabilidad del activo es alta	4
Media	Nivel de probabilidad del activo es media	3
Baja	Nivel de probabilidad del activo es baja	2
Muy baja	Nivel de probabilidad del activo es muy baja	1

Tabla N° 34 – Escala de puntuaciones de la probabilidad

f. Valoración del riesgo

El valor del riesgo se determina por el promedio entre el impacto y la probabilidad:

$$Riesgo = (Impacto + Probabilidad) / 2$$

7. Identificación y Valoración de Amenazas. De acuerdo a las amenazas que se identifican en MAGERIT, éstas se establecen para cada activo determinando su probabilidad o frecuencia de ocurrencia y el impacto que tiene en cada una de las dimensiones de seguridad.

[S] SERVICIOS						
ACTIVOS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
S-SERVICIOS						
Correo Electrónico						
5.3.1. [E.1] Errores de los usuarios	50	0%	0%	0%	0%	0%
5.3.10. [E.15] Alteración accidental de la información	10	0%	75%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.3.9. [E.14] Escapes de información	50	0%	0%	100%	0%	0%
5.4.11. [A.13] Repudio	5	0%	0%	0%	100%	20%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	100%	0%	0%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	10	0%	0%	100%	0%	0%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.3. [A.5] Suplantación de la identidad del usuario	5	0%	0%	75%	75%	20%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	100%	75%	0%	0%
5.4.8. [A.10] Alteración de secuencia	5	0%	100%	0%	100%	0%
5.4.9. [A.11] Acceso no autorizado	10	0%	0%	100%	0%	0%
Gestión de Identidades						
5.3.10. [E.15] Alteración accidental de la información	5	0%	100%	0%	100%	20%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.3.9. [E.14] Escapes de información	50	0%	0%	50%	0%	0%
5.4.11. [A.13] Repudio	5	0%	0%	0%	50%	0%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	100%	100%	0%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	5	0%	0%	100%	0%	0%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.3. [A.5] Suplantación de la identidad del usuario	5	0%	0%	100%	75%	20%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	100%	75%	100%	20%
5.4.9. [A.11] Acceso no autorizado	5	0%	0%	100%	0%	0%
Páginas web de acceso público						
5.3.10. [E.15] Alteración accidental de la información	10	0%	0%	50%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
Servicios Internos						
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	50	100%	0%	0%	0%	0%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%

[SW] SOFTWARE						
ACTIVOS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
SW-SOFTWARE						
Gestores de Bases de Datos						
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	75%	75%	0%	75%
5.3.1. [E.1] Errores de los usuarios	10	5%	5%	5%	0%	0%
5.3.10. [E.15] Alteración accidental de la información	5	75%	75%	0%	75%	0%
5.3.11. [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12. [E.19] Fugas de información	5	0%	100%	100%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	10	50%	75%	75%	0%	0%
5.3.2. [E.2] Errores del administrador	10	50%	50%	50%	0%	0%
5.3.6. [E.8] Difusión de software dañino	5	5%	5%	5%	0%	0%
5.3.9. [E.14] Escapes de información	5	0%	0%	75%	0%	0%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	100%	100%	100%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	5	0%	75%	100%	0%	0%
5.4.16. [A.22] Manipulación de programas	5	0%	50%	50%	0%	0%
5.4.3. [A.5] Suplantación de la identidad del usuario	10	0%	0%	50%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	100%	0%
5.4.5. [A.7] Uso no previsto	5	75%	75%	75%	75%	0%
5.4.6. [A.8] Difusión de software dañino	5	5%	5%	5%	0%	0%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	0%	10%	0%	0%	0%
5.4.8. [A.10] Alteración de secuencia	5	50%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	100%	100%	100%	100%	0%
Ofimática						
5.2.6. [I.5] Avería de origen físico o lógico	10	10%	0%	0%	0%	0%
5.3.1. [E.1] Errores de los usuarios	50	5%	0%	0%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	50	50%	0%	0%	0%	0%
5.3.6. [E.8] Difusión de software dañino	10	50%	0%	0%	75%	0%
5.4.5. [A.7] Uso no previsto	50	0%	0%	0%	0%	0%
5.4.6. [A.8] Difusión de software dañino	5	50%	0%	50%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	50%	0%	0%	0%	0%
Sistemas Operativos						
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.3.1. [E.1] Errores de los usuarios	10	75%	0%	0%	0%	20%
5.3.10. [E.15] Alteración accidental de la información	10	50%	20%	20%	0%	0%
5.3.11. [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12. [E.19] Fugas de información	5	0%	0%	75%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	5	50%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	75%	0%	0%	0%	20%
5.3.6. [E.8] Difusión de software dañino	10	75%	50%	0%	0%	0%
5.3.9. [E.14] Escapes de información	5	0%	0%	5%	0%	0%

5.4.13. [A.15] Modificación deliberada de la información	5	75%	100%	100%	0%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	5	0%	0%	100%	0%	0%
5.4.16. [A.22] Manipulación de programas	5	0%	0%	50%	0%	50%
5.4.3. [A.5] Suplantación de la identidad del usuario	5	100%	100%	100%	0%	20%
5.4.4. [A.6] Abuso de privilegios de acceso	5	100%	100%	100%	0%	20%
5.4.5. [A.7] Uso no previsto	5	50%	0%	0%	0%	0%
5.4.6. [A.8] Difusión de software dañino	5	75%	0%	0%	0%	0%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	50%	0%	0%	0%	0%
5.4.8. [A.10] Alteración de secuencia	5	50%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	75%	75%	0%	20%
Software de Antivirus						
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.3.1. [E.1] Errores de los usuarios	50	50%	0%	0%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	10	50%	0%	0%	0%	0%
5.3.6. [E.8] Difusión de software dañino	10	75%	0%	0%	75%	0%
5.4.5. [A.7] Uso no previsto	5	20%	0%	0%	0%	0%
5.4.6. [A.8] Difusión de software dañino	5	50%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	100%	0%	0%	0%	0%
Software de Desarrollo Propio						
5.2.6. [I.5] Avería de origen físico o lógico	5	20%	0%	0%	0%	0%
5.3.1. [E.1] Errores de los usuarios	50	0%	0%	5%	0%	0%
5.3.10. [E.15] Alteración accidental de la información	5	0%	50%	0%	0%	0%
5.3.11. [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12. [E.19] Fugas de información	5	0%	0%	50%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	50	20%	0%	0%	0%	20%
5.3.2. [E.2] Errores del administrador	10	20%	20%	20%	0%	0%
5.3.6. [E.8] Difusión de software dañino	10	10%	0%	0%	0%	0%
5.3.9. [E.14] Escapes de información	10	0%	20%	20%	0%	0%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	50%	100%	100%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	5	0%	5%	5%	0%	0%
5.4.16. [A.22] Manipulación de programas	5	0%	75%	75%	75%	20%
5.4.3. [A.5] Suplantación de la identidad del usuario	5	0%	50%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	100%	100%	100%	0%
5.4.5. [A.7] Uso no previsto	5	5%	0%	0%	0%	0%
5.4.6. [A.8] Difusión de software dañino	10	50%	0%	0%	0%	0%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	50%	0%	0%	0%	0%
5.4.8. [A.10] Alteración de secuencia	5	100%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	100%	100%	100%	0%	0%

Software Estándar						
5.2.6. [I.5] Avería de origen físico o lógico	5	20%	0%	0%	0%	0%
5.3.1. [E.1] Errores de los usuarios	50	0%	0%	5%	0%	0%
5.3.10. [E.15] Alteración accidental de la información	5	0%	50%	0%	0%	0%
5.3.11. [E.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.3.12. [E.19] Fugas de información	5	0%	0%	50%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (softw are)	50	20%	0%	0%	0%	20%
5.3.2. [E.2] Errores del administrador	10	20%	20%	20%	0%	0%
5.3.6. [E.8] Difusión de softw are dañino	10	10%	0%	0%	0%	0%
5.3.9. [E.14] Escapes de información	5	0%	20%	20%	0%	0%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	50%	100%	100%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	5	0%	5%	5%	0%	0%
5.4.16. [A.22] Manipulación de programas	5	0%	75%	75%	75%	20%
5.4.3. [A.5] Suplantación de la identidad del usuario	5	0%	50%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	100%	100%	100%	0%
5.4.5. [A.7] Uso no previsto	5	5%	0%	0%	0%	0%
5.4.6. [A.8] Difusión de softw are dañino	10	50%	0%	0%	0%	0%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	50%	0%	0%	0%	0%
5.4.8. [A.10] Alteración de secuencia	5	100%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	100%	100%	100%	0%	0%
Software para Correo Electrónico						
5.2.6. [I.5] Avería de origen físico o lógico	10	50%	0%	0%	0%	0%
5.3.1. [E.1] Errores de los usuarios	70	5%	0%	0%	0%	0%
5.3.10. [E.15] Alteración accidental de la información	5	20%	0%	0%	0%	0%
5.3.11. [E.18] Destrucción de información	1	100%	0%	0%	0%	0%
5.3.12. [E.19] Fugas de información	50	0%	0%	100%	0%	0%
5.3.13. [E.20] Vulnerabilidades de los programas (softw are)	10	20%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	10	50%	0%	0%	0%	0%
5.3.6. [E.8] Difusión de softw are dañino	5	20%	0%	20%	0%	0%
5.3.9. [E.14] Escapes de información	5	0%	75%	75%	0%	0%
5.4.13. [A.15] Modificación deliberada de la información	5	0%	50%	50%	0%	0%
5.4.14. [A.18] Destrucción de información	5	100%	0%	0%	0%	0%
5.4.15. [A.19] Divulgación de información	5	0%	0%	0%	100%	0%
5.4.16. [A.22] Manipulación de programas	5	20%	0%	0%	0%	0%
5.4.3. [A.5] Suplantación de la identidad del usuario	5	0%	100%	100%	100%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	75%	100%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	5%	0%	0%	0%	0%
5.4.6. [A.8] Difusión de softw are dañino	5	20%	0%	0%	0%	0%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	5	0%	0%	75%	75%	0%
5.4.8. [A.10] Alteración de secuencia	5	0%	75%	75%	75%	0%
5.4.9. [A.11] Acceso no autorizado	5	50%	75%	75%	0%	20%

[HW] HARDWARE

ACTIVOS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
HW-HARDWARE						
Antenas						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	5%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	50%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	5	5%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o	5	5%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardw are)	5	75%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
Computadoras de Escritorio de Uso Institucional						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardw are)	10	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	20	50%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Computadoras Portátiles de Uso Institucional						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	10%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardw are)	10	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	20	50%	0%	0%	0%	0%

5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Dispositivos de Respaldo						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardw are)	5	50%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	75%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	5	50%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	50%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Escáner						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardw are)	10	75%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%

Firewall						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	20	75%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Impresoras						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	10	75%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
Puntos de Acceso Inalámbricos						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardware)	5	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	20	75%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

Router						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardw are)	5	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	20	75%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Servidores						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardw are)	5	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	20	75%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%
Switch						
5.2.1. [I.1] Fuego	5	100%	0%	0%	0%	0%
5.2.2. [I.2] Daños por agua	5	100%	0%	0%	0%	0%
5.2.6. [I.5] Avería de origen físico o lógico	5	75%	0%	0%	0%	0%
5.2.7. [I.6] Corte del suministro eléctrico	50	100%	0%	0%	0%	0%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	10	75%	0%	0%	0%	0%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos (hardw are)	5	75%	0%	0%	0%	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	5	100%	0%	0%	0%	0%
5.3.17. [E.25] Pérdida de equipos	5	100%	0%	0%	0%	0%
5.3.2. [E.2] Errores del administrador	20	75%	0%	0%	0%	0%
5.4.17. [A.23] Manipulación de los equipos	5	0%	75%	0%	0%	20%
5.4.18. [A.24] Denegación de servicio	5	100%	0%	0%	0%	0%
5.4.19. [A.25] Robo	5	100%	0%	0%	0%	0%
5.4.4. [A.6] Abuso de privilegios de acceso	5	0%	0%	75%	0%	0%
5.4.5. [A.7] Uso no previsto	5	75%	0%	0%	0%	0%
5.4.9. [A.11] Acceso no autorizado	5	75%	0%	75%	75%	0%

[P] PERSONAL						
ACTIVOS	FRECUENCIA	[D]	[I]	[C]	[A]	[T]
P-PERSONAL						
Administrador de Bases de Datos						
5.3.12. [E.19] Fugas de información	5	0%	0%	0%	75%	0%
5.3.18. [E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
5.3.5. [E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%
5.4.22. [A.28] Indisponibilidad del personal	5	50%	0%	0%	0%	0%
Administrador de Comunicaciones						
5.3.12. [E.19] Fugas de información	5	0%	0%	0%	75%	0%
5.3.18. [E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
5.3.5. [E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%
5.4.22. [A.28] Indisponibilidad del personal	5	50%	0%	0%	0%	0%
Administrador de Sistema						
5.3.12. [E.19] Fugas de información	5	0%	0%	0%	75%	0%
5.3.18. [E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
5.3.5. [E.7] Deficiencias en la organización	5	75%	0%	0%	0%	0%
5.4.22. [A.28] Indisponibilidad del personal	5	50%	0%	0%	0%	0%
Desarrolladores de Software						
5.3.12. [E.19] Fugas de información	5	0%	0%	0%	75%	0%
5.3.18. [E.28] Indisponibilidad del personal	10	50%	0%	0%	0%	0%
5.3.5. [E.7] Deficiencias en la organización	5	50%	0%	0%	0%	0%
5.4.22. [A.28] Indisponibilidad del personal	5	50%	0%	0%	0%	0%

Tabla Nro. 35 – Identificación y Valoración de Amenazas

8. **Riesgo Potencial.** Se determina el nivel de riesgo potencial de cada uno de los activos en una valoración cualitativa de acuerdo a las zonas de riesgo que propone MAGERIT. El riesgo es calculado en base al impacto que tiene cada activo y según el tipo de amenaza general (Naturales, Industriales, Errores No Intencionados, Ataques Intencionados); es decir, no se calcula en cada dimensión de seguridad (Disponibilidad, Integridad, Confidencialidad, Autenticidad y Trazabilidad). Sólo se toma en cuenta que ocurra cualquier amenaza dentro de su respectiva categoría y se escoge el peor de los casos.

[SW] SOFTWARE

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
SW_SWP	Software de Desarrollo Propio	MA	M	I*, E*, A*	R_SW_SWP	MA
SW_STD	Software Estándar	MA	M	I*, E*, A*	R_SW_STD	MA
SW_MAI	Software para Correo Electrónico	A	A	I*, E*, A*	R_SW_MAI	MA
SW_DBS	Gestores de Bases de Datos	MA	B	I*, E*, A*	R_SW_DBS	MA
SW_OFM	Ofimática	B	M	I*, E*, A*	R_SW_OFM	B
SW_AVS	Software de Antivirus	M	M	I*, E*, A*	R_SW_AVS	M
SW_OPS	Sistemas Operativos	M	B	I*, E*, A*	R_SW_OPS	M

[HW] HARDWARE

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
HW_BCK	Dispositivos de Respaldo	MA	M	I*, E*, A*	R_HW_BCK	MA
HW_FRW	Firewall	MA	M	I*, E*, A*	R_HW_FRW	MA
HW_ANT	Antenas	A	MB	I*, E*, A*	R_HW_ANT	M
HW_HOS	Servidores	MA	M	I*, E*, A*	R_HW_HOS	MA
HW_PCM	Computadoras Portátiles de Uso Institucional	B	M	I*, E*, A*	R_HW_PCM	B
HW_PCP	Computadoras de Escritorio de Uso Institucional	B	M	I*, E*, A*	R_HW_PCP	B
HW_PRT	Impresoras	MB	M	I*, E*, A*	R_HW_PRT	MB
HW_ROU	Router	A	M	I*, E*, A*	R_HW_ROU	A
HW_SCN	Escáner	MB	M	I*, E*, A*	R_HW_SCN	MB
HW_SWH	Switch	A	M	I*, E*, A*	R_HW_SWH	A
HW_WAP	Puntos de Acceso Inalámbricos	B	M	I*, E*, A*	R_HW_WAP	B

[COM] COMUNICACIONES

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
COM_INT	Internet	A	A	E*, A*	R_COM_INT	MA
COM_LAN	Red de Área Local	MA	A	E*, A*	R_COM_LAN	MA
COM_WIF	Conectividad Inalámbrica	B	A	E*, A*	R_COM_WIF	M

[AUX] EQUIPO AUXILIAR

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
AUX_FBO	Fibra Óptica	MA	M	I*, E*, A*	R_AUX_FBO	MA
AUX_RCK	Rack	A	M	I*, E*, A*	R_AUX_RCK	A
AUX_PWR	Fuente de Alimentación	MA	M	I*, E*, A*	R_AUX_PWR	MA
AUX_UPS	Sistema de Alimentación Ininterrumpida	A	M	I*, E*, A*	R_AUX_UPS	A
AUX_WIR	Cableado Eléctrico	MA	M	I*, E*, A*	R_AUX_WIR	MA

[L] INSTALACIONES

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
L_SIT	Oficina de Sistemas de Información y Telemática	MA	MB	N*, I*, E*, A*	R_L_SIT	A

[P] PERSONAL

CÓDIGO	ACTIVO	IMPACTO	PROBABILIDAD	AMENAZA	RIESGO_ID	RIESGO
P_ADM	Administrador de Sistema	A	B	E*, A*	R_P_ADM	A
P_COM	Administrador de Comunicaciones	MA	B	E*, A*	R_P_COM	MA
P_DBA	Administrador de Bases de Datos	MA	B	E*, A*	R_P_DBA	MA
P_DES	Desarrolladores de Softw are	M	B	E*, A*	R_P_DES	M

Tabla Nro. 36 – Riego Potencial

[S] SERVICIOS

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A NTP ISO/IEC 27001:2014
S_MAI	Correo Electrónico	E*, A*	R_S_MAI	A	DC	▪ S.email Protección del correo electrónico ▪ S.w w w Protección de servicios y aplicaciones w eb	▪ A.13.2.3 ▪ A.12.5.1
S_GID	Gestión de Identidades	E*, A*	R_S_GID	MA	DC	▪ S.A Aseguramiento de la disponibilidad ▪ S.dir Protección del directorio ▪ S.SC Se aplican perfiles de seguridad	▪ A.17.1.* ▪ A.8.2.* ▪ A.9.4.3
S_INT	Servicios Internos	E*, A*	R_S_INT	MA	DC	▪ S.A Aseguramiento de la disponibilidad ▪ S.dns Protección del servidor de nombres de dominio (DNS)	▪ A.17.1.* ▪ A.9.4.*
S_WWW	Páginas w eb de acceso público	E*, A*	R_S_WWW	A	DC	▪ S.A Aseguramiento de la disponibilidad ▪ S.w w w Protección de servicios y aplicaciones w eb	▪ A.17.1.* ▪ A.12.5.1

[SW] SOFTWARE

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A NTP ISO/IEC 27001:2014
SW_SWP	Softw are de Desarrollo Propio	**I*, E*, A***	R_SW_SWP	**MA**	**DC**	▪ SW Protección de las Aplicaciones Informáticas ▪ SW.A Copias de seguridad (backup) ▪ SW.SC Se aplican perfiles de seguridad ▪ SW.start Puesta en producción	▪ A.14.2.* ▪ A.12.3.1
SW_STD	Softw are Estándar	**I*, E*, A***	R_SW_STD	**MA**	**DC**	▪ SW Protección de las Aplicaciones Informáticas ▪ SW.A Copias de seguridad (backup) ▪ SW.SC Se aplican perfiles de seguridad	▪ A.14.2.* ▪ A.12.3.1
SW_MAI	Softw are para Correo Electrónico	**I*, E*, A***	R_SW_MAI	**MA**	**DC**	▪ SW Protección de las Aplicaciones Informáticas ▪ SW.SC Se aplican perfiles de seguridad	▪ A.14.2.*
SW_DBS	Gestores de Bases de Datos	**I*, E*, A***	R_SW_DBS	**MA**	**DC**	▪ SW Protección de las Aplicaciones Informáticas ▪ SW.A Copias de seguridad (backup) ▪ SW.CM Cambios (actualizaciones y mantenimiento) ▪ SW.SC Se aplican perfiles de seguridad	▪ A.14.2.* ▪ A.12.3.1
SW_OFM	Ofimática	**I*, E*, A***	R_SW_OFM	**B**	**DC**	▪ SW Protección de las Aplicaciones Informáticas ▪ SW.A Copias de seguridad (backup) ▪ SW.SC Se aplican perfiles de seguridad	▪ A.14.2.* ▪ A.12.3.1
SW_AVS	Softw are de Antivirus	**I*, E*, A***	R_SW_AVS	**M**	**DC**	▪ SW Protección de las Aplicaciones Informáticas ▪ SW.SC Se aplican perfiles de seguridad	▪ A.12.2.1
SW_OPS	Sistemas Operativos	**I*, E*, A***	R_SW_OPS	**M**	**DC**	▪ SW Protección de las Aplicaciones Informáticas ▪ SW.A Copias de seguridad (backup) ▪ SW.SC Se aplican perfiles de seguridad	▪ A.14.2.* ▪ A.12.3.1 ▪ A.12.2.1 ▪ A.12.5.1 ▪ A.12.6.*

[HW] HARDWARE

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A NTP ISO/IEC 27001:2014
HW_BCK	Dispositivos de Respaldo	**I*, E*, A***	R_HW_BCK	**MA**	**DC**	▪ HW Protección de los Equipos Informáticos	▪ A.11.1.1 ▪ A.11.1.2 ▪ A.11.2.1 ▪ A.12.3.1
HW_FRW	Firew all	**I*, E*, A***	R_HW_FRW	**MA**	**DC**	▪ HW Protección de los Equipos Informáticos ▪ HW.A Aseguramiento de la disponibilidad ▪ HW.SC Se aplican perfiles de seguridad	▪ A.11.1.1 ▪ A.11.1.2 ▪ A.11.2.1
HW_ANT	Antenas	**I*, E*, A***	R_HW_ANT	**M**	**DC**	▪ HW Protección de los Equipos Informáticos	▪ A.11.1.1 ▪ A.11.1.2 ▪ A.11.2.1
HW_HOS	Servidores	**I*, E*, A***	R_HW_HOS	**MA**	**DC**	▪ HW Protección de los Equipos Informáticos ▪ HW.A Aseguramiento de la disponibilidad ▪ HW.SC Se aplican perfiles de seguridad	▪ A.11.1.1 ▪ A.11.1.2 ▪ A.11.2.1
HW_PCM	Computadoras Portátiles de Uso Institucional	**I*, E*, A***	R_HW_PCM	**B**	**DC**	▪ HW Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1
HW_PCP	Computadoras de Escritorio de Uso Institucional	**I*, E*, A***	R_HW_PCP	**B**	**DC**	▪ HW Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1
HW_PRT	Impresoras	**I*, E*, A***	R_HW_PRT	**MB**	**A**	▪ HW Protección de los Equipos Informáticos ▪ HW.print Reproducción de documentos	A.11.1.1 A.11.1.2 A.11.2.1

HW_ROU	Router	**I*, E*, A***	R_HW_ROU	**A**	**DC**	▪ HW Protección de los Equipos Informáticos ▪ HW.A Aseguramiento de la disponibilidad ▪ HW.SC Se aplican perfiles de seguridad	A.11.1.1 A.11.1.2 A.11.2.1
HW_SCN	Escáner	**I*, E*, A***	R_HW_SCN	**MB**	**A**	▪ HW Protección de los Equipos Informáticos	A.11.1.1 A.11.1.2 A.11.2.1
HW_SWH	Switch	**I*, E*, A***	R_HW_SWH	**A**	**DC**	▪ HW Protección de los Equipos Informáticos ▪ HW.A Aseguramiento de la disponibilidad ▪ HW.SC Se aplican perfiles de seguridad	A.11.1.1 A.11.1.2 A.11.2.1
HW_WAP	Puntos de Acceso Inalámbricos	**I*, E*, A***	R_HW_WAP	**B**	**DC**	▪ HW Protección de los Equipos Informáticos ▪ HW.A Aseguramiento de la disponibilidad	A.11.1.1 A.11.1.2 A.11.2.1

[COM] COMUNICACIONES

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
COM_INT	Internet	**E*, A***	R_COM_INT	**MA**	**DC**	▪ COM Protección de las Comunicaciones ▪ COM.A Aseguramiento de la disponibilidad ▪ COM.C Protección criptográfica de la confidencialidad de los datos intercambiados	▪ A.9.1.2 ▪ A.10.1.1 ▪ A.11.2.3 ▪ A.13.1.* ▪ A.13.2.1
COM_LAN	Red de Área Local	**E*, A***	R_COM_LAN	**MA**	**DC**	▪ COM Protección de las Comunicaciones ▪ COM.A Aseguramiento de la disponibilidad ▪ COM.C Protección criptográfica de la confidencialidad de los datos intercambiados	▪ A.9.1.2 ▪ A.10.1.1 ▪ A.11.2.3 ▪ A.13.1.* ▪ A.13.2.1 ▪ A.13.2.2
COM_WIF	Conectividad Inalámbrica	**E*, A***	R_COM_WIF	**M**	**DC**	▪ COM Protección de las Comunicaciones ▪ COM.A Aseguramiento de la disponibilidad ▪ COM.C Protección criptográfica de la confidencialidad de los datos intercambiados ▪ COM.w ifi Seguridad Wireless(WiFi)	▪ A.9.1.2 ▪ A.10.1.1 ▪ A.13.1.* ▪ A.13.2.1 ▪ A.13.2.2

[AUX] EQUIPO AUXILIAR

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A ISO/IEC 27001:2013
AUX_FBO	Fibra Óptica	**I*, E*, A***	R_AUX_FBO	**MA**	**DC**	▪ AUX.A Aseguramiento de la disponibilidad ▪ AUX.AC Climatización ▪ AUX.power Suministro eléctrico	▪ A.11.2.2 ▪ A.11.2.3 ▪ A.11.2.6 ▪ A.13.2.1
AUX_RCK	Rack	**I*, E*, A***	R_AUX_RCK	**A**	**DC**	▪ AUX.A Aseguramiento de la disponibilidad ▪ AUX.AC Climatización ▪ AUX.power Suministro eléctrico	▪ A.11.2.2 ▪ A.11.2.3 ▪ A.13.2.1
AUX_PWR	Fuente de Alimentación	**I*, E*, A***	R_AUX_PWR	**MA**	**DC**	▪ AUX.A Aseguramiento de la disponibilidad ▪ AUX.AC Climatización ▪ AUX.power Suministro eléctrico	▪ A.11.2.2 ▪ A.11.2.3 ▪ A.13.2.1
AUX_UPS	Sistema de Alimentación Ininterrumpida	**I*, E*, A***	R_AUX_UPS	**A**	**DC**	▪ AUX.A Aseguramiento de la disponibilidad ▪ AUX.AC Climatización ▪ AUX.power Suministro eléctrico	▪ A.11.2.2 ▪ A.11.2.3 ▪ A.13.2.1
AUX_WIR	Cableado Eléctrico	**I*, E*, A***	R_AUX_WIR	**MA**	**DC**	▪ AUX.A Aseguramiento de la disponibilidad ▪ AUX.power Suministro eléctrico ▪ AUX.wires Protección del cableado	▪ A.11.2.2 ▪ A.11.2.3 ▪ A.11.2.6 ▪ A.13.2.1

Tabla N° 37 Plan de tratamiento de riesgos

[L] INSTALACIONES

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A NTP ISO/IEC 27001:2014
L_DGIyE	Oficina de Sistemas de Información y Telemática	**N*, I*, E*, A***	R_L_SIT	**A**	**AS**	▪ L. Protección de las Instalaciones ▪ L.A Aseguramiento de la disponibilidad ▪ L.AC Control de los accesos físicos	▪ A.11.1.* ▪ A.17.*

[P] PERSONAL

CÓDIGO	ACTIVO	AMENAZA	RIESGO_ID	RIESGO	TRATAMIENTO	SALVAGUARDAS	ANEXO A NTP ISO/IEC 27001:2014
P_ADM	Administrador de Sistema	**E*, A***	R_P_ADM	**A**	**TT**	▪ PS Gestión del Personal ▪ PS.A Aseguramiento de la disponibilidad ▪ PS.AT Formación y concienciación	▪ A.7.*
P_COM	Administrador de Comunicaciones	**E*, A***	R_P_COM	**MA**	**TT**	▪ PS Gestión del Personal ▪ PS.A Aseguramiento de la disponibilidad ▪ PS.AT Formación y concienciación	▪ A.7.*
P_DBA	Administrador de Bases de Datos	**E*, A***	R_P_DBA	**MA**	**TT**	▪ PS Gestión del Personal ▪ PS.A Aseguramiento de la disponibilidad ▪ PS.AT Formación y concienciación	▪ A.7.*
P_DES	Desarrolladores de Softw are	**E*, A***	R_P_DES	**M**	**TT**	▪ PS Gestión del Personal ▪ PS.A Aseguramiento de la disponibilidad ▪ PS.AT Formación y concienciación	▪ A.7.*

7. SOPORTE

OFICINA GENERAL DE INFORMÁTICA Y ESTADISTICA

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

DECLARACIÓN DE APLICABILIDAD

Código del Documento	SGSIUNDAC01
Versión	1.0
Fecha de Versión	10/07/2018
Propietario	DGIyE-UNDAC
Nivel de Confidencialidad	Baja

7.1 RECURSOS

La implementación de un SGSI pasa necesariamente por disponer de los recursos necesarios para que el sistema de gestión pueda llevarse a cabo según lo planeado.

Sin embargo, la norma no dedica demasiados esfuerzos en los requerimientos para este punto donde se nos pone como requisito:

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de la seguridad de la información.

Sin embargo, la norma a lo largo de toda su redacción deja claro que la responsabilidad de la organización y en concreto de la dirección es la de garantizar en todo momento la disponibilidad de los recursos para llevar a cabo las tareas y cumplir con los objetivos de la seguridad de la información

Dentro del enfoque de procesos la norma NTP ISO/IEC 27001 2014, requiere que se cumplan con las necesidades de recursos para mantener la gestión de la Seguridad a lo largo de todo el ciclo de vida, desde su planificación hasta la revisión y mejora del sistema

Para ello se deberán disponer de medios como:

Inversión económica:

Queda claro que la seguridad no nos va a salir gratis, es por ello que se requerirá un cierto nivel de inversión acorde con la evaluación de riesgos y los criterios para asumir o minimizar los distintos niveles de riesgo

Instalaciones:

El lugar e instalaciones de una organización deben estar preparados para ofrecer niveles de seguridad proporcionales al riesgo al que está expuesta una organización.

Equipos:

En ciertos casos deberemos de contar con equipos específicos para proporcionar sistemas de defensa o detección de intrusiones en nuestros sistemas de información y así mejorar los niveles de seguridad.

Personas:

Dentro de una organización podremos definir responsabilidades para todos los empleados en relación a la seguridad de la información, pero este no será su objetivo principal sino un medio por el cual podrán desempeñar mejor sus funciones contando con la ayuda de la seguridad de la información para conseguir sus objetivos comerciales

En este escenario podremos contar con personas para que asuman responsabilidades para cuidar de la seguridad de la información como su cometido y función principal. En este caso estamos hablando de personas o recursos humanos ligados exclusivamente a las tareas del SGSI.

7.2 COMPETENCIA.

Los requisitos de la norma para determinar la competencia del personal para llevar a cabo las tareas del SGSI se centran en:

- Determinar la competencia necesaria del personal para llevar a cabo el trabajo que afecta al SGSI.
- Asegurar que las personan sean competentes sobre la base de la educación, capacitación o experiencia adecuadas
- Demostrar mediante la información documentada que sea necesaria la competencia del personal en materia de Seguridad de la Información Para garantizar el cumplimiento de estos requisitos podríamos utilizar una matriz de habilidades o requisitos mínimos de cualificación en el módulo de

Recursos Humanos para administrar y realizar un seguimiento de los requisitos anteriormente expuestos

- Una vez establecido, es importante mantener la matriz de requisitos de cualificación y, actualice la información cuando se haya realizado alguna capacitación o formación, agregue nuevos requisitos de habilidades si es necesario y siempre esté vigilante a cualquier incumplimiento.
- La necesidad de competencia no solo se aplica al personal interno, sino que cuando necesite cubrir cualquier responsabilidad o función por un contratista externo, por ejemplo, deberá tener las mismas consideraciones y documentar completamente cómo cumplen los requisitos del SGSI.
- Uno de los medios más utilizados es la realización de capacitaciones tanto internas como externas. En este punto resulta de lo más conveniente asegurarse de que la capacitación que recibida, ya sea interna o externa, cumple con los objetivos propuestos.
- Determinar la competencia del personal significa también que después de las capacitaciones se establezca algún protocolo para evaluar si las personas después de un ciclo formativo han mejorado realmente su capacitación y han mejorado en el desempeño de sus tareas
- Parte de la gestión del proceso de capacitación (y del proceso de comunicación interna) debe hacer que el personal esté al tanto de su papel en la empresa y cómo contribuyen a cumplir los requisitos de la seguridad de la Información
- Proporcionar capacitación o tomar medidas para asegurar que se logre la competencia
- Necesita monitorear regularmente (usted decide) los niveles de competencia y decidir dónde están las brechas.
- A continuación, debe planificar qué va a hacer con respecto a esas brechas.

La importancia de la capacitación

Es de reconocer que los niveles de capacitación en ISO 27001 o sistemas de gestión de la seguridad de la información en las empresas son generalmente muy mejorables actualmente. Además, las posibilidades de dedicar una persona en exclusiva al mantenimiento y gestión del SGSI están al alcance de pocas organizaciones. Es por ello, que cada vez cobra mayor fuerza la consultoría en ISO 27001 realizada por una empresa externa ya que muchas

veces nos aporta no solo la formación necesaria para nuestros cuadros intermedios, sino que además nos mantiene actualizado en los cambios normativos y requisitos de la norma.

7.3 CONCIENCIACIÓN.

Este punto del capítulo 7 se refiere básicamente a que las personas que gestionan el SGSI deben conocer todo lo relacionado con las políticas y los controles que se llevan a cabo en él.

En principio debemos hacernos estas preguntas para saber cómo hemos de abordar este punto

Las personas con responsabilidades en la seguridad de la información

¿Han leído y entendido la política de seguridad de la información de la organización?

¿Entienden la importancia de mantener y mejorar continuamente un SGSI?

¿Entienden las implicaciones de no mantener el SGSI y cumplir los requisitos de la norma ISO 27001?

Pero como todo en un sistema de gestión hay que no solo hacerlo sino también estar preparados para demostrarlo en una auditoria de certificación.

Veamos más en profundidad como afrontar el cumplimiento de este requisito

Los puntos concretos a tener en cuenta podrían ser:

1 .- Establezca un programa de formación y sensibilización o concienciación

2 .-Programe distintas actividades de sensibilización

3.- Utilice todos los medios de comunicación a su alcance, incluyendo charlas presenciales, videoconferencias online, formaciones online adaptadas al ritmo y tiempos de los empleados, otros

4 .-Mantenga informados a todos de las actualizaciones en temas de seguridad tomando en cuenta lo aprendido en los incidentes de seguridad de la información,

5.- Asegúrese de repartir con periodicidad las formaciones y comunicaciones de seguridad para asegurarse que incluyen a todos los empleados y a las nuevas incorporaciones Incluya a los contratistas que sea necesario para garantizar que todos los que realizan trabajos que pueden comprometer la seguridad de la información estén incluidos.

7.4 LA COMUNICACIÓN

La cláusula establece que “la organización debe determinar la necesidad de comunicaciones internas y externas relevantes para el SGSI, lo que incluye”:

Qué comunicar;

Cuando comunicar;

Con quien comunicarse;

Quién se comunicará; y

Los procesos por los cuales se efectuará la comunicación.

Un posible procedimiento que describa las diferentes formas de comunicación, es decir, reuniones formales o informales, lo que esperamos que se analice (puede usar las plantillas de agenda como una guía para las reuniones más formalizadas) y quiénes deberían ser las comunicaciones podría ser el camino para cumplir con este requisito

Una forma sencilla de realizar esta tarea seria mantener una reunión periódica para ponernos al día a la cual podemos añadir un informa que se asocie al perfil de los empleados como una habilidad. Así podemos acometer a la vez la comunicación que ayuda tanto la competencia como la concienciación del personal.

7.5 INFORMACIÓN DOCUMENTADA

Finalmente, están los requisitos para la "información documentada". La nueva norma se refiere a "información documentada" en lugar de "documentos y registros" y requiere que se conserven como evidencia de competencia

Este requisito se relaciona con la creación y actualización de información documentada y con su control. Aunque ya no hay una lista de documentos obligatoria establecida en una sola clausula nos encontramos que NTP ISO/IEC 27001:2014 pone el énfasis en el contenido en lugar del título del documento.

8 OPERACIÓN

OFICINA GENERAL DE INFORMÁTICA Y ESTADISTICA
UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN
PLANIFICACIÓN Y CONTROL OPERACIONAL

Código del Documento	SGSIUNDAC01
Versión	1.0
Fecha de Versión	10/07/2018
Propietario	DGIyE-UNDAC
Nivel de Confidencialidad	Baja

3. PROPÓSITO, ALCANCE Y USUARIOS

El propósito de este documento es definir cuáles controles son los apropiados para ser implementados en la DGIyE de la UNDAC, los objetivos de estos controles y cómo son implementados.

Este documento incluye todos los controles listados en el Anexo del estándar ISO/IEC 27001:2014. Los controles son aplicables a todo el alcance del Sistema de Gestión de la Seguridad de la Información.

8.1 PLANIFICACIÓN Y CONTROL OPERACIONAL.

En pasos anteriores hemos identificado los riesgos y establecido o seleccionado los controles que debemos implementar para abordar los riesgos y oportunidades de la seguridad de la información como parte de la planificación del SGSI.

8.2 EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

Ya hemos visto cuales son los pasos para la evaluación del riesgo de la seguridad de la información:

Identificamos nuestros activos de información determinando las salidas de información de esos activos.

Clasifique información y establezca una prioridad sobre esa información. Por ejemplo, los registros financieros y las contraseñas se clasifican como “información confidencial”.

Evalué la prioridad de cada tipo de información mediante una puntuación o valoración del riesgo.

Finalmente defina los controles necesarios para asegurar la información que supere determinado nivel de riesgo establecido según los criterios de riesgo de la organización

8.3 TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

El proceso de tratamiento de riesgos se lleva a cabo siempre después de cada evaluación de riesgos de seguridad para garantizar que se implementen los controles o mitigaciones correctas.

Los controles para mitigar el riesgo en la seguridad de la información y se determinan siguiendo una selección de los controles enumerados en el Anexo A de ISO 27001 utilizada como guía

Después de definir los controles a implantar según los pasos anteriores deberemos definir las tareas a realizar para su implantación en un plan de tratamiento de riesgos

El plan de tratamiento de riesgos puede ser simplemente un documento donde se recoge la descripción de las actividades a realizar y donde se establezca la trazabilidad entre las medidas a implantar y los riesgos que cada una de ellas pretende mitigar.

No nos olvidemos que además un plan de tratamiento de riesgos debe determinar no solo las actividades a realizar sino las acciones y los responsables de realizarlas junto con los indicadores o métodos para medir o evaluar el grado de cumplimiento de las acciones a emprender.

Es importante tener en cuenta que las métricas deben estar alineadas con los Objetivos de la organización previamente definidos.

Otro aspecto importante es la evaluación del esfuerzo necesario para obtener las medidas y registros. Para ello se recomienda ajustarse a un conjunto de métricas inicial que no suponga un esfuerzo no asumible para la organización y sea más un motivo de desánimo que una tarea asumida por la organización

Los siguientes controles del Anexo A del estándar ISO/IEC 27001:2014 son aplicables:

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**		
A.5.1	***Orientación de la dirección para la gestión de la seguridad de la información***		
A.5.1.1	Políticas para la seguridad de la información	SI	Se redactan y documentan las políticas de seguridad de la información acordes a los objetivos de seguridad acordados y niveles de riesgo tolerables. Este documento se pone a disposición de los empleados y público en general.
A.5.1.2	Revisión de las políticas para la seguridad de la información	SI	Las políticas de seguridad de la información se revisan y evalúan periódicamente y/o cuando sea necesario. La revisión es llevada a cabo por el Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad de la Información y la Dirección Estratégica. Se documentan los cambios y las justificaciones de los mismos.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1	*Organización Interna*		
A.6.1.1	Roles y responsabilidades para la seguridad de la información	SI	Los roles y responsabilidades de la seguridad de la información están definidas.
A.6.1.2	Separación de deberes	SI	El personal está separado por áreas y se les otorga acceso sólo a los activos y/o información estrictamente necesaria para la realización de su trabajo.
A.6.1.3	Contacto con las autoridades	SI	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad mantiene los contactos actualizados para incidentes de seguridad.
A.6.1.4	Contacto con grupos de interés especial	SI	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad mantienen contactos con autoridades nacionales para los incidentes de seguridad para informes en tiempo real y soluciones a implementar.
A.6.1.5	Seguridad de la información en la gestión de proyectos	SI	El Jefe de Seguridad es el encargado de velar por la aplicación de una metodología de análisis y evaluación de riesgos en los proyectos de TI.

A.6.2	*Dispositivos móviles y teletrabajo*		
A.6.2.1	Políticas para dispositivos móviles	SI	Se documenta una política de seguridad apropiada para los móviles. Los dispositivos móviles son configurados bajo las condiciones de seguridad aplicables antes de realizar cualquier conexión a la red institucional.
A.6.2.2	Teletrabajo	NO	

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**		
A.7.1	Antes de asumir el empleo		
A.7.1.1	Selección	**SI**	El personal es seleccionado cuidadosamente en base a su perfil y la idoneidad del trabajo a realizar.
A.7.1.2	Términos y condiciones del empleo	**SI**	Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.
A.7.2	*Durante la ejecución del empleo*		
A.7.2.1	Responsabilidades de la dirección	**SI**	La dirección comprende la importancia de la seguridad de la información y soporta el diseño del SGSI.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad realizan campañas y talleres de formación y educación en la seguridad de la información de forma periódica al personal administrativo.
A.7.2.3	Proceso disciplinario	**SI**	Los funcionarios son sometidos a procesos disciplinarios en caso de incumplimiento con las políticas de seguridad de la información de forma deliberada.
A.7.3	Terminación y cambio de empleo		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	**SI**	El Jefe de Seguridad vela que el funcionario que termine contrato o cambie de responsabilidades, se le sean reasignados los permisos y condiciones de seguridad de la información.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.8	**GESTIÓN DE ACTIVOS**		
A.8.1	***Responsabilidad por los activos***		
A.8.1.1	Inventario de activos	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad junto a los funcionarios, realizan el inventario de activos y se documentan con su clasificación y responsable.
A.8.1.2	Propiedad de los activos	**SI**	Los activos inventariados tienen asignados los funcionarios responsables.
A.8.1.3	Uso aceptable de los activos	**SI**	Los funcionarios se comprometen a utilizar los activos de forma aceptable teniendo en cuenta las políticas de seguridad de información generales.
A.8.1.4	Devolución de activos	**SI**	Se mantienen registros de la devolución de los activos entregados a los empleados. Necesarios para firmar paz y salvo con la organización.
A.8.2	***Clasificación de la información***		
A.8.2.1	Clasificación de la información	**SI**	Cada uno de los activos inventariados contiene la clasificación de la información asociada de acuerdo a los niveles de seguridad establecidos
A.8.2.2	Etiquetado de la información	**SI**	Cada uno de los activos inventariados están etiquetados con la clasificación de la información asociada.
A.8.2.3	Manejo de activos	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad junto a los funcionarios realizan y documentan los procedimientos para el manejo de los activos de acuerdo a la clasificación de cada uno.
A.8.3	***Manejo de medios***		
A.8.3.1	Gestión de medios removibles	**SI**	Existe una política para la gestión de los medios removibles y se clasifican y protegen de acuerdo a su tipo.
A.8.3.2	Disposición de los medios	**SI**	Los medio removibles son dispuestos en lugares seguros y su información es almacenada en medios seguros.
A.8.3.3	Transferencia de medios físicos	**NO**	

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.9	**CONTROL DE ACCESO**		
A.9.1	***Requisitos del negocio para control de acceso***		
A.9.1.1	Política de control de acceso	**SI**	La política de control de acceso está documentada en las Políticas de la Seguridad de Información.
A.9.1.2	Acceso a redes y a servicios en red	**SI**	Las redes están segmentadas en VLAN y el acceso a ella está protegido a personas no autorizadas. Los estudiantes, docentes y administrativos contienen una VLAN separada y que permite el acceso a ella sólo a aquellos que son debidamente autenticados.
A.9.2	***Gestión de acceso de usuarios***		
A.9.2.1	Registro y cancelación de registro de usuarios	**NO**	
A.9.2.2	Suministro de acceso de usuarios	**NO**	
A.9.2.3	Gestión de derechos de acceso privilegiado	**SI**	A los funcionarios se les otorgan los privilegios a los sistemas de acuerdo a las necesidades mínimas de trabajo. Estos privilegios son documentados y los funcionarios son agrupados bajo Perfiles de Usuario.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	**SI**	La entrega de claves de acceso de los sistemas se realiza de forma personal y se fuerza a que sea cambiada inmediatamente en su primer acceso.
A.9.2.5	Revisión de los derechos de acceso de usuarios	**SI**	El Jefe de Seguridad junto a los funcionarios encargados verifican que los permisos y derechos de acceso de los usuarios son los que en realidad tienen asignados. Esta verificación se realiza de forma periódica y cualquier anormalidad es debidamente documentada.
A.9.2.6	Retiro o ajuste de los derechos de acceso	**SI**	El Líder del Proceso de Desarrollo Tecnológico y el Jefe de Seguridad verifican y eliminan los permisos asignados al personal que sea retirado.

A.9.3	***Responsabilidades de los usuarios***		
A.9.3.1	Uso de información de autenticación secreta	**SI**	La información de autenticación del empleado en los sistemas y acceso a información es confidencial.
A.9.4	***Control de acceso a sistemas y aplicaciones***		
A.9.4.1	Restricción de acceso a la información	**SI**	Los derechos de acceso a los sistemas e información son controlados de acuerdo a rol y responsabilidad del empleado en la organización.
A.9.4.2	Procedimiento de ingreso seguro	**SI**	Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro. Se emplean mecanismos seguros de cifrado de información.
A.9.4.3	Sistema de gestión de contraseñas	**SI**	Se implementan mecanismos de recuperación de contraseñas de forma automática y se garantiza que la nueva contraseña del funcionario cumpla con los requisitos de seguridad expuestos en la Política de Seguridad de contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	**SI**	El Líder del Proceso de Desarrollo Tecnológico verifica que los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y licenciados. Se realiza una verificación de forma aleatoria.
A.9.4.5	Control de acceso a códigos fuente de programas	**SI**	El Jefe de Seguridad verifica que los códigos fuentes de los programas permanecen de forma confidencial.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.10	**CRIPTOGRAFÍA**		
A.10.1	***Controles criptográficos***		
A.10.1.1	Política sobre el uso de controles criptográficos	**SI**	Existe una política de seguridad que documente el uso de los controles criptográficos, la escogencia y justificación de los algoritmos de cifrado y su aplicación en los servicios que la requieran.
A.10.1.2	Gestión de llaves	**SI**	Existe una política de seguridad que documente el proceso y ciclo de vida de las llaves criptográficas.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**		
A.11.1	***Áreas Seguras***		
A.11.1.1	Perímetro de seguridad física	**SI**	El perímetro físico controlado por tarjetas de acceso, así como personal de seguridad en la infraestructura que contiene el hardware de las operaciones críticas.
A.11.1.2	Controles de acceso físicos	**SI**	El acceso físico a la infraestructura que contiene el hardware de las operaciones críticas está controlado por medio de tarjetas inteligentes que permiten el acceso a sólo el personal autorizado y registran la fecha y hora de acceso.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	**NO**	
A.11.1.4	Protección contra amenazas externas y ambientales	**SI**	Existe un Plan de Continuidad del Negocio y de Recuperación de Desastres que es puesto a prueba a intervalos regulares.
A.11.1.5	Trabajo en áreas seguras	**NO**	
A.11.1.6	Áreas de despacho y carga	**SI**	Existe un área diseñada y estructurada para recibir el descargue de los equipos que impiden el acceso al interior de la oficina e infraestructura que contiene el hardware de las operaciones críticas.
A.11.2	***Equipos***		
A.11.2.1	Ubicación y protección de los equipos	**SI**	Los equipos están protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, etc. y existen políticas de seguridad de la información documentadas para su uso.
A.11.2.2	Servicios de suministro	**SI**	Los servicios de suministros como energía, agua, ventilación y gas están acordes a la manufacturación de los equipos.
A.11.2.3	Seguridad del cableado	**SI**	El cableado eléctrico está separado del cableado de datos previniendo así interferencias y están protegidos físicamente.
A.11.2.4	Mantenimiento de equipos	**SI**	Los equipos son mantenidos sólo por el personal autorizado bajo las condiciones especificadas y a intervalos programados.
A.11.2.5	Retiro de activos	**SI**	El Jefe de Mantenimiento en concordancia con el Líder del Proceso de Desarrollo Tecnológico documenta el retiro de los activos.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	**NO**	
A.11.2.7	Disposición segura o reutilización de equipos	**SI**	El Jefe de Mantenimiento y el Líder del Proceso de Desarrollo Tecnológicorealizan un procedimiento seguro y documentado para la disposición o reutilización de equipos.
A.11.2.8	Equipos de usuario desatendido	**SI**	Existe un plan de capacitación y campaña de concientización a los funcionarios sobre la seguridad de la información y los riesgos a los que están expuestos los activos.
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	**SI**	El Jefe de Seguridad garantiza que la información confidencial física es almacenada en gabinetes de forma segura impidiendo su acceso físico a personas no autorizadas.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.12	**SEGURIDAD DE LAS OPERACIONES**		
A.12.1	***Procedimientos operacionales y responsabilidades***		
A.12.1.1	Procedimientos de operación documentados	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios documentan los procedimientos de las operaciones relativas a la seguridad de la información de cada uno de los activos.
A.12.1.2	Gestión de cambios	**SI**	El Jefe de Seguridad verifica que los cambios en los equipos que afectan la seguridad de la información son controlados y debidamente planeados y probados.
A.12.1.3	Gestión de capacidad	**SI**	El Líder del Proceso de Desarrollo Tecnológico y los funcionarios realizan un monitoreo continuo a los recursos y la adquisición de los nuevos y se proyecta de acuerdo a las necesidades críticas de la organización.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	**SI**	El Jefe de Seguridad asegura que los ambientes de desarrollo, pruebas y operación están debidamente separados y no ponen en riesgo la información.
A.12.2	***Protección contra códigos maliciosos***		
A.12.2.1	Controles contra códigos maliciosos	**SI**	Existe un plan de capacitación y campaña de concientización a los funcionarios sobre la seguridad de la información y los riesgos a los que están expuestos los activos, especialmente sobre el software de código malicioso. El Jefe de Seguridad y los funcionarios verifican que el software está protegido con antivirus y existe una política documentada de actualización de todo el software utilizado, antivirus y sistema operativo.
A.12.3	***Copias de respaldo***		
A.12.3.1	Respaldo de la información	**SI**	El Jefe de Seguridad y funcionarios pertinentes realizan las copias de seguridad de toda la información a intervalos programados y de acuerdo a las políticas de seguridad. El procedimiento es documentado y se realizan pruebas de recuperación a intervalos programados.
A.12.4	***Registro y seguimiento***		
A.12.4.1	Registro de eventos	**SI**	El Jefe de Seguridad y funcionarios pertinentes revisan periódicamente los registros de los usuarios y las actividades relativas a la seguridad de la información. El proceso es auditado y documentado.
A.12.4.2	Protección de la información de registro	**SI**	Se implementan controles de seguridad que garanticen la protección de la información de los registros.
A.12.4.3	Registros del administrador y del operador	**SI**	Las acciones y registros de los administradores también son almacenados y protegidos de cualquier modificación.
A.12.4.4	Sincronización de relojes	**SI**	El Líder del Proceso de Desarrollo Tecnológico asegura que todos los sistemas están acordes y ajustados en una referencia de tiempo única y sincronizada.

A.12.5	***Control de software operacional***		
A.12.5.1	Instalación de software en los sistemas operativos	**SI**	Existe una documentación sobre el procedimiento de instalación de los sistemas operativos y software, que cumpla con las políticas de seguridad de la información.
A.12.6	***Gestión de la vulnerabilidad técnica***		
A.12.6.1	Gestión de las vulnerabilidades técnicas	**SI**	Existe una metodología de análisis y evaluación de riesgos sistemática y documentada.
A.12.6.2	Restricciones sobre la instalación de software	**SI**	La instalación de software es realizada sólo por el personal autorizado y con software probado y licenciado, además de otorgar el principio del menor privilegio. El procedimiento de instalación es documentado.
A.12.7	***Consideraciones sobre auditorías de sistemas de información***		
A.12.7.1	Controles de auditorías de sistemas de información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes acuerdan sobre las fechas de auditorías internas para los sistemas de información. El procedimiento es documentado.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.13	**SEGURIDAD DE LAS COMUNICACIONES**		
A.13.1	***Gestión de la seguridad de las redes***		
A.13.1.1	Controles de redes	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.13.1.2	Seguridad de los servicios de red	**SI**	El acceso a la red de los proveedores de servicio de red es monitoreado y controlado.
A.13.1.3	Separación en las redes	**SI**	Las redes están segmentadas en VLAN y el acceso a ella está protegido a personas no autorizadas. Los estudiantes, docentes y administrativos contienen una VLAN separada y que permite el acceso a ella sólo a aquellos que son debidamente autenticados.

A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	**SI**	Existe una política documentada que establece los requisitos relativos a la seguridad de la información para la adquisición de los nuevos equipos.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.14.2	***Seguridad en los procesos de desarrollo y soporte***		
A.14.2.1	Política de desarrollo seguro	**NO**	
A.14.2.2	Procedimientos de control de cambios en sistemas	**NO**	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	**SI**	Existe una documentación sobre la implementación de las nuevas aplicaciones y son sometidas a pruebas para garantizar que no haya impactos adversos en la seguridad de la información. El Líder del Proceso del Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes realizan las pruebas bajo simulaciones críticas.
A.14.2.4	Restricciones en los cambios a los paquetes de software	**NO**	
A.14.2.5	Principios de construcción de los sistemas seguros	**NO**	
A.14.2.6	Ambiente de desarrollo seguro	**NO**	
A.14.2.7	Desarrollo contratado	**SI**	El Jefe de Seguridad y los funcionarios pertinentes evalúan
	externamente		el software desarrollado externamente y prueban que cumpla con los requisitos de seguridad establecidos en las políticas de seguridad de la información.
A.14.2.8	Pruebas de seguridad de sistemas	**SI**	El Jefe de Seguridad y los funcionarios pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.2.9	Pruebas de aceptación de sistemas	**SI**	El Jefe de Seguridad y los funcionarios pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.3	Datos de prueba	**SI**	Los funcionarios pertinentes verifican que los datos de prueba son seleccionados cuidadosamente y no presentan riesgo para la violación de confidencialidad de la información.

CONTROL ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**		
A.14.1	***Requisitos de seguridad de los sistemas de información***		
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	**SI**	Existe una política documentada que establece los requisitos relativos a la seguridad de la información para la adquisición de los nuevos equipos.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.14.2	***Seguridad en los procesos de desarrollo y soporte***		
A.14.2.1	Política de desarrollo seguro	**NO**	
A.14.2.2	Procedimientos de control de cambios en sistemas	**NO**	
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	**SI**	Existe una documentación sobre la implementación de las nuevas aplicaciones y son sometidas a pruebas para garantizar que no haya impactos adversos en la seguridad de la información. El Líder del Proceso del Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes realizan las pruebas bajo simulaciones críticas.
A.14.2.4	Restricciones en los cambios a los paquetes de software	**NO**	
A.14.2.5	Principios de construcción de los sistemas seguros	**NO**	
A.14.2.6	Ambiente de desarrollo seguro	**NO**	
A.14.2.7	Desarrollo contratado externamente	**SI**	El Jefe de Seguridad y los funcionarios pertinentes evalúan el software desarrollado externamente y prueban que cumpla con los requisitos de seguridad establecidos en las políticas de seguridad de la información.
A.14.2.8	Pruebas de seguridad de sistemas	**SI**	El Jefe de Seguridad y los funcionarios pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.2.9	Pruebas de aceptación de sistemas	**SI**	El Jefe de Seguridad y los funcionarios pertinentes realizan pruebas de seguridad a los sistemas y documentan los procedimientos.
A.14.3	Datos de prueba	**SI**	Los funcionarios pertinentes verifican que los datos de prueba son seleccionados cuidadosamente y no presentan riesgo para la violación de confidencialidad de la información.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.15	**RELACIONES CON LOS PROVEEDORES**		
A.15.1	***Seguridad de la información en las relaciones con los proveedores***		
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	**SI**	Existe una política de seguridad de la información relacionada con los proveedores.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.2	***Gestión de la prestación de servicios de proveedores***		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	**SI**	Existen los acuerdos documentados con cada uno de los proveedores para el tratamiento de la seguridad de la información y los riesgos asociados.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**		
A.16.1	***Gestión de incidentes y mejoras de la seguridad de la información***		
A.16.1.1	Responsabilidades y procedimientos	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.16.1.2	Reporte de eventos de seguridad de la información	**SI**	Los funcionarios están alertados de los eventos e incidentes correspondientes relativos a la seguridad de la información. Los incidentes son reportados, evaluados y documentados. Se establecen los procedimientos a seguir.

A.16.1.3	Reporte de debilidades de seguridad de la información	**SI**	Existen los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información. Estas notificaciones son evaluadas de forma inmediata por el Jefe de Seguridad.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	**SI**	Existen los formatos documentados disponibles para que los funcionarios reporten las debilidades de la seguridad de la información. Estas notificaciones son evaluadas de forma inmediata por el Jefe de Seguridad.
A.16.1.5	Respuesta a incidentes de seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	**SI**	Los incidentes de la seguridad de la información son documentados especificando las vulnerabilidades, amenazas, riesgos y los posibles controles de seguridad a implementar constituyendo así una base de conocimiento.
A.16.1.7	Recolección de evidencia	**SI**	Existen formatos y documentos para recolectar la evidencia y emitirlos a las autoridades competentes.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
A.17.1	***Continuidad de seguridad de la información***		
A.17.1.1	Planificación de la continuidad de la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.

A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	**SI**	El Líder del Proceso de Desarrollo Tecnológico, el Jefe de Seguridad y los funcionarios pertinentes tienen documentado los procesos y procedimientos para los incidentes de la seguridad de la información. Se tiene documentado el Plan de Continuidad del Negocio donde están identificados claramente los responsables de su ejecución.
A.17.2	***Redundancias***		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	**SI**	En el Plan de Continuidad del Negocio se establece la instalación e infraestructura disponible para el procesamiento de información.

CONTROL_ID	CONTROL	APLICABLE	IMPLEMENTACIÓN
A.18	**CUMPLIMIENTO**		
A.18.1	***Cumplimiento de los requisitos legales y contractuales***		
A.18.1.1	Identificación de la legislación aplicable a los requisitos contractuales	**SI**	Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley.
A.18.1.2	Derechos de propiedad intelectual	**NO**	
A.18.1.3	Protección de registros	**SI**	Los registros están protegidos físicamente contra alteración, modificación, pérdida y acceso de usuarios no autorizados.
A.18.1.4	Privacidad y protección de información de datos personales	**SI**	Los datos personales son almacenados y protegidos de acuerdo a las conformidades de la ley y regulaciones.
A.18.1.5	Reglamentación de controles criptográficos	**SI**	El Jefe de Seguridad y el Administrador de Redes implementan una Infraestructura de Llave Pública (PKI) mediante algoritmos fuertes de cifrado que garanticen la confidencialidad e integridad de la información que se transmite a través de las redes.
A.18.2	***Revisiones de seguridad***		
A.18.2.1	Revisión independiente de la seguridad de la información	**SI**	Existe la documentación para la realización de la auditoría interna del Sistema de Gestión de la Seguridad de la Información.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	**SI**	Existe la documentación para la realización de la auditoría interna del Sistema de Gestión de la Seguridad de la Información con el fin de verificar el nivel de cumplimiento, controles y políticas de seguridad de la información.
A.18.2.3	Revisión del cumplimiento técnico	**SI**	Exista la documentación para la realización periódica de los test de penetración y verificación de resultados e informes.

Tabla Nro. 39 – Aplicabilidad de controles

9 OPERACIÓN

OFICINA GENERAL DE INFORMÁTICA Y ESTADISTICA

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

PLAN DE TRATAMIENTO DE RIESGOS

Código del Documento	SGSIUNDAC01
Versión	1.0
Fecha de Versión	10/07/2018
Propietario	DGIyE-UNDAC
Nivel de Confidencialidad	Baja

PROPÓSITO, ALCANCE Y USUARIOS

El propósito de este documento es definir cuáles controles de seguridad o salvaguardas de MAGERIT son los apropiados para enfrentar las amenazas de cada uno de los activos y mitigar los riesgos en la Dirección General de Informática y Estadística de la UNDAC, así como definir el tratamiento de cada uno de ellos.

Este documento también determina cuáles controles de seguridad del Anexo A del estándar de la NTP ISO/IEC 27001:2014 son aplicables a todo el alcance del Sistema de Gestión de la Seguridad de la Información.

9.1 MONITOREO, MEDICIÓN, ANÁLISIS Y EVALUACIÓN

El primer requisito es determinar qué información necesitamos evaluar para medir el rendimiento del SGSI. Se trata de determinar que debemos medir y controlar, cuándo, quién y cómo.

Optimizar los recursos

Un consejo práctico es evaluar o medir los que necesitamos realmente. No tiene mucho sentido monitorear y hacer mediciones solo porque su organización tiene la capacidad de hacerlo. Solo supervise y mida si cumple con el requisito de evaluar el rendimiento de la seguridad de la información y la eficacia del SGSI

Establecer metas

Cada organización puede tener distintas necesidades de información que además pueden cambiar con el tiempo

Los cinco grupos de procesos importantes del SGSI.

- Procesos de Alineación de TI y negocios
- Proceso de gestión de riesgos de seguridad de la información.
- Procesos de Cumplimiento legal o normativo.
- Proceso de sensibilización y comunicación.
- Procesos de auditoria o revisión del sistema

9.2 AUDITORÍA INTERNA

Se trata de un aspecto clave dentro de un sistema de gestión de seguridad de la información (SGSI), donde los requisitos principales son la planificación y la independencia de los auditores.

Como requisito fundamental ISO 27001 obliga a que la organización realice auditorías internas a intervalos planificados para proporcionar información sobre si el SGSI cumple con los requisitos propios de la organización para su SGSI así como con los requisitos de la norma.

9.3 REVISIÓN POR LA DIRECCIÓN

La norma ISO 27001 nos pone como requisito realizar una revisión o examen periódico del SGSI realizado por la dirección. Si bien no es obligatorio reunirse, a menudo es más fácil programar reuniones de revisión de la gerencia de forma periódica donde junto con las partes interesadas relevantes y revisemos el desempeño del SGSI a intervalos definidos.

¿CON QUÉ FRECUENCIA DEBEN LLEVARSE A CABO LAS REVISIONES?

El único requisito es que las recisiones de la dirección deben realizarse periódicamente para medir la efectividad del sistema de gestión. Si bien ISO 27001 no define el marco de tiempo requerido entre las reuniones, deben realizarse a intervalos regulares para revisar el progreso y las acciones requeridas para mejorar el sistema.

Otro objetivo importante es que los resultados del SGSI se revisen con los propietarios de las acciones o controles de seguridad de forma regular.

Los marcos de tiempo pueden variar pues en un sistema recién implantado puede que al comienzo se identifiquen una gran cantidad de acciones, que disminuirán a medida que el sistema se vuelva más maduro. Por tanto, un periodo inicial de reuniones mensuales o bimensuales puede después

alargarse para hacerse de forma trimestral o semestral dependiendo de las necesidades

1. **TRATAMIENTO DE RIESGOS**

   El tipo de tratamiento que se le dará a cada riesgo: Asumirlos (A), Definir Controles (DC) o Transferirlos a Terceros (TT).

2. **APLICABILIDAD DE CONTROLES DE SEGURIDAD**

   Con el objetivo de alcanzar los objetivos de seguridad del Sistema de Gestión de la Seguridad de la Información, se establecen los siguientes controles de seguridad basados en la metodología de análisis y evaluación de riesgos MAGERIT y los controles del Anexo A de la NTP ISO/IEC 27001:2014.

   DOMINIOS, OBJETIVOS DE CONTROL Y CONTROLES DE SEGURIDAD.

   Se realiza a su vez un Análisis Diferencial referente al Anexo A de la NTP-ISO/IEC 27001:2014 con el fin de determinar el nivel de cumplimiento de los Dominios, Objetivos de Control y Controles de Seguridad. Estos corresponden a los numerales 5 al 18.

<table>
<tr><td>A.5</td><td colspan="3">POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN</td></tr>
<tr><td>A.5.1</td><td colspan="3">Orientación de la dirección para la gestión de la seguridad de la información</td></tr>
<tr><td colspan="4">Objetivo : Brindar orientación y soporte por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.</td></tr>
<tr><td rowspan="5">A.5.1.1</td><td rowspan="5">Políticas para la seguridad de la información</td><td rowspan="5">Control : Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Las políticas de la seguridad de la información proveen un direccionamiento estratégico acorde a los requerimientos de la organización y cumplimiento con leyes y regulaciones. Esta documentación es de carácter obligatorio</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
No se tiene implementado un SGSI ni existe un documento que contemple las políticas de seguridad de la información.</td></tr>
<tr><td rowspan="5">A.5.1.2</td><td rowspan="5">Revisión de las políticas para la seguridad de la información</td><td rowspan="5">Control : Las políticas para la seguridad de la información se deben revisar a intervalos planificados, o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Las políticas de la seguridad de la información deberían ser evaluadas con el fin de responder a los cambios de la organización.</td></tr>
<tr><td>IMPLEMENTA</td></tr>
<tr><td>SI | NO
No existe una revisión de las políticas de seguridad de la información ya que actualmente no se tiene el documento relacionado (ver A.5.1.1).</td></tr>
</table>

Tabla 40. Anexo A de la NTP-ISO/IEC 27001:2014. Políticas de la Seguridad de la Información.

A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1	**Organización Interna**		
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.			
A.6.1.1	Roles y responsabilidades para la seguridad de la información	***Control*** : Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	**APLICA** **SI** / **NO** Los roles y responsabilidades son vitales para la protección de los activos informáticos individuales, así como los procesos específicos para la seguridad de la información. Esta documentación es de carácter obligatorio en laNTP-ISO/IEC 27001:2014 . **IMPLEMENTA** **SI** / **NO** Los roles y responsabilidades relativas a la seguridad de la información aún no están definidas, debido a que no se tiene implementado un SGSI.
A.6.1.2	Separación de deberes	***Control*** : Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.	**APLICA** **SI** / **NO** Ningún empleado debería tener acceso a modificar los activos informáticos sin autorización previa. **IMPLEMENTA** **SI** / **NO** El personal está separado por áreas y se les otorga acceso sólo a los activos y/o información estrictamente necesaria para la realización de su trabajo.
A.6.1.3	Contacto con las autoridades	***Control*** : Se deben mantener contactos apropiados con las autoridades pertinentes.	**APLICA** **SI** / **NO** Deberían existir procedimientos para contactar a las autoridades pertinentes y reportar las incidencias relativas a la seguridad de la información. **IMPLEMENTA** **SI** / **NO** Las incidencias relativas a la seguridad de la información son resueltas internamente.
A.6.1.4	Contacto con grupos de interés especial	***Control*** : Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	**APLICA** **SI** / **NO** Los grupos de interés especial mejoran el conocimiento y las prácticas relativas a la seguridad de la información, así como las actualizaciones de los equipos y/o dispositivos. **IMPLEMENTA** **SI** / **NO** Se mantienen contactos con autoridades nacionales para los incidentes de seguridad para informes en tiempo real y soluciones a implementar.

Tabla 41. Requisito de la NTP-ISO/IEC 27001:2014. Organización de la seguridad de la información.

<table>
<tr><td>A.7</td><td colspan="3">SEGURIDAD DE LOS RECURSOS HUMANOS</td></tr>
<tr><td>A.7.1</td><td colspan="3">Antes de asumir el empleo</td></tr>
<tr><td colspan="4">Objetivo: Asegurar que los empleados y contratistas comprenden las responsabilidades y son idóneos en los roles para que los consideran.</td></tr>
<tr><td rowspan="4">A.7.1.1</td><td rowspan="4">Selección</td><td rowspan="4">Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentaciones y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Aparte de las competencias técnicas, el personal contratado debería ser éticamente correcto y confiable especialmente si accede a información sensitiva de la organización.
IMPLEMENTA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td></td><td></td><td></td><td>El personal es seleccionado cuidadosamente en base a su perfil y la idoneidad del trabajo a realizar.</td></tr>
<tr><td rowspan="4">A.7.1.2</td><td rowspan="4">Términos y condiciones del empleo</td><td rowspan="4">Control: Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.</td><td>APLICA</td></tr>
<tr><td>SI | NO</td></tr>
<tr><td>Los acuerdos contractuales de los empleados deberían tener cláusulas relativas a la confidencialidad de la información y respecto a las leyes y derechos de propiedad intelectual.
IMPLEMENTA</td></tr>
<tr><td>SI | NO
Los acuerdos contractuales actualmente incluyen las responsabilidades asignadas relativas a la seguridad de la información.</td></tr>
</table>

A.7.2	Durante la ejecución del empleo		
Objetivo: Asegurarse de los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.	**APLICA** **SI** / **NO** La dirección asegura que los roles y responsabilidades están claramente definidos antes de brindar acceso confidencial, así como los empleados están comprometidos con las políticas de seguridad de la información. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013. **IMPLEMENTA** **SI** / **NO** No se tiene implementado un SGSI y no existen políticas de la seguridad de la información.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	***Control***: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes a su cargo.	**APLICA** **SI** / **NO** Mediante un programa de entrenamiento relativo a la seguridad de la información, los empleados son conscientes de su importancia y cómo pueden cumplir con las políticas del SGSI. **IMPLEMENTA** **SI** / **NO** No se tiene implementado un SGSI ni un plan de concientización formal relativo a la seguridad de la información.

A.7.2	Durante la ejecución del empleo		
Objetivo: Asegurarse de los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.			
A.7.2.1	Responsabilidades de la dirección	Control: La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.	**APLICA** **SI** / **NO** La dirección asegura que los roles y responsabilidades están claramente definidos antes de brindar acceso confidencial, así como los empleados están comprometidos con las políticas de seguridad de la información. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013. **IMPLEMENTA** **SI** / **NO** No se tiene implementado un SGSI y no existen políticas de la seguridad de la información.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	***Control***: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes a su cargo.	**APLICA** **SI** / **NO** Mediante un programa de entrenamiento relativo a la seguridad de la información, los empleados son conscientes de su importancia y cómo pueden cumplir con las políticas del SGSI. **IMPLEMENTA** **SI** / **NO** No se tiene implementado un SGSI ni un plan de concientización formal relativo a la seguridad de la información.

A.7.2.3	Proceso disciplinario	***Control:*** *Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.*	**APLICA** **SI** / **NO** Los procesos disciplinarios son analizados en base al grado de responsabilidad del empleado y el impacto que tiene en la organización. **IMPLEMENTA** **SI** / **NO** Aunque no se tiene implementado un SGSI y no se tiene plan de concientización relativo a la seguridad de la información, el empleado está sujeto a un proceso disciplinario en caso de haber una incidencia.

A.7.3	**Terminación y cambio de empleo**		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.			
A.7.3.1	Terminación o cambio de responsabilidades de empleo	***Control*** : Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	**APLICA** **SI** / **NO** Los acuerdos contractuales deberían plasmar el compromiso relativo a la confidencialidad de la información aún después de la terminación o cambio de empleo. **IMPLEMENTA** **SI** / **NO** Al terminar o cambiar de empleo no se notifica a al empleado sobre la validez de sus responsabilidades y deberes relativos a la seguridad de la información.

Tabla 42. Anexo A de la NTP-ISO/IEC 27001:2014 Seguridad de los Recursos Humanos.

A.8	GESTIÓN DE ACTIVOS		
A.8.1	**Responsabilidad por los activos**		
***Objetivo**: Identificar los activos organizacionales y definir las responsabilidades apropiadas.*			
A.8.1.1	Inventario de activos	***Control***: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se deben elaborar y mantener un inventario de estos activos.	**APLICA** **SI** / **NO** El inventario y clasificación de activos permite identificar la importancia de cada uno de ellos y su impacto en la organización. Esta documentación es de carácter obligatorio en la NTP-ISO/IEC 27001:2014 **IMPLEMENTA** **SI** / **NO** Actualmente no existe un documento que clasifique la criticidad de la información y de los activos.
A.8.1.2	Propiedad de los activos	***Control***: Los activos mantenidos en el inventario deben tener un propietario.	**APLICA** **SI** / **NO** Los propietarios son responsables del uso de los activos informáticos durante todo su ciclo de vida. Esta documentación es de carácter obligatorio en la NTP-ISO/IEC 27001:2014 . **IMPLEMENTA** **SI** / **NO** No se especifican los propietarios de los activos informáticos inventariados.
A.8.1.3	Uso aceptable de los activos	***Control***: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	**APLICA** **SI** / **NO** Los empleados o contratistas son responsables del uso que le dan a los activos informáticos de la organización. **IMPLEMENTA** **SI** / **NO** No se especifican las reglas para el uso aceptable de los activos.

A.8.1.4	Devolución de activos	***Control*** : Todos los empleados y usuarios de las partes externas deben devolver todos los activos de la organización que se encuentren a su	**APLICA** **SI** | **NO** La devolución de activos debe ser formalizada y la información almacenada en dispositivos personales transferida a la organización.
			IMPLEMENTA **SI** | **NO** Se mantienen registros de la devolución de los activos entregados a los empleados. Necesarios para firmar paz y salvo con la organización.

Tabla 16. Anexo A de la NTP-ISO/IEC 27001:2014. Gestión de Activos.

A.8.2	**Clasificación de la información**		
Objetivo *: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo a su importancia para la organización.*			
A.8.2.1	Clasificación de la información	***Control*** : La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación autorizada.	**APLICA** **SI** | **NO** La clasificación de la información es vital para determinar el grado y control de seguridad que debería tener. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013. **IMPLEMENTA** **SI** | **NO** Actualmente no existe un documento que clasifique la criticidad de la información y de los activos.
A.8.2.2	Etiquetado de la información	***Control*** : Se debe desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	**APLICA** **SI** | **NO** El etiquetado de la información debe reflejar el esquema de clasificación adoptador por la organización (***ver A.8.2.1***). **IMPLEMENTA** **SI** | **NO** Actualmente no existe procedimiento alguno para el etiquetado y/o clasificación de la información.
A.8.2.3	Manejo de activos	***Control*** : Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	**APLICA** **SI** | **NO** El acceso a los activos deberían restringirse de acuerdo a su esquema de clasificación.
			IMPLEMENTA **SI** | **NO** Actualmente no existen procedimientos para el manejo de la información, ya que ésta no está clasificada.

A.8.3	Manejo de medios		
Objetivo *: Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.*			
A.8.3.1	Gestión de medios removibles	***Control*** : Se deben implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación de la organización.	**APLICA** **SI** / **NO** Los medios removibles podrían almacenar información confidencial y deberían tener el mismo tratamiento y esquema de clasificación que cualquier otro activo informático. **IMPLEMENTA** **SI** / **NO** Los medio removibles son protegidos, pero no cuentan con un nivel de clasificación de información (***ver A.8.2.1***).
A.8.3.2	Disposición de los medios	***Control*** : Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.	**APLICA** **SI** / **NO** Los medios removibles podrían almacenar información confidencial y deberían ser removidos almacenando copias de seguridad en lugares seguros y garantizar que su información no sea revocable o legible. **IMPLEMENTA** **SI** / **NO** Los medio removibles son dispuestos en lugares seguros y su información es almacenada en medios seguros.
A.8.3.3	Transferencia de medios físicos	***Control*** : Los medios que contienen información se deben proteger contra acceso no autorizados, uso indebido o corrupción durante el transporte.	**APLICA** **SI** / **NO** Los medios transportados podrían tener información sensitiva.
			IMPLEMENTA **SI** / **NO** Los medio removibles son dispuestos en lugares seguros y su información es almacenada en medios seguros.

Tabla 43. Anexo A de la NTP-ISO/IEC 27001:2014. Gestión de Activos.

A.9	CONTROL DE ACCESO		
A.9.1	**Requisitos del negocio para control de acceso**		
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.			
A.9.1.1	Política de control de acceso	***Control***: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	**APLICA** **SI** / NO El control de acceso físico y lógico con principios del menor privilegio permiten tener un control sobre los riesgos de diseminación de información o acceso físico a los activos a personas no autorizadas. **IMPLEMENTA** **SI** / **NO** Aunque se mantienen controles físicos y lógicos que garantizan el acceso con menor privilegio, no está documentada en una política de seguridad de la información.
A.9.1.2	Acceso a redes y a servicios en red	***Control***: Sólo se debe permitir acceso a los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	**APLICA** **SI** / NO Las redes y servicios de red proveen acceso a diferentes servicios dentro de la organización al personal autorizado. **IMPLEMENTA** **SI** / NO Las redes están segmentadas en VLANS y el acceso a ella está protegido a personas no autorizadas.

A.9.2	Gestión de acceso de usuarios		
Objetivo: Asegurar el acceso a los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.			
A.9.2.1	Registro y cancelación de registro de usuarios	***Control***: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	**APLICA** **SI** / **NO** Los identificadores únicos de los empleados mantienen un registro de las acciones realizadas. **IMPLEMENTA** **SI** / **NO** A los empleados no se les asigna un identificador único dentro de la organización.
A.9.2.2	Suministro de acceso de usuarios	***Control***: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.	**APLICA** **SI** / **NO** Los permisos y privilegios de los usuarios son asignados o revocados de forma automática mediante un proceso formal. **IMPLEMENTA** **SI** / **NO** A los empleados no se les asigna un identificador único dentro de la organización.
A.9.2.3	Gestión de derechos de acceso privilegiado	***Control***: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	**APLICA** **SI** / **NO** Los privilegios de acceso a cualquier sistema o información deberían ser otorgados de acuerdo a las políticas de acceso. **IMPLEMENTA** **SI** / **NO** A los empleados se les otorgan los privilegios a los sistemas de acuerdo a las necesidades mínimas de trabajo.

A.9.2.4	Gestión de información de autenticación secreta de usuarios	***Control***: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	**APLICA** **SI** | **NO** La autenticación de los empleados en los sistemas debería mantenerse confidencial y secreta para evitar alteración y/o modificación de la información por parte de personas no autorizadas. **IMPLEMENTA** **SI** | **NO** La entrega de claves de acceso se realiza de forma personal y se fuerza a que sea cambiada inmediatamente en su primer
A.9.2.5	Revisión de los derechos de acceso de usuarios	***Control***: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	**APLICA** **SI** | **NO** Los derechos de acceso verifican qué puede hacer un usuario sobre la información o sistemas. **IMPLEMENTA** **SI** | **NO** No se realizan verificaciones regulares de los derechos de acceso a los sistemas.
A.9.2.6	Retiro o ajuste de los derechos de acceso	***Control***: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben retirar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	**APLICA** **SI** | **NO** La remoción de los derechos de acceso permite que los empleados no sigan teniendo acceso a información o a los sistemas una vez terminado el contrato o cambio en el cargo. **IMPLEMENTA** **SI** | **NO** No existe un proceso y/o documentación formal de remoción de los privilegios de acceso de los empleados que cambian el cargo o terminan contrato.

A.9.3	Responsabilidades de los usuarios		
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.			
A.9.3.1	Uso de información de autenticación secreta	***Control*** : Se debe exigir a los usuarios que cumplan con las prácticas de la organización para el uso de información de autenticación secreta.	**APLICA** **SI** / **NO** La información confidencial debería ser accedida sólo por las personas autorizadas y para fines de la organización. **IMPLEMENTA** **SI** / **NO** La información de autenticación del empleado en los sistemas y acceso a información es confidencial.

A.9.4	Control de acceso a sistemas y aplicaciones		
Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.			
A.9.4.1	Restricción de acceso a la información	***Control*** : El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	**APLICA** **SI** / **NO** El acceso a la información debe ser granular en pro de evitar revelación o acceso a personas no autorizadas. **IMPLEMENTA** **SI** / **NO** Los derechos de acceso a los sistemas e información son controlados de acuerdo a rol y responsabilidad del empleado en la organización.
A.9.4.2	Procedimiento de ingreso seguro	***Control*** : Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	**APLICA** **SI** / **NO** El inicio de sesión seguro permite que una persona no autorizada tenga acceso a información privilegiada. **IMPLEMENTA** **SI** / **NO** Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro.

A.9.4.3	Sistema de gestión de contraseñas	***Control***: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	**APLICA**	
			SI	**NO**
			Los sistemas de gestión de contraseñas son un mecanismo fuerte de autenticación de usuarios y evita que sean adivinadas por ataques de fuerza bruta y/o	
			IMPLEMENTA	
			SI	**NO**
			Los sistemas están protegidos mediante un mecanismo de inicio de sesión seguro.	
A.9.4.4	Uso de programas utilitarios privilegiados	***Control***: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y los controles de las aplicaciones.	**APLICA**	
			SI	**NO**
			Los programas utilitarios deben ser instalados cuidadosamente para que no afecten a los sistemas o a la información existente.	
			IMPLEMENTA	
			SI	**NO**
			Los sistemas y activos críticos sólo se les instalan los programas estrictamente necesarios y licenciados.	
A.9.4.5	Control de acceso a códigos fuente de programas	***Control***: Se debe restringir el acceso a los códigos fuentes de los programas.	**APLICA**	
			SI	**NO**
			El código fuente contiene la información de cómo se ha implementado el programa y bajo que lenguaje de programación, así como las librerías empleadas.	
			IMPLEMENTA	
			SI	**NO**
			El código fuente sólo es accedido por las personas autorizadas.	

Tabla 44. Anexo A de la NTP-ISO/IEC 27001:2014. Control de Acceso.

A.10.1	Controles criptográficos		
Objetivo *: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o integridad de la información.*			
A.10.1.1	Política sobre el uso de controles criptográficos	***Control*** : Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	**APLICA** **SI** | **NO** La criptografía cifra mediante algoritmos de encriptación los mensajes transmitidos garantizando la confidencialidad, integridad y autenticidad de los mensajes, impidiendo así que sea legible por personas no autorizadas. **IMPLEMENTA** **SI** | **NO** No existe una política sobre el uso de algoritmos de encriptación para el cifrado de la información transmitida.
A.10.1.2	Gestión de llaves	***Control*** : Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas, durante todo su ciclo de vida.	**APLICA** **SI** | **NO** La gestión de llaves criptográficas vela por su seguridad, mantenimiento, renovación, distribución y destrucción. **IMPLEMENTA** **SI** | **NO** No existe una política sobre el uso y distribución de llaves criptográficas.

Tabla 45. Anexo A de la NTP-ISO/IEC 27001:2014. Controles Criptográficos.

A.11	SEGURIDAD FÍSICA Y DEL ENTORNO		
A.11.1	**Áreas seguras**		
***Objetivo** : Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.*			
A.11.1.1	Perímetro de seguridad física	***Control*** : Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	**APLICA** **SI** / **NO** El perímetro de seguridad física impide el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización. **IMPLEMENTA** **SI** / **NO** Existe un perímetro físico controlado por tarjetas de acceso, así como personal de seguridad.
A.11.1.2	Controles de acceso físicos	***Control*** : Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	**APLICA** **SI** / **NO** Los controles de accesos físicos impiden el acceso a personas no autorizadas a los activos informáticos u otros dispositivos de la organización.
			IMPLEMENTA **SI** / **NO** El acceso físico está controlado por medio de tarjetas inteligentes que permiten el acceso a sólo el personal autorizado y registran la fecha y hora de acceso.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	***Control*** : Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	**APLICA** **SI** / **NO** Las oficinas y lugares de trabajo claves deberían estar protegidas impidiendo el acceso físico a personas no autorizadas así como no ser públicamente visibles. **IMPLEMENTA** **SI** / **NO** Las oficinas y lugares de trabajo no están protegidas por medios físicos para controlar el acceso.

A.11.1.4	Protección contra amenazas externas y ambientales	***Control***: Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	**APLICA** **SI** | **NO** Protección física contra los desastres naturales y/o humanos. **IMPLEMENTA** **SI** | **NO** No existe una protección física contra los desastres naturales y/o humanos.
A.11.1.5	Trabajo en áreas seguras	***Control***: Se debe diseñar y aplicar procedimientos para trabajo en áreas seguras.	**APLICA** **SI** | **NO** Las áreas seguras deben estar físicamente aseguradas y revisadas periódicamente. **IMPLEMENTA** **SI** | **NO** No se tienen áreas seguras para ser aseguradas físicamente.
A.11.1.6	Áreas de despacho y carga	***Control***: Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	**APLICA** **SI** | **NO** Los lugares de entrega de equipos y otros dispositivos están controlados y se restringe el acceso a áreas externas de la organización. **IMPLEMENTA** **SI** | **NO** El lugar de entrega de equipos y otros dispositivos ocurre al interior de la oficina.

A.11.2	Equipos		
***Objetivo** : Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.*			
A.11.2.1	Ubicación y protección de los equipos	***Control*** : Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las posibilidades de acceso no autorizado.	**APLICA** **SI** / **NO** Los equipos deberían estar protegidos físicamente de amenazas ambientales (fuego, incendio, agua, humo) y humanas así como evitar el acceso no autorizado. **IMPLEMENTA** **SI** / **NO** Los equipos están protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, etc. De igual forma existen lineamientos para su uso.
A.11.2.2	Servicios de suministro	***Control*** : Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	**APLICA** **SI** / **NO** Los servicios de suministros como energía, agua, ventilación y gas deberían estar acordes a la manufacturación de los equipos. **IMPLEMENTA** **SI** / **NO** Los servicios de suministros como energía, agua, ventilación y gas están acordes a la manufacturación de los equipos.
A.11.2.3	Seguridad del cableado	Control: El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se deben proteger contra interceptación, interferencias o daño.	**APLICA** **SI** / **NO** El cableado provee la transmisión de datos o energía a los dispositivos. **IMPLEMENTA** **SI** / **NO** El cableado eléctrico está separado del cableado de datos previniendo así interferencias y están protegidos físicamente.

A.11.2.4	Mantenimiento de equipos	***Control*** : Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	**APLICA** **SI** | **NO** El mantenimiento de los equipos garantiza su óptimo funcionamiento y rendimiento. **IMPLEMENTA** **SI** | **NO** Los equipos son mantenidos sólo por el personal autorizado bajo las condiciones especificadas y a intervalos programados.

A.11.2.5	Retiro de activos	***Control*** : Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	**APLICA** **SI** | **NO** El retiro de los equipos, eliminación de software e información sólo debería ser realizada por el personal autorizado. **IMPLEMENTA** **SI** | **NO** El retiro de los equipos, eliminación de software e información sólo es realizada por el personal autorizado.

A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	***Control*** : Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.	**APLICA** **SI** | **NO** Los equipos y/o dispositivos que pertenecen a la organización deberían ser gestionados sólo por el personal autorizado, así como tampoco ser utilizado en lugares públicos. **IMPLEMENTA** **SI** | **NO** Los equipos sólo son utilizados dentro de las instalaciones físicas de la organización.

A.11.2.7	Disposición segura o reutilización de equipos	***Control*** : Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software licenciado haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.	**APLICA** **SI** | **NO** Para la disposición o reutilización de equipos se debería tener un procedimiento que garantice la destrucción total de la información contenida con el fin de evitar de ser leída por personas no autorizadas. **IMPLEMENTA** **SI** | **NO** Se realiza un procedimiento seguro para la disposición o reutilización de equipos.
A.11.2.8	Equipos de usuario desatendido	***Control*** : Los usuarios deben asegurarse de que los equipos desatendidos se les de la protección apropiada.	**APLICA** **SI** | **NO** Los usuarios deberían cerrar sesiones y proteger el equipo con contraseñas fuertes cuando no lo estén utilizando ya que podría estar expuesto a acceso no autorizado. **IMPLEMENTA** **SI** | **NO** Aunque no exista una política documentada, los usuarios son conscientes y aplican la seguridad apropiada cuando el equipo está en desuso.
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	***Control*** : Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.	**APLICA** **SI** | **NO** El almacenamiento de información confidencial no debería ser visible al público. **IMPLEMENTA** **SI** | **NO** La información confidencial es almacenada en gabinetes de forma segura impidiendo su acceso físico a personas no autorizadas.

Tabla 46. Anexo A de la NTP-ISO/IEC 27001:2014. Seguridad Física y del Entorno.

A.12	SEGURIDAD DE LAS OPERACIONES		
A.12.1	**Procedimientos operacionales y responsabilidades**		
Objetivo *: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.*			
A.12.1.1	Procedimientos de operación documentados	***Control*** : Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.	**APLICA** **SI** / **NO** Los procedimientos operacionales deberían estar documentados y disponibles para todos los usuarios. Estos procedimientos incluyen las copias de seguridad, almacenamiento, manejo de errores, encendido/apagado de equipos, instalación/configuración de sistemas, etc. Esta documentación es de carácter obligatorio en la NTP-ISO/IEC 27001:2014. **IMPLEMENTA** **SI** / **NO** Los procedimientos operacionales no están documentados, ya que no existe aún una implementación de un SGSI.
A.12.1.2	Gestión de cambios	***Control*** : Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	**APLICA** **SI** / **NO** Los cambios en los equipos que afectan la seguridad de la información deberían ser controlados y debidamente planeados y probados. **IMPLEMENTA** **SI** / **NO** Los cambios en los equipos que afectan la seguridad de la información son controlados y debidamente planeados y probados.
A.12.1.3	Gestión de capacidad	***Control*** : Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido por el sistema.	**APLICA** **SI** / **NO** Los recursos deberían ser monitoreados con el fin de gestionar su capacidad y rendimiento, así como proyectar que responda a las necesidades de la organización a largo plazo. **IMPLEMENTA** **SI** / **NO** Se les realiza un monitoreo continuo a los recursos y la adquisición de nuevos se proyecta de acuerdo a las necesidades críticas de la organización.

A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	***Control*** : Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	**APLICA** **SI** / **NO** La separación de ambientes de desarrollo y pruebas reduce el riesgo de operaciones no autorizadas. **IMPLEMENTA** **SI** / **NO** Los ambientes de desarrollo y prueban están separados.

A.12.2	**Protección contra códigos maliciosos**
Objetivo *: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.*	

A.12.2.1	Controles contra códigos maliciosos	***Control*** : Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	**APLICA** **SI** / **NO** El malware o software malicioso es un riesgo potencial para los sistemas y equipos, ya que pueden hacer que los sistemas operen de forma ineficiente, captura ilegal de información confidencial y borrado total. **IMPLEMENTA** **SI** / **NO** Aunque no existe una política claramente definida contra el malware, los usuarios son conscientes de los efectos nefastos que éstos podrían tener sobre el sistema y/o información. De igual forma, se mantienen los equipos actualizados y con software antimalware licenciado ejecutándose donde son monitoreados continuamente.

A.12.3	**Copias de respaldo**
Objetivo *: Proteger contra la pérdida de datos.*	

A.12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de información, software e imágenes de los sistemas, y ponerlos a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	**APLICA** **SI** / **NO** Las copias de seguridad (*backups*) e imágenes de los sistemas garantizan que la información esencial e instalación de software podría ser recuperada después de fallas o desastres. **IMPLEMENTA** **SI** / **NO** Las copias de seguridad se realizan a intervalos programados y de forma automática.

A.12.4	Registro y seguimiento		
***Objetivo**: Registrar eventos y generar evidencia.*			
A.12.4.1	Registro de eventos	***Control***: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	**APLICA** **SI** / **NO** Los registros (*logs*) almacenan información relevante sobre los eventos ocurridos en la operación de un sistema. **IMPLEMENTA** **SI** / **NO** Se mantienen los registros de los eventos ocurridos en los sistemas.
A.12.4.2	Protección de la información de registro	***Control***: Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	**APLICA** **SI** / **NO** Los registros de eventos deberían ser custodiados para prevenir modificación no autorizada. **IMPLEMENTA** **SI** / **NO** Los registros de eventos están protegidos contra el acceso no autorizado.
A.12.4.3	Registros del administrador y del operador	***Control***: Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.	**APLICA** **SI** / **NO** Los administradores tienen accesos privilegiados y podrían modificar información de los registros de eventos.
			IMPLEMENTA **SI** / **NO** Las acciones y registros de los administradores también son almacenados y protegidos de cualquier modificación.
A.12.4.4	Sincronización de relojes	***Control***: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	**APLICA** **SI** / **NO** La sincronización de los relojes de los sistemas permite mantener una referencia única de tiempo y zona horaria. **IMPLEMENTA** **SI** / **NO** Aunque no existe una política documentada sobre la sincronización de los relojes, todos los sistemas están sincronizados bajo un único formato de tiempo y zona horaria.

A.12.5	Control de software operacional		
***Objetivo**: Asegurarse de la integridad de los sistemas operacionales.*			
A.12.5.1	Instalación de software en los sistemas operativos	***Control***: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	**APLICA** **SI** / **NO** Se debería controlar las instalaciones de software en los sistemas operativos. **IMPLEMENTA** **SI** / **NO** No existe una política documentada o procedimientos sobre la instalación de software en los sistemas operativos.

A.12.6	Gestión de la vulnerabilidad técnica		
***Objetivo**: Prevenir el aprovechamiento de las vulnerabilidades técnicas.*			
A.12.6.1	Gestión de las vulnerabilidades técnicas	***Control***: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	**APLICA** **SI** / **NO** El inventario de los activos se debería mantener actualizado con el fin de identificar a tiempo los riesgos asociados a las vulnerabilidades y amenazas técnicas. **IMPLEMENTA** **SI** / **NO** Aunque existe un inventario de los activos físicos y del software operacional, no se tiene una metodología de riesgos que los evalúe.
A.12.6.2	Restricciones sobre la instalación de software	***Control***: Se debe establecer e implementar las reglas para la instalación de software por parte de los usuarios.	**APLICA** **SI** / **NO** Cualquier persona con elevados privilegios de acceso podría instalar cualquier software en un equipo y/o dispositivo. El no control podría liderar a la instalación de software malicioso o no permitido. **IMPLEMENTA** **SI** / **NO** La instalación de software es realizada sólo por el personal autorizado y con software probado y licenciado, además de otorgar el principio del menor privilegio.

A.12.7	Consideraciones sobre auditorías de sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.			
A.12.7.1	Controles de auditorías de sistemas de información	***Control*** : Los requisitos y actividades que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos de negocio.	**APLICA** **SI** / **NO** Las auditorías de los sistemas deberían ser acordadas, planeadas y controladas sin interferir en el desarrollo normal de los procesos. **IMPLEMENTA** **SI** / **NO** No se tiene un plan de auditoría para la verificación de los sistemas operativos.

Tabla 47. Anexo A de la NTP-ISO/IEC 27001:2014. Seguridad de las Operaciones.

A.13	SEGURIDAD DE LAS COMUNICACIONES		
A.13.1	Gestión de la seguridad de las redes		
Objetivo *: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.*			
A.13.1.1	Controles de redes	***Control*** : Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	**APLICA** **SI** / **NO** Las redes deberían proteger la transmisión de la información garantizando su confidencialidad e integridad y en algunos casos su disponibilidad. **IMPLEMENTA** **SI** / **NO** No existe una Infraestructura de Llave Pública (*PKI*) implementada que garantice que la información transmitida en las redes sea segura.

A.13.1.2	Seguridad de los servicios de red	***Control*** : Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o contraten externamente.	**APLICA** **SI** / **NO** El acceso a la red de los proveedores de servicios de red debería ser controlado y monitoreado. **IMPLEMENTA** **SI** / **NO** El acceso a la red de los proveedores de servicio de red es monitoreado y controlado.

A.13.1.3	Separación en las redes	***Control*** : Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	**APLICA** **SI** / **NO** Los usuarios y servicios deberían estar separados lógicamente en unidades organizacionales o dominios, o **IMPLEMENTA** **SI** / **NO** Los usuarios y servicios están separados a través de dominios y VLANS.

A.13.2	**Transferencia de información**	
Objetivo *: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.*		
A.13.2.1	Políticas y procedimientos de transferencia de información	***Control*** : Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.	**APLICA** **SI** / **NO** Los procedimientos y controles ayudan a mantener la seguridad de la información cuando es transferida a otra **IMPLEMENTA** **SI** / **NO** No existe una documentación sobre los procedimientos y controles a implementar para la transferencia segura de la información.

A.13.2.2	Acuerdos sobre transferencia de información	***Control***: Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	**APLICA** **SI** | **NO** Se deberían tener acuerdos sobre los procedimientos para la transferencia segura de la información. **IMPLEMENTA** **SI** | **NO** No se han implementado controles criptográficos que garanticen la seguridad en la transmisión de la información.
A.13.2.3	Mensajería electrónica	***Control***: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	**APLICA** **SI** | **NO** Se deberían proteger los mensajes enviados internamente de los empleados de la organización. **IMPLEMENTA** **SI** | **NO** No se han implementado controles criptográficos que garanticen la seguridad en la transmisión de la información.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	***Control***: Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	**APLICA** **SI** | **NO** Los acuerdos con los empleados o con entes externos deberían tener acuerdos de confidencialidad de la información. **IMPLEMENTA** **SI** | **NO** En los documentos y acuerdos contractuales de los empleados se estipula el compromiso con la confidencialidad de la información

Tabla 48. Anexo A de la NTP-ISO/IEC 27001:2014. Seguridad de las Comunicaciones.

A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		
A.14.1	**Requisitos de seguridad de los sistemas de información**		
Objetivo *: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que presten servicios sobre redes públicas.*			
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	***Control*** : Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	**APLICA** **SI** / **NO** Los requerimientos de la seguridad de la información deberían ser identificados utilizando varios métodos en concordancia con las políticas y regulaciones. **IMPLEMENTA** **SI** / **NO** No existe una política de seguridad de información que ayude a determinar la adquisición de los nuevos sistemas de información.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	***Control*** : La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	**APLICA** **SI** / **NO** La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad. **IMPLEMENTA** **SI** / **NO** No existe una Infraestructura de Llave Pública (*PKI*) implementada que garantice que la información transmitida en las redes sea segura.
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	***Control:*** *La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.*	**APLICA** **SI** / **NO** La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad. **IMPLEMENTA** **SI** / **NO** No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información transmitida en las redes sea segura

A.14.2	Seguridad en los procesos de desarrollo y soporte		
***Objetivo**: Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.*			
A.14.2.1	Política de desarrollo seguro	***Control***: Se deben establecer y aplicar las reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.	**APLICA** **SI** / **NO** Las políticas y controles de seguridad deberían ser aplicados en el desarrollo de software. **IMPLEMENTA** **SI** / **NO** De acuerdo a las necesidades de la entidad.
A.14.2.2	Procedimientos de control de cambios en sistemas	***Control***: Los cambios de sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formales de control de cambios.	**APLICA** **SI** / **NO** El procedimiento formal de los cambios en el desarrollo de software debería ser documentado para garantizar la integridad del sistema o aplicación. **IMPLEMENTA** **SI** / **NO** Control por versiones.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	***Control***: Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones de seguridad de la organización.	**APLICA** **SI** / **NO** Los cambios en las aplicaciones deberían ser revisados y probados antes de implementarlas de manera que se garantice que no comprometa la seguridad. **IMPLEMENTA** **SI** / **NO** Las aplicaciones y plataformas de operación son revisadas y probadas antes de implementarse.

A.14.2.4	Restricciones en los cambios a los paquetes de software	***Control*** : Se deben desalentar las modificaciones de los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	**APLICA** **SI** / **NO** Limitar las modificaciones de software sólo a lo estrictamente **IMPLEMENTA** **SI** / **NO** Las actualizaciones y modificaciones de software son desarrolladas por el peronal de la
A.14.2.5	Principios de construcción de los sistemas seguros	***Control*** : Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.	**APLICA** **SI** / **NO** Se deberían establecer y documentar los principios de desarrollo de software seguro. **IMPLEMENTA** **SI** / **NO** los sistemas deben ser seguros.
A.14.2.6	Ambiente de desarrollo seguro	***Control*** : Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	**APLICA** **SI** / **NO** Los ambientes de desarrollo de software también deberían estar protegidos de acceso no autorizado o de ejecución de software **IMPLEMENTA** **SI** / **NO** falta infraestructura.
A.14.2.7	Desarrollo contratado externamente	***Control*** : La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.	**APLICA** **SI** / **NO** El software desarrollado externamente debería tener licencia, acuerdos y prácticas de desarrollo y pruebas seguros. **IMPLEMENTA** **SI** / **NO** Se asegura que el software desarrollado externamente contiene las prácticas de desarrollo y pruebas seguros.

A.14.2.8	Pruebas de seguridad de sistemas	***Control*** : Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de seguridad.	**APLICA** **SI** / **NO** Se deberían realizar visitas y pruebas de seguridad al software que se está desarrollando. **IMPLEMENTA** **SI** / **NO** No se realizan pruebas de seguridad al software durante su período de desarrollo.
A.14.2.9	Pruebas de aceptación de sistemas	***Control*** : Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deben establecer programas de prueba para aceptación y criterios de aceptación relacionados,	**APLICA** **SI** / **NO** Se deberían realizar pruebas de seguridad en base a los requerimientos de seguridad de la organización. **IMPLEMENTA** **SI** / **NO** No se realizan las pruebas de seguridad debido a que aún no existen los lineamientos o políticas de la seguridad de la información.
A.14.3	**Datos de prueba**		
Objetivo *: Asegurar la protección de los datos usados para pruebas.*			
A.14.3.1	Protección de datos de prueba	***Control:*** *Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.*	**APLICA** **SI** / **NO** Los datos de prueba deberían ser seleccionados cuidadosamente y que no contengan ninguna información confidencial. **IMPLEMENTA** **SI** / **NO** Los datos de prueba son seleccionados cuidadosamente y no presentan riesgo para la violación de confidencialidad de la información.

Tabla 49. Anexo A de la NTP-ISO/IEC 27001:2014. Adquisición, Desarrollo y Mantenimiento de Sistemas.

A.15	RELACIONES CON LOS PROVEEDORES		
A.15.1	**Seguridad de la información en las relaciones con los proveedores**		
Objetivo *: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.*			
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	***Control*** : Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar y se deben documentar.	**APLICA** **SI** / **NO** La organización debería emplear los controles y procedimientos de seguridad para el acceso a los activos por parte de los proveedores. **IMPLEMENTA** **SI** / **NO** No se tiene una política de seguridad definida.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	***Control*** : Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	**APLICA** **SI** / **NO** Se deberían establecer acuerdos de seguridad documentados entre la organización y los proveedores para el acceso a los activos. **IMPLEMENTA** **SI** / **NO** No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación	***Control*** *: Los acuerdos con los proveedores deben incluir requisitos para tratar los riesgos de seguridad de información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.*	**APLICA** **SI** / **NO** Los suministros de los proveedores deberían estar acordes a las políticas de seguridad de la información de la organización. **IMPLEMENTA** **SI** / **NO** No se establecen los acuerdos documentados ya que no existe una clasificación de seguridad de la información, así como tampoco las políticas y procedimientos.

A.15.2	Gestión de la prestación de servicios de proveedores		
***Objetivo**: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.*			
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	***Control***: Las organizaciones deben hacer seguimiento, revisar y auditar con la regularidad la prestación de servicios de los proveedores.	**APLICA** **SI** / **NO** El monitoreo y acceso de los proveedores debería ser acorde las políticas de seguridad de la organización. **IMPLEMENTA** **SI** / **NO** No existe una política de seguridad de la información y procedimientos.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	***Control***: Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de riesgos.	**APLICA** **SI** / **NO** Los cambios de los proveedores deberían estar acordes a los requerimientos de seguridad de la información de la organización. **IMPLEMENTA** **SI** / **NO** No existe una política de seguridad de la información y procedimientos.

Tabla 50. Anexo A de la NTP-ISO/IEC 27001:2014. Relaciones con los Proveedores.

A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN		
A.16.1	**Gestión de incidentes y mejoras de la seguridad de la información**		
***Objetivo**: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.*			
A.16.1.1	Responsabilidades y procedimientos	***Control***: Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	**APLICA** **SI** / **NO** Los planes y procedimientos para gestionar los incidentes relacionados a la seguridad de la información deberían estar documentados. **IMPLEMENTA** **SI** / **NO** No existen los procedimientos documentados para gestionar los incidentes relativos a la seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	***Control***: Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados, tan pronto como sea posible.	**APLICA** **SI** / **NO** Todos los empleados deben estar pendientes de los eventos y reportes de seguridad de la información. **IMPLEMENTA** **SI** / **NO** Los empleados están alertados de los eventos e incidentes correspondientes relativos a la seguridad de la información.
A.16.1.3	Reporte de debilidades de seguridad de la información	***Control***: Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	**APLICA** **SI** / **NO** Se deberían implementar mecanismos de reportes de incidentes de seguridad de la información en donde todos los empleados deberían reportar las brechas de seguridad con el fin de **IMPLEMENTA** **SI** / **NO** Los empleados están comprometidos en reportar las brechas lo antes posible.

A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	***Control*** : Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	**APLICA** **SI** / **NO** La clasificación y priorización de los incidentes de seguridad ayudan a identificar el impacto en la organización. **IMPLEMENTA** **SI** / **NO** Los activos no están clasificados y no existe una metodología de análisis y evaluación de riesgos informáticos.
A.16.1.5	Respuesta a incidentes de seguridad de la información	***Control*** : Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	**APLICA** **SI** / **NO** Deberían existir procedimientos documentados para dar respuesta a los incidentes restableciendo la operación al nivel de seguridad aceptable lo más pronto posible. **IMPLEMENTA** **SI** / **NO** Aunque las respuestas son inmediatas, los procedimientos de respuesta no están documentados, así como tampoco existe un Plan de Continuidad del Negocio.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	***Control*** : El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto sobre incidentes futuros.	**APLICA** **SI** / **NO** Se debería recolectar información de los incidentes ocurridos con el fin de prevenirlos en el futuro. **IMPLEMENTA** **SI** / **NO** Se recolecta la información de los incidentes y se aplican los controles necesarios para prevenirlos.
A.16.1.7	Recolección de evidencia	***Control*** : La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	**APLICA** **SI** / **NO** Se deberían recolectar las evidencias y registros para tomar acciones legales. **IMPLEMENTA** **SI** / **NO** Las evidencias son recolectadas formalmente para emprender las acciones legales.

Tabla 51. Anexo A de la NTP-ISO/IEC 27001:2014. Gestión de Incidentes de Seguridad de la Información.

A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO		
A.17.1	**Continuidad de seguridad de la información**		
***Objetivo**: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.*			
A.17.1. 1	Planificación de la continuidad de la seguridad de la información	***Control*** : La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.	**APLICA** **SI** / **NO** Los Planes de Continuidad del Negocio (*BCP*) y los Planes de Recuperación de Desastres (*DRP*) deberían estar planificados y documentados para restablecer la operación normal dado un evento. Esta documentación es de carácter obligatorio en la norma ISO 27001:2014. **IMPLEMENTA** **SI** / **NO** No existe la documentación o los procedimientos para los BCP y DRP.
A.17.1. 2	Implementación de la continuidad de la seguridad de la información	***Control*** : La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	**APLICA** **SI** / **NO** Los Planes de Continuidad del Negocio (*BCP*) y los Planes de Recuperación de Desastres (*DRP*) deberían estar planificados y documentados para restablecer la operación normal dado un evento. Esta documentación es de carácter obligatorio en la norma ISO 27001:2014. **IMPLEMENTA** **SI** / **NO** No existe la documentación o los procedimientos para los BCP y DRP.

A.17.1. 3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	***Control*** : La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son válidos y eficaces durante situaciones adversas.	**APLICA** **SI** / **NO** Los procedimientos y controles para la restablecer los servicios se deberían revisar en intervalos regulares con cada uno de los responsables para verificar su efectividad. **IMPLEMENTA** **SI** / **NO** No existe la documentación o los procedimientos para los BCP y DRP.
A.17.2	**Redundancias**		
Objetivo *: Asegurar la disponibilidad de instalaciones de procesamiento de información.*			
A.17.2. 1	Disponibilidad de instalaciones de procesamiento de información	***Control*** : Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	**APLICA** **SI** / **NO** La información debería ser redundante con el fin de mantener la disponibilidad de los servicios y ser probadas en intervalos regulares. **IMPLEMENTA** **SI** / **NO** La organización no dispone de redundancia de la información.

Tabla 52. Anexo A de la NTP-ISO/IEC 27001:2014. Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio.

A.18	CUMPLIMIENTO		
A.18.1	**Cumplimiento de los requisitos legales y contractuales**		
***Objetivo** : Evitar el incumplimiento de las obligaciones legales, estatuarias, de reglamentación o contractuales relacionadas con la seguridad de la información y de cualquier requisito de seguridad.*			
A.18.1.1	Identificación de la legislación aplicable a los requisitos contractuales	***Control*** : Todos los requisitos estatuarios, reglamentarios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.	**APLICA** **SI** | **NO** Los administradores deberían identificar toda la información legislativa aplicable a la organización con el fin de cumplir con los requerimientos del negocio. **IMPLEMENTA** **SI** | **NO** Los requisitos contractuales están identificados y se cumplen con los requerimientos exigidos por la ley.
A.18.1.2	Derechos de propiedad intelectual	***Control*** : Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.	**APLICA** **SI** | **NO** Se deberían definir las políticas y procedimientos para controlar la propiedad intelectual. **IMPLEMENTA** **SI** | **NO** No se desarrolla y/o patenta software.
A.18.1.3	Protección de registros	***Control*** : Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	**APLICA** **SI** | **NO** Los registros deberían estar clasificados de acuerdo al esquema adoptado por la organización de acuerdo al nivel de confidencialidad. **IMPLEMENTA** **SI** | **NO** No existe un nivel de clasificación formal de confidencialidad de los registros.

A.18.1.4	Privacidad y protección de información de datos personales	***Control*** : Se deben asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	**APLICA** **SI** / **NO** Se debería documentar y definir políticas relativas a la protección de datos personales de acuerdo a las reglamentaciones que la ley exige. **IMPLEMENTA** **SI** / **NO** Existe una política relativa a la protección de datos personales conforme a los requerimientos de la ley.
A.18.1.5	Reglamentación de controles criptográficos	***Control*** : Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	**APLICA** **SI** / **NO** Los controles criptográficos permiten garantizar la confidencialidad, integridad y autenticidad de la información. **IMPLEMENTA** **SI** / **NO** No existe una Infraestructura de Llave Pública (*PKI*) implementada que garantice que la información transmitida y/o almacenada sea segura.
A.18.2	**Revisiones de seguridad de la información**		
Objetivo *: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.*			
A.18.2.1	Revisión independiente de la seguridad de la información	***Control*** : El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de información) se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	**APLICA** **SI** / **NO** Se deberían realizar auditorías de los procesos, procedimientos y sistemas por medio de entidades externas. **IMPLEMENTA** **SI** / **NO** No se realizan auditorías con entidades externas.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	***Control***: Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.	**APLICA** **SI** / **NO** Se deberían realizar revisiones de las políticas de seguridad con el fin de verificar su cumplimiento. **IMPLEMENTA** **SI** / **NO** No existen políticas de la seguridad de la información con la cual se permitan comparar los resultados.

A.18.2.3	Revisión del cumplimiento técnico	*Control*: Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de información.	APLICA SI / NO Los test de penetración deben ser realizados por con herramientas automáticas, con personal calificado y en intervalos programados y acordados con el fin de verificar las políticas de seguridad así como los requerimientos. IMPLEMENTA SI / NO Aunque se realizan algunos test de penetración no hay políticas de seguridad o metodología de riesgo que permita comparar los resultados.

Tabla 53. Anexo A de la NTP-ISO/IEC 27001:2014. Cumplimiento.

En resumen, el nivel de cumplimiento para cada uno de los Dominios, Objetivos de Control y Controles de Seguridad del Anexo A de la NTP-ISO/IEC 27001:2014, queda de la siguiente manera:

DOMINIO DE CONTROL	CUMPLE (%)	NO CUMPLE (%)
A5. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN	0	0
A6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	30	70
A7. SEGURIDAD DE LOS RECURSOS HUMANOS	35	75
A8. GESTIÓN DE ACTIVOS	30	70
A9. CONTROL DE ACCESO	40	60
A10. CRIPTOGRAFÍA	20	80
A11. SEGURIDAD FÍSICA Y DEL ENTORNO	50	50
A12. SEGURIDAD DE LAS OPERACIONES	70	30
A13. SEGURIDAD DE LAS COMUNICACIONES	45	55
A14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	60	40
A15. RELACIONES CON LOS PROVEEDORES	30	70
A16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	60	40
A17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	0
A18. CUMPLIMIENTO	25	75

Tabla 54. Anexo A de la NTP-ISO/IEC 27001:2014. Dominios de control.

El nivel de cumplimiento general que se tiene actualmente referente a estos Dominios de Control es el siguiente:

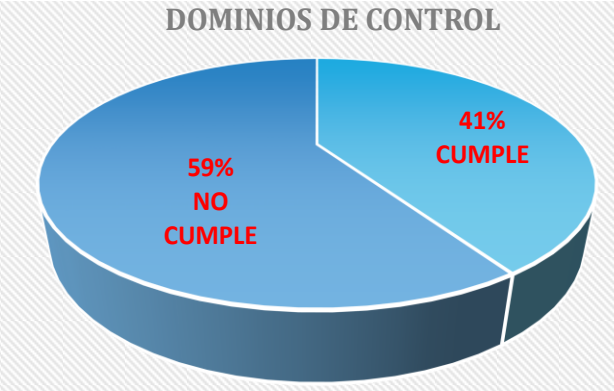


Grafico 02 Nivel de cumplimiento de Dominios de Control la NTP-ISO/IEC 27001:2014.

Mediante este Análisis Diferencial es posible determinar que la Dirección General de Informática y Estadística de la UNDAC, no cumple con la mayoría de los Dominios, Objetivos de Control y Controles de Seguridad propuestos en la NTP-ISO/IEC 27001:2014. Esto se refleja en que no se tiene la documentación correspondiente al estándar, así como tampoco el empleo de mecanismos de seguridad en la transmisión de la información.

Por otro lado, aunque las instalaciones físicas estén protegidas con algunos controles de acceso y vigilancia, el personal y algunos activos informáticos no están lo suficientemente protegidos ante una eventualidad de orden mayor, y no existen procedimientos de contingencia para garantizar la continuidad de las operaciones.

REVISIÓN POR LA DIRECCIÓN

La agenda de revisión de la gestión de la NTP ISO-IEC 27001 2014 consiste en los siguientes elementos:

- Introducción
- Propósito de la reunión
- Comprobación de la lista de asistentes
- Revisión de las Revisiones anteriores
- Revisar informes de reuniones anteriores
- Verificar el estado de las acciones
- Registrar el estado de acciones completadas vs acciones en curso
- Cerrar acciones completadas
- SGSI y gestión de riesgos

- Revisión del el alcance y los objetivos del SGSI.
- Revise el desempeño y la mejora continua del SGSI (objetivos, acciones, no conformidades)
- Revisión de los recursos, presupuestos y otros temas relacionados con las limitaciones del SGSI
- Revise el registro de riesgos y los riesgos pendientes, cubiertos, riesgos residuales
- Revisión de las políticas y procedimientos de seguridad de la información.
- Métricas de rendimiento / KPI:
- Métricas de rendimiento y los KPI
- Análisis de los resultados de incidentes recientes y análisis causal
- Cierre de la reunión
- Confirmar acciones y propietarios de acciones
- Confirmar planificación de tiempo para acciones
- Confirmar fecha y hora de la próxima reunión

10 MEJORA

OFICINA GENERAL DE INFORMÁTICA Y ESTADISTICA

UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN

PLAN DE CONTINUIDAD DEL NEGOCIO

Código del Documento	SGSIUNDAC01
Versión	1.0
Fecha de Versión	10/07/2018
Propietario	DGIyE-UNDAC
Nivel de Confidencialidad	Baja

1. PROPÓSITO, ALCANCE Y USUARIOS

1.1 PROPÓSITO

El propósito de este Plan de Continuidad del Negocio, es preparar a la Dirección General de Informática y Estadística de la UNDAC, en la eventualidad de la interrupción de los servicios causados por factores más allá de nuestro control (ej. Desastres naturales, acciones realizadas por personas, ataques informáticos a gran escala, etc.), y restablecer los servicios en el menor tiempo posible.

1.2 ALCANCE

El alcance de este plan está limitado solamente a la Dirección General de Informática y Estadística de la UNDAC.

1.3 OBJETIVOS

- Servir como guía para el equipo de recuperación de desastres de la Dirección General de Informática y Estadística.
- Referenciar y localizar los datos críticos.
- Proveer los procedimientos y recursos necesarios para ayudar en la recuperación.
- Identificar los entes que deben ser notificados en la eventualidad de un desastre.
- Ayudar para evitar las confusiones durante una crisis por medio de la documentación, pruebas y repaso de procedimientos de recuperación.
- Identificar fuentes alternas para los recursos e infraestructura.

- Establecer procedimientos para el almacenamiento, resguardo y recuperación de documentos vitales.

1.4 SUPUESTOS

- Disponibilidad del personal encargado de la eventualidad del desastre.
- Este documento y todos los registros confidenciales están almacenados en otra ubicación segura donde no se presenta el desastre actual y están accesibles.

1.5 USUARIOS

Los usuarios de este documento son todas aquellas personas internas o externas a la organización que tienen un rol en la continuidad del negocio.

2. DOCUMENTOS DE REFERENCIA

Para más información, se pueden consultar los siguientes documentos:

- NTP ISO/IEC 27001:2014.
- Política de la Continuidad del Negocio.
- Estatutos legales, reguladores y contractuales.

3. PLAN DE CONTINUIDAD DEL NEGOCIO

3.1 CONTENIDO DEL PLAN

Este plan se hace efectivo cuando ocurra un evento catalogado como desastre. Los procedimientos normales de administración iniciarán el plan y quedarán activos hasta que las operaciones y los servicios se reinicien en el lugar original o en reemplazo de ésta siempre y cuando sean aptos para el funcionamiento normal.

En este documento se establecen la composición del equipo encargado de la continuidad de la operación del negocio en la eventualidad de un incidente mayor o desastre, cuándo se activa/desactiva el plan y el orden de los procedimientos y actividades prioritarias.

3.2 ROLES Y RESPONSABILIDADES

El equipo encargado del plan de continuidad del negocio está compuesto por los siguientes roles:

ROL	RESPONSABILIDADES
Administrador Plan de Continuidad del Negocio (BCP Manager)	▪ Establecer la coordinación interna/externa con la alta gerencia, administrativos incluidos en el Plan de continuidad del negocio, entre otros, con el fin de establecer los requerimientos y procesos para el normal funcionamiento de las actividades críticas y estratégicas. ▪ Establecer las políticas para el Plan de continuidad del negocio, desarrollando estrategias que complementen y soporten los riesgos y objetivos de seguridad. ▪ Asegurarse de que los procesos críticos de negocio son lo suficientemente resistentes para continuar con la operación efectiva más allá de los incidentes o desastres.
Administrador del Plan de Recuperación de Desastres	▪ Encargarse de restaurar los procesos y servicios críticos en el tiempo estipulado después del incidente o desastre.
(Plan de Continuidad del negocio Manager)	▪ Evaluar y priorizar los procesos de negocio para la restauración. ▪ Determinar los requerimientos de recuperación teniendo en cuenta la interdependencia de los procesos. ▪ Justificar las inversiones adicionales al plan de recuperación del negocio.
Administración de Evaluación Técnica (Líderes de Recuperación del estado de las redes, bases de datos y de servidores)	▪ Trabajar conjuntamente con los otros responsables del Plan de continuidad del negocio, para proveer evaluación y requerimientos técnicos para una efectiva recuperación. ▪ Diseñar las herramientas de evaluación para determinar el nivel apropiado de los servicios de recuperación. ▪ Evaluar la resistencia y las capacidades de recuperación y riesgos inherentes a la infraestructura de TI. ▪ Proveer el uso de nuevas tecnologías y procesos para soportar la recuperación de desastres de TI.

Tabla Nro. 55 Roles y responsabilidades

3.3 CONTACTOS CLAVES

Datos de contacto de las personas que participarán en el Plan de Continuidad del negocio:

N°	ROL	APELLIDOS y NOMBRES	DEPENDENCIA	TELÉFONOS
1				
2				
3				
4				
5				

Tabla Nro. 56 Contactos claves

3.4 ACTIVACIÓN Y DESACTIVACIÓN DEL PLAN

La activación define las acciones tomadas una vez exista una interrupción en los servicios críticos de la Dirección General de Informática y Estadística de la UNDAC. Se incluyes las actividades para notificar al personal de

recuperación de desastres, conducir una evaluación de la interrupción y activar el Plan de continuidad del negocio.

El Plan de continuidad del negocio, será activado cuando se presenten algunos de los siguientes eventos:

1. El tipo de desastre suponga una interrupción de los servicios en más de 4 horas. Dentro de ellas se encuentran:
   - Falla del Hardware.
   - Interrupción del fluido eléctrico o telecomunicaciones.
   - Fallas en Aplicaciones o corrupción de las bases de datos.
   - Errores humanos, sabotaje o golpes.
   - Ataque y propagación de software malicioso.
   - Hacking no autorizado de los sistemas.
   - Desastres naturales (Inundaciones, Terremotos, Huracanes, etc.).
2. La infraestructura física de la oficina esté dañada o no disponible en un período de 4 horas.
3. Cualquier otro criterio que suponga una interrupción de los servicios críticos de tiempo indefinido.

Las personas con los roles establecidos y que hagan parte de las implementaciones del plan de continuidad del negocio serán notificados inmediatamente.

Independientemente del tipo de desastre o incidente, la vida, salud, bienestar y seguridad de las personas será la prioridad.

3.5 COMUNICACIÓN

Los canales de comunicación se utilizarán en caso del incidente o desastre.

El equipo encargado del Plan de Continuidad del Negocio, utilizará los teléfonos celulares personales y/o corporativos y dispositivos de radio-comunicación. De igual forma, se informará a las autoridades competentes por medio de la radio y medios impresos.

3.6 ORDEN DE RECUPERACIÓN DE ACTIVIDADES

Se realizan los procedimientos formales para las operaciones de recuperación después que haya sido activado el Plan de continuidad del negocio, evaluados las interrupciones y el personal notificado. En esta fase se implementan las estrategias para recuperar el sistema, reparar los daños y reanudar las capacidades originales a la ubicación alternativa.

Después de implementada esta fase, las actividades y procesos críticos de la Dirección de Informática y estadística de la UNDAC serán funcionales.

Para dar continuidad efectivamente en el menor tiempo posible, se deben ejecutar las siguientes actividades generales en el orden aquí establecido:

1. Identificar los recursos requeridos para realizar los procedimientos de continuidad y recuperación.
2. Recuperar las copias de seguridad y los medios de instalación.
3. Recuperar el hardware y los sistemas operativos.
4. Recuperar el sistema desde las copias de seguridad y los medios de instalación.

CONCLUSIONES:

El Diseño del Sistema de Gestión de la Seguridad de la Información bajo el contexto de una organización inteligente, tiene como objetivo la disminución de la incertidumbre y la complejidad en la situación en que se encuentra la seguridad de la información, los cinco niveles que lo integran no se limitan exclusivamente a describir factores que influyen sobre ella, como los gerenciales, el análisis de gestión de riesgo, la planificación estratégica y la cultura organizacional, entre otros. Este modelo incorpora herramientas de una organización alineada con el concepto de la normatividad NTP-ISO/IEC 27001:2014, característica que permite derrumbar algunos mitos y creencias que afectan la instrumentación de acciones que reducen el riesgo potencial de materializarse una amenaza, dada una vulnerabilidad asociada a un activo informático.

El problema de la inseguridad informática no se resuelve únicamente al identificar los servicios de seguridad a proteger, las herramientas de seguridad de las TIC's, la operacionalización de las políticas de seguridad y las normas, la situación es compleja, trasciende los aspectos tecnológicos, involucra el trabajo en conjunto de los trabajadores encargados de la seguridad, el desarrollo continuo de nuevas actitudes y aptitudes, la aplicación del pensamiento sistémico, un factor crítico al incorporar el dogma de las organizaciones inteligentes, sus valores éticos, la visión compartida y los modelos mentales bajo una perspectiva de la seguridad de la información. Sin embargo, en muchas organizaciones, los gerentes y el personal encargado de la seguridad de la información poseen un modelo mental que impide a las organizaciones alcanzar un mayor nivel de madurez en el manejo de la situación.

Otras conclusiones del presente estudio se pueden dar bajo los siguientes puntos:

- Hay decisiones respecto al cumplimiento de políticas dentro del SGSI que deben ser de carácter jerárquico, impulsado por la Alta Dirección, siendo este el primer paso para adaptarse a todo cambio coyuntural dentro de la Universidad. Bajo esta afirmación, la Alta Dirección de la UNDAC no garantizo la participación activa de todos los líderes del proceso, retrasando las actividades programadas y el objetivo previamente dicho: Analizar y evaluar los riesgos a los que estaban sujetos los activos de la información de la DGIyE.
- Un SGSI no puede ser implantado por simple requisito sino siempre buscando objetivos claros que agreguen valor a la Universidad. Toda nueva implementación en pro de mejoras en la seguridad de la información debe ir acompañado de políticas funcionales que direccionen los esfuerzos hacia los objetivos del SGSI, sin embargo, el poco interés de la organización de conocer los riesgos a los cuales están expuestos.
- El eslabón más débil de la cadena son las personas, por lo tanto, dentro del análisis y evaluación del riesgo del SGSI se debe dar el énfasis necesario para considerar este tipo de amenazas. Siempre aplicando en los perfiles el principio del mínimo conocimiento. Dentro del análisis se pudo evidenciar que uno de los factores que afectan la disponibilidad e integridad de la información son por fallas del personal, ya que en gran parte la manipulación de la información no está dada por sistemas operativos óptimos, lo cual genera errores de configuración, de transaccionalidades mal ejecutadas y saltos de información.

RECOMENDACIONES

Dentro del desarrollo del proyecto se pudo evidenciar algunas falencias las cuales pueden ser cruciales en el momento de querer implementar un Sistema de Gestión de Seguridad de la Información, estas recomendaciones se basan bajo el marco referencial NTP-ISO/IEC 27001:2014 y de la recolección de datos establecidos como metodología.

- **Definición de Funciones y Responsabilidades**

  Una de las principales amenazas de la DGIyE de la UNDAC, es el acceso de usuarios no autorizados (internos o externos) que puedan consultar, modificar, borrar e incluso robar información a la que no deberían acceder. El usuario del sistema de información debe ser informado de forma clara y precisa acerca de sus funciones y obligaciones en el tratamiento de los datos.

  Implantación de Medidas

  Se deben definir las funciones y responsabilidades de seguridad para cada uno de los usuarios del sistema de información; para ello se aplicará el principio de establecer los mínimos privilegios necesarios para el desarrollo de dichas labores.

- **Validez jurídica de las evidencias**

  La mayoría de las actuaciones que se llevan a cabo en el marco de la seguridad de la información en la DGIyE de la UNDAC. cumplen con el objetivo de disuadir al usuario, interno o externo, de realizar actuaciones no autorizadas, o bien de impedir la ejecución de dichas actuaciones. No obstante, si se produce una incidencia relacionada con la seguridad de la información, siempre se piensa que las pruebas incriminarán al infractor; pero este extremo resulta del todo inútil si

no se ha contemplado esta finalidad en el diseño de las políticas de seguridad de la organización.

Establecer en todas las medidas de seguridad adoptadas el carácter de prueba para poder demostrar posibles incumplimientos con las normas establecidas en el uso de la información de la organización.

Implantación de Medidas

Será objetivo de un grupo de trabajo multidisciplinar, (en el que se debe contar con apoyo jurídico, técnico y organizativo definido en la presente guía como comité de seguridad), dotar de validez jurídica a las pruebas de incumplimiento de las medidas de seguridad definidas sobre la seguridad de la información y según contrato de concesión.

- **Comunicaciones de información con terceros**

Uno de los procesos que más amenazas puede generar en las relaciones con los terceros es el intercambio de información.

El envío de datos a través de soportes (llaves de seguridad o USB's) o redes de telecomunicaciones (correo electrónico, mensajería), generan amenazas a la integridad de los datos, pero también a la confidencialidad de los mismos. Evitar pérdidas, intercepciones o alteraciones de la información, es una prioridad para que la DGIyE de la UNDAC, evalué y las tenga presente. El procedimiento actual es muy específico y no se encuentra documentado.

Implantación de Medidas

Los subprocesos de Centro de Información y Gestión deben estar perfectamente definidos y regulados en los contratos de prestación de servicios. De forma adicional, se deben establecer normas y mecanismos que permitan realizar

comunicaciones de información de forma segura, dentro de la organización y con terceros.

Dichas normas deben estar recogidas formalmente y ser difundidas a todos los implicados en el envío o recepción de información

- **Contratos con terceros**

La evolución de los sistemas de información permite un mayor grado de subcontratación a las organizaciones, asesorías fiscales y laborales, empresas que ofrecen hosting (alquileres) de servidores o páginas web, copias de seguridad realizadas en remoto, etc, son algunos de la larga lista de servicios que se pueden contratar. Si estos terceros no conocen la política de seguridad de la organización, no podrán ser capaces de prestar los servicios contratados con las garantías mínimas exigidas, es pues recomendable y en algún caso imprescindible, regular formalmente los servicios que involucren a personal o recursos externos a la organización.

Tratar los datos de una forma distinta a la acordada, realizar un uso de los mismos para otra finalidad distinta a la inicialmente contratada, no aplicar las medidas de seguridad exigidas, no informar a los usuarios acerca de su deber de secreto, son aspectos que deben estar perfectamente definidos al regular el contrato de prestación de servicios.

Implantación de Medidas

Todas las relaciones con empresas y organizaciones ajenas, que impliquen el acceso a los datos e información propios de la organización deben estar reguladas mediante contrato, estos contratos deberán contemplar como mínimo:

- La identificación de todas las personas físicas y jurídicas que tendrán acceso a la información.

- La finalidad de la prestación de servicios.
- Los mecanismos de intercambio de información.
- Las medidas de seguridad a aplicar a los datos.
- La obligación de mantener el deber de secreto y de informar del mismo a todos los usuarios que puedan acceder a la información.
- Las condiciones para la finalización del contrato, incluyendo mención específica a las acciones de devolución o destrucción de la información objeto del contrato.

La concientización de la DGIyE de la UNDAC. es un pilar fundamental de la norma, por lo cual las organizaciones deben ingeniosamente buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados. Existen mecanismos como bonos, viajes, cenas o reconocimientos públicos que siempre despiertan interés.

Finalmente, la implementación del Diseño del Sistema de Gestión de Seguridad de la información requiere una participación activa y completa a nivel estratégico. Su papel tiene que ser protagónico en su implementación. Durante el desarrollo del presente estudio se pudo evidenciar una disminución en el compromiso de la Alta Dirección por el cual no se facilitó realizar el proyecto en los tiempos asignados; por tanto la correcta implementación del modelo de cualquier empresa debe seguir pasos metodológicos comprobados y consistentes, que den resultados comparables y reproducibles, y dicho con estas palabras se debe tener mayor dedicación, y esfuerzos compartidos para que un futuro se puede pensar en una posible certificación en NTP-ISO/IEC 27001:2014.

BIBLIOGRÁFIA.

I. REFERENCIAS BIBLIOGRAFICAS

1. **Hernández Sampieri, Roberto:** Metodología de la investigación, Editorial McGRAW-HILL / México.
2. **Valderrama, Santiago:** Pasos para elaborar proyectos de tesis de investigación científica. **1era edición. Editorial San Marcos - Perú**
3. **Chema Alonso**: Libro Hacking Web Technologies Editorial OxWord - España
4. **Vicente Aceituno Canal**: Seguridad de la información: expectativas, riesgos y técnicas de protección - España
5. **Instituto Nacional de Estadística e Informática** – Metodología para la elaboración de un plan de sistemas de información. Perú.
6. **Instituto Nacional de Estadística e Informática** - Amenazas en Internet. Lima - Perú
7. **Dirección general de modernización administrativa**, procedimientos e impulso de la administración electrónica. (2012). Metodología de análisis y gestión de riesgos de los sistemas de información versión 3.0. España
8. **Gordon, A. (2015). Official (ISC)2 Guide to the CISSP** CBK, Fourth Edition. USA: (ISC)2 Press.
9. **Harris, S**. (2013). CISSP All-In-One Exam Guide, 6th Edition. USA: McGraw-Hill.
10. **INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION.** (2016). CISM Review Manual. Chicago: ISACA.
11. **INTERNATIONAL ORGANIZATION FOR STANDARIZATION. (2014).** Information technology – Code of Practice for Information Security Management – INTERNATIONAL STANDARD ISO/IEC 27002:2013. Geneva: ISO.

II. RECURSOS WEB

1. Resolución Ministerial N° 004-2016-PCM de fecha 14 de enero 2016- Norma Técnica Peruana NTP-ISO/IEC 27001-2014
   Disponible en:

   http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf

2. ISO 27001: 2014 obligatorio en el Estado Peruano
   Disponible en:

   http://www.americasistemas.com.pe/iso-27001-2014-obligatorio-en-el-estado-peruano/

3. Blog personal de Chema Alonso, consultor de seguridad en Informática 64
Disponible en:

http://www.elladodelmal.com/

4. Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.
http://tesis.pucp.edu.pe/repositorio/handle/123456789/5677

5. Planeación y diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 – 27002
http://dspace.ups.edu.ec/handle/123456789/3178

6. Recursos de Seguridad de la Información. http://www.isaca.org - http://www.sans.org - http://www.intypedia.com - http://www.welivesecurity.com/la-es

7. Metodología de Análisis y Gestión de Riesgos de los sistemas de información, MAGERIT versión 3.0.
www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/

8. Norma Técnica Peruana NTP ISO 17799:2014 EDI. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información. INDECOPI, 2014.
http://www.bvindecopi.gob.pe/normas/isoiec17799.pdf

9. Norma Técnica Peruana NTP ISO 27001:2014. Tecnología de la Información Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición.
http://portal.indecopi.gob.pe/cidalerta/buscadocdet.aspx?id=21374

10. Sistema de información regional para la toma de decisiones
http://webinei.inei.gob.pe:8080/SIRTOD/inicio.html#

ANEXO

MATRIZ DE CONSISTENCIA

TÍTULO: "DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NTP-ISO/IEC 27001:2014 PARA LA DIRECCIÓN GENERAL DE INFORMÁTICA Y ESTADÍSTICA DE LA UNIVERSIDAD NACIONAL DANIEL ALCIDES CARRIÓN PASCO PERÚ"

PROBLEMA	OBJETIVOS	HIPÒTESIS	VARIABLES	DIMENSIONES/ INDICADORES	METODOLOGÍA TÉCNICAS E INSTRUMENTOS
PROBLEMA GENERAL. ¿El Diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP-ISO/IEC 27001:2014, mejora la integridad, confidencialidad y disponibilidad de los activos de información en la DGIyE de la UNDAC? **PROBLEMAS ESPECÍFICOS.** 1.Elaborar los documentos exigidos por la NTP-ISO/IEC 27001:2014 para el diseño del sistema de gestión de seguridad de la información en la	**OBJETIVO GENERAL**. Diseñar el Sistema de Gestión de Seguridad de la Información basado en la NTP-ISO/IEC 27001:2014, para mejorar la integridad, confidencialidad y disponibilidad de los activos de información en la DGIyE de la UNDAC. **OBJETIVOS ESPECÍFICOS** 1.¿Cuáles son los documentos exigidos por la NTP-ISO/IEC 27001:2014, para diseñar el Sistema de Gestión de Seguridad de la Información en la DGIyE de la UNDAC?	**HIPÓTESIS GENERAL.** Según Carlos Alberto Ramos Galarza, en la Revista UNIFE, plantea que no todas las investigaciones cuantitativas plantean hipótesis. El hecho de que formulamos o no hipótesis depende de un factor esencial: el alcance inicial del estudio. Las investigaciones cuantitativas que formulan hipótesis son aquellas cuyo planteamiento define que su alcance será correlacional o explicativo, o las que tienen un alcance descriptivo, pero que intentan pronosticar una cifra o un hecho.	**VARIABLE INDEPENDIENTE** Sistema de Gestión de Seguridad de la Información **VARIABLE DEPENDIENTE** Nivel de riesgo de los activos de información en la DGIyE de la UNDAC	- Confidencialidad - Integridad - Disponibilidad - Alcance - Análisis de riesgo - Controles de seguridad	**4.1 Tipo de Investigación:** Investigación aplicada. El nivel de la investigación es descriptivo **4.2 Métodos** Método Inductivo – deductivo Método Analítico – Sintético y estadístico. **4.3. Diseño de investigación** investigación no experimental transeccional descriptivo **4.4. Población y muestra.** **Población** En esta investigación, la población estuvo constituida por el personal de la Oficina General de Informática y Estadística de la

DGIyE de la Universidad Nacional Daniel Alcides Carrión. 2.Elaborar la valoración de activos de información para la DGIyE de la Universidad Nacional Daniel Alcides Carrión. 3.Aplicar la metodología MAGERIT para analizar los riesgos de los activos de información en la DGIyE de la Universidad Nacional Daniel Alcides Carrión. 4.Elaborar la lista de controles para mitigar los riesgos de los activos de información detectados en la DGIyE de la Universidad Nacional Daniel Alcides Carrión.	2.¿Existe una valoración de activos a proteger en la DGIyE de la Universidad Nacional Daniel Alcides Carrión? 3.¿Qué metodología usar para el análisis de riesgos en la DGIyE de la Universidad Nacional Daniel Alcides Carrión? 4.¿Cuál será el tratamiento de los riesgos identificados en la DGIyE de la Universidad Nacional Daniel Alcides Carrión?	La presente Tesis tiene un nivel de investigación descriptivo y no pronostica ningún hecho o dato por lo que no se formulará una hipótesis			Universidad Nacional Daniel Alcides Carrión. **Muestra.** Se utilizó un muestreo de tipo no probabilístico, con juicio de experto y criterio de saturación, la cual estuvo conformado por los ocho trabajadores administrativos y el Director General de la DGIyE de la UNDAC. **4.5. Técnicas e instrumentos de recolección de datos.** Para medir las variables dependientes se utilizó la ficha de observación que se muestra en el Anexo A; y para las variables dependientes se utilizaron las encuestas, los reportes de incidencias, registros e informes, tanto del área usuaria como del analista de soporte.

ENCUESTA SOBRE SEGURIDAD DE LA INFORMACIÓN ADMINISTRADA AL ÁREA DE SISTEMAS DE LA DGIE-UNDAC

A continuación, se presenta una serie de preguntas, elaboradas con el propósito de determinar "el nivel de seguridad de la información en la Undac", Para ello se le pide que tenga la gentileza de responder a todas las preguntas con sinceridad y absoluta libertad.

Por favor lea cuidadosamente cada pregunta y marque con una "X" la respuesta que considere reflejar mejor la situación

POLITICA DE SEGURIDAD

1. ¿Conoce las políticas de Seguridad de Información que se aplican en su área de labores?

   a) Sí b) No

2. ¿La DGIE pública y comunica a todos los administrativos y partes externas un documento de política de seguridad de la información?

   a) Sí b) No

3. ¿Los administrativos en su oficina suelen dejar documentos con información institucional que podría ser confidencial encima de su escritorio o en otro lugar de exposición para los demás?

   a. Todo el tiempo
   b. Usualmente
   c. Pocas veces
   d. No es común

4. ¿Qué sucede con los documentos de su oficina que ya no son de utilidad?
   a. Se trituran

b. Se botan al tacho
c. Se almacenan en la oficina
d. Desconozco

5. ¿Cuándo sale de su oficina, bloquea su computadora?
    a. Siempre
    b. A veces
    c. Nunca
6. Los accesos a su centro de labores son a personal autorizado
    a) Sí b) No

7. ¿En la Undac existe un procedimiento para la realización de copia de seguridad?
    a) Sí b) No

8. ¿La Undac cuentan con políticas de contraseña segura? (más de 8 caracteres, contraseña alfanumérica, login diferente al password, etc.)
    a) Sí b) No
9. ¿Se lleva un histórico detallado los incidentes que se han tenido sobre la seguridad de la información?
    a) Sí b) No

10. ¿Existe en la Undac una metodología para la evaluación y gestión del riesgo?
    a) Sí b) No

11. ¿Todo lo relacionado con la seguridad de la información se encuentra documentado?
    a) Sí b) No

12. Realiza backup de su labor diaria
    a) Sí b) No