Universidad Nacional del Nordeste
Facultad de Ciencias Exactas y Naturales y Agrimensura

Maestría en Tecnologías de la Información

Trabajo Final

Diseño de un sistema de gestión y seguridad de la información para la Dirección General de Liquidaciones de Haberes de la Universidad Nacional del Nordeste

Autor: Soler Angel Alejandro

Director: Dr. Rubén Bernal

Año 2022

Dedicatoria

A Dios por estar siempre a mi lado.

A mí amada familia por las horas que me entregaron para poder concluir este trabajo, especialmente un agradecimiento enorme a mi esposa por apoyar este desafío de realización personal y académico. A mis hijos por las horas de plaza y momentos de padre-hijo que postergamos.

A mis compañeros de oficina por todo el aliento y empuje en cada jornada.

A todos los profesores a lo largo de todos estos años, quienes acompañaron y fueron parte fundamental en mi formación, especialmente agradezco la confianza de cada uno de ellos.

¡Gracias!

Resumen

El presente trabajo plantea la elaboración de un Sistema de Gestión de Seguridad de la Información (SGSI) para el área de Tecnologías de la Información (TI) de la Dirección General de Liquidación de Haberes (DGLH) de la Universidad Nacional del Nordeste (UNNE) dentro del marco de la norma ISO 27000 en conjunto con la metodología para el manejo y gestión de riesgos propuestas por Magerit. La DGLH está encargada fundamentalmente de gestionar los procesos y recursos necesarios para el pago de los sueldos de los empleados de la Universidad, además de otras actividades relacionadas con dependencias como AFIP, ANSES y entidades bancarias.

Actualmente la DGLH dispone de recursos para preservar la confidencialidad, integridad y disponibilidad de la información que gestiona, no obstante carece de una definida identificación de sus activos tecnológicos lo cual le imposibilita gestionar de manera eficiente los riesgos asociados a la seguridad de sus activos.

En el presente proyecto se determinarán las bases para diseñar un SGSI y desarrollar una metodología como plan de acción en lo concerniente a la seguridad informática del área en coordinación con los objetivos, estrategias y políticas de la institución educativa.

Este trabajo fue llevado a cabo en el marco del Acta de Acuerdo entre FaCENA y el Instituto Rectorado, ambos de la UNNE aprobado por Resolución N°. 0707/21 CD.

Palabras claves: (*Seguridad de la Información, ISO 27001:2013, Magerit, Vulnerabilidad, Amenazas, Riesgo, Sistemas*)

Abstract

The present work proposes the elaboration of an Information Security Management System (ISMS) for the Information Technology (IT) area of the General Directorate of Asset Settlement (DGLH) of the Universidad Nacional del Nordeste (UNNE) within the framework of the ISO 27000 standard in conjunction with the methodology for handling and managing risks proposed by Magerit. The DGLH is fundamentally in charge of managing the processes and resources necessary for the payment of the salaries of the University's employees, in addition to other activities related to dependencies such as AFIP, ANSES and banking entities.

Currently, the DGLH has resources to preserve the confidentiality, integrity and availability of the information it manages, however it lacks a defined identification of its technological assets, which makes it impossible for it to efficiently manage the risks associated with the security of its assets.

In this project, the bases will be determined to design an ISMS and develop a methodology as an action plan regarding the computer security of the area in coordination with the objectives, strategies and policies of the educational institution.

This work was carried out within the framework of the Memorandum of Agreement between FaCENA and the Instituto Rectorado, both of the UNNE approved by Resolution No. 0707/21 CD.

Keywords: (*Information Security, ISO 27001: 2013, Magerit, Vulnerability, Threats, Risk, Systems*)

Reconocimientos - Agradecimientos

A mi Director, Dr. Rubén Bernal*, por la confianza puesta desde el principio para la realización de este trabajo y el tiempo dedicado al mismo.*

A la ***Magister Gladis N. Dapozo*** *por el apoyo y la confianza puesta en mi persona desde mis inicios como estudiante de grado, con su permanente motivación fueron pilares en mi formación académica.*

A la Secretaria General Administrativa, ***Especialista María Cristina Torres*** *por confiar y apoyar el proyecto de mejora para el área de Liquidación de Haberes.*

A la Directora General de Liquidación de Haberes ***Magister Teresita Bózzola*** *y a la* ***Magister María Elizabeth Sanchez****, compañeras de oficina y de la presente maestría. Su ejemplo y empuje diario hicieron que este trabajo sea una realidad.*

A todos los compañeros de la DGLH y los amigos que me aportaron sus ganas y empuje.

Y principalmente a Dios por estar presente en cada momento, sin Él nada hubiera sido posible.

Índice de contenidos

Índice de Tablas

Índice de Figuras

Lista de Abreviaciones

BCP Manager: Administrador del Plan de Continuidad del Negocio

BCR Manager: Administrador del Plan de Recuperación de Desastres

DGLH: Dirección General de Liquidación de Haberes

FODA: Fortalezas, Oportunidades, Debilidades y Amenazas

ISO: Organización Internacional de Normalización

IT CP: Planificación de Continuidad de TI (IT Continuity Planning)

IT DRP: Planificación de Recuperación de Desastres de TI (IT Disaster Recovery Planning)

ONTI: Oficina Nacional de Tecnologías de Información

SGSI: Sistema de Gestión de Seguridad de la Información

SIU: Sistema Interuniversitario Nacional

TIC: Tecnologías de la información y la comunicación

UA: Unidad Académica

UNNE: Universidad Nacional del Nordeste

Capítulo 1
Introducción

En este capítulo se presentan los conceptos fundamentales de la seguridad informática [1]*, destacando la importancia de preservar la información en todos los niveles. Mediante esta descripción se abordan los objetivos principales del objeto de estudio, determinando además los alcances del proyecto.*

1.1 Introducción

Los sistemas de información de las organizaciones, empresas o entidades son considerados en un grado de importancia tal que podrían ser denominados el alma de las mismas y es a través de una adecuada sistematización y documentación de sus sistemas lo que les permiten concretar sus objetivos y preservarse en el tiempo. Las mismas deben enfrentarse a la realidad de ataques externos e internos y el hecho de subestimar los riesgos y amenazas puede hacer peligrar su normal funcionamiento e incluso su continuidad.

Ante la necesidad de mitigar los riesgos es necesario que hoy en día las organizaciones cuenten con un sistema para gestionar la seguridad de sus activos.

El presente proyecto de TFM se llevó adelante en el área de Tecnologías de la Información (TI) de la DGLH dependiente de la Secretaría General Administrativa (SGA) de la Universidad Nacional del Nordeste.

La propuesta del presente trabajo se basa en la necesidad de contar con un plan de seguridad en el área TI de la DGLH, ya que la misma actualmente no dispone de medidas concretas que aseguren la confidencialidad, integridad y disponibilidad de sus datos e información.

El desarrollo del trabajo consiste en diseñar un Sistema de Gestión de Seguridad de la Información (SGSI) a fin de identificar los riesgos y proponer las políticas y controles que permitan mejorar la seguridad garantizando la continuidad de las operaciones denominadas críticas de la DGLH.

1.2 Organización del TFM

Conforme a los objetivos propuestos en el presente TFM, se organizará con la siguiente estructura:

En el **capítulo 1**, se hace una introducción al problema, se describen los objetivos propuestos, la justificación del tema, el alcance previsto y el estado del arte.

El **capítulo 2** se presenta la fundamentación teórica, las referencias y diferentes normativas en la que se basa el proyecto. Además, se describen los aspectos fundamentales de la seguridad de la información, las normas, herramientas y el estándar ISO 27001 con sus derivados.

En el **capítulo 3** se presenta el estado actual de la realidad del área TI de la DGLH, mediante la implementación de encuestas, entrevistas al personal y la observación directa.

En el **capítulo 4**, se describe el diseño de la metodología propuesta. En la misma se detalla las diferentes políticas de seguridad que conformarán el modelo de seguridad acorde a las necesidades del área y en base a las normas y estándares aprobados.

En el **capítulo 5**, se realiza un análisis de los resultados obtenidos mediante la evaluación del cumplimiento de los objetivos planteados mediante el uso de métricas preestablecidas.

Finalmente, en el **capítulo 6**, se detallan las principales conclusiones del trabajo realizado en cuanto al cumplimiento de cada objetivo planteado, como también las posibles líneas de investigación y acción futuras.

1.2 Motivación

La posibilidad de pérdida de información de manera parcial o total con la consecuente interrupción del negocio (en este caso el pago de los sueldos) es uno de los principales riesgos que conlleva toda organización, la cual no está solo relacionada con fenómenos físicos o fallos tecnológicos sino también con la reputación y el valor de la organización como un importante activo.

El hecho de no contar con una estrategia de seguridad en la DGLH, que pueda ser aplicable ante estas situaciones podría implicar que la Dirección incumpla los objetivos previstos (pago mensual de haberes) provocando pérdidas económicas y de información.

Dentro de los procesos que lleva a cabo la DGLH se encuentra principalmente la liquidación de los sueldos y la acreditación de los mismos a través de la entidad bancaria correspondiente, entidad que luego hace efectivo el depósito de los sueldos a los agentes universitarios. Además la DGLH interactúa con diferentes aplicaciones del Sistema Interuniversitario Nacional SIU [1] (Mapuche, Wichi) y otros sistemas de gestión nacional como AFIP, ANSES y RHUN (Recursos Humanos de Universidades Nacionales).

Como bien puede observarse la DGLH no cuenta con un plan donde se detalle de manera explícita los procedimientos a llevar a cabo ante incidentes, que permita aplicar las medidas preventivas y correctivas para mantener la operatividad del área con un mínimo nivel de error aceptable durante la contingencia.

De esta forma se puede concluir que es fundamental contar con una metodología y con protocolos documentados que permitan poner en práctica soluciones firmes, que puedan ser llevadas a cabo por cualquier técnico o grupo de profesionales capacitados y que puedan actuar ante una situación de emergencia o crisis informática para poder restaurar los servicios y aplicaciones necesarias para continuar con las tareas de correspondientes prosiguiendo con la continuidad del negocio.

Dadas las tareas que tiene como objetivo principal la DGLH, es de absoluta importancia asegurar la confidencialidad, integridad y disponibilidad de sus datos, atributos que son inherentes a un Sistema de Seguridad de la Información (SGSI). En el mismo se establecen y definen, las políticas, procedimientos y controles relacionados con los

[1] Consorcio SIU está conformado por 46 universidades nacionales, entre ellas la UNNE. Desde septiembre de 2013 depende formalmente del Consejo Interuniversitario Nacional (CIN). Viene desarrollando para el sistema de Universidades Nacionales, soluciones integrales que abarcan muchos de sus procesos administrativos, entre los que se encuentran la información de recursos humanos y liquidación de sueldos de los agentes.
[1]SIU-Mapuche recoge toda la información de los RRHH de una institución en un Legajo Electrónico Único (sistema integrado), está diseñado para brindar al operador -ya sea al trabajador del área o al encargado de liquidaciones- todos los servicios necesarios para disminuir las posibilidades de error y hacer más sencillo su trabajo, teniendo en cuenta los cambios en la legislación laboral vigente. Existen distintos canales de comunicación para interactuar con el equipo SIU de la Secretaría de Políticas Universitarias (SPU) y demás miembros de la comunidad.

objetivos de la organización y se propone la mejora continua en sus procesos. Además, con la implementación de un SGSI se intenta generar un compromiso en cuestiones relacionadas a la seguridad de un punto de vista proactivo y la participación de todos los integrantes de la organización.

1.3 Planteamiento del problema

La Universidad Nacional del Nordeste se crea oficialmente el 14 de noviembre de 1956 en la Ciudad de Corrientes a través del Decreto Ley N° 22.299, la misma fue conformada inicialmente con facultades e institutos que dependían de la Universidad del Litoral con sedes en Chaco, Corrientes, Formosa y Misiones. Actualmente la UNNE está conformada por diferentes facultades e institutos de las provincias de Corrientes y Chaco. La UNNE ofrece diferentes carreras en el nivel de Educación Superior ofreciendo formación integral a los estudiantes. La Universidad cuenta en su planta funcional de un área administrativa y un claustro de profesores en sus diferentes categorías, los cuales son denominados Docentes y No Docentes. La totalidad de los empleados de la Universidad perciben sus ingresos a través de las tareas operativas que realiza la DGLH.

En todo el mundo y especialmente en América Latina el aumento de la tecnología ha contribuido también al aumento de los problemas relacionados con el manejo de la información y las vulnerabilidades a las que las instituciones deben hacer frente asegurando la integridad y privacidad de sus datos.

Desde hace unos años la información que se intercambia entre las facultades denominadas Unidades Académicas (UA) se realiza a través de redes informáticas principalmente la intranet, por lo cual las áreas o departamentos de TI deben asegurar el traspaso de la información de manera confiable y controlada. Esta información provista por las UA es la materia prima con la que la DGLH debe manejarse a fin de realizar las liquidaciones de forma correcta para posteriormente informar de las acreditaciones a realizar por parte de la entidad bancaria, las que finalmente ejecutan el pago por diversos medios a los agentes universitarios correspondientes.

La actualización tecnológica y la adopción de nuevas tecnologías marcaron la diferencia de la DGLH en relación con otras áreas. Sin embargo, este crecimiento también trajo cambios a nivel operativo, de procesos y de aplicación de protocolos a nivel de seguridad de la información. Luego de realizar entrevistas con la Dirección y los encargados del área TI de la DGHL además de la observación directa de las instalaciones, se detectaron algunos inconvenientes relacionados a la seguridad de la información como falta de identificación y gestión de activos, ausencia de normativas o plan de continuidad.

1.4 Objetivos del Trabajo Final de Maestría (TFM)

1.4.1 Objetivo general

Elaborar un SGSI en el área de Tecnologías de la Información (TI) para la oficina de la DGLH tomando como base las normas internacionales ISO 27000 en conjunto con la Metodología Magerit a fin de mejorar la seguridad de los activos de información de la misma.

1.4.2 Objetivos específicos

- Identificar los activos y procesos críticos del área de TI, a fin de gestionar los riesgos y vulnerabilidades a los que están expuestos y categorizarlos según su impacto.
- Diagnosticar el grado de cumplimiento de las normas ISO 27001 en la DGLH.
- Diseñar un Sistema para la Gestión de la Seguridad de la Información de los activos.
- Validar el sistema con un caso de estudio del área determinada, definiendo indicadores o métricas que permitan evaluar de forma efectiva la implementación del SGSI.

1.5 Alcances

La metodología propuesta tendrá su ámbito de aplicación en la DGLH de la UNNE, físicamente ubicada en el Instituto Rectorado, calle Mayo Nº 868 de la ciudad de

Corrientes Capital provincia de Corrientes. El presente trabajo cuenta con el total apoyo de la Secretaria General Administrativa de la UNNE ya que el mismo beneficiará de manera directa a la DGLH y a las áreas que participan en los procesos de Liquidación de Haberes: Dirección de Personal de cada una de las facultades que integran la UNNE, Dirección de Legajos, Asesoría Legal y Técnica, Dirección de Administración de Personal, Dirección General Impositiva entre otros.

La DGLH proveerá los recursos necesarios para la determinación de los activos de información y el análisis de los recursos que la conforman, la misma comprende el área de tecnologías de la información (TI), la cual involucra procesos y tareas:

Operacionales: tareas relacionadas con la definición de cálculos y liquidaciones.

Administrativos: funciones y procesos de gestión administrativa.

Técnicos: asignación de recursos, equipos y gestión de los mismos.

Las áreas correspondientes de la tecnología de la información que se analizarán son:

- Redes y Servidores
- Soporte técnico
- Desarrollo de software
- Administración de sistemas

Los resultados obtenidos con esta propuesta permitirán a la DGLH contar con la identificación y gestión de sus activos y de un sistema para la gestión de la seguridad de la información con las ventajas que esto conlleva en la toma de decisiones y la protección de sus datos.

1.6 Recursos

Los recursos disponibles para la realización del presente trabajo están catalogados en humanos y técnicos:

- Recursos humanos: Directivos, administrativos y técnicos del área de la DGLH.

- Recursos técnicos: Equipos informáticos, sistemas operativos, herramientas de software, bases de datos, etc.

Los equipos informáticos están ubicados físicamente en el centro de datos dentro de la oficina donde funciona la DGLH en el Instituto Rectorado de la UNNE, conformados por cuatro servidores HP alojados en dos torres rack con alimentación alternativa y en un ambiente climatizado. En los mismos se virtualizan las diferentes instancias de los sistemas operativos utilizados para la ejecución de los sistemas de gestión y para la administración de los sistemas de bases de datos de la Dirección. Además, se cuenta con equipos personales para la operación de los sistemas y para la realización de las tareas administrativas propias del área.

La oficina de la DGLH, además del centro de datos, cuenta con dos espacios físicos en donde se sitúan los equipos personales y otros dispositivos que dan soporte a los procesos y tareas operacionales y administrativas desarrolladas por el personal directivo, técnico y administrativo que realiza sus tareas de forma diaria de manera presencial.

1.7 Estado del arte

En esta sección se incluye información técnica de los antecedentes hallados en la exploración de trabajos de investigación relacionados con el objeto de estudio del presente proyecto. Siendo uno de los objetivos principales de este proyecto, desarrollar un SGSI para una organización de carácter público como es el caso de una universidad, se procedió a la investigación sobre los sistemas diseñados e implementados en instituciones nacionales e internacionales, intentando hallar aquellas que además de ser casos de éxito puedan aportar el uso de buenas prácticas replicables a la realidad de la UNNE.

En cuanto a la investigación, se hallaron proyectos de creación de un SGSI bajo la norma ISO/IEC 27001, los que luego de analizados en sus técnicas y hallazgos serán tomados como base del presente proyecto trabajo.

Hallazgos en el sector público:

Titulo	Diseño de un sistema de gestión de seguridad de la información para la corporación nacional de telecomunicaciones CNT EP, agencia doral
Autor	Molina Batallas, Luis Fernando
Procedencia	Perú.
Fecha publicación	2016
Resumen	El actual proyecto consiste en el diseño de un sistema de gestión de seguridad de la información SGSI para la Corporación Nacional de Telecomunicaciones CNT EP en la agencia matriz Doral directamente aplicado al área del NOC, en el SGSI propuesto se elaboran políticas de seguridad conforme los requerimientos del área del NOC tomando como referencias que es un área crítica por la función desempeñada dentro de la empresa y por la información manejada internamente.
Claves	Seguridad, informática; protección de datos; diseño de sistemas; telecomunicaciones
URI	http://dspace.udla.edu.ec/handle/33000/6052
Titulo	Guía para la implantación del SGSI con base en la NTE ISO/IEC 27000 para el servicio de agendamiento de citas del Contact Center del Ministerio de Salud Pública del Ecuador.
Autor	Terán Valenzuela, Karina Maribel
Procedencia	Ecuador
Fecha publicación	2018
Resumen	El presente trabajo desarrolla una Guía para la implantación del Sistema de Gestión de Seguridad de la Información (SGSI), alineado a la norma técnica ecuatoriana NTE ISO/IEC 27000 con la finalidad de mejorar el nivel de seguridad de la información del Ministerio de Salud Pública del Ecuador (MSP). Según lo estipulado en el Art. 32 de la Constitución de la República del Ecuador, el MSP tiene como función garantizar el acceso permanente y oportuno derecho a la atención integral de salud.
Claves	seguridad informática, derecho a la informática, confidencialidad de datos, norma NTE ISO/IEC 27000
URI	http://repositorio.espe.edu.ec/handle/21000/13806

Titulo	Diseño de un modelo de gestión de seguridad de la información para el sistema académico de la Universidad Estatal del Sur de Manabí
Autor	Estrella Edison, Conforme Sornoza Carlos
Procedencia	Perú
Fecha publicación	2018
Resumen	Los sistemas de información se han convertido en una necesidad para las instituciones sean estas públicas o privadas, mismas que se ven beneficiadas manteniendo el acceso a la información en tiempo real hacia sus usuarios finales. Las universidades del país optan por desarrollar sistemas informáticos para agilizar sus procesos académicos y así brindar facilidades a sus estudiantes mediante el acceso a su información en cualquier momento y lugar, los mismos contienen información relevante para los procesos internos de cada una. Manteniendo presente que la protección de la información debe ser primordial nace la investigación aquí presentada. El desarrollo de la misma contempla un análisis de la situación actual de la gestión de la seguridad de la información (SGSI), la identificación de las amenazas de mayor impacto en cuanto a la gestión de la seguridad de la información, el análisis de la norma ISO/IEC 27002:2017, para finalmente lograr el desarrollo de un modelo SGSI como herramienta guía para la aplicación de lineamientos de seguridad en el sistema académico de la Universidad Estatal del Sur de Manabí. El análisis de la situación actual previa revisión documental determina que la gestión de la seguridad de la información tiene muy poca acogida, evidenciando la no existencia de normativas de seguridad de información para el sistema académico. La identificación de las amenazas de mayor impacto del sistema académico mediante un análisis de riesgos determina que producto de la falta de normativas ha dado lugar a incidentes de seguridad afectando la integridad, confidencialidad y seguridad de la información. Los resultados del análisis de riesgos conllevaron al análisis de la norma ISO/IEC 27002:2017 la cual contiene controles de seguridad de la información permitiendo identificar los más acordes a ser tomados en consideración para mitigar los vacíos de seguridad revelados. Todo el proceso descrito ha permitido desarrollar un modelo de sistema de gestión de seguridad de la información para el sistema de información académico basado en el estándar internacional ISO/IEC 27002:2017 como apoyo al personal informático de la

	Universidad Estatal del Sur de Manabí permitiéndoles desarrollar sus lineamientos de seguridad de la información acordes a la necesidad institucional, mismo que permitirá incorporar integridad, confidencialidad y seguridad.
	tecnologías de la información, protección de datos, acceso a la información seguridad informática, ISO 27002:2017
URI	http://repositorio.uisek.edu.ec/handle/123456789/3222

Titulo	Implementation of Information Security Management Systems based on the ISO/IEC 27001 Standard in different cultures
Autor	Bahareh Shojaie
Procedencia	Hamburgo
Fecha publicación	2018
Resumen	In this thesis, we investigate the potential relationship between national cultural, political and economic characteristics regarding the adoption of ISO 27001, in terms of the average number of certificates issued (2006–2014). ISO 27001 is the most adopted international ISMS (Information Security Management System) standard, which provides IT governance by protecting sensitive data in a structured way.
Claves	Information Security; ISO/ IEC; 27001
URI	https://ediss.sub.uni-hamburg.de/handle/ediss/7572

Titulo	Plan de implementación de un SGSI basado en la norma ISO 27001:2013 en el ámbito de la Administración Pública Argentina
Autor	Roberti Ferri, Bruno Alejandro
Procedencia	España
Fecha publicación	2020
Resumen	El organismo ha sido pionero en la implementación de sistemas de información en la administración pública nacional (APN) de Argentina, contando con soporte informático para un alto porcentaje de sus procesos. Acorde con el impacto de los sistemas de información en el mismo, en el año 2003 se implementó el "Manual de normas y procedimientos de

	Seguridad Informática" siguiendo los lineamientos de ISO/IRAM 17799:2002, el cual por diversos motivos no fue actualizado hasta el año 2014. En ese año se inició la actualización de la política de seguridad que se encuentra vigente en el organismo de acuerdo a lo expresado por la Decisión Administrativa N° 669/2004 [1] de la Jefatura de Gabinete de Ministros que estableció la obligatoriedad para los organismos del Sector Público Nacional de dictar o bien adecuar sus políticas de seguridad de la información conforme a la "Política de Seguridad de la Información Modelo" dictada por la Oficina Nacional de Tecnologías de la Información (ONTI). La versión implementada en la actualidad en el organismo se corresponde con la aprobada mediante Disposición 3/2013 de ONTI.
Claves	seguridad informática, SGSI
URI	http://hdl.handle.net/10609/126647

Investigaciones halladas sobre el sector privado:

Titulo	Formulación de una propuesta para un modelo de sistema de gestión de seguridad de la información para empresas de la industria bancaria en el sector privado
Autor	Landázuri Benalcázar, María Cristina
Procedencia	Perú
Fecha publicación	2017
Resumen	En la actualidad la industria Bancaria en el Ecuador ha encaminado sus esfuerzos en proveer sistemas de información prácticos y accesibles a sus clientes adaptándose así a los avances tecnológicos de la época, sin embargo se ha evidenciado también, un crecimiento proporcional de amenazas y ataques informáticos que no solo ponen en riesgo los sistemas de información sino la estabilidad de una entidad, por tanto, el concepto de valor de la información como el activo más importante se ha convertido en el objetivo fundamental de las entidades bancarias, de ahí su importancia de establecer un esquema metodológico y procesos documentados para su adecuada gestión. Un Sistema de Gestión de Seguridad de la Información SGSI según la ISO 27001 se basa en la

	preservación de la confidencialidad, integridad y disponibilidad de la información, mediante una gestión de riesgos que garantice que éstos sean conocidos, asumidos, gestionados y minimizados por la organización. El presente proyecto plantea un modelo de sistema de gestión de seguridad de la información SGSI para entidades de la vertical bancaria del sector privado en el Ecuador basándose en las mejores prácticas y principios de las normas ISO, y de marcos de referencia como COBIT y COSO. Se realiza un análisis de la problemática actual con el manejo de información y los requerimientos legales y normativos que son de carácter obligatorio para las entidades de la industria bancaria en el Ecuador y que son regulados por los entes de control, en base a estos requerimientos se propone la implementación de controles determinados en la norma ISO 27001. Una vez determinado los requerimientos se procede a explicar y proponer un esquema o metodología para el desarrollo del SGSI en la fase de "Planeación" que incluye entregables como políticas, análisis de riesgos, clasificación de activos, plan de tratamiento de riesgos, etc. utilizando el modelo de mejora continua PDCA Plan, do, check, act conocido como Ciclo de Deming, en su equivalencia en español es Planificar, hacer, verificar y actuar PHVA, el cual establece un proceso cíclico de mejora continua en la cual se basa esta propuesta. Para finalizar se plantea modelos y estructuras de medición para evaluar el rendimiento de la seguridad de la información y de la eficacia del SGSI.
Claves	sistemas de gestión; seguridad informática; industria bancaria
URI	http://dspace.udla.edu.ec/handle/33000/8191

Titulo	Implementación de un sistema de gestión de seguridad de información basado en la Norma ISO 27001:2013 para el control físico y digital de documentos aplicado a la empresa LOCKERS S.A.
Autor	Lema Vinlasaca, Roberto Carlos, Donoso Gallo, Diego Fernando
Procedencia	Ecuador

Fecha publicación	2018
Resumen	El presente documento establece una metodología para la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) aplicando los requisitos y procedimientos establecidos por la norma ISO/IEC 27001:2013 para empresas cuyo principal proceso de negocio sea el control físico y digital de documentos. El proyecto inicia con la justificación e importancia del desarrollo del proyecto, el planteamiento y formulación del problema, la definición de las hipótesis y objetivos del proyecto. En el segundo capítulo establece la conceptualización de las normas y marcos de referencia a ser utilizadas durante el desarrollo del proyecto, su alcance y aplicación para la gestión de seguridad de la información. En el tercer capítulo se realiza el estudio, análisis y selección del marco de referencia para la planificación y ejecución de la gestión de riesgo en la seguridad de información. Posteriormente, en el cuarto capítulo se desarrolla una propuesta metodológica para la definición, planeación, diseño e implementación de un sistema de gestión de seguridad de la información para empresas de control físico y digital de documentos. Finalmente, en el quinto capítulo se implementa un Sistema de Gestión de Seguridad de la Información sobre la empresa Lockers S. A., acorde a la metodología descrita en el Capítulo 4 para concluir con la emisión de conclusiones y recomendaciones del proyecto.
Claves	riesgos informáticos, sistemas de gestión de seguridad de la información, norma ISO/IEC 27001:2013
URI	http://repositorio.espe.edu.ec/handle/21000/14397

Titulo	Metodología integradora para simplificar la implementación de los componentes de un sistema de gestión de la información (SGSI), en pequeñas y medianas empresas del sector de la información y comunicaciones en la ciudad de Medellín
Autor	González Durango, Cesar Augusto
Procedencia	Colombia
Fecha publicación	2019

Resumen	En la actualidad, existen muchos ataques informáticos cuya tendencia va en ascenso, los cuales afectan, en buena medida, el sector empresarial. Uno de los sectores más vulnerables a estos riesgos es el conformado por las PYMES (Pequeña y mediana empresas. Las cuales, por su tamaño y capacidad financiera, adolecen de mecanismos para la adopción de estándares y normas internacionales en seguridad de la información, que les permita mitigar las amenazas derivadas de los cibera taques, y al mismo tiempo, las convierta en una organización que optimice el recurso humano, hacia unas prácticas que las conduzcan a gestionar los riesgos de una manera más eficiente. Este proyecto propone una metodología basada en estándares internacionales, que busca facilitar el diseño de un sistema de gestión de seguridad de la información (SGSI) en PYMES. Particularmente, para las PYMES del sector de la información y comunicaciones de la ciudad de Medellín. El desarrollo de este proyecto incluyo´ un diagnóstico del nivel de adopción de SGSIs en estas empresas, el análisis de estándares internacionales, cuyas bases fundamentaron la metodología propuesta, y una evaluación de su aplicabilidad en un caso de estudio en una empresa de este sector.
Claves	Seguridad de tecnología; Gestión de la información; Riesgo cibernético; Ciberseguridad; Seguridad de la información; Crimen cibernético; Pymes; Innovaciones organizacionales
URI	http://hdl.handle.net/20.500.12622/2083

Titulo	Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo
Autor	Rojas Viera Cinthia Katherine, Zavaleta Verona Tefhany Lisseth
Procedencia	Chile
Fecha publicación	2019
Resumen	En la presente tesis se pretende elaborar una Guía de implementación de la seguridad basada en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas de información en el Área de Operaciones y Tecnología de Global BPO Center

	Allus Chiclayo. Para la obtención de dicha información y recolección de datos se consideró conveniente el uso de la técnica de recolección de datos: encuestas, como medio para poder extraer la información y su posterior interpretación; y de esta manera medir la realidad problemática apoyado en el uso de la Norma ISO/IEC 27001, lográndose determinar las deficiencias para mejorar los niveles de seguridad y confiabilidad en los sistemas de información de dicha área. Los resultados obtenidos permitieron determinar de forma real que, al incorporar la norma ISO/IEC 27001 basada en una Guía de Implementación. Se logró incrementar los procedimientos utilizados en favor de la empresa permitiéndole la detección de anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla. Con el Plan de tratamiento de Riesgos, se permitió la disminución de los niveles de riesgos con respecto a los activos de información, considerados amenazas y vulnerabilidades en la empresa, esto manifestado en un plan adecuado para abordarlos y tomar las precauciones necesarias que minimicen sus impactos. Finalmente se propuso el Plan de Capacitación y Concienciación para poder incrementar el porcentaje de conocimiento por parte del personal en temáticas orientadas a políticas, estrategias de seguridad que beneficien a la empresa, teniendo como resultado personal comprometido con la seguridad en favor de la empresa. Una correcta implementación del SGSI propuesto en el presente trabajo de investigación permitirá incrementar el nivel de la seguridad en beneficio de la empresa.
Claves	Seguridad, información
URI	https://hdl.handle.net/20.500.12893/5865

Titulo	Plan de gestión de seguridad informática basado en la Norma ISO 27001 para el Departamento de Tecnología de la Información en la Empresa Plasticaucho Industrial S.A.
Autor	Mayorga Mayorga, Franklin Oswaldo, Tigse Moposita, Jorge Luis
Procedencia	Universidad Técnica de Ambato. Ecuador
Fecha publicación	2020

Resumen	La empresa "Plasticaucho Industrial S.A." dedicada a la producción de calzado en varias líneas como: casual, escolar, deportivo, industrial, entre otras, tiene su matriz en la ciudad de Ambato, se encuentra en constante crecimiento tanto a nivel del Ecuador como a nivel internacional en Colombia y Perú, de esta manera requiere contar con personal ampliamente capacitado y recursos que permitan ofrecer productos de calidad de manera eficiente y segura. La tecnología se encuentra en constante desarrollo por lo que es importante mantener actualizado los procesos de seguridad dentro de la empresa, verificando y corrigiendo errores que puedan poner en peligro la información relevante de la entidad, por lo cual existe la necesidad de adaptarse a un modelo de gestión de la información de acuerdo a Normas Internacionales que permitan el control y manejo de datos con total integridad. Plasticaucho Industrial S.A. cuenta con POLÍTICAS DE GESTIÓN DE LA INFORMACIÓN, pero las mismas deben ser analizadas para su control y si se da cumplimiento por parte de los usuarios, además determinar una metodología que pueda ser adaptado a la Norma Internacional ISO 27001 para gestionar la seguridad de los datos, de esta manera obtener una Certificación Internacional para la empresa que le dará más fortaleza y seguridad ante sus competencias. El diseño de un Plan de Gestión de Seguridad Informática basado en la Norma ISO 27001 que se plantea en el presente proyecto permitirá analizar las fortalezas, debilidades y determinar un plan de acción ante un problema que pueda tener a futuro la empresa en la cual puede quedar expuesta la integridad de sus datos.
Claves	Gestión de la información, Seguridad informática, Administración de riesgos.
URI	https://repositorio.uta.edu.ec/jspui/handle/123456789/30696

La investigación llevada a cabo sobre recientes trabajos publicados en los temas de seguridad y los sistemas de Gestión de la Seguridad de la Información a nivel internacional, reflejan la importancia que éstos poseen para las organizaciones y el interés en gestionar los riesgos de las diferentes organizaciones sin considerar su tamaño o los ámbitos a los que estas pertenecen. Instituciones públicas o privadas observan las amenazas que pueden afectar sus activos e intentan aplicar el uso de buenas prácticas o metodologías para gestionar la seguridad de sus datos. Se hallaron varios trabajos

relacionados a la aplicación de normas de la familia ISO 27000 y la gestión de los riesgos con metodologías basadas en COBIT o Magerit. En los estudios analizados los resultados fueron positivos para las organizaciones, otorgando beneficios en la administración de la seguridad de la información.

1.8 Producción derivada con el desarrollo del TFM

Difusiones en eventos académicos y revistas

- M. E. Sánchez, T. Bózzola, A. Soler y S. I. Mariño, "Metodología para el relevamiento y análisis de la información. Una propuesta para la administración central de liquidaciones en la Universidad". Ciencia Latina Revista Científica Multidisciplinar, Ciudad de México, México. ISSN 2707-2207, junio 2020, Volumen 4, Número 1, pp. 99 – 115. [En línea]. Disponible en: https://doi.org/10.37811/cl_rcm.v4i1.44

Capítulo 2
Marco teórico

En el siguiente capítulo 2, se realiza un breve detalle de los antecedentes bibliográficos y de las metodologías del análisis y gestión de riesgos, se describen las características y ventajas de cada una y se detallan los dominios de seguridad de la ISO/IEC 27001.

2.1 Antecedentes Bibliográficos

2.1.1 Fundamentación Filosófica

El presente trabajo centra su investigación hacia un análisis profundo de vulnerabilidades existentes dentro de la organización, partiendo de la determinación de sus activos e información confidencial con el fin de implementar un SGSI, lo que permitirá comprender el uso de buenas prácticas relacionadas con la seguridad y la posibilidad de certificar sus procesos si lo requiriera.

2.1.2 Fundamentación Legal

El hecho de basar la misma en las normas ISO asegura el cumplimiento de los requisitos legales establecidos, y puntualmente hacerlo bajo la norma ISO 27001 determina que los reglamentos contractuales de la seguridad de la información, estarán definidos de forma explícita, actualizados y correctamente documentados.

2.1.3 Fundamentación Teórica

Información

Cuando hablamos de información nos referimos al conjunto de datos organizados que se encuentran en poder de una determinada entidad y para los cuales éstos poseen un determinado valor. Esta información puede estar contenida en diferentes formas y medios:

- Medios escritos, audios, video o imágenes.
- Conocimientos formales e informales.
- Almacenados en medios electrónicos o impresos.

Seguridad

Cuando pensamos en seguridad, nos viene a la mente la confianza o la ausencia de riesgos relacionados a un tema en particular, pero dependiendo del campo donde lo apliquemos tendrá mayor rigurosidad. Sin embargo en cualquiera de los campos donde se haga referencia a la seguridad, se deberá evaluar los riesgos a la que se encuentra sometida [2].

La información es uno de los activos más valiosos dentro de una entidad u organización, por lo cual deben protegerse frente a toda amenaza, las cuales se ven aumentadas por el avance de la tecnología y las posibilidades que esta brinda para su alteración o modificación en los diferentes soportes disponibles. Algunas de las amenazas más habituales son el espionaje, fraude, sabotaje, vandalismo o desastres naturales entre otros.

Seguridad de la información

La seguridad informática tiene como objetivo garantizar la integridad, disponibilidad y autenticidad de la información de una entidad, ofreciendo el mínimo de riesgos sobre los recursos, garantizando la continuidad de las operaciones de la organización, reduciendo costos, preservando una estructura que permita su administración [3].

Por su parte "*La seguridad de los sistemas de información es una disciplina en continua evolución. La meta finalidad de la seguridad es permitir que una organización cumpla con todos sus objetivos de negocio o misión, implementando sistema que tengan en especial cuidado y consideración hacia los riesgos relativos a las TIC de la organización, a sus socios comerciales, clientes, Administración Pública, suministradores, etc*." [4].

Al mencionar a la seguridad y relacionarla con las operaciones de una empresa o institución, por lo general se asocian a situaciones como: robo, daños físicos, privacidad (accesos no autorizados), entre otros; dejando en ocasiones fuera de alcance el aseguramiento de la infraestructura tecnológica (hardware y software) y el mayor bien: la información. Para poder definir los conceptos de seguridad de los recursos informáticos podríamos declararla como: "*un conjunto de procedimientos, métodos, herramientas y técnicas, implementados para asegurar la integridad, confidencialidad y disponibilidad de la información, y por ende de los sistemas informáticos ante cualquier amenaza*" [5].

La seguridad informática no es un bien medible, en cambio sí se pueden emplear herramientas para cuantificar de alguna forma nuestra inseguridad informática. Cabe recalcar, aunque se apliquen las mayores medidas de seguridad a un sistema de información, este no dejará de tener un margen de riesgo, siempre es factible de ser vulnerado. Al establecer medidas de seguridad es necesario determinar los elementos que conforman el sistema, los peligros que le afectan y las medidas que se deben adoptar para prevenir, reducir o controlar los riesgos potenciales.

Al definir seguridad informática es necesario conocer los elementos que esta resguarda, como son los sistemas de información y los sistemas informáticos, los recursos que se disponen.

Elementos de un sistema de información

Los elementos que componen un sistema de información se identifican como: recursos físicos (computadoras, conexiones, periféricos) y recursos lógicos (sistemas operativos, aplicaciones de software); recursos humanos, conformado por las personas que trabajan en la institución; recursos de información, conjunto de datos organizados y generados

para el desenvolvimiento del negocio; y las actividades, propias de la empresa relacionadas o no con la informática. [6]

2.2 Importancia de la seguridad de la información

El manejo de la seguridad de la información está basado, principalmente en la tecnología, siendo sus principales pilares la integridad, la confidencialidad y la disponibilidad. A raíz de esto la información podría clasificarse en:

- Información crítica: aquella que es indispensable para el funcionamiento de la entidad.
- Información valiosa: aquella que se representa como el principal activo dentro de la entidad
- Información sensible: aquella que es altamente privada y exclusiva de unos pocos.

Un término a considerar dentro del campo de la seguridad de la información son los riesgos a los que ésta se encuentra expuesta. Los riesgos se pueden definir como la probabilidad de ocurrencia, las amenazas que ésta conlleva y el impacto que podría ocasionar en la operatividad del negocio.

A fin de mantener y preservar los activos de una organización se deben establecer metodologías, procedimientos y prácticas a fin de minimizar las amenazas y los riesgos a las que esta se debe enfrentar, asegurando la continuidad de la misma.

Tipos de seguridad

Podemos referirnos a un nivel amplio de la seguridad o bien definirlas en activa y pasiva:

- Seguridad activa: *"Es la encargada de que los sistemas informáticos padezcan algún daño, un ejemplo en los ordenadores sería que se usen contraseñas para proteger los datos que esté almacenada, pero se pueden aplicar otras acciones como encriptar datos, usar software de seguridad como los antivirus o establecer contraseñas seguras"* [7].
- Seguridad pasiva: *"La seguridad pasiva es aquella que se encarga de minimizar los efectos o desastres que se originan en un accidente, un ejemplo podría ser el malware hacia los sistemas informáticos y una acción para ello sería la realización de copias de seguridad"* [7].

Riesgos

Al utilizar la palabra "Riesgo", se entiende la posibilidad de que se origine un contratiempo donde algo o alguien sufre un perjuicio o daño; asociando este concepto con la tecnología informática de una organización – "*Conjunto de los instrumentos y procedimientos industriales de un determinado sector o producto*" [8] - se puede precisar lo siguiente: "*Los riesgos de TI son un componente del universo de riesgos a los que está sometida una organización. Otro de los riesgos a los que una organización se enfrenta*

pueden ser riesgos estratégicos, riesgos ambientales, riesgos de mercado, riesgos de crédito, riesgos operativos y riesgos de cumplimiento. En muchas organizaciones, los riesgos relacionados con TI se consideran un componente de riesgo operativo".

"*Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización. Se compone de los eventos relacionados con TI que potencialmente podrían afectar el negocio. Este hecho puede ocurrir con una frecuencia y magnitud inciertas, y supone dificultades para alcanzar las metas y objetivos estratégicos*" [8].

Riesgo informático

Se define al riesgo informático como "la probabilidad de que una amenaza en particular expone a una vulnerabilidad que podría afectar a la organización" [9] o también como "la posibilidad de que algo pueda dañar, destruir o revelar datos u otros recursos" [9].

A fin de comprender en detalle el concepto de riesgo en el contexto de seguridad de la información, se deben analizar algunos términos relacionados para un mejor entendimiento.

Evento: Se determina una situación posible pero no certera. Relacionado al contexto de la evaluación de riesgos siempre la misma es a un evento futuro, la cual tendrá influencia directa o indirecta sobre un determinado resultado. Además, en ese contexto, el evento será un suceso inesperado y por lo tanto considerado negativo.

Activo: Se denominan así a los valores de una organización y son el objetivo directo o indirecto de un evento. En un contexto de seguridad de la información estarán constituidos por el software, el hardware, las aplicaciones, bases de datos, redes informáticas, copias de seguridad y también el personal de la misma.

Resultado: De forma concreta es el impacto que tiene un determinado evento. Dentro del contexto de la seguridad de la información el resultado será siempre una circunstancia no deseada, la cual podría ser una pérdida o una potencial pérdida. La cual siempre tiene un efecto directo sobre el activo, o al menos en una gran parte del mismo.

Probabilidad: Se denomina probabilidad o frecuencia que un evento ocurra sobre un determinado activo.

Gestión del riesgo

La función principal de la gestión del riesgo es mantener un ambiente seguro, identificando los factores que podrían alterar, dañar o comprometer los datos revelándolos, para lo cual se crean medidas que implementen soluciones para mitigar o reducir el posible riesgo. Todo el proceso de gestión del riesgo se lo emplea para

desarrollar estrategias de seguridad de la información, las cuales buscan reducir al máximo el riesgo de la organización [10].

"Para tratar de minimizar los efectos de un problema de seguridad, se realiza el denominado análisis de riesgos, término que hace referencia al proceso necesario para responder a tres cuestiones básicas de seguridad de una organización, que es saber qué queremos proteger, contra quién o qué se quiere proteger y cómo lo vamos a hacer" [4].

Dentro del campo de la seguridad de la información se deben comprender ciertos conceptos relacionados al riesgo: amenazas, vulnerabilidad e impacto.

Amenazas: Es un evento potencial, un posible acto negativo o acción facilitada por una vulnerabilidad. Es también cualquier probabilidad que pueda ocasionar un resultado no deseable para un activo específico o para la organización de forma completa.

Las amenazas cuentan entre sus acciones el daño, la destrucción, la alteración, pérdida o relevancia de los activos de la organización, los cuales podrían impedir su normal funcionamiento o incluso el acceso a la información u organización misma.

Vulnerabilidad: Es una debilidad o falla en los procedimientos, diseño, implementación o controles internos de un determinado sistema de seguridad. Se considera a cualquier ocurrencia potencial que cause un resultado no deseable para un activo específico o para la organización.

Impacto: es la determinada cantidad de daño que puede causar una amenaza haciendo uso o explotando una determinada vulnerabilidad.

A fin de gestionar y administrar de forma adecuada los riesgos de una organización se deben tener en cuenta lo siguiente:

- Evaluar los riesgos inherentes a los procesos informáticos.

- Evaluar las amenazas o causas de los posibles riesgos.

- Minimizar las amenazas a los riesgos utilizando controles.

- Asignar responsables de los procesos informáticos.

- Evaluar los elementos del análisis de riesgos.

2.3 Metodología de Análisis y evaluación de riesgos

Existen diferentes metodologías para gestionar el proceso de análisis, evaluación y gestión de riesgos informáticos, cada una con características propias y destinadas a situaciones y objetivos en particular [11] .

Sin embargo, cada una de estas metodologías cuenta con actividades y componentes en común como son:

- **Identificación de amenazas**: se enfoca en identificar las posibles amenazas a la seguridad de la información. Estas amenazas son los eventos y acciones que podrían alterar o perjudicar los activos relacionados a la seguridad de la información de la organización.

- **Identificación de vulnerabilidades**: se enfoca en identificar las posibles vulnerabilidades que podrían ser explotadas por las amenazas previamente identificadas. Asimismo, la existencia de una vulnerabilidad contribuye a calcular la probabilidad del riesgo.

- **Identificación de activos**: es el proceso en el cual se identifican los activos esenciales o críticos que tienen un impacto directo en la confidencialidad, integridad y disponibilidad de las fuentes de información de la organización.

- **Determinación del impacto**: es el proceso para determinar o medir el impacto de una amenaza sobre un activo. Este impacto puede ser catalogado de forma cuantitativa o cualitativa.

- **Determinación de la probabilidad**: esta actividad tiene como objetivo medir la probabilidad de ocurrencia de una determinada amenaza, para lo cual se le asigna un valor probable.

- **Identificación de controles**: los controles permiten detectar o prevenir las fuentes de amenazas que tratan de explotar las vulnerabilidades. En esta actividad se identifican los controles que se están llevando a cabo sobre un activo y el efecto que tendría sobre la amenaza que se evalúa.

- **Tratamiento de riesgos**: con el objetivo de asegurar la organización es necesario determinar el tratamiento que se le dará a los riesgos analizados y valorados. La aplicación de las medidas, estarán enfocadas de forma principal en aquellos riesgos que representen un impacto catastrófico, la imposibilidad de continuar con servicios esenciales de la organización o que afecten a personas. Asimismo, se tratarán aquellos riesgos cuyas probabilidades de realización sean medios o altos y a fin de mitigarlos será necesario desarrollar estrategias de gestión de riesgos a fin de eliminarlos o reducirlos a niveles aceptables. Entre estas estrategias se encuentran las siguientes:

- **Mitigación o reducción del riesgo**: en este enfoque se utilizan varios mecanismos de control para mitigar los riesgos hallados. Los controles podrán ser técnicos, administrativos o físicos y todos ellos tendrán por objetivo reducir la probabilidad o impacto del riesgo.

- **Asignación o transferencia del riesgo**: permitirá transferir el riesgo de una organización a otra.

- **Aceptación del riesgo**: en este enfoque las organizaciones están conscientes de los riesgos hallados, pero el valor de mitigarlos supera el valor del activo que desean proteger.

- **Eliminación del riesgo**: en este caso las organizaciones deciden no tomar el riesgo, es decir ante la potencial pérdida, la misma supera el valor de la ganancia potencial en caso de continuar con una actividad riesgosa. De esta forma se elimina la amenaza con el cambio del recurso o de la infraestructura informática.

2.4 Sistemas de Gestión de la Seguridad de la Información

En un SGSI definido por la norma ISO/IEC 27001:2013, se deben tener en cuenta las características propias de la organización, debe ser ajustado periódicamente conforme la capacidad de la misma para introducir mejoras en forma permanente [12].

Para desarrollar y establecer un SGSI con base a ISO/IEC 27001:2013, se debe definir el alcance del SGSI en términos de la organización, su ubicación, sus activos y la tecnología utilizada. Una vez identificados estos componentes se procede a calcular el riesgo que afecta a los activos y se diseña la política de seguridad de la organización.

La propuesta tiene como objetivo gestionar los riesgos de los activos de información de la DGLH basando la misma en la metodología propuesta por Magerit.

2.5 Metodologías para la gestión de riesgos

El análisis de los riesgos relacionados con la seguridad y asociados a pérdidas, alteración o interrupción de la información pueden ser aplicados a través del uso de diferentes metodologías. A continuación, se describirán algunas de las metodologías para el análisis y gestión de riesgos disponibles en el mercado actualmente.

Metodología Mehari

Desarrollado en 1996 por la empresa CLUSIF y respaldado por un software administrado por Risicare, MEHARI [13] es un método de análisis y gestión de riesgos que tiene como principal objetivo ayudar a la alta dirección de empresas (gerentes, CEO, auditores) en su tarea de gestionar la seguridad de la información, los recursos informáticos de la misma y reducir los riesgos asociados a éstos. Esta metodología está asociada a la norma ISO

13335 de gestión de riesgos y cumple con los procesos necesarios para un SGSI descrito por la ISO 27001 ya que permite desarrollar planes de seguridad basados en vulnerabilidades identificadas previamente con un monitoreo continuo, ofreciendo un ciclo de mejora continua.

MEHARI provee los siguientes puntos:

1. Bases de conocimiento de acuerdo a situaciones de riesgo.
2. Reglas para consolidación del análisis de riesgos resultantes de un entorno óptimo.
3. Análisis de los principales desafíos de la organización.
4. Análisis de las vulnerabilidades.
5. Disminución y administración de los riesgos.
6. Monitoreo de la seguridad de la información.

Metodología CRAMM

Esta metodología de análisis y manejo de riesgos, CRAMM [14] está basada en el uso de un software, donde destaca los valores cualitativos antes que los cuantitativos, basándose principalmente en tres fases fundamentales, las que se detallan a continuación:

- Evaluación del valor de la información e identificación de los activos que respaldan el proceso comercial de la organización.
- Identificación de las amenazas que puedan afectar al sistema y una estimación de la vulnerabilidad del sistema antes dichas amenazas. El siguiente paso es afrontar dichas medidas de riesgo a través de un análisis de la combinación de amenazas, vulnerabilidades y el correspondiente valor de los activos. Las medidas de riesgo se irán escalando de modo que los requisitos de seguridad establecidos irán variando de acuerdo al riesgo identificado.
- Detección de la forma de contrarrestar los riesgos incluyendo mejoras necesarias para medir los controles existentes.

Metodología RISKIT

Publicada en el año 2009 por ISACA, RISKIT [15] es una metodología de gestión de riesgo con objetivos empresariales. La misma tiene como fin comparar el riesgo de TI evaluado con el riesgo y tolerancia que la organización haya establecido inicialmente. De igual forma, gestiona los riesgos de TI identificados a efectos que las gerencias claves de la empresa los administre y los gestione a fin que no solo queden en manos del departamento TI, sino que tenga un seguimiento adecuado.

La metodología RISKIT permite a los usuarios:

- Integrar la gestión de riesgos en conjunto a la del riesgo empresarial (ERM).

- Comparar los riesgos de TI evaluados con los riesgos de tolerancia definidos por la organización.
- Comprender la gestión de los riesgos.

La conexión del negocio se basa fundamentalmente en los principios sobre los que se basa, la gobernanza empresarial de manera efectiva y su gestión del riesgo TI. A continuación, algunos de sus principios:

- Siempre alinearse con los objetivos del negocio.
- Alinear la administración del riesgo del negocio de TI con el ERM general.
- Balancear costos y beneficios de administrar el riesgo de TI.
- Promover una comunicación abierta y justa en el riesgo de TI.
- Establecer desde la alta dirección, la forma correcta para hacer cumplir la responsabilidad personal y operar en los niveles de tolerancia aceptables.
- Determinar que sea un proceso continuo y diario.

Esta metodología se encuentra agrupada en tres dominios principales:

Gobierno del riesgo: asegura que las prácticas de gestión de riesgos de TI estén integradas en la empresa, permitiendo asegurar una óptima rentabilidad sobre el riesgo. La misma está basada en los procesos:

- Establecer y mantener una visión común del riesgo TI.
- Integrar con ERM.
- Tomar conciencia de las decisiones de riesgos en la organización.

Evaluación ante riesgos: asegura que los problemas, oportunidad y los eventos relacionados con los riesgos de TI se encaren de forma económica y estén alineados con las prioridades comerciales. La misma se basa en los procesos:

- Recopilar información esencial.
- Analizar los riesgos.
- Mantener un perfil de riesgos.

Respuesta ante riegos: aseguro que los problemas, oportunidades y eventos relacionados con los riesgos de TI se aborden de forma práctica y estén correctamente alineados. La misma se basa en los procesos:

- Articular los riesgos.
- Gestionar los riesgos.
- Reaccionar ante eventos de riesgos (incidentes).

Metodología NIST SP 800-30

El Instituto Nacional de Estándares y Tecnología (NIST) ha incluido un estándar publicado como un documento especial para el análisis y gestión de riesgos de seguridad de la información, NIST SP800-30 [16], es un documento especial para el análisis de los sistemas TI. La ley de Gestión de Seguridad de la Información Federal (FISMA) requiera a las entidades federales que se adecuen a los estándares dictados por NIST.

Esta metodología consta básicamente de 9 pasos básicos para el análisis de riesgos, los mismos son:

- Caracterización de sistemas.
- Identificación de amenazas.
- Identificación de vulnerabilidades.
- Análisis de controles.
- Determinación de probabilidades.
- Análisis de impacto.
- Determinación del riesgo.
- Recomendación de controles.
- Documentación de resultados

Metodología MAGERIT

Desarrollada por el Consejo Superior de Administración Electrónica, MAGERIT [17] publicó su primera versión en 1997, la segunda en 2006 y la tercera versión en el año 2012. La metodología MAGERIT se encuentra enfocada principalmente a la Administración Pública, con el objetivo central de minimizar los riesgos propios de la implementación de Tecnologías de la Información en el ambiente público.

La metodología propuesta por Magerit en su versión 3, [18], cataloga a las amenazas en cuatro grupos que son: desastres naturales, de origen industrial, errores y fallos no intencionados, y ataques intencionados. Cada activo tiene asociado un grupo de posibles amenazas las cuales se valoran por la probabilidad de ocurrencia y la degradación de la Disponibilidad, Integridad, y Confidencialidad, permitiendo el análisis para la gestión y determinación de las salvaguardas preventivas y correctivas identificadas dentro del plan de contingencia informática.

La versión 3 de Magerit [19], está conformada por dos libros y una guía de técnicas, el detalle es el siguiente:

> Libro I – Método: En este libro se explican las principales actividades a realizar dentro de la organización, se incluyen además las tareas que forman parte de la metodología.

Libro II – Catálogo de elementos: En este libro se proporcionan las pautas en la aplicación de la metodología, los cuales incluyen:

- Tipos de activos.
- Dimensiones de valoración activos.
- Criterios de valoración de los activos.
- Amenazas típicas sobre los sistemas de información.
- Controles a considerar para proteger los sistemas.

Libro III - Guía de Técnicas: En este libro se da orientación en las técnicas que emplea la metodología para poder llevar un correcto análisis y gestión de los riesgos. En el mismo se presentan las técnicas específicas y generales para el análisis de riesgos.

Metodología OCTAVE Allegro

OCTAVE [20] ha sido desarrollado de forma conjunta por la Universidad Carnegie Mellon (Carnegie Mellon University, CMU) y el Instituto de Ingeniería de Software. Su enfoque apunta a una amplia evaluación del entorno de riesgo operacional de una organización, teniendo como principal objetivo obtener resultados sólidos sin necesidad de profundos conocimientos en la evaluación de riesgos. La metodología OCTAVE se puede llevar a cabo de forma colaborativa, ya que la misma posee cuestionarios, hojas de trabajo y documentación para hacerlo de esa forma según lo define en su documentación.

OCTAVE está conformada por ocho pasos organizados en cuatro fases.

En la primera fase la organización establece los criterios de medición de riesgos. En la segunda fase se perfilan los activos de información que determinarán cuales son los activos críticos a priorizar, definiendo un perfil para cada uno de ellos e identificado sus características. En la tercera fase se identifican los escenarios de amenaza de los activos de información conforme al contexto de cada uno de ellos. En la última fase se identifican y analizan los riesgos de estos activos de información y se inicia el desarrollo de mitigación de los mismos.

ISO 27005

El objetivo de este estándar es proveer lineamientos para la gestión de riesgos de seguridad de la información. Esta norma se basa en los conceptos especificados en la ISO/IEC 27001 [21] y ha sido diseñada para llevar a cabo de forma satisfactoria la implementación de la seguridad de la información en base a un enfoque de gestión de riesgos. En la misma no se especifica ni se recomienda ni se nombra algún método de análisis de riesgos aunque se brinda un sistematizado y riguroso proceso de analizar riesgos para crear posteriormente un plan de tratamiento de los mismos.

Este estándar abarca las buenas prácticas en seguridad de la información, describiendo un conjunto de objetivos de control de seguridad en su contenido.

Entre las fases de esta normativa se encuentran el establecimiento del contexto, identificación, estimación, evaluación, tratamiento, aceptación, revisión y monitoreo del riesgo.

Esta normativa es aplicable a todo tipo de organización que tenga como objetivo gestionar los posibles riesgos que comprometan a la organización.

ISO 31000

Publicado en el año 2009, este estándar proporciona los lineamientos para la implementación de la gestión de riesgos para cualquier tipo de organización. Esta norma permite que todas las tareas tanto estratégicas como de gestión y operativas de diferentes proyectos de una organización, se alineen con los objetivos de negocio.

En sus componentes, la ISO 31000 [22] incluye lo siguiente:

- Transferencia de brechas de rendición de cuentas en la gestión del riesgo empresarial.
- Alineación de objetivos de los marcos de gobernanza con ISO 31000.
- Integración de los mecanismos de informe del sistema de gestión.
- Crear criterios de riesgo uniformes y métricas de evaluación.

2.6 Políticas de seguridad de la información

La seguridad de la información debe estar respaldada por la gerencia, escrita en forma conjunta y alineada con los objetivos que presenta la misma. En esas políticas se deben resaltar los puntos importantes que la organización espera obtener por parte de la seguridad de la información y especialmente definidos los activos que se esperan proteger.

Familias de estándares ISO/IEC 27000

Tabla 1. Familias de estándares de ISO/IEC 27001
Fuente: http://www.iso27001security.com/index.html

Estándares	Descripción
27000. Generalidades y vocabulario	Provee una generalización de los SGSI y emplea un glosario con los términos y definiciones formales que se utilizan en la familia de estándares ISO/IEC 27000.

27001.Especificación Formal del SGSI	Especifica formalmente el SGSI mediante una serie de actividades que conciernen a la gestión de los riesgos de seguridad de la información. Éste estándar es aplicable a las organizaciones de todo tipo y tamaño, pero no dicta formalmente cuáles controles de seguridad se deben utilizar, sino que otorga libertad a las organizaciones de implementar los que mejor se adapten a su situación particular.
02. Controles de Seguridad de la Información	Es un código de buenas prácticas que recomienda los controles de seguridad a implementar que ayudan a cumplir los objetivos de la seguridad de la información relativos a gestionar los riesgos que incidan sobre la confidencialidad, integridad y disponibilidad de la información.
27003. Guía de Implementación	Describe los procesos del diseño y especificación del SGSI a través de las distintas actividades planeadas; desde obtener el soporte por parte de la dirección hasta la planeación de la implementación del proyecto.
27005. Gestión del Riesgo	Provee los lineamientos para la gestión de los riesgos de la seguridad de la información pero no recomienda o especifica una metodología de gestión del riesgo.
27014. Gobierno de Seguridad de la Información	Provee una guía para implementar un Gobierno de Seguridad de la Información, el cual garantiza la alineación con las estrategias y objetivos de la organización generando valor y responsabilidad.
27031. Continuidad del Negocio	Describe los conceptos y guías para garantizar la continuidad del negocio en caso de incidentes de seguridad internos o externos.

Tabla 2. Principales familias de la Norma ISO/IEC 27000
Fuente: http://www.scielo.mec.pt/pdf/rist/n22/n22a06.pdf

Norma	**Descripción**
ISO/IEC 27000	Visión general de la serie 27000
ISO/IEC 27001	Requerimientos para constituir un SGSI.

ISO/IEC 27002	Guía de buenas prácticas en objetivos de control y controles recomendados de Seguridad de la Información.
ISO/IEC 27003	Guía de implementación de SGSI junto a información de uso del esquema PHVA
ISO/IEC 27004	Métricas para la implementación y gestión de la seguridad de la información.
ISO/IEC 27005	Guía de técnicas de Gestión de Riesgos
ISO/IEC 27006	Requisitos para la acreditación de entidades de auditoría y certificación.
ISO/IEC 27007	Guía de auditoría de SGSI
ISO/IEC 27799	Guía para la implementación de ISO 27002
ISO/IEC 27035	Detección y evolución de incidentes de seguridad

2.7 ISO/IEC 27001

La norma ISO/IEC 27001 [23] define los principales requisitos a considerar en un SGSI, ésta deriva de la Norma Británica de Seguridad de la Información, BS 7799, en su primera parte la norma es no certificable y de la cual derivan las normas ISO 17799 y la ISO 27002 [24]. La segunda parte es certificable y de ésta deriva la norma ISO 27001. Esta norma fue publicada en el año 1999 y revisada en el 2002. A través de esta revisión se determinó la incorporación para la publicación del SGSI del ciclo denominado Deming o PHVA (Planificar, Hacer, Verificar, Actuar).

La última revisión de la norma ISO 27001 corresponde al año 2013 a partir de donde se obtiene su propósito: "proporcionar un modelo para el establecimiento, implementación, ejecución, seguimiento, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información".

La adopción de la norma ISO 27001 debe ser considerada ante las necesidades de una decisión estratégica, puesto que el diseño e implementación de un SGSI de una organización esta referenciado por los procesos, los requisitos de necesidad de la misma y los objetivos, estructura y tamaño de la organización.

En la referida versión de la norma se encuentra una estructura definida en dos partes, donde la primera se compone de 10 capítulos y en la segunda parte conformada por el denominado Anexo A, el en cual se establecen los objetivos de control. En el Anexo 13 se encuentra un detalle de los dominios antes nombrados.

La norma ISO 27001 proporciona el marco de trabajo necesario para establecer un SGSI que posteriormente puede ser oficialmente certificado por la entidad internacional ISO.

Dentro de las cláusulas que ofrece la norma ISO 27001 presenta lo siguiente:

1. Objeto y campo de aplicación: Se explica el fin de la norma y el detalle de aplicación dentro de la organización.
2. Referencias normativas: Se indica las bases de referencia que ésta tiene como base, es decir a la ISO 27000.
3. Términos y definiciones: Los mismos se hallan basados en la norma ISO 27000.
4. Contexto de la organización: En el mismo se intenta determinar los aspectos internos y externos que son relevantes para la organización y además intenta comprender las expectativas y necesidades de la misma determinando los alcances del SGSI.
5. Liderazgo: Se detalla el rol que debe asumir la dirección de la organización dentro del SGSI, asumiendo el compromiso, estableciendo las políticas acordes y asignando los roles y responsabilidades dentro de la organización.
6. Planificación: De acuerdo a los criterios establecidos dentro de la contextualización de la organización se debe realizar una valoración, análisis y evaluación de los riesgos de seguridad. Se deben definir los objetivos de seguridad de la organización y se deben realizar un tratamiento de los riesgos de los elementos identificados.
7. Soporte: Los recursos necesarios para la correcta definición del SGSI deben ser proporcionados y determinados por la organización, procurando que todo el personal de la misma, tome conciencia de las políticas establecidas y de la necesidad de realizar las documentaciones de relevancia.
8. Operaciones: Se deberán indicar la planificación, el modo de implementación y control de los procesos necesarios para cumplimentar la normativa planteada, además de la definición de los plazos y tiempos de evaluación y tratamientos de riesgos de seguridad de la información en la organización.
9. Evaluación: Se analizará mediante evaluaciones permanentes, el monitoreo y el análisis del SGSI a través de los resultados obtenidos mediante auditorías internas y las revisiones que se indiquen a través de la dirección del área.
10. Mejoras: Se acompañará el desarrollo del SGSI con acciones correctivas mediante la aplicación de mejoras continuas.

Los objetivos de control de seguridad de la información pertenecientes al Anexo A son la serie más conocidas y utilizadas para la implementación de norma ISO / IEC 27001:2013, la que está conformada por:

- Áreas de Control (14): son los principales temas que incluyen los principales aspectos de la seguridad de la información.
- Objetivos de Control (34): son los controles expresamente detallados.
- Controles (114): son cada uno de los controles que se implementan.

Tabla 3. Áreas de controles del Anexo A
Fuente: https://www.iso27000.es/iso27002.html

N°. Anexo A	Área de Control	N°. de Controles
A5	Políticas de seguridad de la información	2
A6	Organización de la seguridad de la información	7
A7	Seguridad con los recursos humanos	6
A8	Gestión de activos	10
A9	Control de acceso	14
A10	Criptografía	2
A11	Seguridad física y ambiental	15
A12	Seguridad de las operaciones	14
A13	Seguridad de las comunicaciones	7
A14	Adquisición, desarrollo y mantenimiento de sistemas	13
A15	Relaciones con los proveedores	5
A16	Gestión de incidentes de seguridad de la información	7
A17	Aspectos de seguridad de la información en la continuidad de negocio	4
A18	Cumplimiento	8
	Total de controles	114

El proceso de certificación de la Norma ISO 27001:20013 consta principalmente de tres fases que se pueden detallar de la siguiente manera:

1. Antes de la auditoria externa

   a. Implementación del SGSI
   b. Realización de auditorías internas periódicas con adecuación de controles
   c. Selección de equipo de certificación para el SGSI

2. Durante la auditoria externa

   a. Fase 1 de la auditoria, verificar el cumplimiento de requerimientos.
   b. Fase 2 de la auditoria, revisión de la efectividad del SGSI.

3. Luego de la auditoria externa

   a. Confirmación del registro de la certificación, a cargo del auditor líder.
   b. Auditoría para mejora continua cada 6 o 12 meses durante los próximos 3 años.

A fin de complementar la normativa internacional con la finalidad de la protección y confidencialidad de los datos e información se elaboró la ISO 27002.

2.8 ISO/IEC 27002

La norma ISO/IEC 27002 [24] es una guía de las mejores prácticas para la gestión de la Seguridad de la Información la cual anteriormente era denominada ISO 17799:2005, posteriormente en el año 2007 se la renombró y es como se la conoce actualmente.

En esta normativa se encuentran definidos los principales objetivos y las recomendaciones recolectadas en el tema de la Seguridad de la Información, centrada en las principales preocupaciones de la seguridad y los temas que le son afines.

La misma contiene 39 objetivos de control y 133 controles que se hallan agrupados en 11 dominios.

La norma ISO 27002:2005 fue identificada con diferentes nombres según el momento de su publicación en los diferentes países, por ejemplo: IRAM ISO/IEC 27002 en Argentina, NHC ISO 27002 en Chile, NTP ISO/IEC 17799:2007 en Perú, Fondo Norma ISO/IEC 27002 en Venezuela y UNE ISO/IEC 27002:2009 en España.

Dominios de seguridad ISO/IEC 27002:2013

Dado que la seguridad de la información y la gestión de los activos es un tema muy importante y amplio que se refleja en todo tipo y tamaño de organizaciones sea pública o privada, en la norma ISO/IEC 27002 [16]se cubren las principales necesidades de todas ellas y además presenta los riesgos de seguridad ante empleados, consultores, proveedores y la gestión de la continuidad del negocio y el cumplimiento de las mismas. La norma se extiende a la seguridad de la información en todos sus aspectos, datos, documentación, conocimiento, entre otros y no solo en lo referente a la seguridad digital.

En la norma ISO/IEC 27002 se encuentra un inventario de buenas prácticas donde se detallan los puntos clave de la ISO 27001 los que en forma conjunta contemplan la ciberseguridad y la protección de la información en todos los ámbitos posibles.

La estructura que presenta la ISO/IEC 27002:2013 es de 14 dominios, del 0 al 4 se halla una introducción, una norma relacionada y un listado de términos y definiciones. A continuación se describen los puntos más destacados, en la XXX se puede observar la estructura que presentan los dominios y su relación entre sí.

5. Políticas de seguridad

5.1 Directivas de la dirección en seguridad de la información. Proporciona elementos para la dirección y gestión de la seguridad acordes con los requisitos del negocio y las normativas más relevantes.

6. Organización de la Seguridad de la Información

6.1 Organización interna: establece un marco de gestión para implementar la organización y operación dentro de la organización.

6.2 Dispositivos para movilidad y teletrabajo, garantiza la seguridad del teletrabajo y dispositivos.

7. Seguridad de los recursos humanos

7.1 Antes de la contratación: garantiza a los empleados y contratistas sus funciones y responsabilidades del empleo.
7.2 Durante la contratación: garantiza a los empleados y contratistas sobre sus responsabilidades en los temas de seguridad de la información.
7.3 Cese o cambio de puesto de trabajo: protege los intereses de la organización al cambio o terminación del empleo.

8. Gestión de los activos

8.1 Responsabilidad sobre los activos: identifica los activos de la organización y define las responsabilidades de protección acordes.

8.2 Clasificación de la información: asegura la protección de la información acorde a la importancia que tiene para la organización.

8.3 Manejo de los soportes de información: evita la divulgación de la información almacenada en los medios que posee la organización.

9. Control de accesos

9.1 Requisitos de negocio para el control de accesos: limita el acceso físico dentro de la organización.

9.2 Gestión de acceso de usuario: garantiza el acceso a los usuarios y gestiona los permisos a los servicios y sistemas.

9.3 Responsabilidad de usuario: define las responsabilidades de usuarios y su información.

9.4 Control de acceso a sistemas y aplicaciones: gestiona el acceso autorizado a sistemas y aplicaciones.

10. Cifrado

10.1 Controles criptográficos: aplicación de la criptografía para asegurar la confidencialidad, autenticidad e integridad de la información en la organización.

11. Seguridad física y ambiental

11.1 Áreas seguras: gestiona el acceso físico no autorizado, daños a las instalaciones de proceso de la información.

11.2 Seguridad de los equipos: gestiona el daño, robo o pérdida de los activos físicos de la organización y la interrupción de los servicios.

12. Seguridad de las operaciones

12.1 Responsabilidad y procedimientos de operación: asegura la ejecución de las operaciones dentro la organización mediante los procedimientos.

12.2 Protección contra código malicioso: garantizar que las instalaciones estén protegidas contra malware y otras técnicas.

12.3 Copias de seguridad: garantiza los backups de la información en la organización.

12.4 Registros de actividad y supervisión: registra eventos y genera las evidencias de accesos y otros ítems importantes.

12.5 Control de software: garantiza la integridad de los sistemas operativos base.

12.6 Responsabilidad y procedimientos de operaciones: anticipa la prevención de explotación de vulnerabilidades de orden técnico.

13. Seguridad de las comunicaciones

13.1 Gestión de la seguridad de las redes: asegura la protección de la información en las redes y las instalaciones.

13.2 Intercambio de información entre partes: mantiene la seguridad de la información dentro de la organización y con entidades externas.

14. Adquisición de sistemas, desarrollo y mantenimiento

14.1 Requisitos de seguridad de sistemas: asegura que la seguridad de la información forme parte de todo el ciclo de vida de los sistemas.

14.3 Datos de prueba: asegura la protección de los datos utilizados en ambientes de prueba.

15. Relaciones con los proveedores

15.1 Seguridad de la información con los proveedores: asegura la protección de los activos donde puedan intervenir los proveedores.

15.2 Gestión de la prestación de servicios de proveedores: mantiene un nivel de seguridad en la prestación de servicios de los proveedores conforme a los acuerdos realizados.

16. Gestión de incidencias

16.1 Gestión de incidentes de seguridad y mejoras: asegura la gestión eficaz de los incidentes de seguridad de la organización y mantiene una comunicación sobre eventos.

17. Aspecto de seguridad para la gestión y continuidad del negocio

17.1 Continuidad de la seguridad de la información: asegura la continuidad en los procesos definidos como esenciales en la organización.

17.2 Redundancias: mantiene la disponibilidad y el uso de las instalaciones donde se realizan procesos de información en la organización.

18. Conformidad

18.1 Cumplimiento de requisitos legales: evitar incumplimientos legales o reglamentarios relacionados con la seguridad de la información.

18.2 Revisiones de seguridad: asegurar la implementación de las medidas de seguridad de la información conforme a las políticas y procedimientos definidos por la organización.

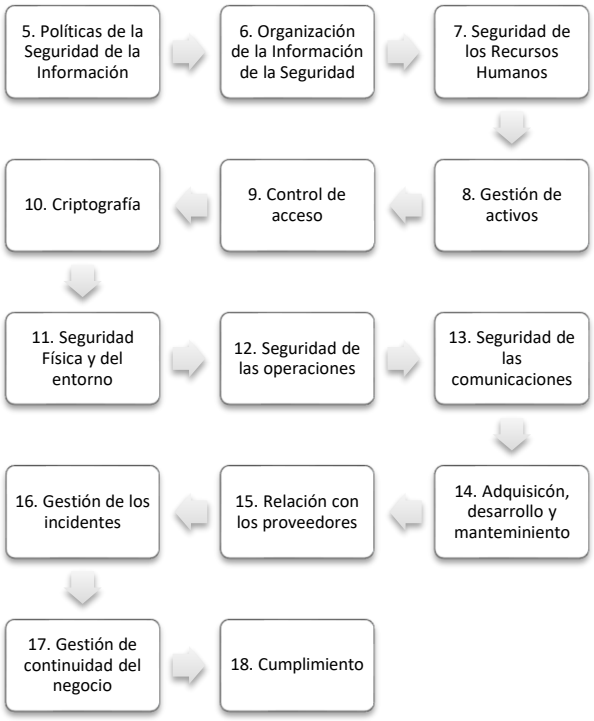

Fig. 1 Dominios de Seguridad de Norma ISO/IEC 27002: 2013
Fuente: Elaboración propia

2.9 Discusiones y Comentarios

Planteadas las consideraciones y definiciones más relevantes en cuanto a la conveniencia de la implementación de un SGSI en el área de la DGLH de la UNNE, mencionados los estándares más importantes que tratan la seguridad de la información y la gestión de riesgo y, detalladas las características principales del estándar ISO 27000 y MAGERIT para la gestión de riesgos, se considera adecuada su aplicación en el presente TFM para el diseño de un sistema que implemente políticas de seguridad y gestión de riesgos informáticos en el área bajo estudio, dado que dicho estándar puede ser utilizado por cualquier tipo de entidad sin importar el sector al que pertenezca, ofreciendo recomendaciones y sugerencias sobre las buenas prácticas de seguridad informática.

Capítulo 3
Descripción del caso de estudio (UNNE)

En el presente capítulo 3, se describe a la organización sobre la que se llevará a cabo el proyecto, la DGLH de la Universidad Nacional del Nordeste. Se realiza la descripción de sus misiones y funciones centrándose en el área de Tecnologías de la Información de la misma.

3. Descripción de la organización y caso de estudio (UNNE)

El 14 de noviembre de 1956 bajo el Decreto Ley Nº 22.299 es creada la Universidad Nacional del Nordeste, la misma fue creada como universidad de alcance regional, comprendiendo institutos y facultades de las provincias de Chaco, Corrientes, Misiones y Formosa, dependientes en ese momento de la Universidad Nacional del Litoral. La UNNE es regulada en su funcionamiento a través de su estatuto universitario y resoluciones del Consejo Superior y se halla comprendida en la Ley Nacional de Educación Superior N° 24.521

Algunos artículos principales del estatuto de la UNNE que rigen su funcionamiento:

En su artículo 1º expresa: *"Es una persona jurídica de derecho público, creada para satisfacer las exigencias de cultura superior en las provincias de Corrientes y Chaco, con sede principal y domicilio legal en la ciudad de Corrientes. Tiene por fin primordial la generación y comunicación de conocimientos del más alto nivel, y la formación ética, cultural, técnica y profesional, contribuyendo al esclarecimiento de los problemas y necesidades de todo orden de la región, para beneficio del hombre y extendiendo su acción y servicios a la comunidad a la que pertenece, en un clima de libertad, justicia, igualdad y solidaridad*".

En su artículo 3 determina que *"es persona jurídica y autónoma académica e institucionalmente autárquica; se da su estatuto, dispone y administra su patrimonio y sanciona su presupuesto conforme a esta última condición jurídica y fija su régimen salarial y de administración de personal. Tiene pleno gobierno de su actividad, proyecta y orienta los estudios, elige sus Autoridades, designa, contrata y remueve profesores, funcionarios y agentes de su administración en la forma que establecen este Estatuto y sus reglamentaciones".*

En el conjunto de actores que conforman el Gobierno de la Universidad se encuentra el Consejo Superior Universitario, conformado por profesores, alumnos, egresados y no docentes quienes conforman el claustro universitario. Este consejo es quien legisla en el ámbito universitario y a través de las Secretarías de cada área es el Rector/a quien lleva a la práctica las decisiones que se toman por el Consejo Superior Universitario.

Dentro de las normativas, las que aplican al personal docente y no docente se hallan:

-Convenio Colectivo para el sector no docente N°366/06.

-Convenio Colectivo para los docentes de las instituciones universitarias nacionales homologado por el Decreto N° 1246/15.

La Universidad Nacional del Nordeste cuenta con 11 facultades; 12 institutos y nodos administrativos: Instituto Rectorado, Instituto de Servicios Sociales, Instituto de Ciencias Criminalísticas e Instituto Medicina Regional, Secretaría General de Asuntos Sociales, Secretaría General de Extensión Universitaria Delegación Corrientes y Delegación Resistencia, Campus Resistencia, Campus Sargento Cabral, Relaciones Laborales, Dirección General de Bibliotecas y Campus Deodoro Roca, ver, además está conformada por una escuela secundaria denominada ERAGIA. Todas estas unidades se encuentran distribuidas geográficamente en las provincias de Corrientes y Chaco.

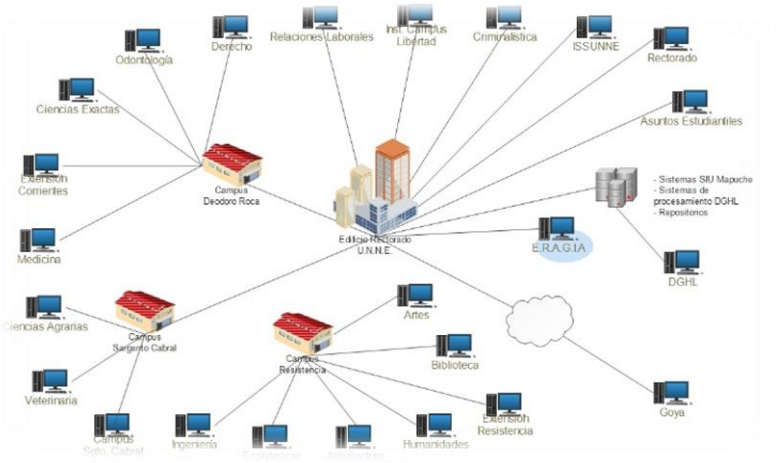

Fig. 2 . Esquema de conexión de las unidades académicas de la UNNE
Fuente: Elaboración propia

El 8 de octubre de 2008 y mediante la Resolución 606/08 del Consejo Superior de la UNNE es aprobado el "Manual de Organización de Unidades Académicas de la Universidad Nacional del Nordeste", el cual comprende la "Estructura orgánico funcional básica y común de Unidades Académicas UNNE" y el respectivo "Manual de Misiones y Funciones".

A su vez el 12 de diciembre de 2019, a través de la Resolución 1115/18 del Consejo Superior es aprobada la "Estructura orgánica-funcional del Rectorado de la Universidad Nacional del Nordeste e Institutos Dependientes", representación que se muestra en el siguiente organigrama de la Fig. 3. Estructura orgánico funcional de la UNNE.

En la misma se puede observar la importante función que posee la DGLH de forma directa para la Secretaria General Administrativa y para Universidad en general.

Entre las funciones que conlleva la DGLH, se encuentran las de liquidar los haberes de los agentes en todos sus escalafones y acreditar los sueldos conforme al Decreto Ley de Plan de Sueldos de la UNNE, para lo cual se nutre de los datos que aportan las diferentes unidades académicas que conforman la institución y las cuales mediante los informes de las novedades de altas o bajas de cargos y agentes generan el activo más importante de la DGLH.

Asimismo, se observa la dependencia que ésta posee, conformando la Dirección de Programación, el Departamento de Procesos y Sistemas y el de Mantenimiento de Software.

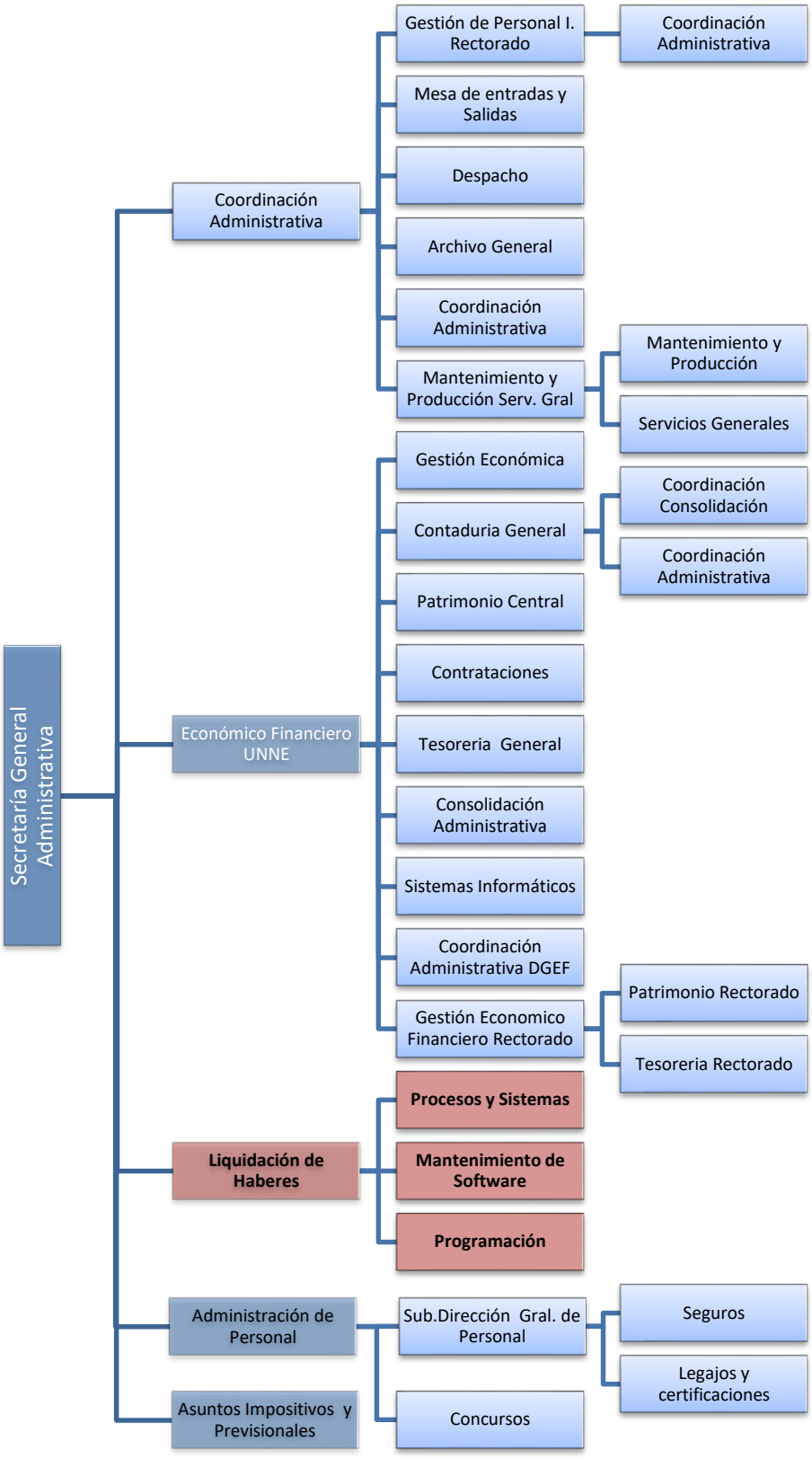

Fig. 3. Estructura orgánico funcional UNNE.
Fuente: Boletín oficial

3.1. Misiones y funciones de la DGLH

El lugar donde se encuentran físicamente las oficinas de la DGLH es en el edificio de Rectorado de la Universidad Nacional del Nordeste en Corrientes Capital. La estructura orgánica de la misma fue aprobada por Resolución N° 11/15 del Consejo Superior y posteriormente modificada por la Resolución 1115/18 de respectivo Consejo. Entre las funciones que tiene a cargo la DGLH se destaca la de aplicar de forma estricta las instrucciones recibidas por la SPU además de las leyes actuales o sus respectivas modificatorias a las ya existentes. En las mismas se elaboran fórmulas, se configuran parámetros y se definen las variables y conceptos necesarios que posteriormente son utilizados en las definiciones de las liquidaciones de haberes mensuales.

Entre otras funciones que lleva a cabo es el proceso de imputaciones contables de cada una de las liquidaciones del mes y posteriormente se eleva ante las autoridades toda la documentación de dichos movimientos contables resúmenes de gastos, liquidaciones bancarias, los cuadros de resumen de las liquidaciones realizadas las que posteriormente y a través de resolución, el Consejo Superior emitirá como gasto.

También conforma lo exigido por el Sistema RHUN de la SPU, la DGLH define y procesa los parámetros, con los que luego exportará un informe de las tareas realizadas.

Por su parte la Dirección también interviene con terceros en relaciones de definición y ejecuciones de aplicaciones y sistemas de SICOSS, SICORE y AFIP.

En su relación con las unidades académicas, lleva adelante planes de capacitación en diferentes temáticas. En los mismos se establecen las normativas a seguir en caso de nuevas aplicaciones a implementar y se los guía en su uso y en nociones de seguridad, privacidad y del manejo de la información.

3.2. Análisis FODA del área de TI de la DGLH

En base al relevamiento de la información obtenida en el área TI de la Dirección General de Liquidación de haberes se realizó un análisis a través de una matriz FODA, ver Tabla 4, en la misma se puede observar de forma general la situación del área. En la misma se puede determinar que a pesar de enfrentarse a importantes amenazas y poseer debilidades

observables también se destacan las fortalezas y oportunidades que pueden ser aprovechadas

Tabla 4. Matriz FODA de la DGLH.
Fuente: Elaboración propia

Fortalezas	**Oportunidades**
• Total apoyo de la Dirección de la DGLH. • Coordinación permanente entre los integrantes del área. • Alto compromiso del personal con sólidas capacidades técnicas y de experiencia. • Formación y capacitación de acuerdo a las necesidades.	• Desarrollo tecnológico. • Políticas de organización apoyando el trabajo de excelente. • Utilización de nuevas tecnologías y buenas prácticas enfocadas en la organización estatal. • Capacidad de adaptación a nuevas herramientas.
Debilidades	**Amenazas**
• Falta de utilización de estándares y buenas prácticas. • Falta de políticas, procedimientos y evaluación en procesos. • Falta de personal técnico específico. • Falta de espacio físico independiente.	• Limitación en la disponibilidad de recursos tecnológicos. • Procedimientos administrativos de carácter burocrático en los procesos de compras. • Pérdidas de información y tiempo.

3.3. Procesos propios de la DGLH

A fin de alinearse con los objetivos estratégicos de la Universidad Nacional del Nordeste, la DGLH innova de forma permanente en el uso y aplicación de herramientas TI, planifica y pone en práctica proyectos que le permiten mantenerse actualizada.

Entre los procesos que lleva de forma operativa se encuentran principalmente la liquidación de sueldos, acreditaciones bancarias, certificaciones para préstamos, generación de RHUN, generación de SICOSS y SICORE de AFIP e informes gerenciales

a las autoridades superiores. Estos se llevan a cabo con el análisis de herramientas TI, el desarrollo de aplicaciones propias y el mantenimiento preventivo de sus equipos informáticos.

3.4. Sistemas de información TI

La DGLH gestiona un importante número de sistemas de información, con los cuales administra y gestiona los datos necesarios para la liquidación de los sueldos de los agentes universitarios. Entre ellos principalmente se halla SIU Mapuche como software principal y algunos otros sistemas con desarrollo propio además de las herramientas ofimáticas típicas para el área administrativa.

3.5. Centro de datos de la DGLH

El área TI de la DGLH dispone de una sala exclusiva para al alojamiento de los servidores que almacenan los datos y realizan los procesos de la Dirección, la sala cuenta con 2 racks en torre donde se alojan los equipos destinados a producción y al almacenamiento de archivos. Esta sala se encuentra debidamente climatizada para evitar sobrecalentamiento de los dispositivos.

La conectividad del centro de datos es provista internamente desde un equipo de comunicaciones que interconecta con los equipos del área TI de Rectorado, el cual enlaza con los diferentes campus y da acceso a las diferentes unidades académicas e institutos el cual además provee salida hacia internet. Teniendo en cuenta que la DGLH ofrece servicios de consulta de recibos digitales para sus empleados y la necesidad de estar disponibles las 24 horas los 365 días del año, para lo cual se procedió a solicitar un servicio externo para la provisión alternativa de internet para el área.

En la siguiente Fig. 4, se puede observar el esquema del centro de datos que posee la DGLH, sus equipos servidores y las conexiones internas y externas.

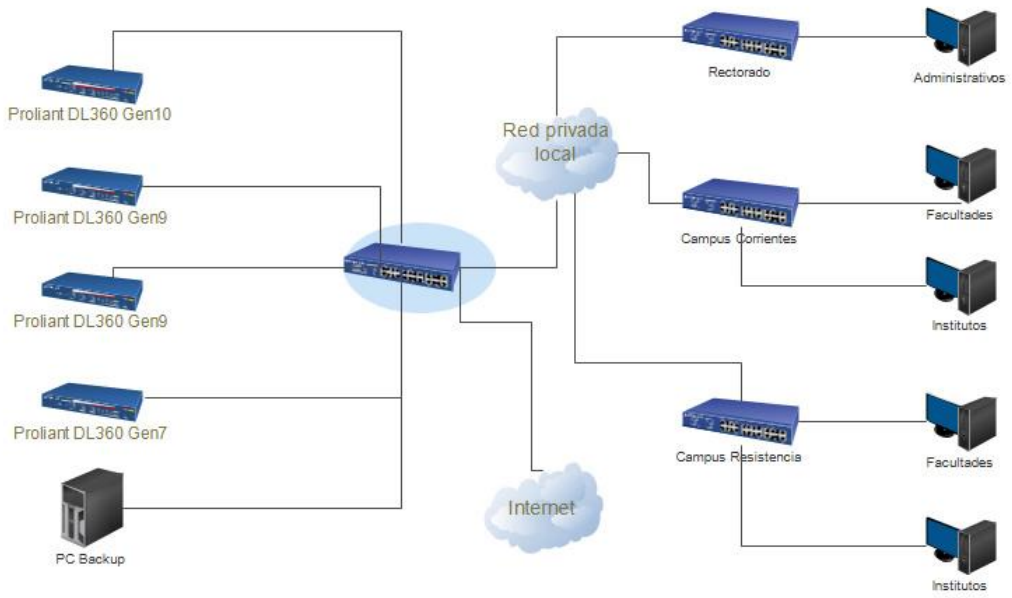

Fig. 4. Esquema de servidores de la DLGH.
Fuente: Elaboración propia

3.6. Relevamiento

La información del área se obtuvo a través de la recopilación de la información tomando en cuenta las siguientes acciones puntuales.

- Examen de documentación que contenga información relacionada con los controles de seguridad, procesos de gestión de seguridad, procedimientos, informes de seguridad y otra información relacionada.
- Entrevistas personales con responsables de la seguridad de la información y con los agentes que llevan a cabo las tareas y operaciones relacionadas con la seguridad informática.
- Encuestas realizadas a través de cuestionarios.
- Revisión de resultados de auditorías internas previas.
- Observación de controles y la seguridad de manera directa en el área.

3.7 Discusiones y Comentarios

Descriptas las características de la historia de la universidad desde su creación, estructura organizativa de las áreas que la componen; detalladas las características

específicas de la DGLH, haciendo foco en su área de tecnología de la información, el desarrollo del presente TFM representa un valioso aporte a la universidad pública en cuanto al cumplimiento de sus objetivos estratégicos y en la elevación de su excelencia a nivel nacional e internacional mediante la implementación de un sistema de seguridad basado en estándares internacionales.

Capítulo 4
SGSI (desarrollo de la propuesta)

En el capítulo 4, se describe el diseño del Sistema para la Gestión de la Seguridad de la Información propuesta. Donde se detallan la metodología y políticas de seguridad que conformarán el modelo de seguridad acorde a las necesidades del área.

4.1 Metodología

A fin de lograr los objetivos propuestos y contar con información que permita servir como documentación de los procesos a seguir, se incluirán las actividades propuestas por la norma ISO/IEC 27001:2013, presentes en la Fig. 5, las cuales están relacionadas a las etapas de diseño o planificación del SGSI:

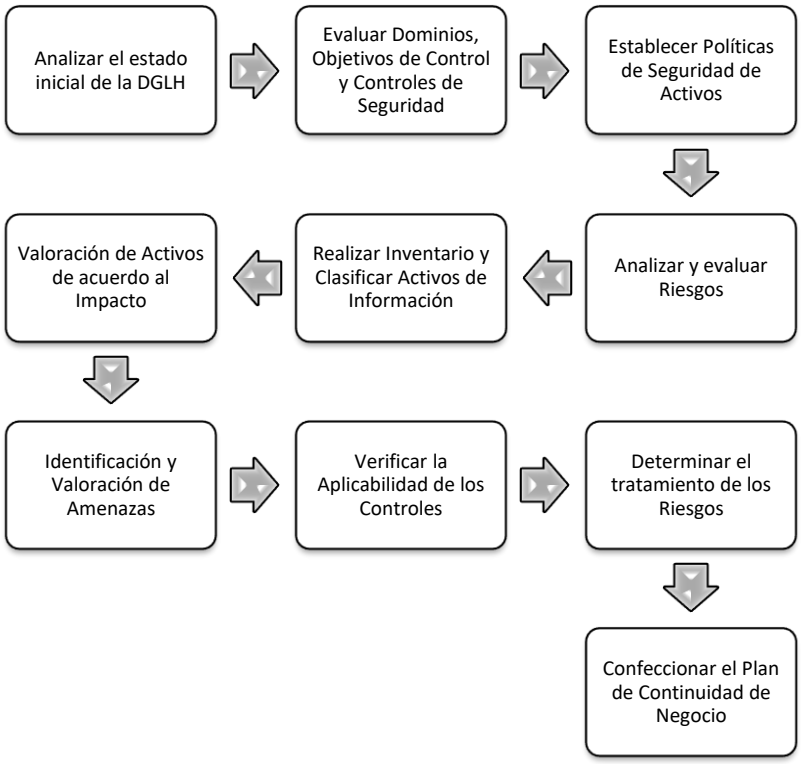

Fig. 5. Metodología del SGSI para la DGLH
Fuente: Elaboración propia.

4.1.1 Análisis del estado inicial de la DGLH

Conforme lo establece la norma ISO 27001:2013 se requieren de ciertos puntos necesarios para establecer, implementar, mantener y realizar una mejora continua el SGSI de la Información en el ámbito de una organización.

Realizar un análisis de brechas (análisis GAP) a los efectos de comprobar el estado actual del cumplimiento de la norma ISO 27001:2013 del área TI de la DGLH de la UNNE, mediante un Análisis Diferencial de los requisitos obligatorios del 4 al 10 de la norma ISO 27001 y del Anexo A (Dominios, Objetivos de Control y Controles de Seguridad).

Este análisis inicial de las condiciones actuales permitirá hallar los problemas y deficiencias en seguridad existentes en el área mediante la determinación del nivel de cumplimiento de la norma ISO 27001 y de esta forma desarrollar un plan de mejoras conforme a los objetivos de seguridad propuestos inicialmente. Asimismo, se podrá observar el nivel de madurez del área TI de la DGLH.

El análisis GAP comprende 4 etapas, las que están relacionadas en la Fig. 6 :

Etapa 1: Elaboración de formularios, conformado por las siguientes actividades:

1. Revisión de la norma ISO/IEC 27001:2013.

2. Elaboración de preguntas por puntos y dominios.

3. Definición de niveles y criterios de madurez a aplicar.

Etapa 2: Entrevistas técnicas en la DGLH con el fin de:

1. Conocer la estructura organizativa.

2. Revisar los perfiles e identificación de los procesos.

3. Entrevistar a la Dirección y personal técnico

Etapa 3: Determinación de resultados, mediante la ejecución de las siguientes actividades:

1. Determinación del nivel de madurez de los puntos exigidos en la norma.

2. Clasificación del nivel de madurez de los dominios

3. Análisis de las calificaciones propuestas.

Etapa 4: Análisis de los resultados, mediante la realización de las siguientes tareas:

1. Cálculo del promedio por puntos de la norma.

2. Cálculo del promedio por dominios de la norma.

3. Elaboración de gráficos de madurez y brecha.

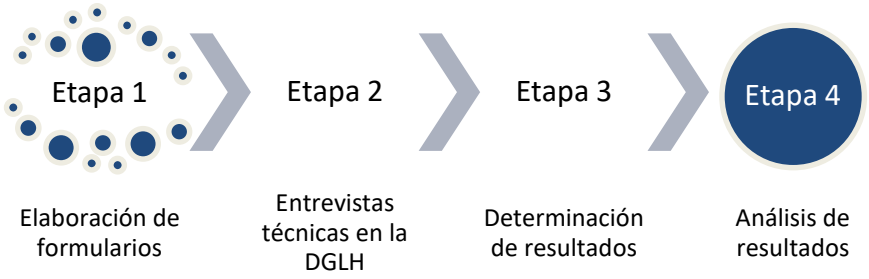

Fig. 6 Etapas del Análisis Gap de la DGLH
Fuente: Elaboración propia.

Etapa 1: Elaboración de formularios, conformado por las siguientes actividades:

1. Revisión de la norma ISO/IEC 27001:2013: se debe analizar los siguientes puntos.

a) **Contexto de la Organización:** tiene como objetivo conocer y entender la organización en su contexto y reconocer y comprender las necesidades y expectativas de todas las partes interesadas en el ámbito de la seguridad de la información. Ver formulario modelo en Anexo 3.
b) **Liderazgo:** aquí se hace referencia a la alta gerencia, que en el caso de estudio del presente trabajo corresponde a las autoridades superiores de la UNNE, en este punto se enfatiza que las cuestiones de seguridad de la información deben ser incumbencia de las autoridades superiores y no solamente de los directores de las áreas. En este apartado se debe explicitar el compromiso gerencial y los roles, responsabilidades y autoridades de la organización. Ver formulario modelo en Anexo 3.

c) **Planificación**: aquí se describe todo lo relacionado con la gestión del riesgo, arrancando desde el entendimiento de la estrategia a aplicar, enlazando la seguridad de la información con los objetivos estratégicos de la organización. En este apartado se tratarán temas relacionados con el análisis FODA, la valoración y tratamiento de los riesgos y la continuidad del negocio. Para ello se utiliza el formulario Anexo 3.

d) **Soporte:** tiene como objetivo el análisis de los recursos, la competencia del personal, la concientización y comunicación. En este caso se utiliza el formulario del Anexo 3.

e) **Operación:** en este apartado se releva todo lo relacionado a la planificación y control de las operaciones, como también la continuidad del negocio. Se utiliza el formulario del Anexo 3.

f) **Evaluación del desempeño:** en este punto se debe poder identificar, describir y documentar la eficiencia de los controles implementados. Para ello se utilizan indicadores y métricas para su medición. Ver formulario en Anexo 3.

g) **Mejora:** aquí se trata la valuación y tratamiento del riesgo, indicando acciones correctivas o planes de acción. Para ello se utiliza el formulario del Anexo 3.

Para la evaluación de los diferentes puntos que propone la norma ISO/IEC 27001:2013 se utiliza la siguiente Tabla 5 de criterios de evaluación de requisitos que contiene los siguientes valores:

Tabla 5. Criterios para evaluar los requisitos de la norma ISO/IEC 27001:2013
Fuente: Elaboración propia

Estado	Valor	Descripción
No diseñado	1	Las tareas o actividades no fueron diseñadas para cumplir con los requisitos de la norma ISO/IEC 27001:2013.
Parcialmente diseñado	2	Las actividades están diseñadas pero no conformes a los requisitos necesarios de la norma ISO/IEC 27001:2013
Diseñado	3	Las actividades están conformes a los requisitos de la norma ISO/IEC 27001:2013 pero no se verifican en su aplicación de forma efectiva.

Parcialmente implementado	4	Las actividades están conformes a los requisitos de la norma ISO/IEC 27001:2013 se verifican parcialmente su aplicación.
Totalmente implementado	5	Las actividades están conformes a los requisitos de la norma ISO/IEC 27001:2013 y se observa su aplicación continua.

4.1.2 Dominios, Objetivos de Control y Controles de Seguridad.

Con el objetivo de determinar el nivel de cumplimiento de los Dominios de Control, Objetivos de Control y Controles de Seguridad conformes al Anexo A de la norma ISO 27001:2013, se procede a realizar un análisis de brechas de seguridad del área TI de la DGLH. Los puntos a analizar corresponden a los puntos del 5 al 18 de dicho anexo.

A tal fin se define la siguiente escala para evaluar los controles hallados:

Tabla 6. *Criterios para evaluar los controles de la norma ISO/IEC 27001:2013*
Fuente: Elaboración propia.

Estado	Valor	Descripción
Sin controles	0	No existen controles de seguridad en los sistemas de información.
Controles iniciales	1	Existen controles iniciales pero no poseen gestión.
Controles repetibles	2	Existen controles de manera informal, con procedimientos manuales. No existen protocolos.
Controles definidos	3	Los controles se hallan documentados y definidos pero no informados por la Dirección.
Controles gestionados	4	Los controles se llevan en base a procedimientos aprobados y formalizados por la Dirección.
Controles optimizados	5	Los controles se aplican en base a procedimientos documentados y aprobados por la Dirección. Se utilizan indicadores para medir su eficacia de forma periódica.

4.1.3 Políticas de seguridad de los activos de información

En este punto se establecen las políticas de seguridad de la información propuestas para el presente SGSI a fin de ser aplicadas al área TI de la DGLH.

a) Políticas de Seguridad General

Los empleados de la DGLH, técnicos, administrativos y funcionarios deben mantener el compromiso de preservar el nivel de confidencialidad de la información que allí se maneja. En todo momento se debe prohibir la reproducción o difusión total o parcial de la documentación clasificada como privada. La información que deba ser hecha pública o deba ser utilizada en otros ámbitos, debe poseer la correspondiente autorización o consentimiento expreso de la organización. Los dispositivos y medios que integren los activos informáticos deben ser preservados con el mayor cuidado posible, teniendo en cuenta su deterioro natural o algún hecho vandálico que acelere su destrucción.

b) Políticas de la seguridad de la información en general

Se deben diseñar las políticas y lineamientos de seguridad de la información necesarios para mantener y preservar los datos de los agentes universitarios y de aquellos relacionados con la información de sueldos y valores, conservándolos en un ambiente seguro.
El diseño de las mismas, tendrán como fin conservar los principios de la Seguridad de la información, Confidencialidad, Integridad y Disponibilidad. Asimismo, se deberá enfocar en los planes de continuidad del negocio y la recuperación de desastres ante posibles contingencias.

c) Políticas de los servicios a los empleados universitarios

Para la utilización de los servicios de la DGLH, se debe solicitar identificación de los agentes, con sus respectivas credenciales, niveles de acceso y permisos a cada uno de los módulos o aplicaciones que estén disponibles. Todos los usuarios deben estar identificados y contar con la respectiva autorización por una autoridad competente, por ejemplo: Decano o Secretario de cada facultad.

d) Políticas para el desarrollo de software propio

Todo el software o aplicaciones que necesite el área, deberá ser preferentemente desarrollado dentro de la institución o bien realizado de forma externa pero acompañado con el personal técnico capacitado de la DGLH, el que deberá cumplir indefectiblemente con los requerimientos institucionales de seguridad. El mismo utilizará datos anonimizados y previos a la puesta en producción, deberá correr de forma paralela durante un periodo de evaluación de los mismos.

Para el desarrollo de software de aplicación por grupos o proyectos de investigación institucionales, se deberán verificar 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.

En el caso de software de aplicación o sitios en los que se procese información con datos sensibles y requieran de credenciales de acceso, éste implementará para los usuarios, el uso de conexiones seguras.

e) Políticas para la gestión de riesgos

Se deberán aplicar mecanismos de gestión de riesgos de forma periódica para el mantenimiento preventivo y normal funcionamiento de los procesos que habitualmente se utilizan en la DGLH. De forma anual se deberá analizar nuevas metodologías para la gestión y análisis de los riesgos en el área.

f) Políticas para la protección de datos

Se deberá utilizar un sistema de acceso basado a los diferentes aplicativos que utilice la DGLH en los cuales se utilice información sensible. Los mismos dispondrán de un acceso determinado por perfiles de usuario, roles y perfiles respectivamente.

g) Políticas de auditoria interna

A fin de contar con una calidad comprobable en los procesos que lleva a cabo la DGLH, se deben programar auditorías internas en el área TI y en los procesos críticos que habitualmente lleva a cabo la Dirección.

h) Políticas de calidad de datos

Desde la Dirección de la DGLH se realizará un compromiso de utilización de controles y determinación de métricas que permitan realizar un seguimiento de los procesos críticos que allí se realizan. Se realizarán evaluaciones periódicas a fin de evaluar la calidad y efectividad de los procesos intervinientes. En los mismos se cumplirán los requerimientos determinados en normas internacionales y/o en las políticas propias de la Universidad.

i) Políticas de dispositivos personales

Todo equipo de uso personal que sea ingresado al área de la DGLH deberá contar con autorización para la utilización de los mismos. Éstos estarán incluidos en los mismos lineamientos institucionales de los equipos de la Dirección a fin de evitar riesgos de infección o propagación de virus. Además, los equipos de uso personal deberán contar con alguno tipo de autenticación aprobados por el área TI de la DGLH.

j) Políticas de dispositivos y medios extraíbles

El uso o instalación de dispositivos deberá ser habilitado solamente en máquinas específicas, las que contará con un sistema de detección de virus actualizado de manera periódica y automática. Se llevará un control de las máquinas que presten este servicio a fin de prestar atención a las alertas que emita.

k) Políticas de alta de usuarios

Los usuarios que deban hacer uso de los sistemas provistos o alojados en el área TI de la DGLH deberán solicitar previamente la autorización por autoridad superior. Para el mismo se utilizará un sistema de perfiles y roles. La autorización del personal nuevo será

con identificación única e intransferible. Se determinarán periodos mínimos necesarios para la creación del alta a los sistemas o bien utilización de módulos de entrenamiento o capacitación del personal nuevo.

l) Políticas de instalación de hardware y/o software

El personal técnico capacitado de la DGLH será el único habilitado para la instalación de hardware o software en los equipos de la institución. Por cada equipo informático se realizará un registro en el inventario de la Dirección, el cual proveerá de la información necesaria de los componentes instalados o existentes en los mismos. De manera periódica se realizarán comprobaciones y pruebas de rutina sobre los equipos. Ante el caso de detección de hardware o software no registrado, se procederá a la notificación y emisión de una alerta.

m) Políticas de comunicación institucional

Toda comunicación institucional o que deba ser realizada, será brindada por los canales oficiales, siempre desde correos institucionales y no de correos personales o de personal no considerado oficial. Toda la documentación que se adjunte a los correos electrónicos y pueda ser descargada, será automáticamente verificada con los antivirus convenientemente instalados.

n) Políticas de responsabilidad del personal

La totalidad del personal de la DGLH: administrativos, técnicos y directivos serán responsables del uso adecuado y de la seguridad de los activos de información que se encuentren en su disposición directa, además se comprometerán a cumplir los lineamientos definidos por la organización y de acuerdo a su reglamentación vigente.

Ante el incumplimiento de estas políticas de responsabilidad, el personal será factible de recibir sanciones de acuerdo a la gravedad del caso.

o) Políticas ante incidentes de seguridad

Todo personal que detecte una vulnerabilidad o una violación ante los procedimientos relacionados a las Políticas de Seguridad de la DGLH deberá comunicar de forma inmediata ante el responsable de los activos de información del área TI. El informe se realizará a través de un documento formal donde se registre los datos del incidente, las posibles causas del mismo y la fecha y hora en el que sucedió o se detectó el incidente.

4.1.4 Análisis y Evaluación de Riesgos

En este punto se define la metodología a aplicar para el análisis y evaluación de riesgos que afectan al área TI de la DGLH de la UNNE, tomando como referencia la normativa ISO/IEC 27001 y la metodología de gestión de riesgos MAGERIT, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información elaborado por CSAE (Consejo Superior de Administración Electrónica), el uso de la misma supone beneficios al utilizar las tecnologías de la información gestionando los riesgos inherentes a la misma.

A continuación, se describe en detalle los pasos a seguir:

a) Análisis y evaluación de los riesgos IT en la DGLH

Tiene como objetivo la determinación de los riesgos que afectan a los activos de TI que forman parte de los procesos y servicios en la oficina de la DGLH siguiendo los pasos que establece Magerit. Los mismos se obtendrán a través de entrevistas, encuestas y observación directa realizados en colaboración con el personal de la dirección.

b) Caracterización de los activos

Tiene como objetivo identificar los activos que forman parte de los servicios y procesos de la DGLH además de la relación y dependencia entre ellos. A tal fin se debe realizar la valoración según su importancia siguiendo el esquema que se detalla la caracterización de los activos de los activos según Fig. 7 .

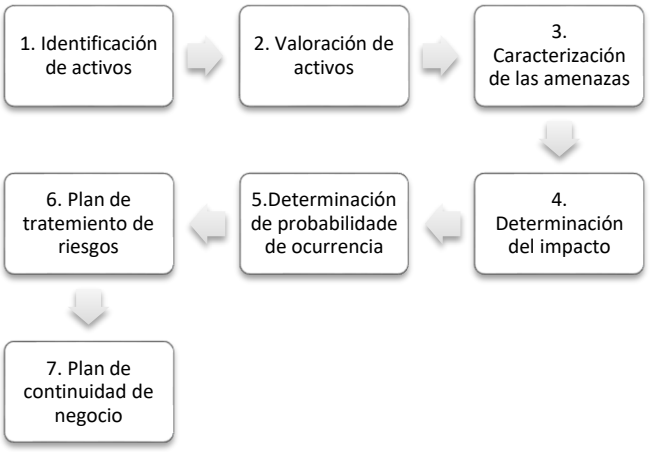

Fig. 7 Caracterización de los activos de la DGLH
Fuente: Elaboración Propia

1. Identificación de los activos (Inventario de activos)

El objetivo en este paso fue identificar a los activos que forman parte de los servicios y procesos de la DGLH de la Universidad Nacional del Nordeste, determinando los atributos y características de cada activo, el código de identificación, el nombre del mismo y una breve descripción.

Los activos son los componentes o funcionalidad de un sistema de información susceptible a ser atacados deliberada o intencionalmente. Asimismo son los elementos que la organización posee para el tratamiento de la información.

Consideraciones:

- Los códigos utilizados para identificar los grupos de activos están tomados como base el catálogo que Magerit ofrece.

Actividad:

Identificar los activos que intervienen en la oficina de la DGLH de la Universidad Nacional del Nordeste a fin de poder realizar el correspondiente análisis y gestión de riesgos.

Recolección de los datos

Los datos y la información utilizada en el presente trabajo fueron obtenidos mediante entrevistas con la Directora General de Liquidación de Haberes y el responsable técnico

del Área de Sistemas de la DGLH, los mismos fueron registrados a través de la utilización de formularios conforme a la norma ISO/IEC 27001:2013, los mismos se encuentran disponibles en la sección de anexos con los nombres: Anexo 3: Formulario para el autodiagnóstico del área de TI de la DGLH (ISO 27001), Anexo 4: Formulario de responsables entrevistados en el autodiagnóstico del área de TI de la DGLH (ISO 27001), Anexo 5: Formulario de estado actual de madurez del área de TI de la DGLH. Requisitos de la Norma (ISO 27001).

Tabla 7. Clasificación de activos según Magerit.
Fuente: Magerit - V 3.0 – Libro 1: Método.

Nomenclatura	Tipo de Activo	Definición
[E]	Esencial	Activo necesario para la continuidad del área. Requerido.
[A]	Archivos	Todo tipo de registros de almacenamiento o consultas en forma digital o físico.
[D]	Datos	Información útil, relevante del área.
[K]	Claves criptográficas	Claves para el tratamiento de la información de manera sensible.
[S]	Servicios	Son los servicios que forman parte del área TI de la oficina.
[SW]	Software / Aplicaciones	Los aplicativos que forman parte del área TI de la oficina.
[HW]	Hardware	Los medios físicos, destinados a soportar directamente o indirectamente los servicios.
[COM]	Redes de comunicaciones	Los dispositivos físicos que permiten realizar algún tipo de comunicación entre otros.
[MED]	Media	Son aquellos dispositivos que permiten almacenar información de forma permanente o durante prolongados periodos de tiempo.
[AUX]	Equipamiento auxiliar	Recursos auxiliares no necesariamente indispensables pero útiles.
[L]	Instalaciones	Son las oficinas donde se realizan las tareas diarias de la DGLH y el centro de datos donde

		se alojan los equipos que brinda servicios al área.
[P]	Personal	Todo el personal gerencial, técnico y administrativo que realiza tareas en la DGLH.

1. Valoración de activos

Tiene como objetivo identificar las dimensiones y el valor del activo de TI perteneciente a la DGLH

Consideraciones:

Se realizó entrevista a la Directora General de Liquidaciones y el Técnico del Área de Sistemas a fin de obtener los datos a valorar.

Los activos se valoraron en las 5 dimensiones que plantea Magerit.

Los criterios de valoración fueron los sugeridos por Magerit pero no se utilizaron todos.

Se consideraron datos importantes como dimensiones y criterios de valuación.

a. Dimensiones

Tabla 8. Definición de dimensiones sugeridas por Magerit.
Fuente: Magerit - V 3.0 – Libro 1: Método.

Nomenclatura	Dimensión	Definición
[D]	Disponibilidad	Propiedad de los activos consistente en que las entidades o procesos autorizados poseen acceso a los mismos cuando lo requieran.
[I]	Integridad	Propiedad consistente de los activos en los que no han sido alterados de manera no autorizada.
[C]	Confidencialidad	Propiedad consistente en que los activos de información no se disponen, ni revela a entidades o procesos no autorizados.
[A]	Autenticidad	Propiedad o característica en la que la una entidad es quien dice ser o garantiza la fuente desde donde proceden los datos.
[T]	Trazabilidad	Propiedad consistente donde las actualizaciones de una entidad pueden ser imputadas a la misma.

b. Criterios de valoración

En el catálogo de Magerit se presentan diferentes criterios para la valoración de los activos. Para este proyecto sólo se tomaron los que se adecuan a los procesos y servicios con los que cuenta la DGLH. Por lo tanto se excluyeron los criterios de Obligaciones Legales, Intereses Comerciales o económicos, Orden Público, Pérdida de Confianza, Tiempo de Recuperación del Servicio e Información Clasificada.

Por ejemplo, Magerit también considera la valoración cuantitativa, aquella que permite calcular el valor de un activo en base al impacto que pueda tener en la organización, es decir el costo o valor monetario. Por su parte, este también puede ser de orden cualitativa, estableciendo órdenes de magnitud (Ej. MA [Muy Alto], A [Alto], M [Medio], B [Bajo] y MB [Muy Bajo]).

Escala de valores

Los criterios utilizados para valorar los activos van en una escala del 0 al 10.

Tabla 9. Escala de valores de Activos
Fuente: Magerit - V 3.0 – Libro 1: Método

Escala de valores		
Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor

Actividad:

En colaboración con la Dirección de la DGLH y el técnico del Área de Sistemas se valoraron los activos identificados de acuerdo a las dimensiones que plantea Magerit.

2. Caracterización de las amenazas

El objetivo fue identificar las amenazas posibles que pueden presentarse sobre los activos determinados en la DGLH y estimar la frecuencia de ocurrencia y la degradación que causa en los mismos.

b. Identificación de las amenazas

El objetivo fue determinar e identificar las amenazas relevantes sobre cada activo de la DGLH.

Consideraciones:

- Se utilizaron las amenazas que brinda Magerit en el libro II Catálogo de amenazas.
- Se utilizaron los activos que previamente fueron identificados en el área TI de la DGLH

Magerit en su metodología agrupa las amenazas en los siguientes grupos:

[N] Desastres Naturales

[I] De origen Industrial

[E] Errores y fallos no intencionados

[A] Ataque intencionados

Actividad:

Mediante entrevista con el responsable de sistemas del área se utilizó la lista de amenazas para determinar cuáles podrían afectar a los correspondientes activos de la DGLH.

c. Valoración de las amenazas

El objetivo fue determinar el grado de afectación sobre los activos en el caso que la misma fuera materializada.

Consideraciones:

-Se utilizó la tabla de degradación de activos que plantea Magerit, la misma se puede consultar en la siguiente tabla:

Tabla 10. Escala de degradación de Activos
Fuente: Magerit - V 3.0 – Libro 1: Método

Degradación de activos	
Porcentaje	Nivel

90- 100%	Muy Alto
60-80%	Alto
30-50%	Medio
10-20%	Bajo
1-5%	Muy Bajo

Actividad:

Se procedió al cálculo de la degradación de cada activo tomando en cuenta los valores de la tabla de valoración de activos y teniendo en cuenta que para algunas amenazas la afectación puede darse en 3 dimensiones.

Tabla 11. Escala de degradación de Activos
Fuente: Elaboración propia en base a Magerit - V 3.0 – Libro 1: Método

Escala cualitativa de la degradación de activos	
Rojo	Mayor desgaste
Amarillo	Medio desgaste
Verde	Bajo desgaste

Para hallar el nivel de la amenaza de cada activo se procedió a la utilización de una escala cuantitativa de degradación, la cual fue definida por la DGLH, tomando como base un rango de 0,01 a 1.

Tabla 12. Escala de rangos de degradación de Activos
Fuente: Elaboración propia en base a Magerit - V 3.0 – Libro 1: Método

Escala cualitativa de la degradación de activos definida por la DGLH	
Nivel	**Rango**
Muy alto	0,81 a 1,00
Alto	0,51 a 0,80
Medio	0,21 a 0,50
Bajo	0,06 a 0,20
Muy bajo	0,01 a 0,05

3. Determinación del impacto

Se procedió a determinar el impacto que las amenazas identificadas podrían causar sobre cada uno de los activos en caso que estas se materializaran.

Consideraciones:

- Se obtuvieron los valores de cada uno de los activos de la de oficina de la DGLH.
- Se obtuvo el valor del nivel de desgaste de cada activo en relación a las amenazas a las cuales se encuentra expuesto.

Actividad:

Para hallar el impacto se procedió a multiplicar el valor que presenta cada activo y el desgaste del mismo.

Se definió una tabla de escalas de valores cuantitativos del impacto de acuerdo a la entidad DGLH.

Se determinó la probabilidad de impacto en colaboración con la dirección de la DGLH y el área de Sistemas, utilizando la escala cualitativa.

Tabla 13. Escala cualitativa de impacto
Fuente: Elaboración propia en base a Magerit - V 3.0 – Libro 1: Método

Escala cualitativa de impacto definida por la DGLH		
Nivel	**Escala cualitativa**	**Rango**
5	Muy alto	7,01 a 10
4	Alto	3,01 a 7
3	Medio	2,01 a 3
2	Bajo	0,06 a 2
1	Muy bajo	0,01 a 0,05

4. Determinación de la probabilidad de ocurrencia

El objetivo fue determinar la probabilidad que se materialice la amenaza.

Consideraciones

- Se tomó como referencia la tabla que plantea Magerit para determinar la probabilidad de ocurrencia de la amenaza y se tomó como base un periodo de 2 años.

Tabla 14. Escala de probabilidad de ocurrencias
Fuente: Elaboración propia en base a Magerit - V 3.0 – Libro 1: Método

Escala de probabilidad de ocurrencia		
Nivel	**Escala cualitativa**	**Descripción**
5	Muy frecuente	Se estima la amenaza ocurra más de 3 veces al año
4	Frecuente	Se estima la amenaza ocurra al menos 2 veces al año
3	Normal	Se estima la amenaza ocurra al menos 1 vez al año
2	Poco frecuente	Se estima la amenaza ocurra al menos 1 vez en los 2 últimos años
1	Muy poco frecuente	Se estima no se haya presentado la amenaza en los últimos 2 años

Mapa de riesgo

El objetivo fue obtener el correspondiente mapa de riesgo para determinar el estado de los riesgos hallados.

Consideraciones: Se tomó como referencia la escala de riesgos planteada por Magerit.

Tabla 15. Escala cualitativa de riesgos
Fuente: Elaboración propia en base a Magerit - V 3.0 – Libro 1: Método

Escala cualitativa riesgos		
Nivel	**Escala cualitativa**	**Leyenda**
5	Inaceptable (Muy Alto)	MA
4	Importante (Alto)	A
3	Moderado (Medio)	M
2	Tolerable (Bajo)	B

1	Aceptable (Muy Bajo)	MB

Actividad

- Se determinaron los niveles de riesgos con la colaboración de la dirección de la DGLH y el personal técnico del Área de Sistemas.

Tabla 16. Mapa de riesgos.
Fuente: Elaboración propia en base a Magerit – V.3-0 – Libro 1: Método

Matriz de Probabilidad e Impacto		Impacto				
		Muy Bajo 1	Bajo 2	Moderado 3	Alto 4	Muy Alto 5
Probabilidad	Muy Baja 1	Aceptable (Muy Bajo)	Aceptable (Muy Bajo)	Tolerable (Bajo)	Moderado (Medio)	Moderado (Medio)
	Baja 2	Aceptable (Muy Bajo)	Aceptable (Muy Bajo)	Tolerable (Bajo)	Moderado (Medio)	Importante (Alto)
	Moderada 3	Aceptable (Muy Bajo)	Tolerable (Bajo)	Moderado (Medio)	Importante (Alto)	Importante (Alto)
	Alta 4	Tolerable (Bajo)	Moderado (Medio)	Moderado (Medio)	Importante (Alto)	Inaceptable (Muy Alto)
	Muy Alta 5	Moderado (Medio)	Moderado (Medio)	Importante (Alto)	Inaceptable (Muy Alto)	Inaceptable (Muy Alto)

Controles de Seguridad o Salvaguardas

Aquellos procedimientos o mecanismos de control que reducen el riesgo en los activos de información se denominan controles de seguridad o Salvaguardas, en los mismos se deben establecer los controles a aplicar por cada activo de la organización.

Los controles de seguridad propuestos en Magerit se clasifican en:

Tabla 17. Controles de seguridad.
Fuente: Elaboración propia en base a Magerit - V 3.0 – Libro 1: Método

Nomenclatura	Control de Seguridad o Salvaguarda
H	Protecciones generales u horizontales

D	Protección de datos / información
K	Protección de claves criptográficas
S	Protección de servicios
SW	Protección de aplicaciones / Software
H	Protección de equipos informáticos / Hardware
COM	Protección de comunicaciones
IP	Protección en los puntos de interconexión
MP	Protección en soportes de información
AUX	Protección de elementos auxiliares
L	Seguridad física / instalaciones
PS	Salvaguardas relacionadas al personal
G	Salvaguardas de tipo organizativo
BC	Continuidad en las operaciones
E	Externalización
NEW	Adquisición y desarrollo

4.1.5 Inventario y clasificación de activos de información

Todos los objetos físicos, objetos abstractos, personal e instalaciones físicas de la organización conforman los activos o recursos informáticos de la misma. Estos incluirán todo el hardware, los sistemas y aplicaciones, el personal administrativo, técnico y gerencial, y las oficinas que lo integran, la relación entre ellos está presente en la Fig. 8

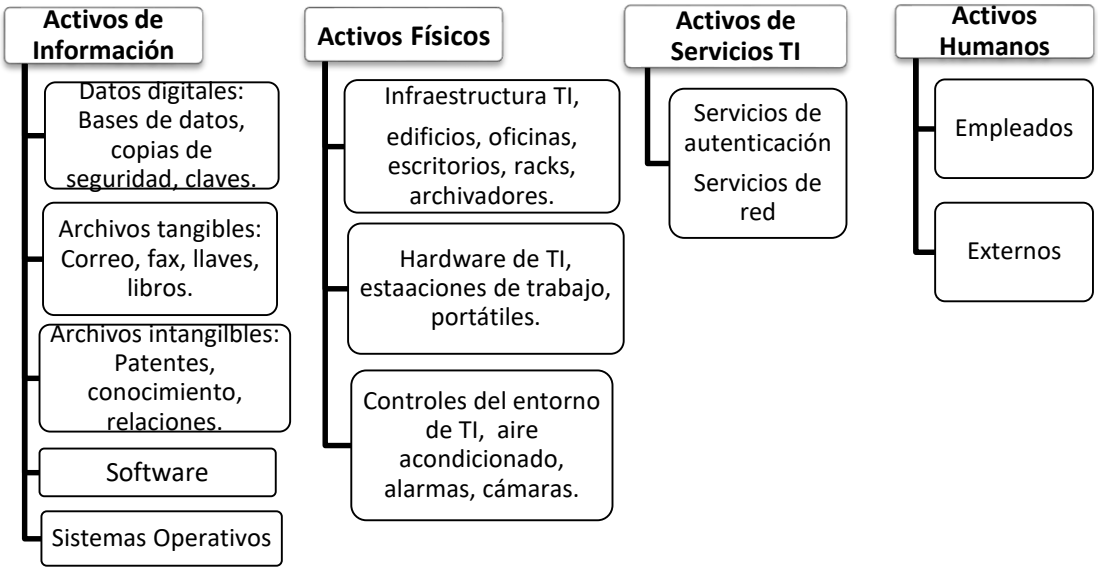

Fig. 8. Clasificación de activos
Fuente: http://www.isootools.org/2013/12/05/en-inventario-de-activos-en-la-implementacion-de-la-norma-iso-27001/

4.1.6 Valoración de activos de acuerdo al impacto

De acuerdo al tipo cualitativo que establece Magerit, se determina la valoración de los activos de información del área TI de la DGLH de la UNNE, asimismo se establece el impacto que tienen los mismos de acuerdo a la presente escala:

Tabla 18. *Valoración cualitativa de los activos de información según Magerit.*
Fuente: Elaboración propia en base a Magerit - V 3.0 – Libro 1: Método

Nomenclatura	Impacto	Valor	Descripción
MA	INACEPTABLE (MUY ALTO)	10	Daño con consecuencias muy graves para la organización. Daños irreversibles.
A	IMPORTANTE (ALTO)	7-9	Daños graves muy perjudiciales para la organización
M	MODERADO	4-6	Daño con consecuencias relevantes para la organización y su operatividad.
B	TOLERABLE (BAJO)	1-3	Daños con consecuencias relevantes pero que no afectan de manera importante a la organización.

MB	ACEPTABLE (MUY BAJO)	0	Daño sin consecuencias para la organización.

4.1.7 Identificación y valoración de amenazas

Conforme a las amenazas que se identifican en Magerit, las mismas se establecen para cada activo de información, determinando la probabilidad o frecuencia de ocurrencia de la misma y el impacto que tienen en cada dimensión de seguridad.

Riesgo potencial: se determina el nivel de riesgo potencial de los activos de información del área TI de la DGLH con una valoración cualitativa conforme a las zonas de riesgo tomando como referencia la propuesta de Magerit. Para el cálculo del riesgo potencial, se tomará cada activo y conforme el tipo de amenaza general (naturales, industriales, errores, ataques intencionados). Para el mismo se evalúa todo tipo de amenaza y se considera el peor de los escenarios.

4.1.8 Declaración de aplicabilidad de los controles

En punto se definen los controles apropiados y la forma para implementarlos en el área TI de la oficina de la DGLH de la UNNE, en el mismo se incluyen los controles listados en el Anexo A de la norma ISO/IEC 27001:2013. Ver Anexo 14. Formulario de aplicabilidad de controles del Anexo A de la Norma ISO/IEC 27001:2013.

4.1.9 Tratamiento de riesgos (salvaguardas)

El objetivo es inicialmente determinar las salvaguardas propuestos por Magerit que sean adecuados para enfrentar cada una de las amenazas a la seguridad de los activos de la DGLH y de forma consecuente mitigar los riesgos que afecten el área TI de la DGLH de la UNNE y de forma secundaria definir el correspondiente tratamiento para cada uno de ellos.

Se determina, además, cuáles serán los controles de seguridad del Anexo A del estándar ISO/IEC 27001:2013 aplicables al SGSI diseñado.

Para el mismo se toman como referencia los siguientes documentos:

- Norma ISO/IEC 27001:2013 (cláusulas 8.2 y 8.3)
- Anexo A de la norma ISO/IEC 27001:2013.
- Norma ISO/IEC 27002:2013

Conforme a lo propuesto por Magerit, las opciones o tipos de tratamientos de los riesgos a considerar serán:

Tabla 19. *Tratamiento de riesgos conforme a Magerit.*
Fuente: Elaboración propia en base a Magerit - V 3.0 – Libro 1: Método

AS	Asumir el riesgo
DC	Definir los controles a aplicar
TT	Transferirlos a un tercero.

A los efectos de cumplir con los objetivos de seguridad inicialmente propuestos para el SGSI, se definen los controles de seguridad basados en la Metodología de Análisis y Evaluación de Riesgos propuesta por Magerit y los correspondientes controles propuestos en el Anexo A de la norma ISO/IEC 27001:2013.

4.1.10 Plan de Continuidad del negocio

El objetivo principal del Plan de Continuidad del Negocio propuesto es brindar al área TI de la DGLH de la UNNE las herramientas necesarias frente a incidentes que lleven a la interrupción de los principales servicios que ésta brinda. Eventos que podrían ser iniciados por causas naturales, accidentales o bien intencionales.

En todos los casos, la acción es reestablecer en el menor tiempo, los servicios críticos que el área brinda acompañados por diferentes medidas preventivas y de acompañamiento de otras áreas (directiva, administrativa, etc.)

El alcance del plan propuesto se encuentra centrado y limitado a la oficina donde funcionan las actividades del área TI de la DGLH de la UNNE.

Objetivos del plan:

- Brindar una guía básica para recuperación ante incidentes en el área TI de la DGLH.
- Determinar los servicios críticos del área.
- Ofrecer recursos de ayuda frente a los incidentes.
- Determinar los referentes a notificar ante los eventos.
- Proveer documentación y pruebas a realizar en modo simulacros.
- Identificar escenarios alternativos en recursos e infraestructura.
- Establecer procedimientos de recuperación de copias de seguridad críticas.

Supuestos:

- Se contará con la disponibilidad del personal adecuado ante el evento registrado.
- Se considerará usuario (externo o interno) del plan a los que posean el determinado rol de continuidad del negocio.
- Toda la información relacionada con el plan de continuidad estará alojado en un lugar externo a las oficinas de la DGLH o al menos fuera del área de desastre y accesible de forma inmediata para su aplicación
- El plan de continuidad y sus procedimientos de recuperación están diseñados para la DGLH, puntualmente para el área TI.

Definiciones:

- Desastre: se denomina así a la interrupción de los servicios que en este caso provee la oficina TI de la DGLH y que son considerados eventos catastróficos para la misma.
- Planificación de Continuidad de TI (IT Continuity Planning – IT CP): son las medidas que permiten asegurar la infraestructura, redes, información, bases de datos y recursos del área de TI a fin de proceder con la operación normal de sus servicios luego de un incidente de seguridad.

- Planificación de Recuperación de Desastres de TI (Disaster Recovery Planning – IT DRP): son los planes y estrategias utilizadas para la recuperación de los servicios y/o sistemas críticos del área TI ante eventos de seguridad.
- Gestión de Crisis: Son las actividades a desarrollar en la gestión de emergencias, principalmente corresponden a las cuestiones sanitarias y de seguridad.

Contenido del Plan de Continuidad

El plan se iniciará ante un evento que sea identificado y catalogado como desastre. El inicio del mismo se dará con la ejecución de los procedimientos habituales de administración y permanecerá activo hasta que los servicios y sistemas denominados críticos puedan darse en las condiciones denominadas normales o bien en los escenarios de reemplazo luego de evento.

En el documento del presente Plan de Continuidad del Negocio se establece la conformación del equipo encargado de la continuidad de las operaciones del área de TI de la DGLH mediante los denominados roles y responsabilidades de los mismos, además se incluyen los inicios de activación y desactivación del plan de continuidad y el correspondiente orden de ejecución de los procedimientos y actividades denominadas esenciales.

Roles y responsabilidades del plan

Los roles intervinientes en el presente Plan de Continuidad del Negocio son los siguientes:

Tabla 20. Roles intervinientes en el Plan de Continuidad de Negocio.
Fuente: Elaboración propia en base a Magerit - V 3.0 – Libro 1: Método

Rol	Responsabilidad
Administrador del Plan de Continuidad del Negocio (BCP Manager)	- Coordinar y establecer la coordinación con la alta dirección y los empleados que formen parte del Plan de Continuidad con el fin objetivo de definir los requerimientos y procesos de las actividades críticas y de gestión. - Desarrollar las políticas del Plan de Continuidad, estableciendo las estrategias necesarias para solventar los riesgos de los objetivos de seguridad.

	- Asegurar que los procesos y servicios críticos continúen funcionando luego de los eventos o desastres.
Administrador del Plan de Recuperación de Desastres (BCR Manager)	- Priorizar los procesos de la organización conforme a su evaluación. - Gestionar posteriormente al evento, los procesos y servicios críticos dentro de los tiempos definidos. - Definir los requerimientos de recuperación conforme a la relación entre los procesos de la organización.
Administrador de Evaluación Técnica	- Verificar los requerimientos técnicos y trabajar relacionados con otros responsables del Plan de Continuidad para la recuperación. - Analizar las capacidades de recuperación y riesgos del Plan de Continuidad en lo referente a la infraestructura y servicios de TI. - Promover el uso de nuevas tecnologías en la recuperación ante desastres de TI.

Lista de contactos esenciales

Ante las situaciones de emergencias, eventos catastróficos o en las situaciones de crisis, es necesario comunicarse rápidamente con las personas que participan en el Plan de Continuidad de Negocio, para ello es necesario contar con una forma rápida de contacto. Ver formulario de contactos en el Anexo 12.

Inicio y fin del Plan de Continuidad de Negocio

El inicio del Plan de Continuidad de Negocio estará dado por la interrupción o posibilidad de interrupción inminente de los servicios o sistemas críticos del área de TI de la DGLH de la Universidad Nacional del Nordeste y definirá las acciones a seguir.

Dentro del plan de acciones se incluirán las actividades para comunicar al personal que forma parte del Plan de Continuidad, la recuperación de desastres y la evaluación de las interrupciones previas a la activación del mismo. La cual será realizada de forma inmediata conforme los roles.

En todos los casos, la vida humana, el bienestar y la seguridad de la persona estará por sobre cualquier tipo de evento o incidente.

A continuación, se definen algunos eventos que indicarían el inicio del mismo:

1. El análisis del tipo de desastre que suponga un corte o interrupción por más de 2 horas. Algunos de los posibles errores a detectar podrían ser:
   - Fallas en equipos físicos (hardware).
   - Interrupción o cortes en la energía eléctrica o comunicaciones.
   - Fallas en las aplicaciones o bases de datos.
   - Errores humanos (no intencionales, sabotaje, etc.).
   - Desastres naturales (inundaciones, tormentas, etc.).
2. No disponibilidad al acceso físico o remoto al área de infraestructura de la oficina de la DGLH por un periodo de 4 horas.
3. Cualquier situación que determine una interrupción de tiempo indefinido en los servicios o sistemas críticos del área de TI de la DGLH.

Comunicación del plan de continuidad

Se establecerán los canales oficiales de comunicación a utilizar en caso de incidentes. Al momento de conformar el equipo encargado del Plan de Continuidad de Negocio se registrarán los números de teléfonos personales y correos electrónicos para una rápida comunicación con los mismos. De forma alternativa se podría considerar un número de contacto telefónico adicional según la necesidad.

Al mismo tiempo se deberá comunicar a las autoridades correspondientes el inicio del plan y el estado del mismo.

Ubicación física

Se determinará un espacio físico alternativo desde donde realizar las operaciones de continuidad del negocio del área de TI de la DGLH.

1. Área de TI de ISSUNNE: Se utilizarán de forma temporal las oficinas donde se alojan los servidores del Instituto de Servicios Sociales de la Universidad Nacional del Nordeste. Este espacio cuenta con la infraestructura y comunicación necesarias para el funcionamiento de los servicios y sistemas críticos del área de TI de la DGLH.

Orden de recuperación

Una vez realizados los procedimientos de restablecimiento de los servicios y sistemas críticos y con el Plan de Continuidad de Negocio iniciado y en marcha, con las evaluaciones de las interrupciones y tanto el personal como los directivos notificados formalmente se procederá a implementar las estrategias de recuperación de los sistemas, reparación de los daños en caso que sea necesario y reanudación de los servicios habituales en modo normal en la ubicación física alternativa, ver esquema en Fig. 9

En esta etapa se establecerán que los servicios y sistemas críticos del área estarán nuevamente en funcionamiento.

El orden previsto para dar continuidad efectiva a los servicios estará conformado por las siguientes actividades:

1. Identificación del lugar alternativo para montar el plan físicamente.
2. Verificación de los recursos disponibles para realizar procedimientos de recuperación y continuidad.
3. Recuperación de las copias de seguridad de los sistemas y bases de datos.
4. Instalación de los equipos físicos y sistemas operativos.
5. Instalación de las copias de seguridad existentes.

Fig. 9. Orden de recuperación del Plan de Continuidad de Negocio
Fuente: Elaboración propia

4.2 Discusiones y Comentarios

Planteado el SGSI a implementar en el área de la DGLH, con las metodologías sugeridas por los estándares ISO y MAGERIT, detallando las políticas de seguridad de la información, inventario y clasificación de activos, análisis y evaluación de riesgos, aplicabilidad de los controles y plan de continuidad, se deriva que el sistema propuesto reúne las características principales mínimas que debe contener un sistema de seguridad de la información para el cumplimiento de su objetivo, por lo que la propuesta resultaría viable para su aplicación en el área bajo estudio.

Asimismo, se destaca la amplia cobertura de todos los temas involucrados con la seguridad de la información que debe tener un área de tecnología de la información para su correcto funcionamiento dentro de los márgenes aceptables de seguridad y en cumplimiento de las normas y reglamentos establecidos para el sector público nacional.

Capítulo 5
Pruebas, análisis de resultados y validación

En el presente capítulo 5, se describen las pruebas llevadas a cabo en el área bajo estudio, los resultados obtenidos y métodos de validación aplicados al SGSI propuesto para el área de TI de la DGLH de la UNNE, cumpliendo con los objetivos planteados en el capítulo 1 del presente trabajo.

5.1 Flujo de trabajo

Se propone un flujo de trabajo donde se identifican adecuadamente las acciones a realizar a fin de validar los objetivos propuestos y realizar un seguimiento adecuado al SGSI, el mismo corresponde a la gráfica propuesta en la Fig. 10 .

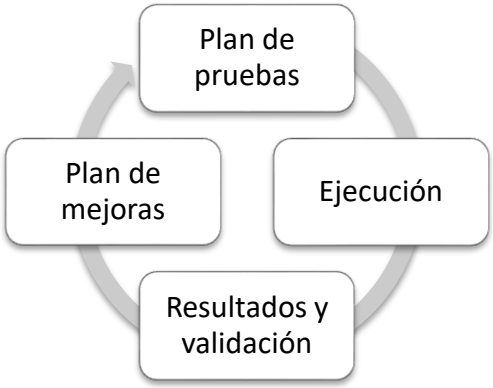

Fig. 10. Flujo de trabajo para la validación de pruebas
Fuente: Elaboración propia

Pruebas: En las mismas se determinará y seleccionará el método de validación para aplicar en el tratamiento del objetivo propuesto, se indicarán las actividades y recursos a utilizar en la evaluación correspondiente.

Ejecución: Se llevará a cabo la ejecución del método de validación.

Resultados: Se analizará la información obtenida en las pruebas realizadas y se validará conforme a los indicadores de logros y métricas establecidos.

Mejoras: Correspondiendo al ciclo de mejora continua para las pruebas y resultados se propondrán mejoras sobre los objetivos específicos planteados en caso que existieran.

5.2 Ejecución del Plan de Pruebas

5.2.1 Resultados de nivel de cumplimiento de normas y dominios

Requisito de la Norma ISO/IEC 27001:2013. **Contexto de la Organización**

4. Contexto de la organización		**Cumple**	**Que se tiene**	**Recomendaciones**
4.1	Conocimiento de la organización y de su contexto.	SI	Se cuenta con el total conocimiento de la organización, la misión de la misma, su visión y objetivos estratégicos y operacionales.	-
4.2	Comprensión de las necesidades y expectativas de las partes interesadas.	SI	Se tiene conocimiento del contexto y de la necesidad de contar e implementar con un SGSI, necesario para un óptimo funcionamiento del área TI de la DGLH.	-
4.3	Determinación del alcance del sistema de gestión de la seguridad de la información	SI	El SGSI se establecerá y diseñará para el área TI la oficina de la DGLH de la Universidad Nacional del Nordeste, encargada principalmente de la liquidación de los sueldos de la misma.	-
4.4	Sistema de gestión de seguridad de la información	NO	Actualmente el área no tiene implementado un SGSI y realiza tareas aisladas sin documentación a seguir.	Implementar un SGSI dará beneficios a la DGLH.

Requisito de la Norma ISO/IEC 27001:2013. **Liderazgo**

5. Liderazgo		**Cumple**	**Que se tiene**	**Recomendaciones**
5.1	Liderazgo y compromiso	SI	La Directora de la oficina DGLH posee los conocimientos de contar con beneficios de un SGSI	Establecer compromisos de manera formal con los agentes del

			y apoya su implementación y futura certificación de la norma para sus procesos.	área, motivando y llevando tareas de liderazgo.
5.2	Política	NO	No se cuenta con políticas de seguridad de la información definidas de manera formal.	Definir y compartir políticas generales para la seguridad de la información para que otras áreas puedan tomar conocimiento y aplicarlas en su contexto.
5.3	Roles, responsabilidades y autoridades en la organización	NO	Los roles y responsabilidades están asignadas de manera general y no oficialmente ni por escrito.	Documentar los roles y responsabilidades en base a la seguridad de la información.

Requisito de la Norma ISO/IEC 27001:2013. **Planificación**

6. Planificación		**Cumple**	**Que se tiene**	**Recomendaciones**
6.1	Acciones para tratar riesgos y oportunidades	NO	Se iniciaron tareas y acciones sobre los riesgos del área, las que se realizan de forma paulatina.	Realizar planificaciones concretas sobre las áreas, estableciendo objetivos claros.
6.1.1	Generalidades	-	Se cuenta con condiciones ideales para diseñar e implementar un SGSI en el área TI de la DGLH las que denotaran un mejoramiento en la seguridad de sus operaciones.	Diseñar y aplicar un SGSI permitirá conocer y gestionar los activos del área
6.1.2	Valoración de riesgos de la seguridad de la información	NO	No se cuenta con definición de sus activos de manera formal ni tampoco se cuenta con	Analizar diferentes metodologías para la evaluación de riesgos y

			metodologías claras para la gestión de los riesgos de la seguridad de la información. Se conocen los riesgos de manera informal.	seleccionar la que mejor se adapte a las necesidades de la institución, realizando la documentación que acompañe los procesos. Determinar los principales riesgos que afectan al área.
6.1.3	Tratamientos de los riesgos de la seguridad de la información	NO	No se cuenta con una matriz de riesgos en los principales procesos del área, es necesario realizarla y complementar los riesgos de seguridad que afectan a la misma.	Definir los controles necesarios a fin de mitigar los riesgos hallados en el análisis del área. Documentar los planes de tratamiento a seguir.
6.2	Objetivos de seguridad de la información y planes para lograrlo.	NO	No se cuenta con objetivos formalmente definidos de la seguridad de la información del área.	Definir los objetivos de la seguridad de la información del área y establecer los planes para llevarlo a cabo, promoviendo el compromiso de los empleados.

Requisito de la Norma ISO/IEC 27001:2013. **Soporte**

7. Soporte		**Cumple**	**Que se tiene**	**Recomendaciones**
7.1	Recursos	SI	Se cuenta parcialmente con los recursos para el diseño e implementación de un SGSI en el área además de un total apoyo	Para aplicar de forma integral un SGSI total, la organización debe garantizar los recursos para la

			de la Dirección de la organización.	implementación, mantenimiento y mejoramiento en todas sus fases contratando el personal calificado necesario.
7.2	Competencia	SI	Se tiene la persona con el conocimiento necesario relativo para la fase de diseño y planeación del SGSI, no obstante podría llegar a ser necesario sumar personal capacitado para la implementación y seguimiento.	Sumar personal calificado en gestión y seguridad de la información y adicionalmente personal capacitado para certificar en la norma ISO 27001:2013.
7.3	Toma de conciencia	NO	No existen acuerdos de confidencialidad entre los empleados ni tampoco políticas ni objetivos definidos para la seguridad de la información en el área. No se cuenta con una clasificación de los riesgos en los procesos.	Realizar acuerdos de confidencialidad de la información e informar y capacitar a los empleados sobre los riesgos de la seguridad de la información. Promover la capacitación y actualización de las medidas de seguridad de la información.
7.4	Comunicación	NO	No se cuenta con medios de comunicación oficial sobre la seguridad de la información, se hacen de manera informal por los diferentes canales de comunicación.	Utilizar los medios de comunicación organizacional para dar a conocer información relevante a la seguridad de la información en diferentes niveles.
7.5	Información documentada			

7.5.1	Generalidades	NO	El área no cuenta con información relevante para un Sistema General de Seguridad de la Información (SGSI).	Se debe analizar, redactar y documentar la información requerida por el estándar ISO 27001:2013.
7.5.2	Creación y actualización	NO	No existe documentación relacionada a la seguridad de la información.	Una vez creada la documentación, mantenerla actualizada conforme a la norma.
7.5.3	Control de la información documentada	NO	No existe un control de la documentación del SGSI ya que no hay uno implementado de manera formal.	Mantener un control y actualización permanente de la documentación del SGSI preservando su confidencialidad, integridad, disponibilidad y autenticidad.

Requisito de la Norma ISO/IEC 27001:2013. **Operación**

8. Operación		**Cumple**	**Que se tiene**	**Recomendaciones**
8.1	Planificación y control operacional	NO	No existe control de los procesos que permitan alcanzar los objetivos de la seguridad de la información.	Establecer los procesos necesarios para planear, implementar, mantener y mejorar el SGSI.
8.2	Valoración de riesgos de seguridad de la información	NO	No se cuenta con una valoración de los riesgos informáticos que permitan determinar la criticidad o el nivel de	Definir un esquema de clasificación de riesgos informáticos que permita

			riesgos de los procesos del área.	analizarlos y valorarlos para determinar los controles a implementar con el fin de aceptarlos o mitigarlos.
8.3	Tratamiento de los riesgos de seguridad de la información	NO	No existe definido un plan para el tratamiento de riesgos del área.	Documentar y llevar un plan de tratamiento de riesgos informáticos. Mantenerlo actualizado.

Requisito de la Norma ISO/IEC 27001:2013. **Evaluación del desempeño**

9. Operación		**Cumple**	**Que se tiene**	**Recomendaciones**
9.1	Seguimiento, medición, análisis y evaluación	NO	No se cuenta con los métodos, procesos y controles de seguridad para analizar, evaluar y llevar el seguimiento.	Definir los métodos para realizar el seguimiento, medición, análisis y evaluación de los procesos y controles de seguridad necesarios en todo SGSI.
9.2	Auditoria interna	NO	Las auditorías internas que existen no se centran específicamente en la seguridad de la información.	Planear, implementar y mantener un plan de auditoría interna que permita medir el estado de la seguridad de la información en base a la norma ISO 27001:2013.

9.3	Revisión por la dirección	NO	No está documentado un plan de la revisión del SGSI por parte de la dirección.	Realizar la documentación y planear revisiones al SGSI de forma general y a las políticas de seguridad de la información a fin de implementar las acciones de mejora continua.

Requisito de la Norma ISO/IEC 27001:2013. **Mejora**

10. Mejora		**Cumple**	**Que se tiene**	**Recomendaciones**
10.1	No conformidades y acciones correctivas	NO	No existe documentación relacionada al manejo de las no conformidades del Sistema General de Seguridad de la Información el SGSI.	Definir y documentar las causas de las no conformidades al SGSI e implementar acciones correctivas necesarias, identificando las vulnerabilidades halladas.
10.2	Mejora continua	NO	No existen de manera formal ya que no se cuenta con el SGSI implementado.	Sugerir la propuesta de un sistema que permita mejorar continuamente el SGSI mediante un proceso sistemático.

Análisis de Resultados

Mediante la utilización de la Tabla 5: Criterios para evaluar los requisitos de la norma ISO/IEC 27001:2013, se obtuvo el nivel de cumplimiento para cada uno de los requisitos mínimos de la norma ISO/IEC 27001:2013 y se resume de la siguiente manera:

Tabla 21. Nivel de cumplimiento de requisitos de la Norma ISO/IEC 27001:2013 en la DGLH.

Requisito	Cumple en %	No cumple en %	Nivel de Madurez
4. Contexto de la organización	75%	25%	No diseñado
5. Liderazgo	30%	70%	No diseñado
6. Planificación	0%	100%	No diseñado
7. Soporte	70%	30%	No diseñado
8. Operación	0%	100%	No diseñado
9. Evaluación del desempeño	0%	100%	No diseñado
10. Mejora	0%	100%	No diseñado

Gráficamente, el nivel de cumplimiento general de los requisitos mínimos se refleja a continuación en la Fig. 11 y el Diagrama de barras de implementación de los controles en la Fig. 12 , además se complementa con el Diagrama de radar de la implementación de los controles en la DGLH según se observa en la Fig. 13 .

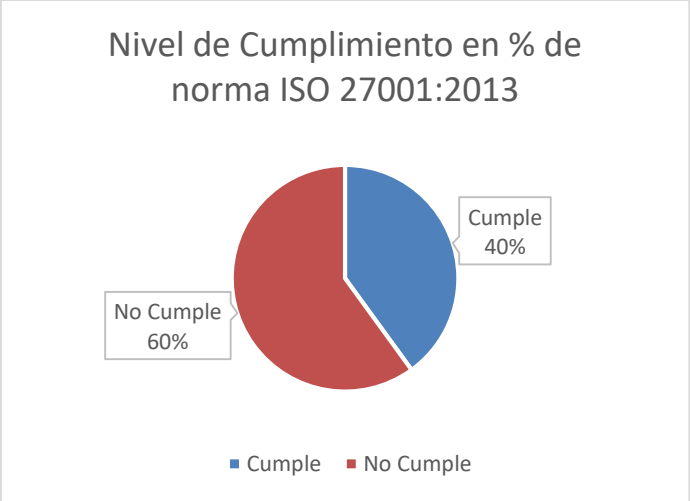

Fig. 11. Nivel de Cumplimiento de los requisitos mínimos de la Norma ISO/IEC 27001:2013
Fuente: Elaboración propia

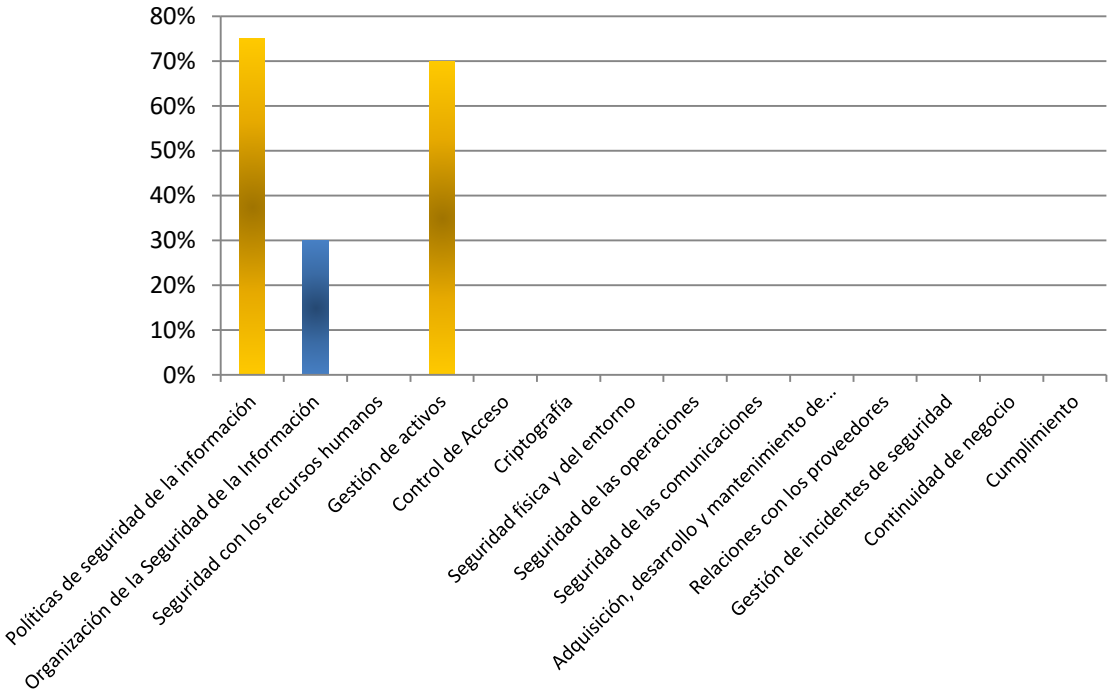

Fig. 12. Diagrama de barras de la implementación de controles de ISO/IEC 27001
Fuente: Elaboración propia

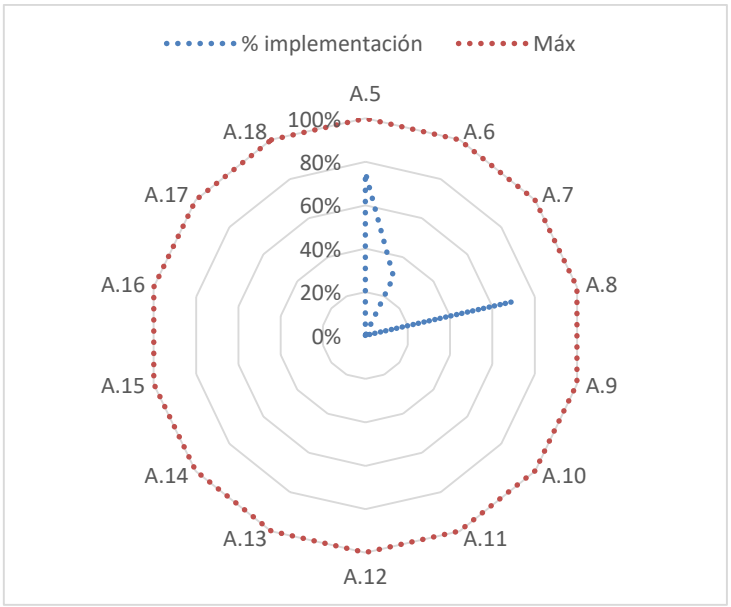

Fig. 13. Diagrama de radar de la implementación de controles de la ISO/IEC 27002
Fuente: Elaboración propia

A través del Análisis Diferencial realizado en el área TI de la DGLH de la UNNE se puede observar que la Dirección comprende la importancia y la necesidad de contar con un SGSI alineado con el proceso de desarrollo tecnológico que sigue la organización,

además se destaca que la misma posee el liderazgo y gestión necesaria para lograrlo de manera exitosa. Para el mismo se deben establecer formalmente la metodología de análisis y evaluación de riesgos informáticos, además del tratamiento de los mismos y la documentación requerida por la norma ISO 27001:2013.

5.2.2 Resultados de Dominios, Objetivos de Control y Controles de Seguridad.

A continuación, en las Tablas 22 a la 35, se exponen los resultados obtenidos del relevamiento llevado a cabo en el área bajo estudio en cuanto a la Organización de la Seguridad de la Información según la ISO/IEC 27001.

Tabla 22. Organización de la Seguridad de la Información.
Anexo A de la Norma ISO/IEC 27001

<table>
<tr><td>A.6</td><td colspan="3">Organización de la Seguridad de la información</td></tr>
<tr><td>A.6.1</td><td colspan="3">Organización interna</td></tr>
<tr><td colspan="4">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.</td></tr>
<tr><td rowspan="6">A.6.1.1</td><td rowspan="6">Roles y responsabilidades para la seguridad de la información</td><td rowspan="6">Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información</td><td>Aplica</td></tr>
<tr><td>Si | No</td></tr>
<tr><td>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 la norma ISO 27001:2013.</td></tr>
<tr><td>Implementa</td></tr>
<tr><td>Si | No</td></tr>
<tr><td>Al no tener definido e implementado un SGSI no se aplica una definición de roles u responsabilidades de la seguridad de la información.</td></tr>
</table>

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, 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 Los agentes de la DGLH se encuentran separados por áreas y perfiles y se les otorga acceso solo a los activos y/o información necesarios.

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 Todos los incidentes de seguridad se comunican de forma directa con las autoridades superiores.

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	**Aplica** Si / No Los grupos de interés especial mejoran el conocimiento y las prácticas relativas a la seguridad

		profesionales especializadas en seguridad.	de la información, así como las actualizaciones de los equipos y/o dispositivos.
			Implementa
			Si / No
			Existe relación con grupos afines, como la Comunidad SIU donde se comparten temas afines.

A.6.1.5	Seguridad de la información en la gestión de proyectos	**Control**: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyectos.	**Aplica**
			Si / No
			Una metodología de análisis de riesgos debería ser parte del proceso de implementación de un proyecto de TI con el fin de direccionarlos y controlarlos.
			Implementa
			Si / No
			Los riesgos asociados a la seguridad informática no son tenidos en cuenta en el inicio de los proyectos.

A.6.2	**Dispositivos móviles y teletrabajo**		
Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.			
A.6.2.1	Políticas para dispositivos móviles	**Control**: Se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos	**Aplica**
			Si / No
			Los dispositivos móviles son un riesgo potencial para la seguridad de la información.
			Implementa

		por el uso de dispositivos móviles.	SI / **No** La DGLH no cuenta con políticas de seguridad para los dispositivos móviles.

A.6.2.2	Teletrabajo	**Control**: Se debe implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	**Aplica** **Si** / No El teletrabajo debería tener una política de seguridad sobre las condiciones y restricciones. **Implementa** Si / **No** No está habilitado el acceso remoto a los recursos informáticos. Solo personal capacitado tiene acceso a los mismos.

Tabla 23. Seguridad de los Recursos Humanos.
Anexo A de la Norma ISO/IEC 27001

A.7	**Seguridad de los Recursos Humanos**		
A.7.1	Antes de asumir el empleo		
Objetivo: Asegurar que los empleados y contratistas comprenden las responsabilidades y son idóneos en los roles para que los consideran.			
A.7.1.1	Roles y responsabilidades para la seguridad de la información	**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	**Aplica** **Si** / No Aparte de las competencias técnicas, el personal contratado debería ser éticamente correcto y confiable especialmente si accede a información sensitiva de la organización.

		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.	**Implementa** Si / **No** El personal nuevo, es dado de alta sin realizar exámenes o capacitación en las tareas específicas. El mismo es tomado en base a recomendaciones externas.

A.7.1.2	Términos y condiciones del empleo	**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.	**Aplica** **Si** / No 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** Si / **No** No existen acuerdos o políticas para el manejo de la información dentro de la organización.

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	**Aplica** **Si** / No La dirección asegura que los roles y responsabilidades están claramente definidos antes de brindar acceso confidencial, así como los empleados están

		acuerdo a las políticas y procedimientos establecidos por la organización.	comprometidos con las políticas de seguridad de la información. Esta documentación es de carácter obligatorio en la norma ISO 27001:2013.
			Implementa
			Si / **No**
			Actualmente la oficina de la DGLH no 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**
			Actualmente la oficina de la DGLH no tiene implementado un SGSI y no existen políticas de 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	**Aplica**
			Si / No
			Los procesos disciplinarios son analizados en base al grado de responsabilidad del empleado y

		contra empleados que hayan cometido una violación a la seguridad de la información.	el impacto que tiene en la organización. **Implementa** Si / **No** No existen sanciones ni procesos disciplinarios correctivos ante violaciones o faltas en la seguridad de la información.

A.7.3	**Terminación y cambio de empleo**		
Objetivo: Proteger los interés 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 finalizar un empleo no se notifica a al empleado sobre la validez de sus responsabilidades y deberes relativos a la seguridad de la información.

Tabla 24. Gestión de activos.
Anexo A de la Norma ISO/IEC 27001

A.8	**Gestión de activos**

<table>
<tr><td>A.8.1</td><td colspan="3">Responsabilidad de los activos</td></tr>
<tr><td colspan="4">Objetivo: Identificar los activos organizacionales y definir las responsabilidades apropiadas.</td></tr>
<tr><td>A.8.1.1</td><td>Inventario de activos</td><td>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.</td><td>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 norma ISO 27001:2013.
Implementa
Si | No
El área no posee documentación o clasificación alguna de su información y de la criticidad de los activos que posee.</td></tr>
</table>

<table>
<tr><td>A.8.1.2</td><td>Propiedad de los activos</td><td>Control: Los activos mantenidos en el inventario deben tener un propietario.</td><td>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 norma ISO 27001:2013.
Implementa
Si | No
Los activos de información no poseen propietarios de forma explícita. Todo pertenece al área.</td></tr>
</table>

A.8.1.3	Propiedad 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 les dan a los activos informáticos de la organización. **Implementa** Si / No No se existen reglas o políticas para el uso aceptable de los activos del área.

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 cargo, al terminar su empleo, contrato o acuerdo.	**Aplica** Si / No La devolución de activos debe ser formalizada y la información almacenada en dispositivos personales transferida a la organización. **Implementa** Si / No No existen registros de la toma de los activos por parte de los empleados.

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,	**Aplica** Si / No La clasificación de la información es vital para

		criticidad y susceptibilidad a divulgación o a modificación autorizada.	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 (No)
			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 (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 (No)
			No se cuenta con procedimientos para el etiquetado de la información en el área.

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 (Si) / No
			El acceso a los activos debería restringirse de acuerdo a su esquema de clasificación.
			Implementa
			Si / No (No)
			No existen procedimientos ni normativas para el manejo de la

			información, la misma no se halla clasificada (ver A.8.2.1).

A.8.3	**Manejo de medios**		
Objetivo: Evitar la divulgación, modificación, el retiro o la destrucción 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 no cuentan con un nivel de clasificación de información y tampoco está convenientemente protegidos (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

			No existe un área segura exclusiva para el almacenamiento de los medios.

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: Si Los medios transportados podrían tener información sensitiva. **Implementa** Si / No: No No existe un movimiento o transporte de los medios fuera del área.

Tabla 25. Control de accesos.
Anexo A de la Norma ISO/IEC 27001

A.9	**Control de accesos**		
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: Si El control de acceso físico y lógico con principios del menor privilegio permite tener un control sobre los riesgos de diseminación de información o acceso físico a los activos a personas no autorizadas. **Implementa** Si / No: No No se cuenta con controles físicos y lógicos y no están

			documentadas en una política de seguridad de la información.

A.9.1.2	Acceso a redes y a servicios de 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
			Se cuenta con una intranet para los servicios del área, solo para el acceso autorizado desde facultades.	

A.9.2	**Gestión de acceso a 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
			Los agentes poseen identificación en los diferentes sistemas pero no poseen un control y seguimiento de los mismos.	

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 Los agentes no poseen asignación de un identificador único dentro de la organización, dependen de cada aplicación a utilizar. (ver A.9.2.1).

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	**Aplica** Si / No La autenticación de los empleados en los sistemas debería mantenerse confidencial

		de un proceso de gestión formal.	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 pero no se obliga al cambio de manera periódica.

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	**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

		cuando se hagan cambios.	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 de los agentes en los sistemas y acceso a la información es confidencial y privada.
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 / Ni 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 de inicio de sesión seguro en todos los casos.

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 diccionario. **Implementa** Si / No Los sistemas de gestión de contraseñas no son interactivos ya que es otorgada de forma manual.

A.9.4.4		**Control:** Se debe restringir y controlar	**Aplica** Si / No

	Uso de programas utilitarios privilegiados	estrictamente el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y los controles de las aplicaciones.	Los programas utilitarios deben ser instalados cuidadosamente para que no afecten a los sistemas o a la información existente. **Implementa** Si / **No** En los sistemas y activos críticos sólo se instalan aplicaciones estrictamente necesarias pero no existe un registro o bitácora.

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 personal técnico capacitado.

Tabla 26. Controles criptográficos.
Anexo A de la Norma ISO/IEC 27001

A10.1	**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	**Aplica** **Si** / No La criptografía cifra mediante algoritmos de encriptación los mensajes son transmitidos

		la protección de la información.	garantizando la confidencialidad, integridad y autenticidad de los mensajes, impidiendo así que sea legible por personas no autorizadas. **Implementa** Si / **No** No existen políticas sobre el uso de algoritmos de encriptación para el cifrado de la información transmitida o almacenada.

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 (ver A.10.1.1).

Tabla 27. Seguridad física y del entorno.
Anexo A de la Norma ISO/IEC 27001

A.11	**Seguridad física y del entorno**		
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	**Aplica** **Si** / No

		seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	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 de acceso restringido pero sin dispositivos 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 no está controlado, se permite el acceso sin registro de fecha y hora. Débil 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 están protegidas por medios físicos para controlar el acceso pero no así el centro de datos.

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 desastres naturales y/o intencionales.

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 Las áreas de trabajo no se verifican periódicamente.

A.11.1.6	Área y despacho de cargas	**Control:** Se deben controlar los puntos de acceso tales como	**Aplica** Si / No

		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.	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** No se cuenta con un lugar de entrega de equipos y otros dispositivos, los mismos se entregan en la misma oficina.

A11.2	**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 no están protegidos físicamente contra amenazas ambientales tales como fuego, incendio, agua, humo, etc. Existen sensores de humo y extintores adecuados.

A.11.2.2			**Aplica**

	Servicios de suministro	**Control:** Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.	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 y ventilación se encuentran correctamente instalados y asegurados.

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 se encuentra adecuadamente separado del cableado de datos.

A.11.2.4	Mantenimiento de equipo	**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, pero no existe un mantenimiento periódico ni programado.

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, la instalación o eliminación de software sólo es realizado por el personal técnico 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 de la oficina sólo son utilizados dentro de las

			instalaciones físicas de la misma.

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 No existen procedimientos seguros 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 existan políticas documentadas, los usuarios son conscientes y aplican la seguridad apropiada cuando el equipo no está siendo utilizado.

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 no es almacenada en forma segura, se encuentra en los servidores con acceso sin seguridad.

Tabla 28. Seguridad de las operaciones.
Anexo A de la Norma ISO/IEC 27001

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 En toda situación, los procedimientos operacionales deberían estar documentados y disponibles para todos los usuarios. Estos procedimientos incluyen las copias de seguridad, almacenamiento, manejo de errores, encendido y/o apagado de equipos, instalación y/o configuración de sistemas, etc. Documentación de carácter obligatorio en la norma ISO 27001:2013.

			Implementa Si / **No** No existe procedimientos operacionales documentados, los mismos se están empezando a realizar de manera paulatina.

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 no son planificados ni probados anteriormente a su instalación. Se realizan a medida de las necesidades de la organización.

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**

			No existe un monitoreo continuo de los recursos, los mismos se realizan de acuerdo a las necesidades del momento.

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: **Si** La separación de ambientes de desarrollo y pruebas reduce el riesgo de operaciones no autorizadas. **Implementa** Si / No: **No** No se cuenta con ambientes separados de producción y de prueba. Las pruebas se realizan con algunas copias de seguridad de los archivos y configuraciones más importantes.

Tabla 29. Protección contra códigos maliciosos.
Anexo A de la Norma ISO/IEC 27001

A12.2	**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	**Aplica** Si / No: **Si** 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

		usuarios, para proteger contra códigos maliciosos.	ilegal de información confidencial y borrado total. **Implementa** Si / No No se cuenta con políticas para la lucha contra el malware. Los usuarios poseen sus estaciones de trabajo con antivirus para evitar este tipo de ataque pero no están atendidos periódicamente.

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 de forma diaria, de forma automática y programada sobre los archivos y bases de datos más importantes del área.

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 No existe una documentación de cómo llevar el seguimiento de los registros de los eventos ocurridos en los sistemas o bases de datos.
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 No existen registros de eventos, salvo los propios de cada sistema operativo. Los cuales pueden ser accedidos por los administradores de cada sistema.
A.12.4.3	Registros del administrador y del operador	**Control:** Las actividades del administrador y del operador del sistema se deben	**Aplica** Si / No Los administradores tienen accesos privilegiados y podrían

		registrar, y los registros se deben proteger y revisar con regularidad.	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 No existen políticas definidas para sincronización de los relojes del área, todos los sistemas no se encuentran 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

			En el área no existen políticas documentadas o procedimientos definidos sobre la instalación de software en los sistemas operativos reales o virtualizados.

A12.6	**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: **Si** 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: **No** No existe un inventario de los activos físicos y del software operacional, de igual manera 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 usuario.	**Aplica** Si / No: **Si** 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 (No)
			La instalación de software es realizada por el personal técnico o por los usuarios de cada terminal de trabajo.

A.12.7	**Consideraciones sobre auditorías de sistemas de información**		
Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.			
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 (Si)
			Las auditorías de los sistemas deberían ser acordadas, planeadas y controladas sin interferir en el desarrollo normal de los procesos.
			Implementa
			Si / No (No)
			No se cuenta con un plan de auditoría para la verificación de los sistemas operativos del área.

Tabla 30. Seguridad de las comunicaciones.
Anexo A de la Norma ISO/IEC 27001

A.13	**Seguridad de las comunicaciones**		
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.			
A.13.1.1	Control de redes	**Control**: Las redes se deben gestionar y controlar para	**Aplica**
			Si / No (Si)

		proteger la información en sistemas y aplicaciones.	Las redes deberían proteger la transmisión de la información garantizando su confidencialidad e integridad y en algunos casos su disponibilidad.
			Implementa
			SI / **No**
			No se cuenta con gestión de las redes de forma óptima.

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 controlado y gestionado por el área TI de la Rectorado.

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 a través de VLANs.
			Implementa
			Si / No

			Los usuarios y servicios están separados a través de dominios y VLANs por facultades y campus.

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 entidad. **Implementa** SI / No No se cuenta con documentación sobre los procedimientos y controles a implementar para la transferencia segura de la información ni tampoco formación al respecto.

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 que garanticen la

			seguridad en la transmisión de la información de forma externa.

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 existen controles que garanticen la seguridad en la transmisión de la información de manera interna.

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 Los acuerdos de confidencialidad se establecen de manera informal sobre el compromiso de los agentes y el uso de los sistemas.

Tabla 31. Adquisición, desarrollo y mantenimiento de sistemas.
Anexo A de la Norma ISO/IEC 27001

<table>
<tr><td>A.14</td><td colspan="3">Adquisición, desarrollo y mantenimiento de sistemas</td></tr>
<tr><td>A.14.1</td><td colspan="3">Requisitos de seguridad de los sistemas de información.</td></tr>
<tr><td colspan="4">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.</td></tr>
<tr><td rowspan="6">A.14.1.1</td><td rowspan="6">Análisis y especificación de requisitos de seguridad de la información</td><td rowspan="6">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.</td><td>Aplica</td></tr>
<tr><td>Si | No</td></tr>
<tr><td>Los requerimientos de la seguridad de la información deberían ser identificados utilizando varios métodos en concordancia con las políticas y regulaciones.</td></tr>
<tr><td>Implementa</td></tr>
<tr><td>SI | No</td></tr>
<tr><td>No existe una política de seguridad de información o protocolos que permitan determinar la adquisición de los nuevos sistemas de información.</td></tr>
<tr><td rowspan="6">A.14.1.2</td><td rowspan="6">Seguridad de servicios de las aplicaciones en redes públicas</td><td rowspan="6">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</td><td>Aplica</td></tr>
<tr><td>Si | No</td></tr>
<tr><td>La comunicación de los servicios y aplicaciones debería estar garantizada bajo esquemas de encriptación de datos garantizando su confidencialidad e integridad.</td></tr>
<tr><td>Implementa</td></tr>
<tr><td>Si | No</td></tr>
</table>

		modificación no autorizadas.	No existe una Infraestructura de Llave Pública (PKI) implementada que garantice que la información entre las partes.

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

			No se cuenta con políticas ni procedimientos definidos para el desarrollo de software en el área.

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 No existen procedimientos para el seguimiento del ciclo de vida los sistemas desarrollados en el área, ni tampoco registro formal de los cambios realizados.

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 implementadas y probadas

			brevemente directamente en producción.

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 necesario. **Implementa** Si (■) / No Las modificaciones de software son realizadas sobre necesidades puntuales y con seguimiento.

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 (■) No se cuenta con documentación de los sistemas desarrollados ni tampoco con manuales de usuarios de los mismos.

A.14.2.6	Ambiente de desarrollo seguro	**Control:** Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros	**Aplica** Si (■) / No Los ambientes de desarrollo de software también deberían estar protegidos de acceso no

		para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	autorizado o de ejecución de software malicioso. **Implementa** Si / **No** No se cuenta con un área o espacio de desarrollo separado del área de producción.

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 El software utilizado es de desarrollo propio y los desarrollos externos son controlados y 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 Se realizan pruebas de seguridad al software en su etapa 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 Para los datos de prueba se utilizan copias de producción. En caso de tener que realizar pruebas fuera de la oficina, se los anonimiza preventivamente.

Tabla 32. Relación con los proveedores.
Anexo A de la Norma ISO/IEC 27001

<table>
<tr><td>A.15</td><td colspan="3">Relación con los proveedores</td></tr>
<tr><td>A.15.1</td><td colspan="3">Seguridad de la información en las relaciones con los proveedores</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores</td></tr>
<tr><td rowspan="5">A.15.1.1</td><td rowspan="5">Política de seguridad de la información para las relaciones con proveedores</td><td rowspan="5">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.</td><td>Aplica</td></tr>
<tr><td>Si | No</td></tr>
<tr><td>La organización debería emplear los controles y procedimientos de seguridad para el acceso a los activos por parte de los proveedores.</td></tr>
<tr><td>Implementa</td></tr>
<tr><td>Si | No
No se cuenta con una política de seguridad definida para el trato con proveedores.</td></tr>
<tr><td rowspan="5">A.15.1.2</td><td rowspan="5">Tratamiento de la seguridad dentro de los acuerdos con proveedores</td><td rowspan="5">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.</td><td>Aplica</td></tr>
<tr><td>Si | No</td></tr>
<tr><td>Se deberían establecer acuerdos de seguridad documentados entre la organización y los proveedores para el acceso a los activos.</td></tr>
<tr><td>Implementa</td></tr>
<tr><td>Si | No
No existe documentación ni tampoco clasificación de seguridad de la información para el tratamiento con los proveedores y activos.</td></tr>
</table>

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 existe documentación ni tampoco clasificación de seguridad de la información para el tratamiento con los proveedores y activos.

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 existen políticas de seguridad de la información o procedimientos.

A.15.2.2	Gestión de cambios en los	**Control:** Se deben gestionar los cambios en el	**Aplica** Si / No

	servicios de los proveedores	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.	Los cambios de los proveedores deberían estar acordes a los requerimientos de seguridad de la información de la organización. **Implementa** Si / **No** No existen políticas de seguridad de la información o procedimientos.

Tabla 33. Gestión de incidentes de seguridad de la información.
Anexo A de la Norma ISO/IEC 27001

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 procedimientos o protocolos para gestionar los incidentes relacionados con 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 notificados de los posibles 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 prevenir incidentes. **Implementa** Si / No Los empleados están comprometidos en reportar las brechas, pero no existen canales

			oficiales para registrar los eventos.

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 de información no están clasificados y no existe una metodología de análisis y evaluación de riesgos.

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 Los procedimientos de respuesta no están documentados, así como tampoco existe un Plan de Continuidad del Negocio, aunque la respuesta a los incidentes es inmediata.

A.16.1.6	Respuesta a 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: Si Se debería recolectar información de los incidentes ocurridos con el fin de prevenirlos en el futuro. **Implementa** Si / No: No No se registra la información de los incidentes y tampoco 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: Si Se deberían recolectar las evidencias y registros para tomar acciones legales. **Implementa** Si / No: No Las evidencias de los incidentes no son recolectadas ni registradas con lo cual no se pueden realizar acciones legales.

Tabla 34. Aspectos de seguridad de la información de la gestión de continuidad del negocio. Anexo A de la Norma ISO/IEC 27001

A.17	**Aspectos de seguridad de la información de la gestión de la continuidad del negocio**
A.17.1	Gestión de incidentes y mejoras de la 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 27001:2013. **Implementa** Si: No: ■ No existe documentación o procedimientos para los BCP y DRP del área en cuanto a sus procesos o servicios.

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 27001:2013. **Implementa** Si: No: ■ No existe documentación o procedimientos para los BCP y

			DRP del área en cuanto a sus procesos o servicios.
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 documentación o procedimientos para los BCP y DRP del área en cuanto a sus procesos o servicios.

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 No se cuentan con réplicas a fin de cumplir con los requisitos de disponibilidad para el procesamiento de la información.

Tabla 35. Cumplimiento. Anexo A de la Norma ISO/IEC 27001

<table>
<tr><td>A.18</td><td colspan="3">Cumplimiento</td></tr>
<tr><td>A.18.1</td><td colspan="3">Cumplimiento de los requisitos legales y contractuales.</td></tr>
<tr><td colspan="4">Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.</td></tr>
<tr><td>A.18.1.1</td><td>Identificación de la legislación aplicable a los requisitos contractuales</td><td>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.</td><td>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
No se cuenta con documentación a seguir oficialmente.</td></tr>
<tr><td>A.18.1.2</td><td>Derechos de propiedad intelectual</td><td>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.</td><td>Aplica
Si | No
Se deberían definir las políticas y procedimientos para controlar la propiedad intelectual.
Implementa
Si | No
El software desarrollado no posee derechos de patentes o propiedad intelectual sobre los mismos.</td></tr>
</table>

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 se cuenta con un nivel de clasificación 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
			No se cuenta con una política relativa a la protección de datos personales a nivel de la organización.	

A.18.1.5		**Control:** Se deben usar controles criptográficos, en	**Aplica**	
			Si	No

	Reglamentación de controles criptográficos	cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.	Los controles criptográficos permiten garantizar la confidencialidad, integridad y autenticidad de la información. **Implementa** Si / **No** No existe una Infraestructura de Llave Pública (PKI) que garantice que la información almacenada y/o transmitida 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 existen auditorías con organismos externos y las auditorías internas no son específicamente técnicas y no se encuentran lo suficientemente preparadas.

A.18.2.2			**Aplica**

	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.	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 ni tampoco registros que permita realizar comparaciones de 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 No se realizan test de penetración a los sistemas, ni tampoco existen políticas de seguridad que permitan comparar los resultados.

Análisis de Resultados

Conforme al análisis realizado en el área TI de la DGLH se puede observar el siguiente detalle de cumplimiento para cada uno de los Dominios, Objetivos de Control y Controles de Seguridad del Anexo A de la norma ISO/IEC 27001:2013 (ISO/IEC 27002:2013) en la Tabla 36.

Tabla 36. Nivel de cumplimiento de los Dominios de Control de la Norma ISO/IEC 27002: 2013
Fuente: Elaboración propia

Dominios de Control	Cumple en %	No cumple en %	Nivel de Madurez
A5. Políticas de seguridad de la información	75%	25%	Control inicial
A6. Organización de la seguridad de la información.	30%	70%	Control inicial
A7. Seguridad de los recursos humanos.	0%	100%	Sin control
A8. Gestión de activos	70%	30%	Control inicial
A9. Control de acceso	0%	100%	Sin control
A10. Criptografía	0%	100%	Sin control
A11. Seguridad física y del entorno	0%	100%	Sin control
A.12. Seguridad de las operaciones	0%	100%	Sin control
A.13. Seguridad de las comunicaciones	0%	100%	Sin control
A.14. Adquisición, desarrollo y mantenimiento de sistemas	0%	100%	Sin control
A.15. Relaciones con los proveedores	0%	100%	Sin control
A.16. Gestión de incidentes de seguridad de la información	0%	100%	Sin control
A.17. Aspectos de seguridad de la información de la gestión de continuidad del negocios	0%	100%	Sin control
A.18. Cumplimiento	0%	100%	Sin control

Desde un punto de vista de cumplimiento general de manera actual sobre los dominios de control del área se puede observar en la Fig. 14 .

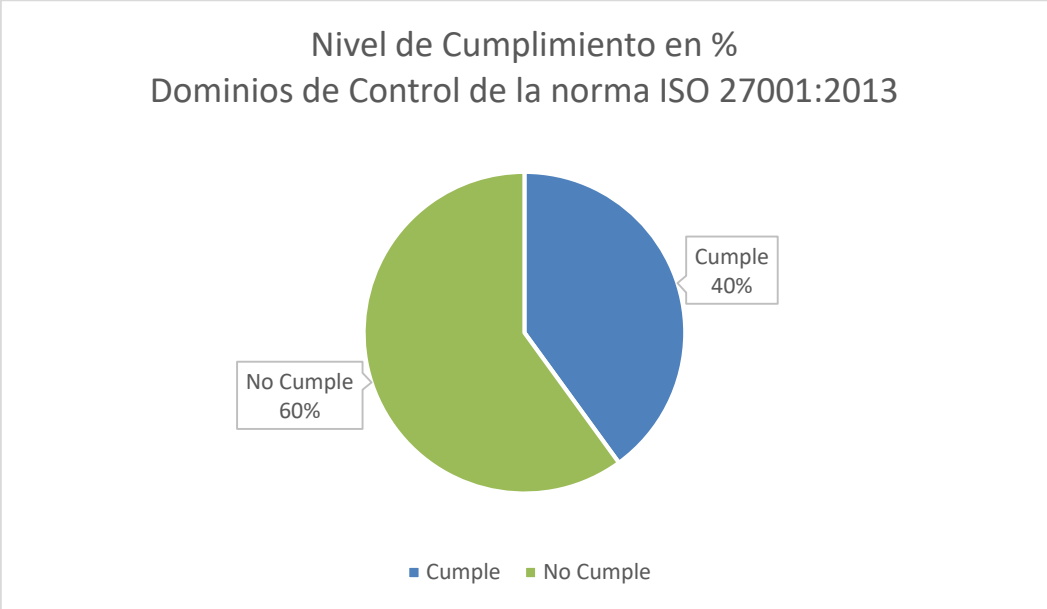

Fig. 14. *Nivel de cumplimiento de los Dominios de Control de la Norma ISO/IEC 27001:2013*
Fuente: Elaboración propia

Como se puede observar, el área TI de la DGLH de la UNNE no posee un cumplimiento en la mayoría de los Dominios, Objetivos de Control y Controles de seguridad conforme al requerimiento propuesto por la norma ISO 27002:2013 y tampoco aplica la utilización de mecanismos de seguridad de la información.

En cuanto a los activos de la misma, el personal, los controles de acceso y las instalaciones se puede observar que no cuentan con la suficiente protección ante eventualidades y no se cuenta con procedimientos de contingencia que puedan ser aplicados antes imprevistos.

5.2.3 Resultados del Análisis y Evaluación de Riesgos

El área TI de la DGLH de la UNNE está conformada por los siguientes activos o recursos informáticos:

Tabla 37. *Recursos informáticos del área de TI de la DGLH.*
Fuente: Elaboración propia

Recursos	**Descripción**
Copias de seguridad	Copias de seguridad de bases de datos, de archivos instalados y de sistemas operativos.

Sistemas en producción	Sistemas utilizados en el área, por ejemplo SIU Mapuche, sistemas de desarrollo propio, etc.
Código fuente	Código fuente de los desarrollos propios y de terceros que se utilizan.
Servicios internos	Servicios que brinda el área, portal de inicio, servicios de mensajería, repositorios de archivos.
Sistemas operativos	Sistemas operativos instalados en las computadoras personales y virtualizados en los servidores.
Servidores físicos	Equipos destinados a la instalación de hipervisores para virtualización de sistemas operativos.
Computadoras personales	Estaciones de trabajo de cada personal, administrativo, técnico o directivos.
Impresoras	Equipos destinados a la impresión de documentación del área.
Escaners	Equipos destinados a la digitalización de documentos del área.
Routers	Equipos de comunicaciones para la gestión de la red externa.
Switchs	Equipos de comunicaciones para la gestión de la red interna.
Racks	Dispositivos para el alojamiento y organización de los servidores.
Sistemas de alimentación UPS	Sistema de alimentación secundario para la gestión de servidores ante fallas en la energía eléctrica.
Cableado eléctrico	Cableado e instalaciones destinadas a la alimentación eléctrica del área.
Red de área local	Cableado e instalaciones destinadas a la conectividad interna y externa del área.
Punto de acceso inalámbrico	Sistema de acceso a internet inalámbrico para el área.

Tabla 38. *Listado de activos de TI del Área de la DGLH.*
Fuente: Elaboración propia

N	Código	Nombre del activo de Información	Activo	Descripción	Contenido	Responsable
1	HW_SRV1	HP DL360GEN 10– Archivos	[HW]	Servidor físico con virtualización de MV para gestión de archivos	Máquinas virtuales para gestión de Archivos	Administrador técnico de la DGLH
2	HW_SRV2	HP DL160GEN 9 - Procesos	[HW]	Servidor físico con virtualización de MV para gestión de procesos	Máquinas virtuales para gestión de Procesos	Administrador técnico de la DGLH
3	HW_SRV3	HP DL360GEN 7– Secundario	[HW]	Servidor físico con virtualización de MV de procesos secundarios	Máquinas virtuales de procesos Secundarios	Administrador técnico de la DGLH
4	HW_SRV4	HP DL360GEN 10 - Principal	[HW]	Servidor físico con virtualización de MV de procesos principales	Máquinas virtuales de procesos Principales	Administrador técnico de la DGLH
5	HW_SRV5	PC– Backups	[HW]	Servidor físico con virtualización de MV de copias de seguridad	Máquinas virtuales de Copias de Seguridad	Administrador técnico de la DGLH
6	HW_PRT1	Impresora Kyocera Ecosys P3045dn	[HW]	Impresora láser principal del área	Impresora láser principal área administrativa	Administrador técnico de la DGLH
7	HW_PRT2	Impresora Kyocera Ecosys FS 4300DN	[HW]	Impresora láser secundaria del área	Impresora láser principal área operativa	Administrador técnico de la DGLH
8	HW_PRT3	Impresora Kyocera Ecosys FS 4300DN	[HW]	Impresora láser secundaria del área	Impresora láser secundaria área administrativa	Administrador técnico de la DGLH
9	HW_SCN1	Scanner HP – Scanjet Pro 4500 FN 1	[HW]	Scanner principal del área de TI	Scanner principal área administrativa	Administrador técnico de la DGLH

10	HW_SCN1	Scanner Multifunción HP – F4180	[HW]	Scanner principal del área de TI	Scanner principal área operacional	Administrador técnico de la DGLH
11	HW_PC1	Equipos de cómputo para gestión del desarrollo tecnológico.	[HW]	Computadoras de escritorio uso tecnológico, desarrollo	Computadoras para el uso de desarrollo	Administrador técnico de la DGLH
12	HW_PC2	Computadoras de escritorio (equipos desarrollo / producción).	[HW]	Computadoras de escritorio uso tecnológico, desarrollo	Computadoras para el uso de desarrollo / producción	Administrador técnico de la DGLH
13	HW_PC3	Computadoras de escritorio (equipos administrativos).	[HW]	Computadoras de escritorio uso administrativo.	Computadoras para el uso del área administrativa.	Administrador técnico de la DGLH
14	SW_PROC	Server AppsViejoProcesosDGLH	[SW]	Sistema Operativo (Debian 8) virtualizado	Sistema operativo Debian 8 con PostgreSQL 11. Aplicaciones con PHP 7.1. Código fuente propio.	Administrador técnico de la DGLH
15	SW_OTROS	Server Otros Mapuche	[SW]	Sistema Operativo (Debian 9) virtualizado	Sistema operativo Debian 8 con PostgreSQL 11. Aplicaciones con PHP 7.1. Código fuente SIU Mapuche. Becas, Fondos, Contratos.	Administrador técnico de la DGLH
16	SW_PAMPI	Server Pampito	[SW]	Sistema Operativo (Windows2012) virtualizado	Sistema operativo Windows 2012. Ofimática para uso	Administrador técnico de la DGLH

					compartido (Excel, Access). Código fuente, SQL, consultas propias.	
17	SW_HISTO	Server Histo	[SW]	Sistema Operativo (Debian 8) virtualizado	Sistema operativo Debian 8 con PostgreSQL 9.6. Aplicaciones con PHP 7.3. Código fuente SIU Mapuche versiones anteriores.	Administrador técnico de la DGLH
18	SW_RECIBO	Server Recibos DDJJ	[SW]	Sistema Operativo (Debian 9) virtualizado	Sistema operativo Debian 9 con PostgreSQL 11. Aplicación web de Recibo Digital y DDJJ. Código fuente propio.	Administrador técnico de la DGLH
19	SW_MSJE	Server Mensajería	[SW]	Sistema Operativo (Debian 9) virtualizado	Sistema operativo Debian 8 con MySQL. Aplicaciones con PHP 7.1. Server Mensajería Spark.	Administrador técnico de la DGLH
20	SW_SISTE	Server AppsNuevo Sistemas DGLH	[SW]	Sistema Operativo (Debian 9) virtualizado	Sistema operativo Debian 9 con PostgreSQL 11. Últimas aplicaciones web con PHP 7.3. Código fuente propio.	Administrador técnico de la DGLH
21	SW_NUXEO	Server NuxeoDigi	[SW]	Sistema Operativo (Debian 9) virtualizado	Sistema operativo Debian 9 con PostgreSQL	Administrador técnico de la DGLH

					11. Digitalización de aplicaciones de SIU Mapuche. Código fuente propio.	
22	SW_PRODUC	Server Produccion	[SW]	Sistema Operativo (Debian 9) virtualizado	Sistema operativo Debian 9 con PostgreSQL 11. PHP 7.3. SIU Mapuche principal. Portal de inicio de aplicaciones. Código fuente propio.	Administrador técnico de la DGLH
23	SW_BCKP	Server Backups	[SW]	Sistema Operativo (Debian 9) virtualizado	Sistema operativo Debian 8 y PHP 7.1. Servidor FTP para copias de BD de los sistemas en producción más importantes.	Administrador técnico de la DGLH
24	D_PROC	Server AppsViejo Procesos DGLH	[D]	Registros del Sistema Operativo (Debian 9) virtualizado	Registros del Sistema operativo Debian 8 con PostgreSQL 11. PHP 7.1. Sistemas de Altas, etc. Bases de datos, tablas, registros propios.	Administrador técnico de la DGLH
25	D_OTROS	Server Otros Mapuche	[D]	Registros del Sistema Operativo (Debian 9) virtualizado	Registros del Sistema operativo Debian 9 con PostgreSQL 11. Aplicaciones con PHP 7.3.	Administrador técnico de la DGLH

					Bases de datos, tablas, registros propios.	
26	D_PAMPI	Server Pampito	[D]	Datos y registros del Server Pampito	Archivos, registros, informes. Datos utilizados por los agentes administrativos. Consultas, SQLs, propios.	Administrador técnico de la DGLH
27	D_HISTO	Server Histo	[D]	Bases de datos del servidor de históricos de SIU Mapuche	Registros del Sistema operativo Debian 8 con PostgreSQL 9.6. Aplicaciones con PHP 7.1. Bases de datos SIU Mapuche con registros propios.	Administrador técnico de la DGLH
28	D_RECIBO	Server Recibos DDJJ	[D]	Bases de datos del servidor de Recibos y DDJJ	Registros del Sistema operativo Debian 9 con PostgreSQL 11. Aplicaciones con PHP 7.3. Bases de datos, tablas, registros propios.	Administrador técnico de la DGLH
29	D_MSJE	Server Mensajería	[D]	Bases de datos y archivos del servidor de Mensajería	Registros del Sistema operativo Debian 8 con MySQL. Aplicaciones con PHP 7.1. Logs de acceso, Mensajería Spark.	Administrador técnico de la DGLH

30	D_SISTE	Server AppsNuevo Sistemas DGLH	[D]	Bases de datos y archivos del servidor de AppsNuevo	Registros del Sistema operativo Debian 9 con PostgreSQL 11. Aplicaciones con PHP 7.3. Bases de datos, tablas, registros propios.	Administrador técnico de la DGLH
31	D_NUXEO	Server NuxeoDigi	[D]	Bases de datos y archivos del servidor de Digitalización Nuxeo	Registros del Sistema operativo Debian 9 con PostgreSQL 11. Aplicaciones con PHP 7.3. Bases de datos, tablas, registros propios digitalizados.	Administrador técnico de la DGLH
32	D_PRODUC	Server Producción	[D]	Bases de datos y archivos del servidor de Producción	Registros del Sistema operativo Debian 9 con PostgreSQL 11. Aplicaciones con PHP 7.3. Bases de datos SIU con registros propios. Bases de datos, tablas, registros propios.	Administrador técnico de la DGLH
33	D_BCKP	Server Backups	[D]	Archivos, copias de seguridad de bases de datos y archivos.	Archivos, copias de bases de datos de los principales sistemas utilizados en el área de la DGLH. Copias de	Administrador técnico de la DGLH

					backup de archivos en Server Pampito.	
34	COM_SWT 1	Puntos de acceso alámbrico (switch central)	[COM]	Equipo de conectividad	Switch de conectividad cableada provisto por el área TI de rectorado	Área TI de Rectorado
35	COM_SWT 2	Puntos de acceso alámbricos (switch datacenter)	[COM]	Equipo de conectividad del centro de datos	Switch de conectividad cableada dentro del centro de datos	Administrador técnico de la DGLH
36	COM_SWT 3	Puntos de acceso inalámbricos (switch datacenter)	[COM]	Equipo de conectividad inalámbrica	Switch de conectividad inalámbrica dentro del centro de datos.	Administrador técnico de la DGLH
37	COM_PC1	Teléfono voz ip – Yealink HD T21P E2	[COM]	Equipo de Telefonía digital	Teléfono para voz IP de escritorio	Área TI de Rectorado
38	COM_PC1	Teléfono voz ip – Yealink HD T21P E2	[COM]	Equipo de Telefonía digital	Teléfono para voz IP de escritorio	Área TI de Rectorado
39	COM_LOC	Red de área local	[COM]	Conexión de área local	Red de datos local	Área TI de Rectorado
40	COM_INA	Conectividad inalámbrica	[COM]	Conexión de área inalámbrica	Red de datos inalámbrica	Administrador técnico de la DGLH
41	COM_TEL	Línea telefónica	[COM]	Línea telefónica	Línea telefónica de toda el área	Área TI de Rectorado
42	SE_ISP	Proveedor de servicio de internet (ISP) - Principal	[SE]	Proveedor de internet	Proveedor de internet, servicio oficial provisto por el área TI de Rectorado	Área TI de Rectorado
43	SE_ISP	Proveedor de servicio de internet (ISP) – Secundario	[SE]	Proveedor de internet secundario	Proveedor de internet, servicio secundario	Administrador técnico de la DGLH

					para acceso alternativo.	
44	SE_MAIL	Correo electrónico Institucional	[SE]	Servicio de correo institucional	Servicio de correos oficial provisto por el área TI de Rectorado (@unne.edu.ar)	Área TI de Rectorado
45	P_DIRE	Personal Directivo	[P]	Personal Directivo	Directora y sub directora de la DGLH de la UNNE	Directora de la DGLH
46	P_TECN	Personal Técnico	[P]	Personal Técnico	Personal técnico informático de la DGLH de la UNNE	Directora de la DGLH
47	P_ADMI	Personal Administrativo	[P]	Personal Administrativo	Personal administrativo de la DGLH de la UNNE	Directora de la DGLH
48	L_CENT	Centro de datos	[L]	Área del centro de datos	Área de servidores del área de TI de la DGLH de la UNNE	Administrador técnico de la DGLH
49	L_ADM	Oficina administrativa	[L]	Oficina administrativa	Oficina administrativa de la DGLH de la UNNE	Directora de la DGLH
50	L_DIRE	Oficina dirección	[L]	Oficina directiva	Oficina directivas de la DGLH de la UNNE	Directora de la DGLH
51	AUX_ACO1	Aire acondicionado 10000 Frigorías	[AUX]	Equipos de refrigeración	Acondicionador de aire central de la DGLH	Área de mantenimiento de Rectorado
52	AUX_ACO2	Aire acondicionado 5500 Frigorías	[AUX]	Equipos de refrigeración	Acondicionador de aire de la DGLH	Área de mantenimiento de Rectorado
53	AUX_ACO3	Aire acondicionado 5500 Frigorías	[AUX]	Equipos de refrigeración	Acondicionador de aire del centro de datos	Área de mantenimiento de Rectorado
54	AUX_UPS	Sistema de alimentación	[AUX]	UPS	Sistema de alimentación para los equipos	Área TI de Rectorado

		ininterrumpida (UPS)			principales del centro de datos	
55	AUX_RAC	Rack	[AUX]	Estanterías	Armarios con puertas y refrigeración para el alojamiento de los principales equipos del centro de datos de la DGLH	Administrador técnico de la DGLH
56	AUX_ELEC	Cableado eléctrico	[AUX]	Sistema de cableado	Cableado y sistema eléctrico para la alimentación de toda la oficina de la DGLH	Área de mantenimiento de Rectorado

Valoración de activos de acuerdo al impacto

De acuerdo a Tabla 39, los resultados obtenidos en la valoración cuantitativa de los activos de información de la DGLH se obtuvieron los siguientes resultados:

Tabla 39. *Valoración cualitativa de los activos de información de la DGLH según Magerit. Fuente: Elaboración propia.*

IDENTIFICACION DEL RIESGO			**ANÁLISIS Y EVALUACIÓN DEL RIESGO**	
N.	**Código**	**Nombre del activo de Información**	**Valoración del riesgo**	**Razón**
1	HW_SRV1	HP DL360GEN10 - Archivos	MODERADO (MEDIO)	Los archivos de copias de seguridad son importantes en la recuperación
2	HW_SRV2	HP DL160GEN9 - Procesos	IMPORTANTE (ALTO)	Servidor importante para la ejecución de procesos de liquidación del área de TI. Importante
3	HW_SRV3	HP DL360GEN7 - Secundario	IMPORTANTE (ALTO)	Servidor que almacena algunas aplicaciones

				para de uso secundario dentro de las tareas de la DGLH.
4	HW_SRV4	HP DL360GEN10 - Principal	INACEPTABLE (MUY ALTO)	Servidor importante, aloja el sistema principal de SIU Mapuche de producción sobre el cual se realizan las cargas de novedades y cálculos de liquidación.
5	HW_SRV5	PC- Backups	INACEPTABLE (MUY ALTO)	Servidor importante para el alojamiento de los archivos de copias de seguridad de las bases de datos de los sistemas SIU Mapuche.
6	HW_PRT1	Impresora Kyocera Ecosys P3045dn	ACEPTABLE (MUY BAJO)	Impresora principal del área administrativa. Puede ser reemplazada por la utilización de otra impresora.
7	HW_PRT2	Impresora Kyocera Ecosys FS 4300DN	ACEPTABLE (MUY BAJO)	Impresora secundaria del área operativa. Puede ser reemplazada por la utilización de otra impresora.
8	HW_PRT3	Impresora Kyocera Ecosys FS 4300DN	ACEPTABLE (MUY BAJO)	Impresora principal del área operativa. Puede ser reemplazada por la

				utilización de otra impresora.
9	HW_SCN1	Scanner HP – Scanjet Pro 4500 FN 1	ACEPTABLE (MUY BAJO)	Scanner del área administrativa, no es de utilización diaria, puede ser reemplazado por otro.
10	HW_SCN1	Scanner Multifunción HP – F4180	ACEPTABLE (MUY BAJO)	Scanner del área operativa, no es de utilización diaria, puede ser reemplazado por otro.
11	HW_PC1	Equipos de cómputo para gestión del desarrollo tecnológico.	TOLERABLE (BAJO)	Equipo para el desarrollo, estación de trabajo para codificar o realizar tareas técnicas.
12	HW_PC2	Computadoras de escritorio (equipos desarrollo / producción).	TOLERABLE (BAJO)	Equipo para el desarrollo, estación de trabajo para codificar o realizar tareas técnicas.
13	HW_PC3	Computadoras de escritorio (equipos administrativos).	ACEPTABLE (MUY BAJO)	Equipo para el trabajo administrativo, puede ser reemplazado por cualquier otro. Los archivos de trabajo se alojan en el servidor de FTP en Pampito Server
14	SW_PROC	Server AppsViejoProcesosDGLH	IMPORTANTE (ALTO)	Servidor que aloja las aplicaciones para la ejecución de

				diversas operaciones diarias en el proceso de liquidación de haberes.
15	SW_OTROS	Server OtrosMapuche	IMPORTANTE (ALTO)	Servidor que aloja diferentes versiones de meses anteriores de SIU Mapuche para el cálculo de Becas, Contratos, etc.
16	SW_PAMPI	Server Pampito	IMPORTANTE (ALTO)	Servidor Windows que almacena los archivos compartidos sobre los que trabaja el área administrativa. Acceso remoto. Tiene copia en el servidor de Backups.
17	SW_HISTO	Server Histo	IMPORTANTE (ALTO)	Servidor que aloja las aplicaciones para la ejecución de diversas operaciones diarias en el proceso de liquidación de haberes.
18	SW_RECIBO	Server RecibosDDJJ	INACEPTABLE (MUY ALTO)	Servidor importante para la ejecución de procesos de liquidación del área de TI. Importante
19	SW_MSJE	Server Mensajería	MODERADO (MEDIO)	Servidor de mensajería interna, Spark. Utilizado para transferencia de

				archivos en la intranet.
20	SW_SISTE	Server AppsNuevoSistemasDGLH	IMPORTANTE (ALTO)	Servidor importante que aloja las aplicaciones para la ejecución de diversas operaciones diarias críticas en el proceso de liquidación de haberes.
21	SW_NUXEO	Server NuxeoDigi	MODERADO (MEDIO)	Servidor que digitaliza los archivos que envían los jefes de personal de las facultades y que utiliza SIU Mapuche de producción.
22	SW_PRODUC	Server Producción	IMPORTANTE (ALTO)	Sistema SIU Mapuche utilizado para el cálculo de los procesos de liquidación del mes. Archivos del sistema personalizado y la base de datos alojada en PostgreSQL 11. Es de absoluta importancia.
23	SW_BCKP	Server Backups	IMPORTANTE (ALTO)	Servidor que incluye FTP donde se almacenan y consultan las copias de seguridad de los principales sistemas del área.
24	D_PROC	Server AppsViejoProcesosDGLH	INACEPTABLE (MUY ALTO)	Datos, registros que almacenan las copias de seguridad de

				las bases de datos de los sistemas más importantes que utiliza el área.
25	D_OTROS	Server OtrosMapuche	MODERADO (MEDIO)	Datos de los registros de sistemas SIU Mapuche: Becas, Contratos, etc.
26	D_PAMPI	Server Pampito	INACEPTABLE (MUY ALTO)	Archivos, registros sobre los que trabajan los usuarios administrativos de la DGLH. Notas, cálculos, informes, etc.
27	D_HISTO	Server Histo	MODERADO (MEDIO)	Datos de los registros de sistemas SIU Mapuche en versiones anteriores.
28	D_RECIBO	Server RecibosDDJJ	INACEPTABLE (MUY ALTO)	Datos de los recibos de los agentes universitarios y alta de DDJJ anual para la gestión de sus datos personales.
29	D_MSJE	Server Mensajería	IMPORTANTE (ALTO)	Base de datos del servidor de mensajería interna, Spark. Registros y logs. Utiliza MySQL 9.5
30	D_SISTE	Server AppsNuevoSistemasDGLH	IMPORTANTE (ALTO)	Bases de datos de los sistemas de Apps Nuevos de la oficina de DGLH. PostgreSQL 9.6
31	D_NUXEO	Server NuxeoDigi	IMPORTANTE (ALTO)	Bases de datos donde se alojan los archivos

				digitalizados para SIU Mapuche de producción y otros de novedades
32	D_PRODUC	Server Producción	INACEPTABLE (MUY ALTO)	Base de datos del sistema en Producción SIU Mapuche en su última versión. A partir del cual se calculan las liquidaciones mensuales. Es de absoluta importancia.
33	D_BCKP	Server Backups	INACEPTABLE (MUY ALTO)	Registros, logs del sistema de backups de las bases de datos más importantes.
34	COM_SWT1	Puntos de acceso alámbrico (switch central)	IMPORTANTE (ALTO)	Sistema de conectividad, conmutador de red que interconecta la red de área local de la UNNE. Salida a internet a través del ISP de Rectorado.
35	COM_SWT2	Puntos de acceso alámbricos (switch datacenter)	TOLERABLE (BAJO)	Sistema de conectividad, conmutador de red que interconecta la red de área local dentro del área de la DGLH.
36	COM_SWT3	Puntos de acceso inalámbricos (switch datacenter)	ACEPTABLE (MUY BAJO)	Sistema de conectividad, conmutador de red inalámbrico que interconecta la red de área

				local de la DGLH y con el ISP externo.
37	COM_PC1	Teléfono voz ip – Yealink HD T21P E2	ACEPTABLE (MUY BAJO)	Central telefónica que ofrece servicios de comunicación a través de la red IP de la UNNE.
38	COM_PC1	Teléfono voz ip – Yealink HD T21P E2	ACEPTABLE (MUY BAJO)	Central telefónica que ofrece servicios de comunicación a través de la red IP de la UNNE.
39	COM_LOC	Red de área local	IMPORTANTE (ALTO)	Red de área local que permite interconectar los diferentes dispositivos dentro de la DGLH y de manera externa con los campus.
40	COM_INA	Conectividad inalámbrica	MODERADO (MEDIO)	Red inalámbrica de área local que permite interconectar los diferentes dispositivos dentro de la DGLH.
41	COM_TEL	Línea telefónica	ACEPTABLE (MUY BAJO)	Línea telefónica para llamadas de voz, no se encuentra digitalizada.
42	SE_ISP	Proveedor de servicio de internet (ISP) - Principal	MODERADO (MEDIO)	Proveedor de internet gestionado por el área TIC de Rectorado, brinda el acceso a internet.

43	SE_ISP	Proveedor de servicio de internet (ISP) - Secundario	ACEPTABLE (MUY BAJO)	Proveedor de internet gestionado por el área de TI de la DGLH, brinda el acceso a internet de forma alternativa al oficial.
44	SE_MAIL	Correo electrónico Institucional	MODERADO (MEDIO)	Servicio de correo institucional, brindado por el área TIC de Rectorado. Es importante para la comunicación con entidades externas como el caso de los bancos.
45	P_DIRE	Personal Directivo	INACEPTABLE (MUY ALTO)	Personal directivo de la DGLH. Encargado y responsable de la dirección. Coordina y dirige el total funcionamiento del mismo y establece las relaciones con los campus y las entidades bancarias para las acreditaciones.
46	P_TECN	Personal Técnico	INACEPTABLE (MUY ALTO)	Personal a cargo del área de TI. Administra, gestiona los equipos informáticos, la infraestructura del mismo. Mantiene los

				sistemas y las copias de seguridad. Gestiona los usuarios y permisos.
47	P_ADMI	Personal Administrativo	INACEPTABLE (MUY ALTO)	Personal a cargo de las tareas administrativas del área. Recepción, control de novedades, atención de agentes, etc.
48	L_CENT	Centro de datos	MODERADO (MEDIO)	Oficina donde se alojan los equipos servidores de datos. Se halla dentro del área de la dirección, refrigerada adecuadamente. No posee acceso directo.
49	L_ADM	Oficina administrativa	MODERADO (MEDIO)	Oficina de uso del área administrativa, aloja las computadoras, impresoras, scanners y mobiliario necesario.
50	L_DIRE	Oficina dirección	MODERADO (MEDIO)	Oficina de la Dirección del área. Lugar desde donde se realizan las tareas de mando y gestión de la DGLH. Posee mobiliario y se comparte con el área técnica.
51	AUX_ACO1	Aire acondicionado 10000 Frigorías	ACEPTABLE (MUY BAJO)	Equipo de refrigeración central que se

				encarga de acondicionar el área administrativa.
52	AUX_ACO2	Aire acondicionado 5500 Frigorías	ACEPTABLE (MUY BAJO)	Equipo de refrigeración individual para la refrigeración del área de la dirección.
53	AUX_ACO3	Aire acondicionado 5500 Frigorías	IMPORTANTE (ALTO)	Equipo de refrigeración individual para la refrigeración del centro de cómputos. Encendido las 24 horas los 365 días del año.
54	AUX_UPS	Sistema de alimentación ininterrumpida (UPS)	TOLERABLE (BAJO)	Sistema de alimentación de energía ininterrumpida para los servidores más importantes del área. Duración aproximada 30 minutos
55	AUX_RAC	Rack	ACEPTABLE (MUY BAJO)	Soporte físico que aloja los equipos servidores del área de TI. Se halla dentro del centro de datos. Posee conexiones eléctricas y coolers de refrigeración.
56	AUX_ELEC	Cableado eléctrico	INACEPTABLE (MUY ALTO)	Sistema de alimentación eléctrica que permite alimentar todos los equipos informáticos además de la iluminación y

				refrigeración de toda la oficina DGLH.

Identificación y valoración de amenazas

Conforme a las amenazas que se identifican en Magerit, las mismas se establecen para cada activo de información, determinando la probabilidad o frecuencia de ocurrencia de la misma y el impacto que tienen en cada dimensión de seguridad. Ver Anexo 15. Tabla de identificación y valoración de amenazas del área TI de la DGLH.

Valoración de riesgos según el impacto y la probabilidad en el área de sistemas del caso de estudio de DGLH

Tabla 40. *Identificación de riesgos de activos de la DGLH, análisis y evaluación de riesgos. Fuente: Elaboración propia.*

IDENTIFICACION DEL RIESGO					ANÁLISIS Y EVALUACIÓN DEL RIESGO		
Código	**Nombre del activo de Información**	**Activo**	**Tipo Riesgo**		**Probabilidad**	**Impacto**	**Valoración del riesgo**
1	HW_SRV1	HP DL360GEN10 - Archivos	[HW]	6.Tecnología	3	3	MODERADO (MEDIO)
2	HW_SRV2	HP DL160GEN9 - Procesos	[HW]	6.Tecnología	4	4	IMPORTANTE (ALTO)
3	HW_SRV3	HP DL360GEN7 - Secundario	[HW]	6.Tecnología	4	3	MODERADO (MEDIO)
4	HW_SRV4	HP DL360GEN10 - Principal	[HW]	6.Tecnología	5	5	INACEPTABLE (MUY ALTO)
5	HW_SRV5	PC- Backups	[HW]	6.Tecnología	5	5	INACEPTABLE (MUY ALTO)
6	HW_PRT1	Impresora Kyocera Ecosys P3045dn	[HW]	6.Tecnología	3	1	ACEPTABLE (MUY BAJO)
7	HW_PRT2	Impresora Kyocera Ecosys FS 4300DN	[HW]	6.Tecnología	3	1	ACEPTABLE (MUY BAJO)

8	HW_PRT3	Impresora Kyocera Ecosys FS 4300DN	[HW]	6.Tecnología	3	1	ACEPTABLE (MUY BAJO)
9	HW_SCN1	Scanner HP – Scanjet Pro 4500 FN 1	[HW]	6.Tecnología	1	1	ACEPTABLE (MUY BAJO)
10	HW_SCN1	Scanner Multifunción HP – F4180	[HW]	6.Tecnología	1	1	ACEPTABLE (MUY BAJO)
11	HW_PC1	Equipos de cómputo para gestión del desarrollo tecnológico.	[HW]	6.Tecnología	2	3	TOLERABLE (BAJO)
12	HW_PC2	Computadoras de escritorio (equipos desarrollo / producción).	[HW]	6.Tecnología	2	3	TOLERABLE (BAJO)
13	HW_PC3	Computadoras de escritorio (equipos administrativos).	[HW]	6.Tecnología	1	1	ACEPTABLE (MUY BAJO)
14	SW_PROC	Server AppsViejoProcesosDGLH	[SW]	3. Operativo	3	4	IMPORTANTE (ALTO)
15	SW_OTROS	Server OtrosMapuche	[SW]	3. Operativo	3	4	IMPORTANTE (ALTO)
16	SW_PAMPI	Server Pampito	[SW]	3. Operativo	3	4	IMPORTANTE (ALTO)
17	SW_HISTO	Server Histo	[SW]	3. Operativo	3	4	IMPORTANTE (ALTO)
18	SW_RECIBO	Server RecibosDDJJ	[SW]	3. Operativo	5	5	INACEPTABLE (MUY ALTO)
19	SW_MSJE	Server Mensajería	[SW]	3. Operativo	4	2	MODERADO (MEDIO)
20	SW_SISTE	Server AppsNuevoSistemasDGLH	[SW]	3. Operativo	3	4	IMPORTANTE (ALTO)
21	SW_NUXEO	Server NuxeoDigi	[SW]	3. Operativo	3	3	MODERADO (MEDIO)
22	SW_PRODUC	Server Producción	[SW]	3. Operativo	3	4	IMPORTANTE (ALTO)
23	SW_BCKP	Server Backups	[SW]	3. Operativo	3	4	IMPORTANTE (ALTO)
24	D_PROC	Server AppsViejoProcesosDGLH	[D]	3. Operativo	5	5	INACEPTABLE (MUY ALTO)
25	D_OTROS	Server OtrosMapuche	[D]	3. Operativo	5	2	MODERADO (MEDIO)
26	D_PAMPI	Server Pampito	[D]	3. Operativo	5	4	INACEPTABLE (MUY ALTO)
27	D_HISTO	Server Histo	[D]	3. Operativo	5	2	MODERADO (MEDIO)
28	D_RECIBO	Server RecibosDDJJ	[D]	3. Operativo	5	5	INACEPTABLE (MUY ALTO)

29	D_MSJE	Server Mensajería	[D]	3. Operativo	3	5	IMPORTANTE (ALTO)
30	D_SISTE	Server AppsNuevoSistemasDGLH	[D]	3. Operativo	5	3	IMPORTANTE (ALTO)
31	D_NUXEO	Server NuxeoDigi	[D]	3. Operativo	5	3	IMPORTANTE (ALTO)
32	D_PRODUC	Server Producción	[D]	3. Operativo	5	5	INACEPTABLE (MUY ALTO)
33	D_BCKP	Server Backups	[D]	3. Operativo	4	5	INACEPTABLE (MUY ALTO)
34	COM_SWT1	Puntos de acceso alámbrico (switch central)	[COM]	6.Tecnología	2	3	TOLERABLE (BAJO)
35	COM_SWT2	Puntos de acceso alámbricos (switch datacenter)	[COM]	6.Tecnología	2	3	TOLERABLE (BAJO)
36	COM_SWT3	Puntos de acceso inalámbricos (switch datacenter)	[COM]	6.Tecnología	2	3	TOLERABLE (BAJO)
37	COM_PC1	Teléfono voz ip – Yealink HD T21P E2	[COM]	6.Tecnología	2	1	ACEPTABLE (MUY BAJO)
38	COM_PC1	Teléfono voz ip – Yealink HD T21P E2	[COM]	6.Tecnología	2	1	ACEPTABLE (MUY BAJO)
39	COM_LOC	Red de área local	[COM]	6.Tecnología	3	5	IMPORTANTE (ALTO)
40	COM_INA	Conectividad inalámbrica	[COM]	6.Tecnología	5	1	MODERADO (MEDIO)
41	COM_TEL	Línea telefónica	[COM]	6.Tecnología	3	1	ACEPTABLE (MUY BAJO)
42	SE_ISP	Proveedor de servicio de internet (ISP) - Principal	[SE]	6.Tecnología	3	3	MODERADO (MEDIO)
43	SE_ISP	Proveedor de servicio de internet (ISP) - Secundario	[SE]	6.Tecnología	3	1	ACEPTABLE (MUY BAJO)
44	SE_MAIL	Correo electrónico Institucional	[SE]	6.Tecnología	5	2	MODERADO (MEDIO)
45	P_DIRE	Personal Directivo	[P]	6.Tecnología	5	5	INACEPTABLE (MUY ALTO)
46	P_TECN	Personal Técnico	[P]	6.Tecnología	5	5	INACEPTABLE (MUY ALTO)
47	P_ADMI	Personal Administrativo	[P]	6.Tecnología	5	5	INACEPTABLE (MUY ALTO)
48	L_CENT	Centro de datos	[L]	6.Tecnología	1	5	MODERADO (MEDIO)

49	L_ADM	Oficina administrativa	[L]	6.Tecnología	1	5	MODERADO (MEDIO)
50	L_DIRE	Oficina dirección	[L]	6.Tecnología	1	5	MODERADO (MEDIO)
51	AUX_ACO1	Aire acondicionado 10000 Frigorías	[AUX]	6.Tecnología	2	2	ACEPTABLE (MUY BAJO)
52	AUX_ACO2	Aire acondicionado 5500 Frigorías	[AUX]	6.Tecnología	2	2	ACEPTABLE (MUY BAJO)
53	AUX_ACO3	Aire acondicionado 5500 Frigorías	[AUX]	6.Tecnología	2	2	ACEPTABLE (MUY BAJO)
54	AUX_UPS	Sistema de alimentación ininterrumpida (UPS)	[AUX]	6.Tecnología	3	2	TOLERABLE (BAJO)
55	AUX_RAC	Rack	[AUX]	6.Tecnología	1	1	ACEPTABLE (MUY BAJO)
56	AUX_ELEC	Cableado eléctrico	[AUX]	6.Tecnología	1	5	MODERADO (MEDIO)

El área de tecnologías de la Información de la DGLH de la Universidad Nacional del Nordeste presenta sus principales activos con un nivel Muy Alto de riesgos (MA) y en algunos casos Alto Riesgo (A). Los riesgos de la DGLH se asocian principalmente a las posibles fallas de Hardware y el procesamiento de los datos. Con lo cual se desprende la importancia que presentan los equipos de cómputo y su efectivo funcionamiento en el procesamiento de la información, la cual a su vez debe cumplimentar los requisitos de la seguridad de la información: confidencialidad, integridad y disponibilidad.

Otro tema a considerar es la alta disponibilidad del servicio de internet, puesto que las unidades académicas (UA) deben presentar sus novedades durante un determinado tiempo durante cada mes y la provisión de energía eléctrica correspondiente ya que en esta zona es habitual que se produzcan cortes de energía eléctrica con lo cual es posible que existan fallas o ausencia de alimentación en los equipos.

Se observa además que es esencial considerar la mayor seguridad posible para los datos alojados en los servidores ya que un acceso o filtración de seguridad podría generar dudas sobre la integridad de los mismos o bien faltas en la confidencialidad y exposición de información de los agentes universitarios. Se podría considerar la posibilidad de incorporar mecanismos de cifrado o encriptación para las comunicaciones en los servicios más críticos.

Por su parte en el área administrativa es habitual la utilización de software ofimático y las estaciones de trabajo poseen un riesgo bajo, puesto que la principal operación y los procesos de ésta área poseen muy bajo impacto en el nivel general.

En lo que respecta a los riesgos ambientales y/o desastres naturales que puedan afectar a las instalaciones, el cuidado que presenta es mínimo, considerando que la zona geográfica donde se encuentran alojados los servidores no posee mayores riesgos de temblores, huracanes o derrumbes. Un tema a tener en cuenta es que el centro de datos se encuentra cercano a zona costera de ríos, con lo cual existiría una alguna posibilidad de inundaciones naturales. Conforme a los registros consultados, el mayor desastre natural correspondió a una inundación que dejó el agua del río Paraná a unos 100 metros de donde están los servidores. Por este motivo se podría pensar en instalar una réplica de los mismos en otra zona alejada a la ubicación actual para brindar una mayor seguridad.

En lo que respecta a la seguridad física, el acceso a las instalaciones posee una empresa de seguridad que se encarga de registrar el acceso y egreso de los empleados en el edificio de Rectorado y para el registro a cada oficina es necesario pasar por la detección biométrica en la zona de personal, la cual no es obligatoria sino más bien a los efectos de controlar la asistencia de los agentes.

El acceso a la oficina de DGLH posee mecanismos físicos de seguridad para el acceso general al mismo, pero la puerta es de vidrio blindado, al igual que otras paredes del área técnica y una puerta secundaria al mismo.

En cuanto al acceso físico a los servidores del área no dispone de dispositivos de seguridad, cerrojos ni elementos que limiten su ingreso al mismo. Ahora, los dos racks que albergan los servidores sí poseen llaves en sus puertas, pero se pueden acceder a través de su parte trasera, deslizándose por uno de los lados, con lo cual es evidente de una debilidad en su acceso físico con lo cual se podrían presentar daños voluntarios o involuntarios en el hardware que brinda los principales servicios al área con la consecuencia de fallas o ausencias de los mismos.

Se podrían incluir como medidas físicas el uso de tarjetas de control de acceso, algún tipo de seguridad biométrica y cámaras de vigilancia para el registro y control de los agentes,

principalmente el personal técnico que brinda el soporte técnico dentro del área de TI de la DGLH.

Por otro lado, los eventos naturales como tormentas o huracanes no son habituales en la zona, pero, el hecho que la oficina se encuentra alojada a unas 3 cuadras de la costa del Río Paraná hacen que se considere como importante dentro del plan de contingencia tener que reubicar los equipos en caso de crecidas del río. Consultando algunos antecedentes de crecidas importantes, las aguas llegaron a una cuadra de las oficinas de Rectorado.

Se pueden observar de forma gráfica, los riesgos de activos en área de TI de la DGLH la Fig. 15.

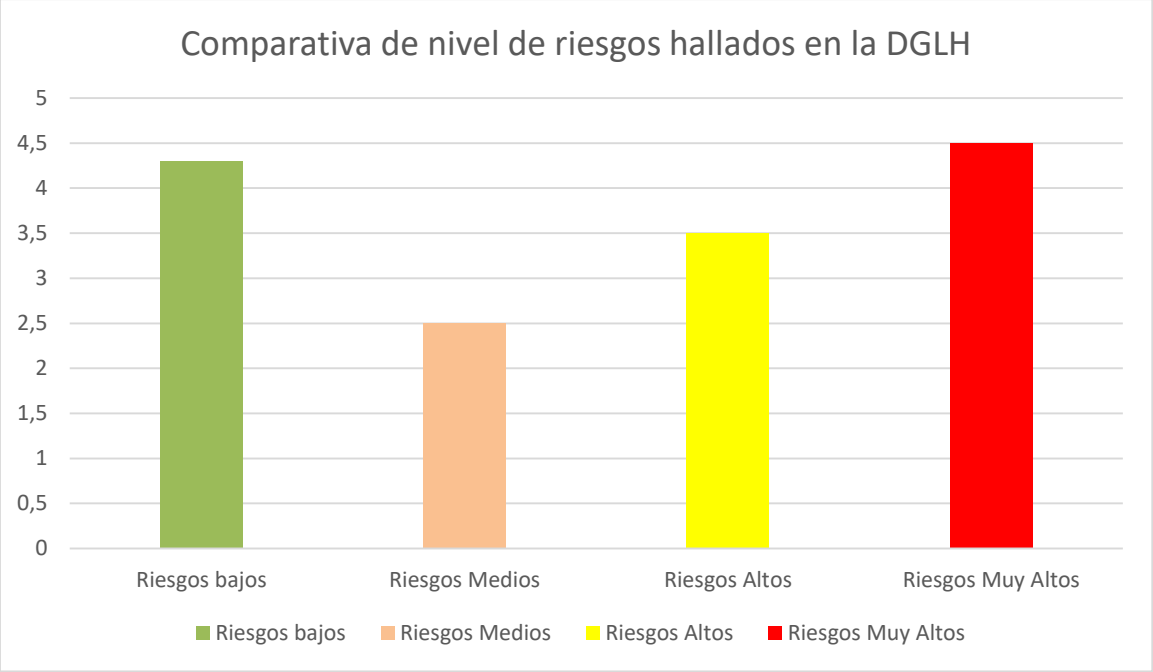

Fig. 15. Gráfica de riesgos hallados en el área de TI de la DGL
Fuente: Elaboración propia.

5.2.4 Resultados de la Aplicabilidad de controles

En este punto se visualizan los resultados de la aplicabilidad de los controles listados en el Anexo A de la norma ISO/IEC 27001:2013.

Tabla 41. A.5. Políticas de seguridad.
Aplicabilidad de controles

A.5. **Políticas de seguridad**			
A.5.1 Política de seguridad de la información: Orientación de la dirección para la gestión de la seguridad de la información			
ID	Control	Aplicable	Implementación
A.5.1.1	Políticas para la seguridad de la información	SI	Se establece y se acuerdan los objetivos de seguridad de la información del área, se establecen niveles de riesgos aceptables y se pone a disposición las políticas establecidas de forma interna entre los agentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	SI	El responsable técnico o el jefe de seguridad en conjunto con la Dirección establecen las evaluaciones periódicas a llevar a cabo en el área.

Tabla 42. A.6. Organización de la seguridad de la información.
Aplicabilidad de controles

A.6. **Organización de la seguridad de la información**			
A.6.1 Organización interna			
ID	Control	Aplicable	Implementación
A.6.1.1	Roles y responsabilidades para la seguridad de la información	SI	Se establecen por escrito los roles y responsabilidades de la seguridad de la información en el área.
A.6.1.2	Separación de deberes	SI	Se establecen separaciones del personal en áreas y otorgar acceso solo a los activos necesarios para el trabajo de cada agente.
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 jefe o responsable de seguridad es el vínculo con otros grupos de interés.
A.6.1.5	Seguridad de la información en la gestión de proyectos	SI	El jefe o responsable de seguridad es el encargado de velar por la gestión de los proyectos IT del área.
A.6.2	Dispositivos móviles y teletrabajo		
A.6.2.1	Política para dispositivos móviles	SI	Se establecen políticas para el uso de los dispositivos móviles. Cualquier dispositivo a conectar a la red de la institución debe cumplir las condiciones de seguridad establecidas.
A.6.2.2	Teletrabajo	Si	Solo el personal debidamente autorizado podrá acceder al uso de los activos de forma remota. Se establece tiempos de acceso y roles.

Tabla 43. A.7. Seguridad de los recursos humanos.
Aplicabilidad de controles

A.7. **Seguridad de los recursos humanos**			
A.7.1 Antes de asumir el empleo			
ID	Control	Aplicable	Implementación
A.7.1.1	Selección	SI	La selección del personal seleccionado está dada por el perfil e idoneidad para realizar las funciones previstas.
A.7.1.2	Términos y condiciones del empleo	SI	Se incluyen responsabilidades de la

			seguridad de la información en todos los acuerdos contractuales del área.
A.7.2	**Durante la ejecución del empleo**		
A.7.2.1	Responsabilidades de la dirección	SI	El diseño y soporte del SGSI está comprendido por la Dirección del área.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	SI	Se capacita de forma periódica en temas de seguridad de la información mediante talleres y gacetillas, promovidos por el jefe de seguridad o responsable tecnológico del área.
A.7.2.3	Proceso disciplinario	SI	Ante incumplimiento de las políticas de seguridad de la información, la Dirección establece los procedimientos a ejecutar procesos disciplinarios.
A.7.3	**Terminación y cambio de empleo**		
A.7.3.1	Terminación o cambio de responsabilidades de empleo	SI	El responsable o jefe de seguridad reasigna roles y permisos ante cambios de la situación del empleo de los agentes.

Tabla 44. A.8. Gestión de activos
Aplicabilidad de controles

A.8. **Gestión de activos**			
A.8.1 Responsabilidad por los activos			
ID	Control	Aplicable	Implementación
A.8.1.1	Inventario de activos	SI	La Dirección en conjunto con el responsable o jefe de seguridad realiza los inventarios de activos, la

			clasificación y correspondiente documentación.
A.8.1.2	Propiedad de los activos	SI	Los activos en los inventarios tienen asignados responsables.
A.8.1.3	Uso aceptable de los activos	SI	Los agentes tienen el compromiso de la utilización de los activos de forma responsable conforme a las políticas de seguridad general.
A.8.1.4	Devolución de los activos	SI	Se mantienen registros de la devolución de los activos asignados a los agentes.
A.8.2	**Clasificación de la información**		
A.8.2.1	Clasificación de la información	SI	Los activos inventariados están clasificados conforme a los niveles de seguridad definidos de forma global.
A.8.2.2	Etiquetado de la información	SI	Los activos inventariados se hallan etiquetados de acuerdo a la clasificación de la información de cada proyecto.
A.8.2.3	Manejo de activos	SI	Los activos clasificados e inventariados son documentados por la Dirección o responsable y el jefe de seguridad.
A.8.3	**Manejo de medios**		
A.8.3.1	Gestión de medios removibles	Si	Existe definida las políticas para la gestión de los medios removibles, clasificados conformes a su tipo.

A.8.3.2	Disposición de los medios	SI	Existen lugares seguros para el almacenamiento de los dispositivos móviles.
A.8.3.3	Transferencia de medios físicos	NO	No se trasladan medios fuera del área.

Tabla 45. A.9. Control de acceso.
Aplicabilidad de controles

A.9. **Control de acceso**			
A.9.1 Requisitos del negocio para control de acceso			
ID	Control	Aplicable	Implementación
A.9.1.1	Políticas de control de acceso	SI	La política de control de acceso en sus diferentes niveles se encuentra documentada en las Políticas de la Seguridad de Información.
A.9.1.2	Acceso a redes y a servicios en red	SI	La red de la entidad se halla segmentada y todos los dispositivos conectados deben ser registrados por sus correspondientes MAC para el acceso a la misma. La intranet es sólo accesible desde las unidades académicas.
A.9.2	**Gestión de acceso de usuarios**		
A.9.2.1	Registro y cancelación de registro de usuarios	SI	Se cuenta con la gestión de usuarios y un registro de sus actividades.
A.9.2.2	Clasificación de la información	NO	No aplica.
A.9.2.3	Gestión de derechos de acceso privilegiado	SI	Los directivos poseen privilegios de acuerdo a solicitudes. Los privilegios son documentados y registrados en un perfil de

			usuario con privilegios adicionales.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	SI	Toda clave y el acceso a los sistemas son considerados de modo personal e intransferible. Se obliga al cambio inicial de la clave al primer ingreso y su renovación periódica.
A.9.2.5	Revisión de los derechos de acceso de usuarios	SI	El jefe o responsable de seguridad en conjunto con los Directivos o asignado debe verificar los perfiles, permisos y derechos de acceso de los usuarios de los sistemas. La verificación se realiza periódicamente y se debe realizar registro de lo verificado.
A.9.2.6	Retiro o ajuste de los derechos de acceso	SI	El responsable o jefe de seguridad verifica y ajusta o elimina los permisos de los agentes que sea removido o no pertenezca a un determinado proyecto.
A.9.3	**Responsabilidades de los usuarios**		
A.9.3.1	Uso de información de autenticación secreta	SI	La autenticación de los agentes en los sistemas y la información de los mismos están dada de forma personal y en modo confidencial.
A.9.4	**Control de acceso a sistemas y aplicaciones**		
A.9.4.1	Restricción de acceso a la información	SI	Los perfiles de acceso son determinados por los roles y funciones de cada agente.
A.9.4.2	Procedimiento de ingreso seguro	SI	Los sistemas poseen un inicio de sesión con autenticación cifrada.

A.9.4.3	Sistema de gestión de contraseñas	SI	Los sistemas implementan recuperación de contraseñas de forma automática, exigiendo requisitos para la misma, definidos en las políticas de gestión de contraseñas.
A.9.4.4	Uso de programas utilitarios privilegiados	SI	El responsable o jefe de seguridad verifica en los sistemas críticos que solo se cuente con programas necesarios. Se realizan verificaciones periódicas de forma aleatoria sobre los sistemas.
A.9.4.5	Control de acceso a códigos fuente de programas	SI	Los códigos fuentes de los programas utilizados son verificados de forma periódica por el responsable de seguridad a fin de evitar permisos innecesarios o modificaciones. Se registran alteraciones.

Tabla 46. A.10. Criptografía.
Aplicabilidad de controles

A.10. **Criptografía**			
A.10.1 Controles criptográficos			
ID	Control	Aplicable	Implementación
A.10.1.1	Política sobre el uso de controles criptográficos	SI	Se cuenta con políticas de seguridad documentadas para el uso de controles criptográficos, los algoritmos utilizados y su aplicación.
A.10.1.2	Gestión de llaves	SI	Existe el uso de llaves criptográficas y políticas de seguridad documentadas en

			todo el ciclo de vida de las mismas.

Tabla 47. A.11. Seguridad física y del entorno.
Aplicabilidad de controles

A.11. **Seguridad física y del entorno**			
A.11.1 Áreas seguras			
A.11.1.1	Perímetro de seguridad física	SI	El área posee acceso restringido en el perímetro físico, el mismo es controlado por personal de seguridad y tarjetas de acceso.
A.11.1.2	Controles de acceso físicos	SI	Solo personal autorizado tiene acceso físico a la infraestructura donde se realizan operaciones críticas. Se registran los accesos con fechas y horas de entradas y salidas.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones	SI	El acceso a las oficinas posee seguridad y las llaves están limitadas a personal con privilegios.
A.11.1.4	Protección contra amenazas externas y ambientales	SI	Se cuenta con un Plan de Continuidad del Negocio y de Recuperación de Desastres que es testeado de forma periódica y aleatoria.
A.11.1.5	Trabajo en áreas seguras	NO	No aplica.
A.11.1.6	Áreas de despacho y carga	NO	No aplica.
A.11.2	**Equipos**		
A.11.2.1	Ubicación y protección de los equipos	SI	Los equipos se encuentran alojados en un área especial, protegidos físicamente contra amenazas ambientales de inundación,

			fuego y humo. Se cuenta con políticas de seguridad de la información para su aplicación en el área.
A.11.2.2	Servicios de suministro	SI	Los servicios básicos de suministros como energía eléctrica, agua y ventilación se encuentran conformes a la reglamentación de los mismos. Para la provisión de un nuevo servicio se debe cumplimentar con los protocolos existentes.
A.11.2.3	Seguridad del cableado	SI	La red de datos se halla protegida físicamente y separada del cableado eléctrico previniendo interferencias.
A.11.2.4	Mantenimiento de equipos	SI	Todos los equipos que conforman el área y son mantenidos por personal autorizado. Se lleva registros y planificaciones programadas a intervalos periódicos.
A.11.2.5	Retiro de activos	SI	Se registra y documenta todo retiro de activos, con el conocimiento y aprobación del jefe de seguridad.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones	NO	No aplica.
A.11.2.7	Disposición segura o reutilización de equipos	SI	En caso de reutilización de equipos, se realiza un procedimiento seguro y documentado. Interviene el jefe de mantenimiento y el líder o jefe de seguridad.
A.11.2.8	Equipos de usuario desatendido	SI	Se cuenta con campañas de concientización entre los agentes sobre la seguridad

			de la información y el riesgo existente a los que se exponen los activos.
A.11.2.9	Políticas de escritorio limpio y pantalla limpia	SI	Se garantiza que la información confidencial física se almacena de forma segura, el mismo está dado por el control del jefe de seguridad o responsable del área.

A.12. **Seguridad de las operaciones**			
A.12.1 Procedimientos operacionales y responsabilidades			
ID	Control	Aplicable	Implementación
A.12.1.1	Procedimientos de operación documentados	SI	Se documentan los procedimientos de operaciones relacionadas a la seguridad de la información de todos los activos del área. En el mismo interviene el jefe de seguridad o responsable.
A.12.1.2	Gestión de cambios	SI	Todo cambio que afecte la seguridad de la información es registrado, los mismos incluyen control por el jefe de seguridad. Son planificados y testeados.
A.12.1.3	Gestión de capacidad	SI	Se realiza un monitoreo permanente en los recursos y ante nuevos proyectos por parte del líder técnico o responsable tecnológico.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	SI	La intervención del jefe o responsable de seguridad establece entornos de

			prueba y producción a fin de no comprometer la información.
A.12.2	**Protección contra códigos maliciosos**		
A.12.2.1	Controles contra códigos maliciosos	SI	Se promueve la capacitación permanente y campañas para concientizar sobre los riesgos de la seguridad de la información y la posible explotación por parte de los códigos maliciosos. El responsable de seguridad verifica los antivirus y software de protección en los equipos. Se cuenta con políticas documentadas sobre la utilización de software a utilizar.
A.12.3	**Copias de respaldo**		
A.12.3.1	Respaldo de la información	SI	El responsable o jefe de seguridad realiza las copias de seguridad y verifica los procesos realizados de manera automática conforme las políticas previstas. Los procedimientos son documentados y se realizan pruebas de restauración en periodos programados sobre diferentes entornos.
A.12.4	**Registro y seguimiento**		
A.12.4.1	Registro de eventos	SI	El responsable o jefe de seguridad del área se encarga de verificar los registros de eventos (errores, accesos, etc.) de los usuarios y otros sistemas. El proceso es

			auditado y documentado en su ejecución.
A.12.4.2	Protección de la información de registro	Si	Se establecen controles a implementar para asegurar la protección de los registros del sistema y de las aplicaciones.
A.12.4.3	Registros del administrador y del operador	SI	Se realiza un almacenamiento de los eventos realizados por los administradores y usuarios a fin de evitar modificaciones en su contenido.
A.12.4.4	Sincronización de relojes	SI	El jefe de seguridad o responsable se encarga de asegurarse que todos los sistemas se encuentren ajustados y acordes a 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	La instalación de software y los sistemas operativos en todos los equipos se encuentra documentada en sus procesos de instalación y cumple con las políticas de seguridad.
A.12.6	**Gestión de la vulnerabilidad técnica**		
A.12.6.1	Gestión de las vulnerabilidades técnicas	SI	La evaluación y análisis de riesgos se gestiona a través de metodología sistematizada y documentada.
A.12.6.2	Restricciones sobre la instalación de software	SI	Toda instalación de software en los equipos es realizada por personal autorizado. El software es previamente testeado y la

			instalación se documenta en sus procesos.
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.

Tabla 48. A.13. Seguridad de las comunicaciones.
Aplicabilidad de controles

A.13. **Seguridad de las comunicaciones**			
A.13.1 Gestión de la seguridad de las redes			
ID	Control	Aplicable	Implementación
A.13.1.1	Controles de redes	SI	El encargado o jefe de seguridad en conjunto con el administrador de redes se encargan de implementar una infraestructura de Llave Pública (PKI) a través de algoritmos de cifrado que garanticen la seguridad de la información en las redes.
A.13.1.2	Seguridad de los servicios de red	SI	Existe un monitoreo y control del acceso a la red de los proveedores de servicios.
A.13.1.3	Separación en las redes	SI	Existe segmentación en las redes mediante VLAN y el acceso cuenta con protección. Solamente es posible el acceso desde las facultades que se encuentren en la intranet

			con las MAC debidamente registradas y autorizadas.
A.13.2	**Transferencia de la información**		
A.13.2.1	Políticas y procedimientos de transferencia de información	SI	Los procedimientos y políticas para la transferencia de la información se hallan documentados y bajo los mecanismos necesarios para garantizar la confidencialidad e integridad de la información.
A.13.2.2	Acuerdos sobre transferencia de información	SI	Existen acuerdos y documentación sobre los algoritmos de cifrado utilizados para garantizar la transferencia de la información de forma confidencial y con integridad.
A.13.2.3	Mensajería electrónica	SI	El encargado o jefe de seguridad en conjunto con el administrador de redes se encargan de implementar una infraestructura de Llave Pública (PKI) a través de algoritmos de cifrado que garanticen la seguridad de la información en las redes entre ellos la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación	SI	Existen acuerdos contractuales debidamente documentados donde se estipula el real compromiso de los empleados con el manejo de la seguridad y la confidencialidad de la información.

Tabla 49. Adquisición, desarrollo y mantenimiento de sistemas.
Aplicabilidad de controles

A.14 **Adquisición, desarrollo y mantenimiento de sistemas**			
A.14.1 Requisitos de seguridad de los sistemas de información			
ID	Control	Aplicable	Implementación
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	SI	Los requisitos relacionados a la seguridad de la información para la adquisición de nuevos equipos se encuentran dentro de las políticas de seguridad debidamente documentadas.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	SI	Se establece una política de seguridad para los servicios de aplicaciones en redes públicas, el cual se encuentra correctamente documentada.
A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones	SI	Existe una política definida para la protección de las transacciones en los servicios de aplicaciones.
A.14.2	**Seguridad en los procesos de desarrollo y soporte**		
A.14.2.1	Política de desarrollo seguro	SI	Se cuenta con políticas debidamente documentadas para el desarrollo de aplicaciones seguras. En el mismo se establecen las pautas para de integridad y confidencialidad de la información.
A.14.2.2	Procedimientos de control de cambios en sistemas	SI	Se cuenta con procedimientos para el registro y seguimiento de los controles de cambios realizados en los sistemas.

A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	SI	Se cuenta con documentación a seguir en la implementación de nuevas aplicaciones y los testeos necesarios para evitar impactos. Las pruebas se realizan por el jefe de seguridad y/o encargados con simulaciones críticas en ambientes controlados.
A.14.2.4	Restricciones en los cambios a los paquetes de software	NO	No aplica.
A.14.2.5	Principios de construcción de los sistemas seguros	NO	Existen políticas a seguir para la construcción de sistemas seguros, las mismas se detallan y están previamente documentadas y versionadas.
A.14.2.6	Ambiente de desarrollo seguro	SI	Existen políticas documentadas a seguir para la definición de entornos seguros con datos anonimizados.
A.14.2.7	Desarrollo contratado externamente	NO	No aplica.
A.14.2.8	Pruebas de seguridad de sistemas	SI	El responsable de seguridad y/o encargado se encarga de realizar de forma periódica y aleatoria, distintas pruebas de seguridad donde se documentan los procedimientos aplicados.
A.14.2.9	Pruebas de aceptación de sistemas	SI	Existen diversas pruebas de seguridad a los sistemas previos a su aceptación para el uso. Las mismas son realizadas por los responsables de seguridad y con procedimientos documentados.

A.14.3	Datos de prueba	SI	Todos los datos utilizados en entornos de pruebas son anonimizados o ficticios, no presentan riesgos de violación de confidencialidad. Se verifican su uso por parte de los responsables de seguridad y se registra su utilización.

Tabla 50. A.15. Relaciones con los proveedores.
Aplicabilidad de controles

A.15 **Relaciones con los proveedores**			
A.15.1 Seguridad de la información en las relaciones con los proveedores			
ID	Control	Aplicable	Implementación
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores	SI	Existen políticas de seguridad de la información relacionada con los proveedores la cual se halla documentada.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	SI	Los acuerdos con los proveedores están documentados 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 políticas de seguridad de la información relacionada con los proveedores la cual está documentada.
A.15.2	**Gestión de la prestación de servicios de proveedores**		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores	NO	No aplica.
A.15.2.2	Gestión de cambios en los servicios de los proveedores	SI	Existen políticas de seguridad de la información relacionada con los

			proveedores la cual está documentada.

Tabla 51. A.16. Gestión de incidentes de seguridad de la información.
Aplicabilidad de controles

A.16 **Gestión de incidentes de seguridad de la información**			
A.16.1 Gestión de incidentes y mejoras de la seguridad de la información			
ID	Control	Aplicable	Implementación
A.16.1.1	Responsabilidades y procedimientos	SI	El responsable o el jefe de seguridad y los directivos del área cuentan con la documentación de los procesos y procedimientos relacionados con los incidentes de seguridad. El plan de continuidad de negocio contiene la identificación de los responsables de los mismos.
A.16.1.2	Reporte de eventos de seguridad de la información	SI	Los directivos y responsables de seguridad se encuentran alertados de los eventos e incidentes relacionados con la seguridad de la información. Los incidentes son reportados de forma rápida, evaluados y posteriormente documentados. Se establecen los procedimientos a seguir conforme la gravedad.
A.16.1.3	Reporte de debilidades de seguridad de la información	SI	Existen los formatos documentados disponibles para que los directivos o responsables del área reporten las debilidades de la seguridad de la información. Estas

			notificaciones son evaluadas de forma inmediata por el Jefe de Seguridad y registradas.
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	SI	Existen formatos disponibles para los reportes de debilidades o fallas de seguridad halladas en el área, los mismos se encuentran documentados. Estos reportes son analizados por el jefe de seguridad o encargado de manera inmediata a fin de tomar medidas.
A.16.1.5	Respuesta a incidentes de seguridad de la información	NO	Ante los incidentes hallados, el jefe de seguridad o bien el responsable tiene la correspondiente información para responder de forma segura ante los mismos. El Plan de Continuidad de Negocio está definido y cuenta con los responsables de ejecución de cada proceso.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	SI	Toda la información obtenida de los incidentes de la seguridad de la información son documentados y registrados en un base de conocimiento, en la misma se especifican las vulnerabilidades, amenazas, riesgos y los posibles controles de seguridad a implementar.
A.16.1.7	Recolección de evidencia	SI	Al momento de recolectar la evidencia de los eventos, existen formatos

			documentados para la recolección de los mismos e informes modelos para elevar a las autoridades correspondientes.

Tabla 52.A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio. Aplicabilidad de controles

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			
ID	Control	Aplicable	Implementación
A.17.1.1	Planificación de la continuidad de la seguridad de la información	SI	El jefe de seguridad o responsable de la misma en forma conjunta con los directivos del área planifican los pasos a seguir para la continuidad del negocio luego de eventos e incidentes de seguridad. En el mismo se cuenta con los responsables de ejecución de cada proceso o activo.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	SI	El jefe de seguridad o persona a cargo en forma conjunta con los indicados como responsables de activos y/o procesos, serán los encargados de implementar la continuidad del negocio conforme el plan previsto y documentado, el mismo debe cumplir las políticas establecidas.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	El jefe de seguridad o persona a cargo en forma conjunta con los indicados como responsables de activos y/o procesos, serán

			los encargados de verificar, revisar y evaluar la continuidad del negocio conforme el plan previsto y documentado, el mismo debe cumplir las políticas establecidas en los mismos.
A.17.2	**Redundancias**		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información	SI	Existe un detalle específico en el plan de continuidad de negocio en el cual se establece la infraestructura disponible para realizar todo el procesamiento de la información en forma segura. El mismo se encuentra conforme a las políticas de seguridad de la información del área y está documentado.

Tabla 53. A.18. Cumplimiento.
Aplicabilidad de controles

A.18 Cumplimiento			
A.18.1 Cumplimiento de los requisitos legales y contractuales			
ID	Control	Aplicable	Implementación
A.18.1.1	Identificación de la legislación aplicable a los requisitos contractuales	SI	Se encuentran identificados los requisitos contractuales que se deben cumplir de acuerdo a lo requerido por la reglamentación actual. Los mismos se hallan documentados, se actualizan conforme a nuevas normativas y se verifica su cumplimiento.
A.18.1.2	Derechos de propiedad intelectual	NO	Todo el software o documentación creada en el área está bajo la propiedad

			de la DGLH, no obstante no existe reglamentación
A.18.1.3	Protección de registros	SI	Toda la información crítica del área se encuentra protegida físicamente contra la modificación, alteración, eliminación y acceso no autorizado por personal no autorizado.
A.18.1.4	Privacidad y protección de información de datos personales	SI	Toda la información de tipo personal, se encuentra protegida y almacenada conforme a la política de protección de datos vigente.
A.18.1.5	Reglamentación de controles criptográficos	SI	Existe reglamentación relacionada sobre la implementación de una infraestructura de llave pública (PKI) y los algoritmos de cifrado para garantizar la confidencialidad e integridad de la información.
A.18.2	**Revisiones de seguridad**		
A.18.2.1	Revisión independiente de la seguridad de la información	SI	Las auditorías internas poseen documentación necesaria para la ejecución de las mismas en el Sistema de Gestión de la Seguridad de la Información a fin de obtener una mejora continua.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad	SI	La documentación existente sobre auditoría interna del Sistema de Gestión de la Seguridad de la Información permite verificar el nivel de cumplimiento de los

			controles y políticas de la seguridad del área.
A.18.2.3	Revisión del cumplimiento técnico	SI	Se cuenta con la documentación que avala la ejecución periódica de test internos de penetración en el área de seguridad de la información.

5.3 Validación de los resultados obtenidos

5.3.1 Nivel de Cumplimiento de la norma ISO/IEC 27001:2013

Objetivo específico: Determinar el estado actual de cumplimiento de la Norma ISO/IEC 27001:2013 en el área de TI de la DGLH de la Universidad Nacional del Nordeste.

Indicador del logro: Informe de análisis de la DGLH

Métricas a utilizar:

- Porcentaje de cumplimiento de los puntos o cláusulas propuestas en la Norma ISO/IEC 27001:2013
- Porcentaje de cumplimiento de los dominios propuestos en la Norma ISO/IEC 27002:2013

Indicador N° 1					
ID:	METRICA1	**Fecha:**	01/12/2020	**Versión:**	1.0
Frecuencia:	Semestral (recolección e informes)			**Formato:**	Gráfico de barras
Nombre:	Nivel de cumplimiento de la norma ISO/IEC 27001:2013				
Objetivo:	Determinar el nivel de madurez de la norma ISO/IEC 27001:2013 y de los controles propuestos para el SGSI.				
Fuente:	Informe realizado sobre objetivos de control y dominios de la norma ISO/IEC 27001:2013 de la DGLH. Ver Anexos 1 y 2.				

Fórmulas de los cálculos aplicados:	Estado de cumplimiento del SGSI = (Total de nivel de madurez actual/Cantidad de cláusulas aplicables) * 100
	Nivel de madurez de los controles = (Total de grado de cumplimiento actual/Cantidad de controles aplicables) * 100
Indicador:	5: Nivel óptimo alcanzado. 4. Nivel deseado, se debe monitorizar y medir. 3: Existen procedimientos, sin embargo, hay incumplimientos. 2: No existen procedimientos, se requiere observación para no llegar al nivel rojo. 1: Se requiere intervención reevaluación de los riesgos.

Detalles

Este indicador precisa del informe detallado del nivel de madurez que presenta el área de TI de la DGLH y de cada uno de los controles de seguridad de la información obtenidos en las entrevistas y encuestas realizadas. Seguidamente tomando las evaluaciones de cumplimiento propuestas por la Norma ISO/IEC 27001:2013 y de los dominios correspondientes de la Norma ISO/IEC27002:2013 donde cada indicador representa los valores de:

- Requisitos: grado de cumplimiento actual de la Norma ISO/IEC 27001:2013 (cláusulas del 4 al 10).
- Controles: grado de cumplimiento actual de la Norma ISO/IEC 27002:2013 (dominios del 5 al 18)

Aplicando los datos a las fórmulas presentadas anteriormente se obtendrá un reporte gráfico que permitirá obtener un reporte para el posterior análisis y evaluación, se pueden observar de forma gráfica en Fig. 16 .

Consideraciones

Se propone una frecuencia de actualización semestral para la revisión de las métricas, las que estarán definidas por el responsable o persona a cargo del SGSI.

Resultados

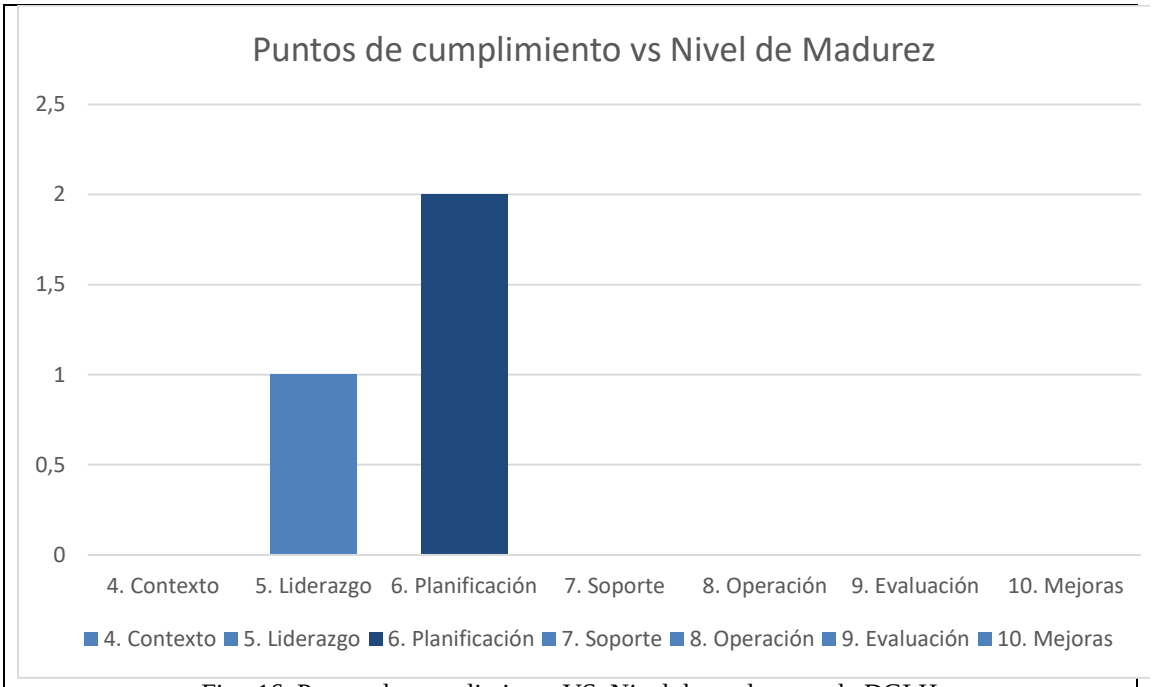

Fig. 16. Puntos de cumplimiento VS. Nivel de madurez en la DGLH
Fuente: Elaboración propia.

Conforme los gráficos observados en los puntos a considerar de la Norma ISO/IEC 27001:2013, la mayoría de ellos poseen un nivel de "No diseñado", motivo suficiente para determinar que los controles existentes no se hallan correctamente preparados.

5.3.2 Determinación de activos críticos

Objetivo específico: Identificar los activos de información críticos en el área de TI de la DGLH de la Universidad Nacional del Nordeste.

Indicador del logro: Inventario de activos de información.

Métricas a utilizar:

- Porcentaje de activos críticos de información.

Indicador N° 2					
ID:	METRICA2	**Fecha:**	12/12/2020	**Versión:**	1.0
Frecuencia:	Semestral (recolección e informes)			**Formato:**	Gráfico de barras

Nombre:	Determinación de activos críticos
Objetivo:	Determinar los activos críticos identificados dentro del área de TI de la DGLH
Fuente:	Inventario de activos de información del área de TI de la DGLH, obtenidos a través de encuestas con las áreas correspondientes. Ver en Tabla 38. *Listado de activos de TI del Área de la DGLH.* *Fuente: Elaboración propia*
Fórmulas de los cálculos aplicados:	Porcentaje de activos críticos = (Total de activos críticos/Total de activos de información) * 100
Indicador:	Rojo > 60% Amarillo entre 30 y 60% Verde < 30 % Rojo: la mayor cantidad de activos son críticos Amarillo: Parcialmente son críticos Verde: la mayor cantidad de activos no son críticos

Detalles

Este indicador precisa del inventario de activos del área de TI de la DGLH, el cual fue registrado para el presente trabajo, en el mismo se detalla los activos de información de la oficina de la DGLH de la UNNE.

A fin de obtener la información correspondiente se realizaron encuestas con la Directora del área y el personal a cargo de la seguridad informática y técnica. Mediante esta tarea se pudo determinar cuáles son los activos de información que están involucrados en los procesos que se realizan en el área.

A continuación se les determinó el valor de cada uno de ellos de acuerdo a tus importancia y criticidad para la oficina de la Liquidaciones, tomando como referencia el nivel de pérdida o afectación que puede llegar a provocar en la DGLH si se llegase a materializar algún tipo de amenaza sobre los activos de la misma. La escala utilizada

conforme a Magerit se halla en la Escala de Valores de Activos, Tabla 9 . Este indicador representa los siguientes valores:

- Críticos: cantidad de activos con valor ALTO o MUY ALTO
- Total: cantidad de activos de información

Aplicando los datos a las fórmulas presentadas anteriormente se obtendrá un reporte gráfico que permitirá obtener un reporte para el posterior análisis y evaluación, los mismos se pueden observar en Fig. 17 .

Consideraciones

Se propone una frecuencia de actualización semestral para la revisión de las métricas, las que estarán definidas por el responsable o persona a cargo del SGSI.

Se aconseja realizar periódicamente la recolección de los datos de activos ya que estos pueden variar y afectar considerablemente los resultados del informe.

Resultados

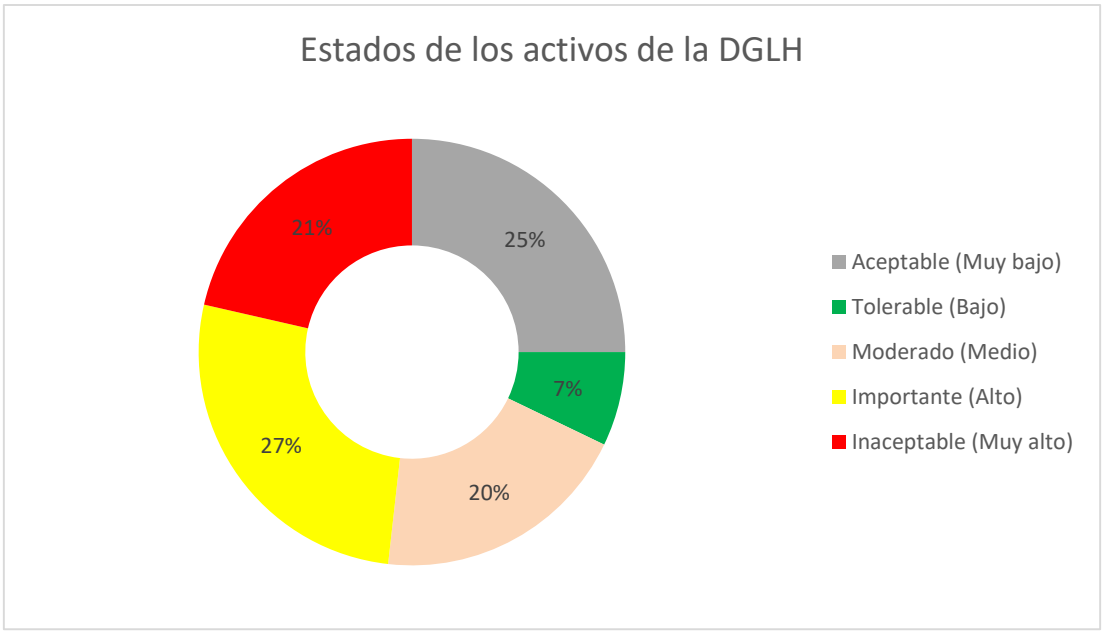

Fig. 17. Estado de los activos de la DGLH

Fuente: Elaboración propia

5.3.3 Identificación y evaluación de riesgos

Objetivo específico: Identificar los riesgos críticos en el área de TI de la DGLH de la Universidad Nacional del Nordeste.

Indicador del logro: Matriz de riesgos.

-	**Indicador N° 3**				
ID:	METRICA3	**Fecha:**	18/12/2020	**Versión:**	1.0
Frecuencia:	Anual (recolección e informes)			**Formato:**	Gráfico de barras
Nombre:	Determinación de riesgos críticos				
Objetivo:	Determinar los riesgos críticos identificados dentro del área de TI de la DGLH que podrían afectar los procesos más importantes de la misma.				
Fuente:	Matriz de riesgos. Ver detalles en Tabla 40. *Identificación de riesgos de activos de la DGLH, análisis y evaluación de riesgos. Fuente: Elaboración propia.*				
Fórmulas de los cálculos aplicados:	Porcentaje de riesgos críticos = (Total de riesgos críticos/Total de riesgos) * 100				
Indicador:	Rojo > 60% Amarillo entre 30 y 60% Verde < 30 % Rojo: la mayor cantidad de activos son críticos Amarillo: Parcialmente son críticos Verde: la mayor cantidad de activos no son críticos				
Detalles					
Este indicador precisa del informe extraído a partir de la matriz de Análisis y Evaluación de Riesgos del área de TI de la DGLH, el cual fue registrado para el presente trabajo, en el mismo se detalla los riesgos que presenta en los procesos de la oficina de la DGLH de la UNNE, además de los incidentes que pudieran ser catalogados como 'riesgo'.					

El objetivo con este indicador es visualizar los riesgos críticos de seguridad de la información del área y en caso que se materialice el evento de riesgo, cuáles son las pérdidas posibles.

A fin de obtener la información correspondiente se realizaron encuestas con la Directora del área y el personal a cargo de la seguridad informática y técnica. Este indicador representa los siguientes valores:

- Críticos: cantidad total de riesgos hallados como críticos.
- Total: cantidad total de riesgos identificados

Para el cálculo correspondiente se utilizará la fórmula propuesta en el indicador.

Aplicando los datos a las fórmulas presentadas anteriormente se obtendrá un reporte gráfico que permitirá obtener un reporte para el posterior análisis y evaluación.

Consideraciones

Se propone una frecuencia de actualización anual para la revisión de las métricas, las que estarán definidas por el responsable o persona a cargo del SGSI. Se aconseja realizar una actualización anual de la matriz de riesgos.

Resultados

Resultados: Los resultados obtenidos a partir de este indicador son de rangos altos debido a que la Dirección aún no posee una metodología para la gestión de los riesgos detectados en sus activos de información.

Mejoras: En esta etapa del proyecto de diseño de un SGSI no considera la inclusión de mejoras en la gestión de riesgos o en su implementación.

5.4 Matriz de riesgos

Tabla 54. Matriz de probabilidad e impacto general de la DGLH

Matriz de Probabilidad e Impacto		Impacto				
		Muy Bajo 1	Bajo 2	Moderado 3	Alto 4	Muy Alto 5
Probabilidad	Muy Baja 1	4	0	0	0	3
	Baja	2	3	3	0	

	2					
	Moderada 3	5	1	3	7	2
	Alta 4	0	1	0	1	1
	Muy Alta 5	1	3	5	1	10

Tabla 55. Matriz de probabilidad e impacto de la categoría Hardware (HW)

Matriz de Probabilidad e Impacto		Impacto				
		Muy Bajo 1	Bajo 2	Moderado 3	Alto 4	Muy Alto 5
Probabilidad	Muy Baja 1	3	0	0	0	0
	Baja 2	0	0	2	0	0
	Moderada 3	3	0	1	0	0
	Alta 4	0	0	0	1	0
	Muy Alta 5	0	0	1	0	2

Tabla 56. Matriz de probabilidad e impacto de la categoría Software (SW)

Matriz de Probabilidad e Impacto		Impacto				
		Muy Bajo 1	Bajo 2	Moderado 3	Alto 4	Muy Alto 5
Probabilidad	Muy Baja 1	0	0	0	0	0
	Baja 2	0	0	0	0	0
	Moderada 3	0	0	1	7	0
	Alta 4	0	1	0	0	0

	Muy Alta 5	0	0	0	0	1

Tabla 57. Matriz de probabilidad e impacto de la categoría Datos (D)

Matriz de Probabilidad e Impacto		Impacto				
		Muy Bajo 1	Bajo 2	Moderado 3	Alto 4	Muy Alto 5
Probabilidad	Muy Baja 1	0	0	0	0	0
	Baja 2	0	0	0	0	0
	Moderada 3	0	0	0	0	1
	Alta 4	0	0	0	0	1
	Muy Alta 5	0	2	2	1	3

5.4 Análisis de resultados de la implementación del SGSI

Conforme los datos presentados se pueden observar que en la oficina de la DGLH y en lo que respecta al área de TI de la Universidad Nacional del Nordeste, los riesgos allí hallados se pueden clasificar dentro de las zonas de riesgo inaceptable (MA) y riesgo importante (A) sobre los cuales se debe prestar el mayor cuidado posible. Los mismos se basan principalmente en el correcto funcionamiento del hardware y los sistemas que allí se ejecutan, los datos que allí se almacenan y procesan además de las redes de comunicaciones, fundamentalmente en la disponibilidad de los datos para la correcta operación de los procesos y servicios denominados críticos.

Uno de los riesgos más importantes son las posibles filtraciones de la información allí alojada y de la alteración, modificación o eliminación de los mismos, las cuales se pueden dar por accesos no autorizados, violación en la confidencialidad de los datos por ausencia de mecanismos de encriptación y/o cifrado en las comunicaciones.

Por otro lado, todo el software de uso ofimático y los equipos que intervienen en el área administrativa no presentan riesgos importantes, por lo cual se pueden catalogar en una zona de riesgo muy bajo (MB) a medio, ya que estos no forman parte de los procesos críticos del área.

La falta de personal de seguridad de manera proactiva, cámaras de vigilancia, accesos de control, control biométrico y el control de acceso personal tanto técnico y administrativo podría ocasionar daños voluntarios o involuntarios en los equipos (hardware) y en los servicios que allí se prestan.

Por su parte, las posibilidades de catástrofes naturales son relativamente bajas puesto que el centro de datos y la oficina de la DGLH no se encuentran en lugares muy próximos a los ríos o expuestas a temperaturas realmente extremas. Tampoco se registran fuerzas naturales de nivel destructivo como tornados o huracanes.

Se puede observar que los riesgos hallados se encuentran catalogados como MUY ALTOS y ALTOS, ello se puede visualizar la correspondiente valoración en Fig. 18.

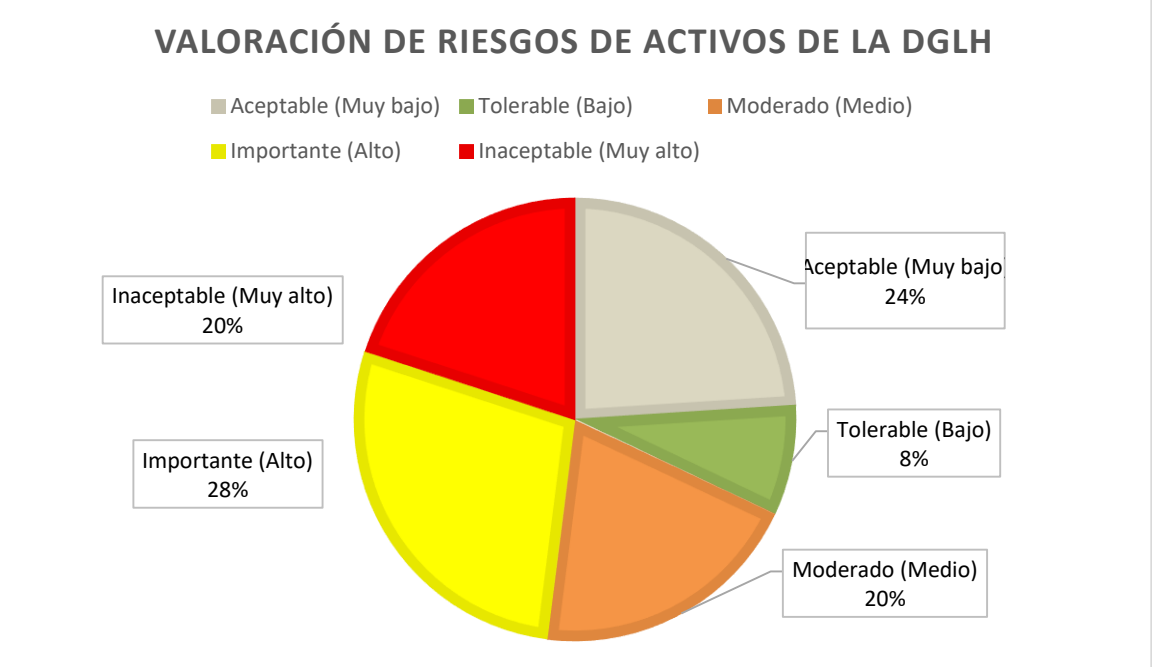

Fig. 18. Gráfica de valoración de los riesgos del área TI de la DGLH
Fuente: Elaboración propia.

5.5 Discusiones y Comentarios

Presentado y descripto el SGSI propuesto para el área de la DGLH de la UNNE en el capítulo anterior, analizados y validados los resultados obtenidos de la ejecución del plan de pruebas en cuanto al nivel de cumplimiento de normas y dominios, objetivos de control, evaluación de riesgos informáticos, aplicabilidad de los controles, determinación de los activos existentes y análisis general de los resultados de la implementación del SGSI mediante la utilización de métricas específicas, se puede concluir que el sistema propuesto permitió obtener un diagnóstico certero de la situación actual del área de tecnología de la información del área bajo estudio en cuanto a seguridad de la información, resaltando las vulnerabilidades existentes y clasificándolas según su impacto, lo cual permite priorizar las cuestiones más urgentes, facilitando así la toma de decisiones a nivel gerencial.

Capítulo 6
Conclusiones

A continuación en el capítulo 6, se presentan las conclusiones que se obtuvieron luego de realizar las pruebas conforme al SGSI propuesto para el área de TI de la DGLH de la UNNE, en el mismo se detalla a través de un análisis los beneficios que se proponen mediante su implementación y se sugieren medidas futuras de acción.

6.1 Conclusiones

A pesar que el uso de la tecnología nos presenta elementos para obtener ventajas y beneficios ante competidores, en la gestión de procesos y administración del tiempo, los sistemas de información y el uso adecuado de las TIC, éstas presentan riesgos que en muchos casos son desconocidos o no tratados de manera adecuada por los encargados de la gerencia o la dirección de las organizaciones. O bien no se invierte en ellos para hacer frente a los problemas que la seguridad de la información intenta cubrir con la implementación de modelos adecuados.

En el análisis realizado a través de este proyecto, se pudo obtener de manera real, los beneficios y oportunidades que trae aparejado el diseño e implementación de un SGSI en cualquier tipo de organización, considerando puntualmente el caso del área TI de la oficina de la DGLH de la Universidad Nacional del Nordeste, tomando como referencia la aplicación de la norma ISO/IEC 27001:2013, al cual a través de su fase de diseño para establecer la documentación requerida conforme a la misma y su planteamiento de mejora continua.

Con el desarrollo del mismo se pudo obtener el estado actual de los dominios, objetivos y controles de seguridad de la información del área. Los cuales a través del análisis diferencial y el detalle del nivel de cumplimiento tomando como base al Anexo A de la Norma ISO 27001:2013 se pudo elaborar las Políticas de Seguridad de la Información de forma general para el área TI de la DGLH, las cuales deberían ser informadas a cada uno de los empleados que integran la Dirección con el compromiso de promover el uso de buenas prácticas y llevar los niveles de riesgos de sus activos de información en niveles aceptables.

Como tarea importante, se pudo clasificar los activos de información del área y a su vez determinar el nivel de riesgo potencial que los afecta. Para lograrlo se aplicó la metodología de gestión de riesgos de TI propuesta por Magerit, en la misma se identifican los activos y procesos críticos, los cuales revelan mayor importancia en la organización, y a los que se debe prestar mayor seguimiento y aplicar los controles de seguridad necesarios dado el impacto que presentan en los servicios y procesos esenciales del área.

Como propuesta se obtuvo un documento que plantea un Plan de Continuidad de Negocio con el objetivo de mantener los servicios en funcionamiento o bien reestablecerlos en el menor tiempo.

Líneas futuras de acción

Conforme al análisis realizado y a fin de obtener beneficios del presente proyecto, se recomienda que el diseño de un SGSI sea implementado en el área TI de la oficina de la DGLH de la Universidad Nacional del Nordeste. Además, se sugiere que el mismo sea acompañado no solamente por la Dirección de la misma, sino que también sea elevado al área TI del Instituto Rectorado y también generalizado a otras áreas de la Universidad conforme al cumplimiento de la misión y objetivos estratégicos, es decir alineados a los mismos en un nivel más amplio.

Se recomienda el desarrollo de herramientas de software para la gestión de riesgos a fin de obtener los valores de riesgo potencial y residual de los activos, realizar comparaciones con niveles de riesgo aceptables y poder actuar en consecuencia, aceptándolos o mitigándolos. En caso de no contar con el equipo técnico para el desarrollo de la aplicación se podría evaluar la compra de un software que satisfaga los requerimientos. Asimismo se aconseja la inclusión de otros indicadores adicionales a fin de tener métricas que permitan observar las mejoras posibles.

A fin de estar actualizados de forma permanente ante amenazas a los activos de información, se promueve la participación en listas técnicas, en foros especializados en seguridad y vulnerabilidades. La participación activa en comunidades permitirá no solo

mostrar presencia institucional, sino, además, obtener retroalimentación sobre las cuestiones relacionadas a la seguridad.

Por último, se sugiere la incorporación adicional de personal técnico capacitado en temas relacionados con la seguridad, manejo de activos y procesos informáticos a efectos de acompañar la viabilidad y concreción del proyecto de un SGSI.

Referencias

[1] H. Kuna. "Curso de Auditoria y Seguridad Informática". Facultad de Ciencias Exactas Naturales y Agrimensura. Universidad Nacional del Nordeste. Corrientes, Argentina, 2017

[2] M. Raffino. "¿Que es seguridad?", [Online]. Disponible en: https://concepto.de/seguridad/. [Fecha de consulta: 23/09/2021]

[3] S. M. Valencia, M. Quiroz Zambrano y D. G. Macías. "Seguridad Informática 3era ed. Vol.3", Polo de Capacitación, Investigación y Publicación (POCAIP), 2017

[4] J. A. Bertolín. "Seguridad de la Información. Redes, Informática y Sistemas de Información", Buenos Aires, Argentina, Paraninfo, 2008

[5] P. López. "Seguridad Informática", España, Madrid, Editex S.A., 2010

[6] M. Agé, S. Baudru, R. Crocfer, N. Crocfer, F. Ebel, J. Hennecart, S. Lasson, D. Puche y R. Rault. "Seguridad informática: Ethical Hacking", España, Barcelona, Eni Ediciones, 2015

[7] N. F. García, J. S. Delgado y S. V. Rodríguez. "Seguridad activa y pasiva", [En línea]. Disponible en: https://sites.google.com/site/seguridadinformaticasjn/seguridad-activa-y-pasiva. [Fecha de consulta: 06/11/2021]

[8] R.A.E., "Real Academia Española", [En línea]. Disponible en: http://lema.rae.es/drae/srv/search?key=riesgo . [Fecha de consulta: 03/09/2021]

[9] D. Kim and M. G. Solomon. "Fundamentals of Information System Security" Jones & Bartlett Learning, 2nd edición, USA, Learning International, 2012

[10] J. M. Stewart, E. Tittel, M.Chapple. "CISPP: Certified Information Systems Security Professional Guide 5th.", USA, Wiley Publishing, 2011

[11] R. M. Martin.. "Information Security Risk Assessment Toolkit: Practical Assessment Throught Data Collection and Data Analysis", USA, Syngres Publishing, 2013

[12] A. G. Alexander, D. Buitrago y L. Javier. "Diseño de un Sistema de Gestión de Seguridad de Información" óptica ISO 27001, Colombia, Alfaomega, 2015

[13] ISOTools Excellence. "Metodología Mehari para el análisis de Riesgos en SGSI", [En línea]. Disponible en: https://www.pmg-

ssi.com/2021/09/metodologia-mehari-para-el-analisis-de-riesgos-en-sgsi/. [Fecha de consulta: 23/09/2021]

[14] A. Huerta. "Introducción al análisis de riesgos – Metodologías (I), CRAMM", 2012. [En línea]. Disponible en: https://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/. [Fecha de consulta: 08/11/2021]

[15] J.J. Montenegro Hoyos y M.C. Rivera Restrepo. "Risk IT como complemento a la gestión de riesgos en compañías de la industria de software", [En línea]. Disponible en: https://repository.icesi.edu.co/biblioteca_digital/bitstream/10906/68005/1/rivera_gestion_software_2011.pdf . [Fecha de consulta: 23/09/2021]

[16] ISOTools Excellence. "Metodología NIST SP 800 para el análisis de Riesgos en SGSI", [En línea]. Disponible en: https://www.pmg-ssi.com/2021/08/metodologia-nist-sp-800-30-para-el-analisis-de-riesgos-en-sgsi/. [Fecha de consulta: 23/09/2021]

[17] A. Huerta. "Análisis de Riesgos con Magerit en el ENS (I)", 2012. [En línea]. Disponible en: https://www.securityartwork.es/2012/04/24/analisis-de-riesgos-con-magerit-en-el-ens-i/. [Fecha de consulta: 08/11/2021]

[18] M. A. Amutio Gómez, J. Candau y J.A. Mañas. "Magerit V. 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de información", Madrid, España, Ministerio de Hacienda y Administraciones Públicas, 2012

[19] Ministerio de Hacienda y Administraciones Públicas de España. "Magerit V.3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" - Libro I - Método, Madrid, España, 2012

[20] R. Caralli, J. Stevens, L. Young y W. Wilson. "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania, Technical Report CMU/SEI-2007-TR-012, 2007 [En línea]. Disponible en: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419 .[Fecha de consulta: 08/11/2021]

[21] ISO/IEC 27001. Tecnologías de la Información, Técnicas de seguridad, Sistemas de Gestión de la Seguridad de la Información, [En línea]. Disponible en: https://normaiso27001.es/liderazgo-en-iso-27001/#h3. [Fecha de consulta: 25/07/2021]

[22] ISO/IEC 3100. “Gestión del riesgo, Directrices”, [En línea]. Disponible en: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es. [Fecha de consulta: 04/09/2021]

[23] ISO/IEC 27001, Tecnologías de la Información, Técnicas de seguridad, Sistema de Gestión de la Seguridad de la Información, Requisitos, [En línea]. Disponible en: https://www.iso.org/standard/54534.html [Fecha de consulta: 01/08/2021]

[24] ISO/IEC 27002, Tecnologías de la Información, Técnicas de seguridad, Código de buenas prácticas de la Seguridad de la Información, [En línea]. Disponible en: http://www.iso27000.es/iso27002.html. [Fecha de consulta: 11/09/2021]

Anexos

Anexo 1. Análisis GAP de los puntos de la norma ISO/IEC 27001:2013 de la DGLH

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
4	**CONTEXTO DE LA ORGANIZACIÓN**			
4.1	**Comprender la organización y su contexto**			
	Comprender la organización y su contexto La organización debe determinar los asuntos externos e internos que son importantes para su objetivo y que afecte su capacidad para lograr el(los) resultados(s) esperado(s) de su sistema de gestión de la seguridad de la información.	No diseñado	1	La organización cuenta con misión y objetivos definidos, no obstante en lo que respecta a la seguridad informática no existen planes sólidos. Se sugiere incluir planes de seguridad de la información.
4.2	**Comprender las necesidades y expectativas de las partes interesadas**			
	La organización debe determinar : a) Las partes interesadas que son pertinentes para el SGSI	No diseñado	1	Se sugiere determinar las partes interesadas en base a las expectativas y necesidades del área.
	b) Los requisitos de estas partes interesadas que sean pertinentes para la seguridad de la información	No diseñado	1	Se sugiere determinar los requisitos relevantes del área.
4.3	**Determinar el alcance del SGSI**			
	La organización debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance	No diseñado	1	Se sugiere determinar los límites de aplicabilidad del SGSI.
	Cuando se determina el alcance de la organización se debe considerar: a) los aspectos externos e internos referidos en 4.1	No diseñado	1	Se recomienda tener en cuenta los aspectos sugeridos en el punto indicado.

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	b) Los requisitos referidos en 4.2	No diseñado	1	
	c) Las interfaces y dependencias entre las actividades de la organización y aquellas realizadas por otras organizaciones	No diseñado	1	
	El alcance está disponible como información documentada	No diseñado	1	
4.4	Sistema de gestión de seguridad de la información			
	La organización debe establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información, según los requerimientos de esta norma.	No diseñado	1	Es aconsejable establecer un SGSI a fin de aplicar un plan para la mejora continua.
5.	**LIDERAZGO**			
5.1	**Liderazgo y compromiso**			
	La alta dirección debe demostrar liderazgo y compromiso con respecto al SGSI: a) asegurar que los objetivos de la política de seguridad de la información y la seguridad de la información se establezcan y sean compatibles con la dirección estratégica de la organización.	No diseñado	2	
	b) asegurar la integración de los requisitos del sistema de gestión de la seguridad de la información a los procesos de la organización;	No diseñado	2	
	c) Asegurar que los recursos necesarios para el SGSI estén disponibles	No diseñado	2	La Dirección debe asegurar los recursos necesarios con el presupuesto para implementar y gestionar el SGSI.
	d) Comunicar la importancia de la seguridad de la información efectiva y del cumplimiento de los requisitos del SGSI.	No diseñado	1	
	e) Asegurar que el SGSI logre los resultados esperados.	No diseñado	1	

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	f) Dirigir y apoyar a las personas para que contribuyan a la eficacia del SGSI	No diseñado	1	
	g) Promover la mejora continua.	No diseñado	1	
	h) Apoyar otros roles de gestión relevantes para demostrar su liderazgo, según corresponda a sus áreas de responsabilidad.	No diseñado	1	
5.2	**Política**			
	a) La alta dirección debe establecer una política de seguridad de la información que sea pertinente con el objetivo de la organización.	No diseñado	1	Se sugiere establecer dentro de los objetivos de seguridad de la información de la DGLH, conforme el punto 6.2 estableciendo las políticas necesarias para la oficina, haciéndola disponible para toda la Dirección.
	b) La alta dirección debe establecer una política de seguridad de la información que incluya los objetivos de seguridad de la información o que proporcione el marco de trabajo para establecer los objetivos de seguridad dela información.	No diseñado	1	
	c) La alta dirección debe establecer una política de seguridad de la información que incluya un compromiso para la mejora continua del sistema de gestión de la seguridad de la información.	No diseñado	1	
	d) La política de seguridad de la información debe ser comunicada dentro de la organización y estar disponible para las partes interesadas, según corresponda.	No diseñado	1	
	e) La política de seguridad de la información debe estar disponible como información documentada.	No diseñado	1	
	f) La política de seguridad de la información debe ser comunicada dentro de la organización.	No diseñado	1	
	g) La política de seguridad de la información debe estar disponible para las partes interesadas, según corresponda.	No diseñado	1	
5.3	Roles, responsabilidades y autoridades organizacionales	No diseñado	1	

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	La alta dirección debe asegurar que las responsabilidades y las autoridades para los roles pertinentes a la seguridad de la información son asignados y comunicados.	Parcialmente diseñado	2	
	a) La alta dirección debe asignar la responsabilidad y la autoridad para asegurar que el SGSI cumpla con los requisitos de esta norma.	No diseñado	1	
	b) La alta dirección debe asignar la responsabilidad y la autoridad para informar a la alta dirección sobre el desempeño del SGSI.	Parcialmente diseñado	2	Se debe designar de manera formal el responsable de seguridad del área, el que reportará a la Dirección sobre el SGSI y llevará las funciones del cargo.
6	**PLANIFICACION**			
6.1	**Acciones para tratar los riesgos y las oportunidades**			
6.1.1	**Generalidades**			
	Al planificar el SGSI, la organización debe considerar los requisitos tratados en 4.1 y 4.2, y determinar los riesgos y oportunidades que necesitan ser cubiertos para: a) Asegurar que el S.GSI pueda lograr los resultados esperados; b) Evitar o disminuir efectos no deseados; y c) Lograr una mejora continua	No diseñado	1	
	La organización debe planificar: d) Acciones para abordar estos riesgos y oportunidades; y	No diseñado	1	
	e) Como: 1. integrar e implementar las acciones en los procesos del sistema de gestión de seguridad de la información; y 2. evaluar la eficacia de estas acciones	No diseñado	1	
6.1.2	**Evaluación de riesgo de la seguridad de la información**			

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	La organización debe definir y aplicar un proceso de evaluación de riesgo de la seguridad de la información que: a) Establezca y mantenga los criterios de riesgo de la seguridad de la información que incluya: 1. los criterios de aceptación del riesgo; y 2. los criterios para realizar las evaluaciones de riesgo de la seguridad de la información;	No diseñado	1	Se recomienda la definición de procedimientos para mantener los criterios mínimos en la valoración de los riesgos del área.
	b) Asegure que las evaluaciones de riesgo de la seguridad de la información producen resultados consistentes, válidos y comparables, una y otra vez;	No diseñado	1	
	c) Identifica los riesgos de la seguridad de la información: 1. aplica el proceso de evaluación del riesgo de la seguridad de la información para identificar los riesgos asociados a la pérdida de la confidencialidad, integridad y disponibilidad para la información dentro del alcance del SGSI; y 2. identifica los propietarios del riesgo;	No diseñado	1	Se sugiere hallar una metodología adecuada para la gestión de los riesgos de seguridad de la información del área.
	d) Analiza los riesgos de la seguridad de la información; 1. Evalúa las posibles consecuencias que podrían resultar si los riesgos identificados en 6.1.2. c) 1. Se hicieran realidad; 2. Evalúa la probabilidad realista de la ocurrencia de los riesgos identificados en 6.1.2 c) 1.; y 3. determina los niveles de riesgo;	No diseñado	1	
	e) Evalúa los riesgos de la seguridad de la información; 1. Compara los resultados del análisis de riesgo con los criterios de riesgo definidos en 6.1.2 a); y 2. Prioriza los riesgos analizados para el tratamiento de riesgo.	No diseñado	1	

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	La organización debe conservar la información documentada acerca del proceso de evaluación de riesgo de la seguridad de la información.	No diseñado	1	
6.1.3	**Tratamiento de riesgos de la seguridad de la información**			
	La organización debe definir y aplicar un proceso de tratamiento de riesgo de la seguridad de la información para:	No diseñado	1	
	a) Seleccionar las opciones apropiadas de tratamiento de riesgo de la seguridad de la información, tomando en consideración los resultados de la evaluación de riesgo;	No diseñado	1	
	b) determinar todos los controles que son necesarios para implementar las opciones de tratamiento de riesgo de la seguridad de la información escogida;	No diseñado	1	
	c) comparar los controles definidos en 6.1.3 b) más arriba con aquellos en Anexo A y verificar que ningún control necesario fue omitido;	No diseñado	1	
	d) generar una Declaración de Aplicabilidad que contenga los controles necesarios [consultar 6.1.3 b) y c), y además la justificación de inclusiones, sean estas implementadas o no y la justificación para exclusiones de controles de Anexo A;	No diseñado	1	
	e) formular un plan de tratamiento del riesgo de seguridad de la información; y	No diseñado	1	
	f) obtener la aprobación del propietario del riesgo del plan de tratamiento del riesgo de la seguridad de la información y la aceptación de los riesgos de la seguridad de la información residual.	No diseñado	1	

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	La organización debe conservar la información documentada acerca del proceso de tratamiento del riesgo de la seguridad de la información.	No diseñado	1	
6.2	**Objetivos de seguridad de la información y planificación para conseguirlos**			
	La organización debe establecer los objetivos de seguridad de la información en niveles y funciones relevantes.	No diseñado	1	
	Los objetivos de seguridad de la información deben: a) ser consistentes con la política de seguridad de la información;	No diseñado	1	
	b) ser medible (si es posible);	No diseñado	1	
	c) tomar en consideración los requisitos de seguridad de la información aplicable y los resultados de la evaluación de riesgo y el tratamiento de riesgo;	No diseñado	1	
	d) ser comunicados; y			
	e) estar actualizados según corresponda.			
	La organización debe conservar la información documentada sobre los objetivos de la seguridad de la información. Al planificar cómo lograr sus objetivos de seguridad de la información, la organización debe determinar: f) qué se hará; g) qué recursos se necesitarán; h) quién será responsable; i) cuándo se terminará; y j) cómo se evaluarán los resultados.	No diseñado	1	
7	**SOPORTE**			
7.1	**Recursos**			
	La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.	No diseñado	1	

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
7.2	**Competencia**			
	La organización debe determinar las competencias necesarias de las personas que trabajan bajo su control que afecta su desempeño de seguridad de la información.	No diseñado	1	Se aconseja la capacitación de personal técnico para llevar a cabo las tareas relacionadas con la seguridad de la información, gestión, documentación entre otras.
	a) Determinar la competencia necesaria de la(s) persona(s) que trabajan bajo su control que afecta su desempeño en seguridad de la información;	No diseñado	1	
	b) Asegurar que estas personas son competentes sobre la base de educación, capacitación, o experiencia adecuados;	No diseñado	1	
	c) Cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas; y	No diseñado	1	
	d) Retener información documentada apropiada como evidencia de competencia.	No diseñado	1	
7.3	**Conocimiento**			
	Las personas que trabajen bajo el control de la organización deben estar al tanto de:	No diseñado	1	Se recomienda el manejo de la seguridad de la información del área en al menos otra persona que pueda llevar a cabo las tareas que implica un SGSI.
	a) la política de seguridad de la información.	No diseñado	1	
	b) su contribución a la efectividad del SGSI, incluyendo los beneficios de un mejor desempeño de la seguridad de la información;	No diseñado	1	

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	c) las implicancias de no tener conformidad con los requisitos del sistema de gestión de seguridad de la información.	No diseñado	1	
7.4	**Comunicación**			
	La organización debe determinar la necesidad de comunicaciones internas y externas que sean pertinentes al SGSI que incluya: - qué comunicar; - cuándo comunicarlo; - con quién comunicarlo; y - los procesos que se verán afectados por la comunicación.	No diseñado	1	
7.5	**Información documentada**			
7.5.1	**General**			
	El sistema de gestión de la seguridad de la información debe incluir: a) información documentada necesaria para esta norma; y	Parcialmente diseñado	2	Se sugiere incluir toda la documentación relacionada con la gestión de seguridad informática.
	b) información documentada, definida por la organización como necesaria para la efectividad del sistema de gestión de la seguridad de la información.	No diseñado	1	Se debería contar con una planificación en materia de seguridad que involucre al menos a los activos y procesos críticos del área.
7.5.2	**Creación y actualización**			
	Al crear y actualizar la información documentada, la organización debe asegurar la correspondiente: a) identificación y descripción (por ejemplo, un título, fecha, autor o número de referencia);	No diseñado	1	
	b) formato (por ejemplo, idioma, versión de software, gráficos) y medio (por ejemplo, papel, digital); y	No diseñado	1	
	c) revisión y aprobación para conveniencia y suficiencia.	No diseñado	1	

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
7.5.3	**Control de la información documentada**			
	La información documentada necesaria por el sistema de gestión de la seguridad de la información y por la norma debe ser controlada para asegurar que: a) está disponible y apropiada para su uso, donde y cuando sea necesario; y	No diseñado	1	Se recomienda el control y verificación de la documentación que exige la norma ISO/IEC 27001:2013, la cual deberá cumplimentar los requisitos de confidencialidad, integridad y disponibilidad.
	b) está debidamente protegida (por ejemplo de pérdidas de confidencialidad, uso inapropiado o pérdida de integridad).	No diseñado	1	
	Para el control de la información documentada, la organización debe abordar las siguientes actividades, según corresponda: c) distribución, acceso, recuperación y uso;	No diseñado	1	
	d) almacenamiento y conservación, incluida la conservación de la legibilidad;	No diseñado	1	
	e) control de cambios (por ejemplo, control de versión); y	No diseñado	1	
	f) retención y disposición.	No diseñado	1	
	Información documentada de origen externo, determinada por la organización, de ser necesario, para la planificación y operación del sistema de gestión de la seguridad de la información debe ser identificado como apropiado y controlado.	No diseñado	1	
8	**OPERACIÓN**			
8.1	**Planificación y control operacional**			

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información y para implementar las acciones definidas en 6.1. La organización además debe implementar los planes para lograr los objetivos de seguridad de la información, definidos en 6.2.	No diseñado	1	Se sugiere una planificación, implementación y control de los procesos necesarios dentro de la Dirección a fin de lograr los objetivos de seguridad previstos.
	La organización debe mantener la información documentada hasta que sea necesario y tener la certeza que los procesos se llevaron a cabo según lo planeado.	Parcialmente diseñado	2	Se aconseja que toda la información relacionada con la seguridad informática se encuentre documentada.
	La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no planificados, al tomar acciones para mitigar cualquier efecto adverso, según sea necesario.	No diseñado	1	
	La organización debe asegurar de que los procesos externalizados se determinan y controlan.	No diseñado	1	
8.2	**Evaluación de riesgos de seguridad dela información**			
	La organización debe realizar evaluaciones de riesgo de la seguridad de la información, en intervalos planificados o cuando se propongan u ocurran cambios significativos, considerando los criterios establecidos en el 6.1.2.	No diseñado	1	Se recomienda planificar intervalos para la evaluación de los riesgos de seguridad de la Dirección, documentando sus procesos.
	La organización debe conservar la información documentada de los resultados de las evaluaciones de riesgo de la seguridad de la información.	No diseñado	1	
8.3	**Tratamiento de riesgos de seguridad de la información**			

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	La organización debe implementar el plan de tratamiento de riesgo de la seguridad de la información.	No diseñado	1	Se sugiere implementar un plan para el tratamiento de los riesgos de la Dirección.
	La organización debe conservar la información documentada de los resultados del tratamiento de riesgo de la seguridad de la información.	No diseñado	1	Los riesgos de seguridad y sus tratamientos deben ser documentados.
9	**EVALUACIÓN DEL DESEMPEÑO**			
9.1	**Monitoreo, medición, análisis y evaluación**			
	La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del SGSI. La organización debe determinar: a) qué se necesita monitorear y medir, incluidos los controles y procesos de la seguridad de la información;	No diseñado	1	
	b) los métodos para monitorear, medir, analizar y evaluar, según corresponda, para asegurar resultados válidos;	No diseñado	1	
	c) cuándo se deben llevar a cabo el monitoreo y la medición;	No diseñado	1	
	d) quién debe monitorear y medir;	No diseñado	1	
	e) cuándo se deben analizar y evaluar los resultados del monitoreo y la medición; y	No diseñado	1	
	f) quién debe analizar y evaluar estos resultados	No diseñado	1	
	La organización debe conservar la información documentada correspondiente, como evidencia de os resultados de monitoreo y medición.	No diseñado	1	
9.2	**Auditoría interna**			

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	La organización debe llevar a cabo auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de la seguridad de la información: a) cumple con: 1. los propios requisitos de la organización para su sistema de gestión de la seguridad de la información; y 2. los requisitos de esta norma;	No diseñado	1	Se sugiere que la Dirección acompañe su gestión con auditorías internas periódicas, a fin de contar con información actualizada para suministrar al SGSI.
	b) está debidamente implementada y mantenida. La organización debe:	No diseñado	1	
	c) planificar, establecer, implementar y mantener programa(s) de auditoría, incluida la frecuencia, métodos, responsabilidades, requisitos de planificación e informes. El (los) programa(s) de auditoría debe(n) considerar la importancia de los procesos en cuestión y los resultados de las auditorías anteriores;	No diseñado	1	
	d) definir los criterios de auditoría y el alcance para cada auditoría;	No diseñado	1	
	e) seleccionar auditores y realizar auditorías que aseguren la objetividad y la imparcialidad del proceso de auditoría;	No diseñado	1	
	f) asegurar que los resultados de las auditorías son informados a la dirección pertinente; y	No diseñado	1	
	g) conservar la información documentada como evidencia de los programas de auditoría y los resultados de la auditoría.	No diseñado	1	
9.3	**Revisión por la gerencia**			
	La alta dirección debe revisar el sistema de gestión de la seguridad de la información en los plazos planificados para asegurar su conveniencia, suficiencia y efectividad continua. La revisión de la dirección debe considerar: a) el estado de las acciones, a partir de las revisiones de gestión anteriores;	No diseñado	1	

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	b) los cambios en los asuntos externos e internos que son pertinentes al sistema de gestión de la seguridad de la información;	No diseñado	1	
	c) los comentarios sobre el desempeño de la seguridad de la información, incluidas tendencias en: 1. no conformidades y acciones correctivas; 2. resultados del monitoreo y mediciones; 3. resultados de auditoria; y 4. cumplimiento de los objetivos de seguridad de la información;	No diseñado	1	
	d) comentarios de las partes interesadas;	No diseñado	1	
	e) resultados de la evaluación de riesgo y el estado del plan de tratamiento de riesgo; y	No diseñado	1	
	f) las oportunidades para la mejora continua.	No diseñado	1	
	Los resultados de la revisión de dirección deben incluir las decisiones relacionadas a las oportunidades de mejora y cualquier necesidad de cambios al SGSI.	No diseñado	1	
	La organización debe conservar la información documentada como evidencia de los resultados de las revisiones de gestión.	No diseñado	1	
10	**MEJORAS**			
10.1	**No conformidades y acción correctiva**			
	Cuando ocurre una no conformidad, la organización debe: a) reaccionar frente a la no conformidad y si corresponde: 1. tomar acciones para controlarlo y corregirlo; y 2. encargarse de las consecuencias;	No diseñado	1	Se recomienda diseñar e implementar un SGSI y llevar a cabo un plan de mejora continua, manteniendo la

Puntos	Requisitos ISO/IEC 27001:2013	Estado Actual	Nivel de	Comentarios
	b) evaluar la necesidad de acción para eliminar las causas de no conformidad, y que así esto no vuelva a ocurrir o que ocurra en otro lugar, al: 1. revisar la no conformidad; 2. determinar las causas de las no conformidades; y 3. determinar si existe una no conformidad similar o podría ocurrir.	No diseñado	1	organización y sus procesos actualizados y con los riesgos controlados.
	c) implementar cualquier acción necesaria;	No diseñado	1	
	d) revisar la efectividad de cualquier acción correctiva implementada; y	No diseñado	1	
	e) hacer cambios al sistema de gestión de la seguridad de la información, si es necesario.	No diseñado	1	
	Las acciones correctivas deben ser pertinentes a los efectos de las no conformidades halladas.	No diseñado	1	
	La organización debe conservar la información documentada como evidencia de: f) la naturaleza de las no conformidades y las subsecuentes acciones implementadas, y	No diseñado	1	
	g) los resultados de cualquier acción correctiva.	No diseñado	1	
10.2	**Mejora continua**			
	La organización debe mejorar de manera continua la convivencia, suficiencia y efectividad del SGSI.	No diseñado	1	

Anexo 2. Análisis GAP de los dominios de la norma ISO/IEC 27001:2013 de la DGLH

	Objetivos de control y controles de seguridad		Preguntas	Estado Actual	Nivel de Madurez	Comentarios
5.	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**					
5.1	**Orientación de la dirección de gestión para la seguridad de la información**					
Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y las leyes pertinentes						
5.1.1	Políticas de seguridad de la información	**Control:** La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información	¿Existen políticas publicadas y aprobadas para apoyar la seguridad de la información?	Sin control	0	La DGLH no posee políticas de seguridad de la información de manera oficial.
5.1.2	Revisión de las políticas de seguridad de la información	**Control:** Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios	¿Las políticas de seguridad de la información son revisadas y actualizadas?	Sin control	0	La DGLH no posee documentos relacionados con políticas de seguridad de forma oficial.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		significativos, para asegurar su conveniencia, suficiencia, y eficacia continua.				
6.	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**					
6.1	**Organización interna**					
	Roles y responsabilidades de la seguridad de la información	**Control:** Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.	¿Están definidas todas las responsabilidades de seguridad de la información?	Sin control	0	El área de la DGLH no cuenta específicamente con el responsable de seguridad de la información.
6.1.2	Segregación de funciones	**Control:** Se deben segregar las funciones y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales, o el uso indebido de los activos de la organización.	¿Se han segregado las diversas áreas de responsabilidad sobre la seguridad de la información para evitar usos y accesos indebidos?	Sin control	0	Las funciones técnicas y de seguridad se encuentran solapadas. No existe un responsable formal de la seguridad.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
	Contacto con autoridades	**Control:** Se deben mantener los contactos apropiados con las autoridades pertinentes	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la seguridad de la información?	Sin control	0	El contacto del soporte técnico del área se comunica directamente con su Directora y esta con el Área Administrativa de nivel superior.
6.1.4	Contacto con grupos especiales de interés	**Control:** Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales.	¿Existen definidos contactos con grupos de interés especial o asociaciones profesionales?	Sin control	0	La DGLH posee contacto con la Comunidad SIU pero para temas generales.
6.1.5	Seguridad de la información en la gestión del proyecto	**Control:** Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto.	¿Los proyectos consideran aspectos relacionados con la seguridad de la información?	Sin control	0	No se analizan los riesgos de proyectos existentes o de futuros.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
6.2 Dispositivos móviles y trabajo remoto						
Objetivo: Garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles						
6.2.1	Política de dispositivos móviles	**Control:** Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados al usar dispositivos móviles.	¿Existen reglas definidas para el manejo seguro de los dispositivos móviles?	Sin control	0	No existen reglas o protocolos para el uso de dispositivos móviles en el área.
6.2.2	Teletrabajo	**Control:** Una política y medidas de seguridad de apoyo deben ser implementadas para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo.	¿Se aplican criterios de seguridad para los accesos de teletrabajo?	Sin control	0	El teletrabajo solo se permite a los agentes técnicos y administrativos directos al área.
7.	**Seguridad en los recursos humanos**					
7.1	Antes del empleo					

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
Objetivos: asegurar que los empleados y contratistas entiendan sus responsabilidades y que sean aptos para los roles para los cuales están siendo considerados.						
7.1.1	Selección	**Control:** Las verificaciones de los antecedentes de todos los candidatos a ser empleados deben ser llevadas a cabo en concordancia con las leyes, regulaciones y ética relevantes, y debe ser proporcional a los requisitos del negocio, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.	¿La organización realiza verificaciones de antecedentes de los candidatos para el empleo o para los contratistas?	Sin control	0	La DGLH no realiza selección de personal, salvo necesidades técnicas muy específicas, las que a su vez son autorizadas o rechazadas por la superioridad.
7.1.2	Términos y condiciones del empleo	**Control:** Los acuerdos contractuales con los empleados y contratistas deben estipular responsabilidades de éstos y de la organización respecto	¿Existen acuerdos con los empleados y contratistas donde se especifiquen las responsabilidades de seguridad de la información?	Sin control	0	El área no determina las condiciones de empleo.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		de la seguridad de la información.				
7.2	Durante el empleo					
Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.						
7.2.1	Responsabilidades de la gerencia	**Control:** La gerencia debe requerir a todos los empleados y contratistas aplicar la seguridad de la información en concordancia con las políticas y procedimientos establecidos por la organización.	¿El cumplimiento de las responsabilidades sobre la seguridad de la información es exigida de forma activa a empleados y contratistas?	Sin control	0	
7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información.	**Control:** Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información,	¿Existen procesos de información, formación y concientización sobre las responsabilidades sobre la seguridad de la información?	Control inicial	1	No existen capacitaciones o formaciones al personal técnico ni administrativo. Al ingresar un nuevo personal se lo instruye con las cuestiones básicas

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que cumplen.				y sus responsabilidades.
7.2.3	Proceso disciplinario	**Control:** Debe haber un proceso disciplinario formal y comunicado para tomar acción contra los empleados que hayan cometido una infracción a la seguridad de la información	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la seguridad de la información?	Sin control	0	No existen planes disciplinarios, ni se cuenta con políticas de seguridad para aplicar por incumplimiento o faltas.
7.3	**Terminación y cambio del empleo**					
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.						
7.3.1	Terminación o cambio de responsabilidades del empleo	**Control:** Las responsabilidades y deberes de seguridad de la información que siguen	¿Existen acuerdos que cubren las responsabilidades de seguridad de la	Sin control	0	La DGLH no realiza cuestiones relacionadas con el inicio o la

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		siendo válidos luego de la terminación o cambio de empleo deben ser definidos, comunicados al empleado o contratista y forzar el cumplimiento.	información que siguen siendo válidas después de la terminación del empleo?			finalización de contratos del personal.
8.	**GESTIÓN DE ARCHIVOS**					
8.1.1	Inventario de activos	**Control:** Información, otros activos asociados con información e instalaciones de procesamiento de información deben ser identificados y un inventario de estos activos debe ser elaborado y mantenido	¿Se ha realizado un inventario de activos que den soporte al negocio y de información?	Sin control	0	En la DGLH no se cuenta con inventarios de los activos físicos ni los activos de información. A nivel global se lleva un registro parcial de los activos físicos de cada oficina.
8.1.2	Propiedad de los activos	**Control:** Los activos mantenidos en el inventario deben ser propios.	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?	Sin control	0	No figuran inventarios ni tampoco la propiedad de ellos.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
8.1.3	Uso aceptable de los activos	**Control:** Las reglas para el uso aceptable de la información y activos asociados con la información y con las instalaciones de procesamiento de la información deben ser identificadas, documentadas e implementadas.	¿Se han establecido normas para el uso de activos en relación a su seguridad?	Sin control	0	No posee definiciones del uso aceptable de los activos del área.
8.1.4	Retorno de activos	**Control:** Todos los empleados y usuarios de partes externas deben retornar todos los activos de la organización en su posesión a la conclusión de su empleo, contrato o acuerdo.	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?	Control Repetible	1	Al finalizar un contrato de un agente, éste debe reintegrar el equipo y los recursos asignados. No existe una gestión de los mismos.
8.2	**Clasificación de la información**					
Objetivo: Asegurar que la información recibe un nivel apropiado en concordancia con su importancia para la organización.						

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
8.2.1	Clasificación de la información	**Control:** La información deber ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad específicas?	Control inicial	1	En el área de la DGLH toda la información es confidencial y crítica, no obstante esta no se halla clasificada.
8.2.2	Etiquetado de la información	**Control:** Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.	¿Existen procedimientos que definan el etiquetado de los activos?	Sin control	0	
8.2.3	Manejo de activos	**Control:** Los procedimientos para el manejo de activos deber ser desarrollados e implementados en	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?	Control inicial	1	No existen procedimientos complejos para el manejo de la información.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		concordancia con el esquema de clasificación de la información adoptado por la organización.				
8.3	**Manejo de los medios**					
Objetivo: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.						
8.3.1	Gestión de los medios removibles	**Control:** Se debe implementar procedimientos para la gestión de medios removibles en concordancia con el esquema de clasificación adoptado por la organización.	¿Existen procedimientos que definen cómo manejar los soportes extraíbles (uso, cifrado, borrado, etc.)?	Sin control	0	No existen políticas de uso de medios removibles. El cuidado corresponde a cada agente en su PC.
8.3.2	Disposición de medios	**Control:** Se debe poner a disposición los medios de manera segura cuando ya no se requieran, utilizando procedimientos formales.	¿Existen procedimientos formales para la eliminación de medios?	Sin control	0	Al dañarse un equipo se solicita su reparación al área técnica de Rectorado, se desconoce el fin del equipo fallado.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
8.3.3	Transferencia de medios físicos	**Control:** Los medios que contienen información deben ser protegidos contra el acceso no autorizado, el mal uso o la corrupción durante el transporte.	¿Son protegidos los medios que contienen información sensible durante el transporte?	Sin control	0	La DGLH no posee protección de medios físicos.
9.	**CONTROL DE ACCESO**					
9.1	**Requisitos de la empresa para el control de acceso**					
Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la información.						
9.1.1	Política de control de acceso	**Control:** Una política de control de acceso deber ser establecida, documentada y revisada en requisitos del negocio y de seguridad de la información.	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?	Sin control	0	La DGLH no posee políticas de control de acceso a la información definidas de manera formal.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
9.1.2	Acceso a redes y servicios de red	**Control:** Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizadas a usar.	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?	Control inicial	1	Existen procedimientos establecidos para asignar perfiles a los nuevos agentes
9.2	**Gestión de acceso de usuario**					
Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.						
9.2.1	Registro y baja de usuarios	**Control:** Un proceso formal de registro y baja de usuarios deber ser implementado para permitir la asignación de derechos de acceso.	¿Existen procesos formales de registros y baja de usuarios?	Control repetible	2	La DGLH cuenta con procedimientos de alta y baja de usuarios pero no está documentado.
9.2.2	Aprovisionamiento de acceso a usuario	**Control:** Un proceso formal de aprovisionamiento de acceso a usuarios debe ser implementado para asignar o revocar los derechos de acceso para todos los tipos	¿Existen procesos formales para asignación de perfiles de acceso?	Control repetible	2	Se cuenta con grupos y perfiles de usuarios asignados según roles pero no se encuentra documentado.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		de usuarios a todos los sistemas y servicios.				
9.2.3	Gestión de derechos de acceso privilegiados.	**Control:** La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.	¿Se define un proceso específico para la asignación y autorización de permisos privilegiados de administración de accesos?	Sin control	0	El acceso a internet es libre, no existen privilegios de acceso o limitaciones.
9.2.4	Gestión de información de autentificación secreta de usuarios.	**Control:** La asignación de información de autentificación secreta deber ser controlada a través de un proceso de gestión formal.	¿Las contraseñas y otra información de autenticación secreta, son proporcionadas de forma segura?	Control repetible	2	Son muchas aplicaciones las que se utilizan en la DGLH, las cuales poseen autenticación por cada una de ellas. No se hallan documentadas.
9.2.5	Revisión de los derechos de acceso de usuarios	**Control:** Los propietarios de los activos deben revisar los derechos de acceso de	¿Se establecen periodos concretos para renovación de permisos de acceso?	Sin control	0	La DGLH no posee revisión de los accesos de sus agentes.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		usuario a intervalos regulares.				
9.2.6	Remoción o ajuste de derechos de acceso	**Control:** Los derechos de acceso a información e instalaciones de procesamientos de información de todos los empleados y de los usuarios de partes	¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?	Control definido	3	Al terminar el contrato se bloquea la cuenta del agente y se eliminan sus permisos.
9.3	**Responsabilidades de los usuarios**					
Objetivo: Hacer que los usuarios respondan por la salvaguarda de su información de autentificación.						
9.3.1	Uso de información confidencial para la autenticación	**Control:** Los usuarios deben ser exigidos a que sigan las prácticas de la organización en el uso de información de autentificación secreta.	¿Existen reglas para los usuarios sobre cómo proteger las contraseñas y otra información de autenticación?	Control inicial	1	La capacitación es informal y personal para cada agente. No existe documentación.
9.4	**Control de acceso a sistema y aplicación**					
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.						

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
9.4.1	Restricción del acceso a la información	**Control:** El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.	¿El acceso a la información en los sistemas es restringido según la política de control de acceso?	Control repetible	2	La información que se maneja posee restricciones para su acceso. No existen políticas de control de acceso.
9.4.2	Procedimientos seguros de inicio de sesión	**Control:** Donde la política de control de acceso lo requiera, el acceso a los sistemas y a las aplicaciones debe ser controlado por un procedimiento de ingreso seguro.	¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla, etc.?	Control repetible	2	El acceso a la intranet se encuentra disponible solo para las facultades. Las aplicaciones poseen controles de acceso en su mayoría.
9.4.3	Sistema de gestión de contraseñas	**Control:** Los sistemas de gestión de contraseñas deber ser interactivos y deben asegurar contraseñas de calidad.	¿Los sistemas de gestión de contraseñas utilizados por los usuarios de la organización les ayuda a manejar de forma	Control repetible	2	Las políticas de contraseñas establecen contraseñas seguras pero no

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
			segura su información de autenticación?			exigen fechas de cambio
9.4.4	Uso de programas utilitarios privilegiados	**Control:** El uso de programas utilitarios que podrían ser capaces de pasar por alto los controles del sistema y de las aplicaciones deber ser restringido y controlarse estrictamente.	¿El uso de herramientas de utilidad es controlado y limitado a empleados específicos?	Sin control	0	Cualquier agente puede instalar aplicaciones no autorizadas en sus computadoras.
9.4.5	Control de acceso al código fuente de los programas	**Control:** El acceso al código fuente de los programas debe ser restringido.	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?	Control repetible	2	El código fuente de las aplicaciones no está disponible para los usuarios.
10.	**CRIPTOGRAFIA**					
10.1	**Controles criptográficos**					
Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.						

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
10.1.1	Política sobre el uso de controles criptográficos	**Control:** Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada.	¿Existe una política para regular la encriptación y existen otros controles criptográficos?	Sin control	0	La DGLH no tiene implementada políticas para la utilización de controles criptográficos.
10.1.2	Gestión de claves	**Control:** Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.	¿Existe un control del ciclo de vida de las claves criptográficas?	Sin control	0	La DGLH no tiene implementada políticas para la utilización de controles criptográficos.
11	**SEGRUIDAD FISICA Y AMBIENTAL**					
11.1	**Áreas seguras**					
Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las instalaciones de procesamiento de la información de la organización.						
11.1.1	Perímetro de seguridad física	**Control:**	¿Se establecen perímetros de seguridad física donde sea	Control repetible	2	El acceso a las instalaciones de Rectorado y a la

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		Perímetros de seguridad deben ser definidos y utilizados para proteger áreas que contienen información sensible o crítica e instalaciones de procesamiento de la información.	necesario con barreras de acceso?			oficina de la DGLH es por puerta principal, controlada por personal de seguridad externo.
11.1.2	Controles de ingreso físico	**Control:** Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	¿Existen controles de acceso a personas autorizadas en áreas restringidas?	Sin control	0	No existen controles físicos para el ingreso de personal en áreas restringidas.
11.1.3	Seguridad de oficinas, áreas e instalaciones	**Control:** Seguridad física para oficinas, áreas e instalaciones debe ser diseñada e implementada.	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas, etc. en áreas accesibles a personal externo?	Control inicial	1	El centro de datos es la zona restringida en las instalaciones de la DGLH, pero no posee dispositivos de seguridad salvo el frente del

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
						gabinete de servidores
11.1.4	Protección contra amenazas externas y ambientales	**Control:** Protección física contra desastres naturales, ataque malicioso o accidentes debe ser diseñada y aplicada.	¿Existen instaladas alarmas, sistemas de protección contra incendios y otros sistemas?	Control repetible	2	Las instalaciones de la DGLH poseen extintores de incendios. La amenaza natural más probable son las inundaciones.
11.1.5	Trabajo en áreas seguras	**Control:** Procedimientos para el trabajo en áreas seguras debe ser diseñado y aplicado.	¿Existen definidos procedimientos para las zonas seguras?	Sin control	0	No existen controles físicos para el acceso a las zonas seguras.
11.1.6	Áreas de despacho y carga	**Control:** Los puntos de acceso, como las áreas de despacho, carga y otros puntos en donde personas no autorizadas pueden ingresar al local deben ser controlados, y si fuera posible, aislarlos de	¿Se controlan las áreas de carga y descarga con procedimientos de control de mercancías entregadas, etc.?	Control inicial	1	La atención a personas externas al área se realiza de forma controlada. No se llevan registros de las personas que

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		las instalaciones de procesamiento de la información para evitar el acceso no autorizado.				ingresan a la oficina.
11.2	**Equipos**					
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.						
11.2.1	Emplazamiento y protección de los equipos	**Control:** Los equipos deben ser ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales, así como las oportunidades para el acceso no autorizado.	¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?	Control repetible	2	Los servidores de la DGLH se encuentran en un espacio especial, restringido. Las computadoras personales están accesibles en los escritorios.
11.2.2	Servicios de suministro	**Control:** Los equipos deben ser protegidos contra fallas de electricidad y otras alteraciones causadas por	¿Se protegen los equipos contra fallos de suministro de energía?	Control inicial	1	Los servidores poseen UPS y son mantenidos pero no se testean periódicamente.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		fallas en los servicios de suministro.				
11.2.3	Seguridad del cableado	**Control:** El cableado de energía y telecomunicaciones que llevan datos o servicios de información de soporte debe ser protegido de la interceptación, interferencia o daño.	¿Existen protecciones para los cableados de energía y de datos?	Sin control	0	No existen controles del estado o protección del cableado o energía eléctrica.
11.2.4	Mantenimiento de equipos	**Control:** Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?	Sin control	0	La DGLH no posee una gestión de sus equipos informáticos ni tampoco mantenimiento o reemplazos.
11.2.5	Remoción de activos	**Control:** Los equipos deben mantenerse de manera correcta para asegurar su	¿Se controlan y autorizan la salida de equipos, aplicaciones, etc. que puedan tener información?	Control repetible	2	No está permitida la salida de ningún bien de las oficinas de Rectorado sin autorización.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		continua disponibilidad e integridad.				
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	**Control:** La seguridad debe ser aplicada a los activos que están fuera de su lugar tomando en cuenta los distintos riesgos de trabajar fuera de las instalaciones de la organización.	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?	Sin control	0	No se utilizan equipos de la Dirección fuera de la oficina.
11.2.7	Disposición o reutilización segura de equipos	**Control:** Todos los elementos del equipo que contengan medios de almacenamiento deben ser verificados para asegurar que cualquier dato sensible y software con licencia se haya eliminado o se haya sobre escrito de manera segura	¿Se establecen protocolos para proteger o eliminar información de equipos de baja o que van a ser reutilizados?	Sin control	0	No se cuenta con protocolos para eliminar los equipos que se den de baja en la DGLH.
11.2.8	Equipos de usuario	**Control:**	¿Se establecen normas para proteger la	Sin control	0	La DGLH no posee protocolos

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
	desatendidos	Los usuarios deben asegurarse de que el equipo desatendido tenga la protección apropiada.	información de equipos cuando los usuarios abandonan el puesto de trabajo?			para la protección de la información de los agentes.
11.2.9	Política de escritorio limpio y pantalla limpia	**Control:** Una política de escritorio limpio de papeles y de medios de almacenamiento removibles, así como una política de pantalla limpia para las instalaciones de procesamientos de la información debe ser adoptada.	¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo?	Sin control	0	No se cuenta con políticas de escritorio limpio o bloqueos de pantalla. Los equipos PC de los agentes pueden ser accedidos por otros agentes.
12.	**SEGURIDAD EN LAS OPERACIONES**					
12.1	**Procedimientos y responsabilidades operativas**					
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras						
12.1.1	Procedimientos operativos documentados		¿Se documentan los procedimientos y se establecen responsabilidades?	Control repetible	1	Los principales procesos del área se encuentran documentados y se

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
						está trabajando sobre los restantes.
12.1.2	Gestión de cambios	**Control:** Los cambios en la organización, procesos de negocio, instalaciones de procesamiento de la información y sistemas que afectan la seguridad de la información deben ser controlados.	¿Se controla que la información sobre procedimientos se mantenga actualizada?	Sin control	0	Se está trabajando sobre los mismos.
12.1.3	Gestión de la capacidad	**Control:** El uso de recursos debe ser monitoreado, afinado y se debe hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.	¿Los recursos son monitoreados y se realizan planes para asegurar su capacidad para cumplir con la demanda de los usuarios?	Sin control	0	No existe una monitorización de la capacidad de los recursos.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
12.1.4	Separación de los entornos de desarrollo, pruebas y operaciones	**Control:** Los entornos de desarrollo, pruebas y operaciones deben ser separados para reducir los riesgos de acceso no autorizado o cambios al entorno operativo.	¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?	Sin control	0	El área de TI de la DGLH solo posee un espacio para el desarrollo donde se llevan todos los proyectos.
12.2	**Protección contra códigos maliciosos**					
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información estén protegidas contra códigos maliciosos.						
12.2.1	Controles contra códigos maliciosos	**Control:** Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios.	¿Existen sistemas de detección para software malicioso o malware?	Control inicial	0	Todas las estaciones de trabajo poseen antivirus pero no se encuentran mantenidos.
12.3	**Respaldo**					
Objetivo: Proteger contra la pérdida de datos						

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
12.3.1	Respaldo de la información	**Control:** Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una política de respaldo acordada.	¿Existe una política de backup definida y se lleva a cabo correctamente?	Control repetible	2	Se realizan copias de respaldo de forma automática de las aplicaciones y archivos más importantes conforme a los requisitos de seguridad.
12.4	**Registros y monitoreo**					
Objetivo: Registrar eventos y generar evidencia						
12.4.1	Registro de eventos	**Control:** Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, mantenidos y regularmente revisados.	¿Se realiza un registro de eventos? (intentos de acceso fallidos/exitosos, desconexiones del sistema, alertas de fallos, etc.)	Sin control	0	La DGLH no cuenta con procedimientos de registros de logs, cambios. Solo algunas aplicaciones de forma interna.
12.4.2	Protección de información de registros	**Control:**	¿Se ha establecido un sistema de protección	Sin control	0	La protección de los registros es a

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		Las instalaciones para registros (logs) y la información de los registros (logs) deben ser protegidas contra la adulteración y el acceso no autorizado.	para los registros mediante segregación de tareas o copias de seguridad?			través del sistema operativo. No existen controles de resguardo.
12.4.3	Registros del administrador y del operador	**Control:** Las actividades del administrador del sistema y del operador del sistema deben ser registradas y los registros (logs) deben ser protegidos y revisados regularmente	¿Se protege convenientemente y de forma específica los accesos de los administradores?	Sin control	0	No existen controles para el resguardo de los registros de las operaciones en red.
12.4.4	Sincronización de reloj	**Control:** Los relojes de todos los sistemas de procesamiento de la información relevantes dentro de una organización o dominio de seguridad deben estar sincronizados a	¿Existe un control de sincronización de los distintos sistemas?	Sin control	0	La DGLH no posee sincronización de relojes.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		una fuente de tiempo de referencia única.				
12.5	**Control del software operacional**					
Objetivo: Asegurar la integridad de los sistemas operacionales						
12.5.1	Instalación de software en sistemas operacionales	**Control:** Procedimientos deben ser implementados para controlar la instalación de software en sistemas operacionales.	¿Las instalaciones de nuevas aplicaciones de software o modificaciones son estrictamente controladas?	Sin control	0	No existe un control de los programas o aplicaciones que se instalan en los equipos de la DGLH.
12.6	**Gestión de vulnerabilidad técnica**					
Objetivo: Asegurar la integridad de los sistemas operacionales						
12.6.1	Gestión de vulnerabilidades técnicas	**Control:** Información sobre vulnerabilidades técnicas de los sistemas de información utilizados debe ser obtenida de manera oportuna, la exposición de la organización a dichas	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético", etc.?	Sin control	0	No existen controles para la detección de vulnerabilidades y tampoco se lleva un registro de eventos. El personal

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		vulnerabilidades debe ser evaluada y las medidas apropiadas deben ser tomadas para resolver el riesgo asociado.				capacitado cumple varias funciones en su rol técnico.
12.6.2	Restricciones sobre la instalación de software	**Control:** Reglas que gobiernan la instalación de software por parte de los usuarios deben ser establecidas e implementadas.	¿Se establecen medidas restrictivas para la instalación de software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?	Sin control	0	No existen protocolos para la instalación de software en los equipos por parte de los agentes.
12.7	**Consideraciones para la auditoría de los sistemas de información**					
Objetivo: Minimizar el impacto de las actividades de auditoría en los sistemas operacionales						
12.7.1	Controles de auditoria de los sistemas de información	**Control:** Requisitos de las auditorías y las actividades que involucran la verificación de sistemas operacionales deben ser cuidadosamente planificados y acordados para minimizar la	¿Están las auditorías de sistemas de información planeadas y se ejecutan correctamente?	Control inicial	1	Las auditorias que se realizan son externas al área de la DGLH, la misma no posee auditorias propias.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		interrupción a los procesos del negocio.				
13.	**SEGURIDAD DE LAS COMUNICACIONES**					
13.1	**Gestión de seguridad de la red**					
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.						
13.1.1	Controles de la red	**Control:** Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?	Control inicial	1	El acceso a la intranet no se halla administrada por la DGLH. Existen restricciones de conexión de equipos por bloqueos de IP.
13.1.2	Seguridad de servicios de red	**Control:** Mecanismos de seguridad, niveles de servicio y requisitos de gestión de todos los servicios de red deben ser identificados e incluidos en acuerdos de servicios de red, ya sea que	¿Se establecen condiciones de seguridad en los servicios de red tanto propios como subcontratados?	Control inicial	1	El área TIC de Rectorado se encarga de la administración de la intranet y de la provisión de internet. No se cuenta con

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		estos servicios se provean internamente o sean tercerizados.				procedimientos formales.
13.1.3	Segregación en redes	**Control:** Grupos de servicios de información, usuarios y sistemas de información deben ser segregados en redes.	¿Existe separación o segregación de redes tomado en cuenta condiciones de seguridad y clasificación de activos?	Sin control	0	La segregación de redes es a modo de organización, la misma es administrada por el área TIC de Rectorado.
13.2	**Transferencia de información**					
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.						
13.2.1	Políticas y procedimientos de transferencia de la información	**Control:** Políticas, procedimientos y controles de transferencia formales deben aplicarse para proteger la transferencia de información a través del uso de todo tipo de instalaciones de comunicación.	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?	Sin control	0	No existen políticas definidas en la DGLH para la transferencia de la información.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
13.2.2	Acuerdo sobre transferencia de información	**Control:** Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?	Sin control	0	No hay acuerdos definidos en la DGLH para la transferencia de la información.
13.2.3	Mensajes electrónicos	**Control:** La información involucrada en mensajería electrónica debe ser protegida apropiadamente.	¿Se establecen normas o criterios de seguridad en mensajería electrónica?	Sin control	0	La administración del correo electrónico oficial no es administrada por el área. Se permite el uso de correos gratuitos.
13.2.4	Acuerdos de confidencialidad o no divulgación	**Control:** Requisitos para los acuerdos de confidencialidad o no divulgación que reflejan las necesidades de la organización para la protección de la información deben ser identificados, revisados	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades?	Sin control	0	La DGLH no posee acuerdos de confidencialidad ni manejo de la información que allí se administra.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		regularmente y documentados.				
14.	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**					
14.1	**Requisitos de seguridad de los sistemas de información**					
Objetivo: Garantizar que la seguridad de la información es una parte integral de los sistemas de información a través del ciclo de vida completo. Esto también incluye los requisitos para sistemas de información que proporcionen servicios sobre redes públicas.						
14.1.1	Análisis y especificación de requisitos de seguridad de la información	**Control:** Requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.	¿Se definen y documentan los requisitos de seguridad de la información para los nuevos sistemas de información?	Sin control	0	No existen políticas definidas de manera formal en la DGLH para la gestión de la seguridad de la información en los sistemas.
14.1.2	Aseguramiento de servicios de aplicaciones sobre redes públicas	**Control:** La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales, y su	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?	Sin control	0	No existen políticas específicas sobre accesos públicos.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		divulgación y modificación no autorizada.				
14.1.3	Protección de las transacciones de servicios de aplicación	**Control:** La información implicada en transacciones de servicio de aplicación de debe proteger para evitar la transmisión incompleta, la omisión de envío, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.	¿Se establecen medidas de protección para transacciones online?	Sin control	0	No se realizan transacciones electrónicas que involucren pagos.
14.2	**Seguridad en los procesos de desarrollo y soporte**					
Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.						
14.2.1	Política de desarrollo seguro	**Control:** Reglas para el desarrollo de software y sistemas deben ser establecidas y aplicadas	¿Se establecen procedimientos que garanticen el desarrollo seguro del software?	Sin control	0	En la DGLH no se cuenta con procedimientos formales o definidos para el

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		a desarrollos dentro de la organización.				desarrollo de software de manera segura.
14.2.2	Procedimientos de control de cambio del sistema	**Control:** Cambios a los sistemas dentro del ciclo de vida del desarrollo deben ser controlados por medio del uso de procedimientos formales de control de cambios.	¿Se gestiona el control de cambios en relación al impacto que puedan tener en los sistemas?	Sin control	0	No existen procedimientos formales del control de cambios en los sistemas.
14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	**Control:** Cuando se cambian las plataformas operativas, las aplicaciones críticas para el negocio deben ser revisadas y probadas para asegurar que no haya impacto adverso en las operaciones o en la seguridad de la organización.	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?	Control inicial	1	Se realizan pruebas básicas sobre las aplicaciones o sistemas instalados o actualizados.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
14.2.4	Restricciones sobre cambios a los paquetes de software	**Control:** Modificaciones a los paquetes de software deben ser disuadidas, limitadas a los cambios necesarios y todos los cambios deben ser estrictamente controlados.	¿Se establecen procesos formales para cambios de versiones o nuevas funcionalidades para software de terceros?	Control inicial	1	No existen procedimientos formales para la actualización de versiones.
14.2.5	Principios de ingeniería de sistemas seguros	**Control:** Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información.	¿Se definen políticas de seguridad de la información en procesos de ingeniería de sistemas?	Sin control	0	No existen procedimientos formales de desarrollo seguro.
14.2.6	Ambientes de desarrollo seguro	**Control:** Las organizaciones deben establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración	¿Es seguro el ambiente de desarrollo de software?	Sin control	0	Las tareas de desarrollo se realizan sobre las estaciones de trabajo del personal técnico.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		de sistemas que cubren todo el ciclo de vida del desarrollo del sistema.				
14.2.7	Desarrollo contratado externamente.	***Control:*** La organización debe supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.	¿Se acuerdan los requisitos de seguridad de la información para software desarrollado por terceros?	Sin control	0	La DGLH no mantiene contrato para el desarrollo externo con terceras partes.
14.2.8	Pruebas de seguridad del sistema	**Control:** Pruebas de funcionalidad de la seguridad deben ser llevadas a cabo durante el desarrollo.	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?	Sin control	0	Las pruebas se realizan sobre el mismo sistema en fases de desarrollo
14.2.9	Pruebas de aceptación del sistema	**Control:** Programas de pruebas de aceptación y criterios relacionados deben ser establecidos para nuevos sistemas de información,	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?	Sin control	0	No se realizan pruebas de aceptación para nuevos sistemas o actualizaciones.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		actualizaciones y nuevas versiones.				
14.3	**Datos de prueba**					
Objetivo: Asegurar la protección de datos utilizados para las pruebas						
14.3.1	Protección de datos de prueba	**Control:** Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?	Control inicial	1	En los casos que la información deba ser probada por externos (SIU) se anonimizan los datos y se los convierte en datos de prueba
15.	**RELACIONES CON LOS PROVEEDORES**					
15.1	**Seguridad de la información en las relaciones con los proveedores**					
Objetivo: Asegurar protección a los activos de la organización que son accesibles por los proveedores.						
15.1.1	Política de seguridad de la información para las relaciones con los proveedores	**Control:** Requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso por parte del	¿Existe una política de seguridad de la información para proveedores que acceden a activos de la	Sin control	0	La DGLH no mantiene relación con proveedores, sino a través del

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		proveedor a los activos de la organización deben ser acordados con el proveedor y documentados.	información de la empresa?			área TIC de Rectorado.
15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	**Control:** Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.	¿Se han establecido requisitos de seguridad de la información en contratos con terceros?	Sin control	0	La DGLH no mantiene relación con proveedores, sino a través del área TIC de Rectorado.
15.1.3	Cadena de suministro de tecnología de información y comunicación	**Control:** Los acuerdos con proveedores deben incluir requisitos para abordar los riesgos de seguridad de la información asociados con	¿Se fijan requisitos para extender la seguridad de la información a toda la cadena de suministros?	Sin control	0	La DGLH no mantiene relación con proveedores, sino a través del área TIC de Rectorado.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		los servicios de tecnología de la información y comunicaciones y la cadena de suministro de productos.				
15.2	**Gestión de entrega de servicios del proveedor**					
Objetivo: Mantener un nivel de seguridad de la información y entrega de servicios acordado en línea con los acuerdos con proveedores.						
15.2.1	Monitoreo y revisión de servicios de los proveedores	**Control:** Las organizaciones deben monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.	¿Se controla el cumplimiento de los requisitos establecidos con proveedores externos?	Sin control	0	La DGLH no mantiene relación con proveedores, sino a través del área TIC de Rectorado.
15.2.2	Gestión de cambios a los servicios de proveedores	**Control:** Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser	¿Se controlan los posibles impactos en la seguridad ante cambios de servicios de proveedores externos?	Sin control	0	La DGLH no mantiene relación con proveedores, sino a través del área TIC de Rectorado.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.				
16.	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**					
16.1	**Gestión de incidentes de seguridad de la información y mejoras**					
Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.						
16.1.1	Responsabilidades y procedimientos	**Control:** Las responsabilidades de gestión y los procedimientos deben ser establecidos para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la seguridad de la información?	Sin control	0	No se cuenta con procedimientos para la gestión de incidentes de seguridad en el área.
16.1.2	Reporte de eventos de seguridad de la información	**Control:** Los eventos de seguridad de la información deben ser	¿Se han implementado canales adecuados para la comunicación de	Sin control	0	No se han determinado de manera formal los

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		reportados a través de canales de gestión apropiados tan rápido como sea posible.	incidentes en la seguridad de la información?			canales para la comunicación de incidentes. Se utiliza el correo oficial y otras redes.
16.1.3	Reporte de debilidades de seguridad de la información	**Control:** Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o dela que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.	¿Se promueven y se hayan establecidos canales para comunicar o identificar puntos débiles en la seguridad de la información?	Sin control	0	No existe un canal oficial para reportar incidentes. El personal utiliza desde lo oral a las redes de mensajería.
16.1.4	Evaluación y decisión sobre eventos de seguridad de la información	**Control:** Los eventos de seguridad de la información deben ser evaluados y debe decidirse si son clasificados como	¿Se ha establecido un proceso para gestionar los incidentes en la seguridad de la información?	Sin control	0	No se cuenta con procesos de gestión de la seguridad de la

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		incidentes de seguridad de la información.				información en el área.
16.1.5	Respuesta a incidentes de seguridad de la información	**Control:** Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	¿Existen mecanismos para dar una respuesta a los eventos de la seguridad de la información?	Control inicial	1	Se buscan soluciones para los eventos de seguridad pero no se los gestiona a través de procedimientos.
16.1.6	Aprendizaje de los incidentes de seguridad de la información	**Control:** El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.	¿La información proporcionada por los eventos en la seguridad de la información es tratada para tomar medidas preventivas?	Sin control	0	No se lleva un registro de los incidentes de seguridad ocurridos en la DGLH.
16.1.7	Recolección de evidencia	**Control:** La organización debe definir y aplicar procedimientos para la identificación, recolección,	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la información?	Sin control	0	

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		adquisición y preservación de información que pueda servir como evidencia.				
17.	**ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTION DE CONTINUIDAD DEL NEGOCIO**					
17.1	**Continuidad de seguridad de la información**					
Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización.						
17.1.1	Planificación de continuidad de seguridad de la información	**Control:** La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de seguridad de la información?	Sin control	0	No existen planes de continuidad de manera formal sobre los principales sistemas o procesos. No existe documentación actualizada.
17.1.2	Implementación de continuidad de seguridad de la información	**Control:** La organización debe establecer, documentar, implementar y mantener	¿Se ha implementado las medidas de recuperación previstas en el plan de	Sin control	0	No existen planes para la continuidad de manera formal.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.	continuidad del negocio?			
17.1.3	Verificación, revisión y evaluación de continuidad de seguridad de la información	**Control:** La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.	¿Se han verificado o probado las acciones previstas en el plan de continuidad del negocio?	Sin control	0	No existen planes para la continuidad de manera formal.
17.2	**Redundancias**					
Objetivo: Asegurar la disponibilidad de las instalaciones y procedimientos de la información.						
17.2.1	Instalaciones de procesamiento de la información	**Control:** Las instalaciones de procesamiento de la	¿Se ha evaluado la necesidad de redundar	Sin control	0	No se cuenta con la definición de los activos y procesos críticos de manera

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	los activos críticos de la información?			formal o desde procedimientos que permitan resguardarlos.
18.	**CUMPLIMIENTO**					
18.1	**Cumplimiento con requisitos legales y contractuales**					
Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.						
18.1.1	Identificación de requisitos contractuales y de legislación aplicables	**Control:** Todos los requisitos legislativos, estatutarios, regulatorios y contractuales relevantes así como el enfoque de la organización para cumplir con estos requisitos deben ser explícitamente identificados, documentados y mantenidos al día para	¿Son conocidos los requisitos legislativos, regulatorios, contractuales y cualquier otro requisito relativo a seguridad?	Sin control	0	

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		cada sistema de información y para la organización.				
18.1.2	Derechos de propiedad intelectual	**Control:** Procedimientos apropiados deben ser implementados para asegurar el cumplimiento de requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y uso de productos de software propietario.	¿Existen procedimientos implementados sobre la propiedad intelectual?	Sin control	0	No existen procedimientos sobre la propiedad intelectual formalmente definidos. La información alojada en las PC pertenece a la DGLH.
18.1.3	Protección de registros	**Control:** Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos,	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?	Sin control	0	Los datos y archivos se protegen en las bases de datos de los principales sistemas y mediante las copias de seguridad.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		regulatorios, contractuales y del negocio.				
18.1.4	Privacidad y protección de datos personales	**Control:** La privacidad y la protección de datos personales deben ser aseguradas tal como se requiere en la legislación y regulación relevantes donde sea aplicable.	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?	Sin control	0	No existen medidas o aplicación de la protección de datos personales en el área de la DGLH.
18.1.5	Regulación de controles criptográficos	**Control:** Controles criptográficos deben ser utilizados en cumplimiento con todos los acuerdos, legislación y regulación relevantes.	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?	Sin control	0	En la DGLH no se utiliza el cifrado criptográfico.
18.2	**Revisiones de seguridad de la información**					
Objetivo: Asegurar que la seguridad de la información está implementada y es operada de acuerdo con las políticas y procedimientos organizativos.						

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
18.2.1	Revisión independiente de la seguridad de la información	**Control:** El enfoque de la organización para manejar la seguridad de la información y su implementación (por ejemplo objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) debe ser revisado independientemente a intervalos planeados o cuando ocurran cambios significativos.	¿Se revisan los controles de la seguridad de la información por personal independiente a los responsables de implementar los controles?	Sin control	0	La DGLH no posee un SGSI y tampoco se lleva un control de la seguridad de la información.
18.2.2	Cumplimiento de políticas y normas de seguridad	**Control:** Los gerentes deben revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la seguridad de la información?	Sin control	0	Los controles se lo hacen sin seguir una planificación ni documentación guía como un SGSI.

Objetivos de control y controles de seguridad			Preguntas	Estado Actual	Nivel de Madurez	Comentarios
		área de responsabilidad con las políticas, normas y otros requisitos de seguridad apropiados.				
18.2.3	Revisión del cumplimiento técnico	**Control:** Los sistemas de información deben ser revisados regularmente respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?	Sin control	0	Las revisiones son de manera informal sin seguir procedimientos al no contar con un SGSI.

Anexo 3. Formulario para el autodiagnóstico del área de TI de la DGLH (ISO 27001)

A continuación debe completar las siguientes preguntas marcando en la casilla correspondiente conforme a lo que corresponda según cumpla: **S**i, **N**o, **P**arcialmente o **N**o **A**plica.

A.5	**POLITICAS DE SEGURIDAD**	Cumple (S/N/P/NA)
	¿Existen documento(S) de políticas de seguridad de Sistemas de Información?	
	¿Existen normativas relacionadas a la seguridad de los Sistemas de Información?	
	¿Existen procedimientos relativos a la seguridad de Sistemas de Información?	
	¿Existe un responsable de las políticas, normas y procedimientos?	
	¿Existen mecanismos para la comunicación a los usuarios de las normas?	
	¿Existen controles regulares para verificar la efectividad de las políticas?	
A.6	**ORGANIZACIÓN DE LA SEGURIDAD**	
	¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?	
	¿Existe un responsable o encargado de evaluar la adquisición y cambios de Sistemas de Información?	
	¿La dirección y las áreas de la organización participan en temas de seguridad?	
	¿Existen condiciones contractuales de seguridad con terceros?	
	¿Existen criterios de seguridad en el manejo de terceras partes?	
	¿Existen programas de formación en seguridad para los agentes en las diferentes áreas y perfiles?	
	¿Existe un acuerdo de confidencialidad de la información que se accede o se visualiza?	
	¿Se revisa la organización de la seguridad periódicamente por una empresa externa?	
A.7	**SEGURIDAD DE LOS RRHH**	
	¿Se tienen definidas las responsabilidades y roles de seguridad?	
	¿Se tiene en cuenta la seguridad en la selección y baja del personal?	
	¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?	

	¿Se imparte la formación adecuada de seguridad y tratamiento de activos?	
	¿Existe un canal y procedimientos claros a seguir en caso de incidentes de seguridad?	
	¿Se recogen los datos de los incidentes de forma detallada?	
	¿Informan los usuarios de las vulnerabilidades observadas o sospechadas dentro del área?	
	¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia probar las vulnerabilidades?	
	¿Existe un proceso disciplinario de la seguridad de la información?	
A.8	**ADMINISTRACIÓN DE ACTIVOS**	
	¿Existe un inventario de activos actualizado?	
	¿El inventario contiene activos de datos, software, equipos y servicios?	
	¿Se dispone de una clasificación de la información según la criticidad de la misma?	
	¿Existe un responsable de los activos?	
	¿Existen procedimientos para clasificar la información?	
	¿Existen procedimientos de etiquetado de la información?	
A.9	**CONTROL DE ACCESOS**	
	¿Existe una política de control de accesos?	
	¿Existe un procedimiento formal de registro y baja de accesos?	
	¿Se controla y restringe la asignación y uso de privilegios en entornos multiusuario?	
	¿Existe una gestión de las claves de los usuarios?	
	¿Existe una revisión de los derechos de acceso de los usuarios?	
	¿Existe el uso de claves en los accesos?	
	¿Se protege el acceso de los equipos no atendidos?	
	¿Existen políticas de limpieza en el puesto de trabajo?	
	¿Existe una política de uso de los servicios de red?	
	¿Se asegura la ruta (path) desde el terminal al servicio?	
	¿Existe una autenticación de usuarios en conexiones externas?	
	¿Existe una autenticación de los nodos?	

	¿Existe un control de la conexión de redes?	
	¿Existe un control de routing de las redes?	
	¿Existe una identificación única de usuario y una automática de terminales?	
	¿Existen procedimientos de log-on al terminal?	
	¿Se han incorporado medidas de seguridad a la computación móvil?	
	¿Está controlado el teletrabajo por la organización?	
A.10	**CRIPTOGRAFIA**	
	¿Existen políticas de utilización de criptografía?	
	¿Se gestionan las claves aplicando criptografía?	
A.11	**SEGURIDAD FÍSICA Y DEL AMBIENTE**	
	¿Existe perímetro de seguridad física (una pared, puerta con llave) al centro de datos?	
	¿Existen controles de entrada para protegerse frente al acceso de personal no autorizado?	
	¿Existe un área segura, cerrada, aislada y protegida de eventos naturales?	
	¿En las áreas de carga y expedición están aisladas de las áreas de SI?	
	¿La ubicación de los equipos está de tal manera que se minimicen los accesos innecesarios?	
	¿Existen protecciones frente a fallas de la alimentación eléctrica?	
	¿Existe seguridad en el cableado frente a daños e intercepciones?	
	¿Se asegura la disponibilidad e integridad de todos los equipos?	
	¿Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente?	
	¿Se incluye la seguridad en los dispositivos móviles?	
A.12	**GESTIÓN DE OPERACIONES**	
	¿Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados?	
	¿Están establecidas las responsabilidades para controlar los cambios de equipos?	
	¿Están establecidas las responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?	
	¿Existe algún método para reducir el mal uso accidental o deliberado de los sistemas?	
	¿Existe una separación de los entornos de desarrollo y producción?	

	¿Existen contratistas externos para la gestión y desarrollo de los Sistemas de Información?	
	¿Existe un Plan de capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento?	
	¿Existen criterios de aceptación de nuevos Sistemas de Información, incluyendo actualizaciones y nuevas versiones?	
	¿Existen controles contra software malicioso?	
	¿Se realiza copias de seguridad de la información esencial para la continuidad del negocio?	
	¿Existen registros (logs) para las actividades realizadas por los operadores y administradores?	
	¿Existen registros (logs) de los fallos detectados?	
	¿Existen registros de las auditorías realizadas?	
A.13	**GESTIÓN DE COMUNICACIONES**	
	¿Existe algún control en las redes?	
	¿Hay controles establecidos para realizar la gestión de los medios informáticos (cintas, discos removibles, informes impresos?	
	En la eliminación de los medios informáticos. ¿Pueden disponer de información sensible en ellos?	
	¿Existe seguridad de la documentación de los sistemas?	
	¿Existen acuerdos para intercambio de información y software?	
	¿Existen medidas de seguridad de los medios en el tránsito?	
	¿Existen medidas de seguridad en el comercio electrónico?	
	¿Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada?	
	¿Existen medidas de seguridad en las transacciones en línea	
	¿Se monitorean las actividades relacionadas a la seguridad?	
A.14	**DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS**	
	¿Se asegura que la seguridad está implementada en los Sistemas de Información que se desarrollen?	
	¿Existe seguridad en las aplicaciones?	
	¿Existen controles criptográficos?	
	¿Existe seguridad en los archivos de los sistemas?	
	¿Existe seguridad en los procesos de desarrollo, testing y soporte?	
	¿Existen controles de seguridad para los resultados de los sistemas?	

	¿Existe la gestión de los cambios en los sistemas operativos?	
	¿Se controlan las vulnerabilidades de los equipos?	
A.15	**RELACION CON LOS PROVEEDORES**	
	¿Existen políticas de seguridad en relación con los proveedores?	
	¿Existen requisitos de seguridad en contratos con terceros?	
A.16	**ADMINISTRACION DE INCIDENTES**	
	¿Se comunican los eventos de seguridad?	
	¿Se comunican las debilidades de seguridad detectadas?	
	¿Se encuentran definidas las responsabilidades ante un incidente?	
	¿Existe un procedimiento formal de respuesta?	
	¿Existe la gestión de incidentes?	
A.17	**GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**	
	¿Existen procesos para la gestión de la continuidad?	
	¿Existe un plan de continuidad del negocio y análisis de impacto?	
	¿Existe un diseño, redacción e implementación de planes de continuidad?	
	¿Existe un marco de planificación para la continuidad del negocio?	
	¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?	
A.18	**CUMPLIMIENTO**	
	¿Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas?	
	¿Existe el resguardo de propiedad intelectual?	
	¿Existe el resguardo de los datos de la organización?	
	¿Existe una revisión de la política de seguridad y de la conformidad técnica?	
	¿Existen consideraciones sobre las auditorias de los sistemas?	

Anexo 4. Formulario de responsables entrevistados en el autodiagnóstico del área de TI de la DGLH (ISO 27001)

Dominio	Subdominio	Responsable	Fecha de Reunión
A.5 Políticas de seguridad de la información			
A.5.1	Directivas de gestión de la seguridad de la información		
A.6. Organización de la seguridad de la información			
A.6.1	Organización interna		
A.6.2	Los dispositivos móviles y el teletrabajo		
A.7 Seguridad relativa a los recursos humanos			
A.7.1	Antes del empleo		
A.7.2	Durante del empleo		
A.7.3.	Finalización del empleo o cambio en el puesto de trabajo		
A.8. Gestión de activos			
A.8.1	Responsabilidad sobre los activos		
A.8.2	Clasificación de la información		
A.8.3	Manipulación de los soportes		
A.9 Control de acceso			
A.9.1	Requisitos de negocio para el control de acceso		
A.9.2	Gestión de acceso de usuario		
A.9.3	Responsabilidades del usuarios		
A.9.4	Control de acceso a sistemas y aplicaciones		
A.10 Criptografía			
A.10.1	Controles criptográficos		
A.11 Seguridad física y del entorno			
A.11.1	Áreas seguras		

A.11.2	Seguridad de los equipos		
A.12 Seguridad de las operaciones			
A.12.1	Procedimientos y responsabilidades operacionales		
A.12.2	Protección contra el software malicioso (malware)		
A.12.3	Copias de seguridad		
A.12.4	Registro y supervisión		
A.12.5	Control del software en explotación		
A.12.6	Gestión de la vulnerabilidad técnica		
A.12.7	Consideraciones sobre la auditoria de sistemas de información		
A.13 Seguridad de las comunicaciones			
A.13.1	Gestión de la seguridad de redes		
A.13.2	Intercambio de información		
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información			
A.14.1	Requisitos de seguridad en sistemas de información		
A.14.2	Seguridad en el desarrollo y en los procesos de soporte		
A.14.3	Datos de prueba		
A.15 Relación con proveedores			
A.15.1	Seguridad en las relaciones con proveedores		
A.15.2	Gestión de la provisión de servicios del proveedor		
A.16 Gestión de incidentes de seguridad de la información			
A.16.1	Gestión de incidentes de seguridad de la información y mejoras		
A.17 Aspectos de seguridad de la información para la gestión de la continuidad del negocio			
A.17.1	Continuidad de la seguridad de la información		
A.17.2	Redundancias		
A.18 Cumplimiento			

A.18.1	Cumplimiento de los requisitos legales y contractuales		
A.18.2	Revisiones de la seguridad de la información		

Anexo 5. Formulario de estado actual de madurez del área de TI de la DGLH. Requisitos de la Norma (ISO 27001)

Requisitos de la Norma ISO/IEC 27001:2013		Cumple (Si/No)
4.	**CONTEXTO DE LA ORGANIZACION**	
4.1	Comprensión de la organización y su contexto	
4.2	Comprensión de las necesidades y expectativas de las partes interesadas	
4.3	Determinación del alcance del sistema de seguridad de la información	
4.4	Sistema de gestión de seguridad de la información	
5.	**LIDERAZGO**	
5.1	Liderazgo y compromiso	
5.2	Política	
5.3	Roles organizacionales, responsabilidades y autoridad	
6.	**PLANIFICACION**	
6.1	Acciones para tratar los riesgos y oportunidades	
6.1.1	Consideraciones generales	
6.1.2	Evaluación de riesgos de seguridad de la información	
6.1.3	Tratamiento de los riesgos de seguridad de la información	
6.2	Objetivos de la información y planificación para su consecución	
7.	**SOPORTE**	
7.1	Recursos	
7.2	Competencia	
7.3	Concienciación	
7.4	Comunicación	
7.5	Información documentada	
7.5.1	Consideraciones generales	
7.5.2	Creación y actualización	

7.5.3	Control de la información documentada	
8.	**OPERACIÓN**	
8.2	Evaluación de riesgos de seguridad de la información	
8.3	Tratamiento de riesgos de seguridad de la información	
9.	**EVALUACION DEL DESEMPEÑO**	
9.1	Seguimiento, medición, análisis y evaluación	
9.2	Auditoria interna	
9.3	Revisión de la dirección	
10.	**MEJORA**	
10.1	No conformidades y acciones correctivas	
10.2	Mejora continua	

Anexo 6. Formulario para la identificación de activos del área de TI de la DGLH

Complete la información conforme lo solicitado.

Formulario de identificación y evaluación de activos			
ID Activo:		**Fecha:**	
Responsable:		**Área:**	
Nombre:			
Descripción:			
Categoría:			
Actividades			
Valor:		**Nivel de Criticidad:**	

Anexo 6. Test de Relevamiento de la DGLH basado en la Norma ISO 27001

4	**La organización y su contexto**		
4.1	**Entendiendo la organización y su contexto**	Si	No
1.	¿Están identificados los objetivos del SGSI Sistema de Gestión de la Seguridad de la Información?		
2.	¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?		
3.	¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?		
4.2	**Expectativas de las partes interesadas**	Si	No
1.	¿Se han identificado las partes interesadas?		
2.	¿Existe un listado de requisitos sobre Seguridad de la Información de las partes interesadas?		
3.	¿Existe un listado de requisitos sobre Seguridad de la Información referente a reglamentos, requisitos legales y requisitos contractuales?		
4.3	**Alcance del SGSI**	Si	No
1.	¿Se ha determinado el alcance del SGSI y se conserva información documentada?		
4.4	SGSI Sistema de Gestión de la Seguridad de la información	Si	No
1.	¿El sistema de Gestión de Seguridad de la información SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?		
5	**LIDERAZGO**		
5.1	**Liderazgo y compromiso**	Si	No
1.	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?		
2.	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?		
3.	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?		

5.2	**Política de la Seguridad de la Información**	Si	No
1.	¿Se ha definido una Política de la Seguridad de la Información?		
2.	¿Se ha establecido un marco que permita el establecimiento de objetivos?		
3.	¿Se ha comunicado la política de la Seguridad de la información a las partes interesadas y a toda la empresa?		
4.	¿Se mantiene información documentada de la política del SGSI y de sus objetivos?		
5.3	**Roles y Responsabilidades**	Si	No
1.	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?		
2.	¿Se han comunicado convenientemente las responsabilidades y autoridades para la Seguridad de la Información?		
6	**PLANIFICACIÓN**		
6.1	**Tratamiento de Riesgos y Oportunidades**	Si	No
1.	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?		
2.	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?		
3.	¿Se ha definido un proceso de tratamiento de riesgos?		
4.	¿Se han establecido criterios para elaborar una declaración de aplicabilidad?		
5.	¿Se mantiene información documentada de los puntos anteriores?		
6.2	**Planificación para consecución de objetivos**	Si	No
1.	¿Se han establecido objetivos de la Seguridad de la Información medibles y acordes a los objetivos del negocio?		
2.	¿Los objetivos de la Seguridad de la Información están planificados mediante? -Asignación de responsabilidades -Cronograma de ejecución temporal -Método de evaluación		

3	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?		
7	**SOPORTE**		
7.1	**Recursos**	Si	No
1.	¿Se identifican y asignan los recursos necesarios para el SGSI?		
7.2	**Competencia**	Si	No
1.	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?		
2.	¿Se mantiene información actualizada sobre la competencia del personal?		
7.3	**Concienciación**	Si	No
1.	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?		
2.	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?		
7.4	**Comunicación**	Si	No
1.	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?		
2.	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?		
7.5	**Información Documentada**	Si	No
1.	¿Se dispone de la documentación requerida por la norma más la requerida por la organización incluyendo? -La política de la Seguridad de la Información y el alcance del Sistema de Gestión -Los procesos principales de la seguridad de la Información-Los Documentos exigidos por la Norma ISO 27001, incluyendo registros -Los Documentos propios de Seguridad de la Información identificados por la empresa (instrucciones técnicas etc.)		
2.	¿Existe un control documental donde se verifica? - Quien publica el documento - Quien lo autoriza y como se revisan		

	- Formatos y Soportes de publicación - Su almacenamiento y protección		
3.	¿Se controlan los documentos de origen externo?		
8	**OPERACIÓN**		
8.1	**Control Operacional**	Si	No
1.	¿Los procesos de seguridad de la Información están documentados para controlar que se realizan según lo planificado?		
2.	¿Existe un proceso para evaluar los riesgos en la Seguridad de la Información antes de realizar cambios en el Sistema de Gestión o procesos de Seguridad?		
3.	¿Se establecen medidas y planes para mitigar los riesgos en la Seguridad de la Información ante cambios realizados?		
4.	¿Se identifican y controlan los procesos externalizados en cuanto a los riesgos para la Seguridad de la Información?		
8.2	**Análisis de riesgos de la Seguridad de la Información**	Si	No
1.	¿Se ha establecido un proceso documentado de análisis y evaluación de riesgos para la Seguridad de la Información donde se identifique? -El propietario del riesgo -La importancia del riesgo o nivel de impacto -La probabilidad de ocurrencia		
8.3	**Tratamiento de riesgos de la Seguridad de la Información**	Si	No
1.	¿Se ha implementado un plan de tratamiento de riesgos dónde? -Los propietarios del riesgo están informados y han aprobado el plan -Se documentan los resultados		
2.	¿Se identifican todos los controles necesarios para mitigar el riesgo justificando su aplicación?		
3.	¿Se documenta el nivel de aplicación de todos los controles a aplicar?		
9	**EVALUACIÓN DEL DESEMPEÑO**		
9.1	**Seguimiento y medición**	Si	No

1.	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?		
2.	¿Se ha establecido un proceso documentado para evaluar los resultados de las mediciones y de que estos resultados son tomados en cuenta por los responsables tanto de los procesos como de la Seguridad de la Información?		
9.2	**Auditorías Internas**	Si	No
1.	¿Se ha establecido una programación de Auditorías Internas y asignado responsables?		
2.	¿Se ha definido el alcance y los requisitos para el informe de auditoría?		
3.	¿Se consideran acciones correctivas y propuestas de cambio en los informes de auditoría?		
9.3	**Informe de Revisión por la Dirección**	Si	No
1.	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?		
2.	¿Se documentan los resultados de los informes y la dirección se implica tanto en su conocimiento como en la toma de decisiones sobre los aspectos cruciales para el SGSI?		
10	**MEJORA**		
10.1	**No Conformidades y acciones correctivas**	Si	No
1.	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?		
2.	¿Dentro de las acciones correctivas existe una diferenciación entre acciones correctivas sobre la no conformidad y sobre las causas de la misma?		
10.2	**Mejora continua**	Si	No
1.	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?		

Anexo 7. Especificaciones técnicas de hardware (equipos servidores)

ProLiant DL360 Gen10	
	Núcleos de CPU: 8 x 1.7GHz Tipo de Procesador: Intel(R) Xeon(R) Bronze 3106 Sockets de Procesadores: 1. Núcleos por Socket: 8. Procesadores Lógicos: 8. Número de NICs: 4 Memoria Principal: 32516.52MB (32GB). Total de Discos Rígidos: 2. Capacidad por Disco Rígido: 2000GB (2 TB). Configuración RAID: Sí RAID1. Capacidad de Almacenamiento Total: 2TB.
ProLiant DL360 Gen10	
	Núcleos de CPU: 8 x 1.7GHz Tipo de Procesador: Intel(R) Xeon(R) Bronze 3106 Sockets de Procesadores: 1. Núcleos por Socket: 8. Procesadores Lógicos: 8. Número de NICs: 4 Memoria Principal: 32516.52MB (32GB). Total de Discos Rígidos: 2. Capacidad por Disco Rígido: 2000GB (2TB). Configuración RAID: Sí RAID1. Capacidad de Almacenamiento Total: 2 TB.
ProLiant DL160 Gen9	
	Núcleos de CPU: 8 x 1.7GHz Tipo de Procesador: Intel(R) Xeon(R) Bronze 3106 Sockets de Procesadores: 1. Núcleos por Socket: 8. Procesadores Lógicos: 8. Número de NICs: 4 Memoria Principal: 32516.52MB (32GB). Total de Discos Rígidos: 2. Capacidad por Disco Rígido: 2000GB (2TB). Configuración RAID: Sí RAID1. Capacidad de Almacenamiento Total: 2 TB

ProLiant DL360 G7	
	Núcleos de CPU: 4 x 2.67GHz Tipo de Procesador: Intel(R) Xeon(R) CPU E5640 Sockets de Procesadores: 1. Núcleos por Socket: 4. Procesadores Lógicos: 4. Número de NICs: 4 Memoria Principal: 23990.52MB (24GB). Total de Discos Rígidos: 3. Capacidad por Disco Rígido: 600GB. Configuración RAID: Si, RAID 50. Capacidad de Almacenamiento Total: 1.17 TB.
Estación Backup (Equipo PC)	
	Sistema Operativo: Linux Debian 8.10 32bits Número de NICs: 1 Memoria: 4096 MB (4GB) Capacidad de Almacenamiento 1°: 1TB Capacidad de Almacenamiento 2°: 2TB Núcleos de Procesador: 4 x 2.67GHz Capacidad de Almacenamiento Total: 3.0 TB.

Anexo 8. Tabla de Conectividad

Marca: Mikrotik **Modelo**: RB750G3	Sistema Operativo: Linux Generic Mikrotik Memoria: 256MB Almacenamiento: 16MB Núcleos de Procesador: 4 x 880MHz Puertos LAN/WAN (5 ports)
Marca: Mikrotik **Modelo**: RB951G-2Hnd	
Switch Tenda TEF1016D	16 ports

Anexo 9. Listado de aplicaciones disponibles en los servidores físicos

HP DL360GEN7

[RD_DDJJ_D9]
ReciboDigital
[Spark2019] - Mensajería
Mensajería interna

HP DL160GEN9

[Históricos]
Archivos mapuche anteriores

HP DL360GEN10

[LiqApp Debian 8] - Apps Viejo
Procesos DGLH *
[Otros Mapuche Debian 8] - Otros
Becas, contratos, fondos, extras old
[Pampito WinSR2012]
Archivos compartidos Pampa / Office

HP DL360GEN10

[Aplicaciones Debian 8.11] - Apps Nuevo
Sistemas DGLH **
[Nuxeo Debian 8.11]
Digitalización
[Producción Debian 9]
Mapuche producción / Hist 21 / Extras 21

Server PC- Backup

[Backups]
Archivos de backup

Anexo 10. Listado de las aplicaciones en los Sistemas: Procesos DGLH y Sistemas DGLH

Procesos DGLH *
Acreditaciones
Solicitud de cuentas
Incorporación de cuentas
Generación de novedades
Listados Multipropósitos
Préstamos
Conceptos y acumuladores
Listados refresh
Mutuales
Verificación agentes
Embargos
Comprobantes de pago
Validación de CBU
Backup de bases
Consultas de licencias de maternidades

Sistemas DGLH **
Documentador
Gestión de usuarios y perfiles
Embargos
Planillas de novedades
Novedades
Gráficas de control
Altas

Anexo 11. Formulario para el dimensionamiento del SGSI

Como parte del dimensionamiento del proyecto para la implementación del Sistema de gestión en Seguridad de la Información (SGSI), basado en ISO 27001:2013, le agradecemos responder las siguientes preguntas:

No.	Preguntas
1	¿La Organización tiene claramente definido el alcance del SGSI?
2	Por favor describir brevemente los procesos de negocio que hacen parte del alcance del SGSI. De ser posible, adjuntar cadena de valor o mapa de procesos general.
3	¿Cuántos empleados / funcionarios tiene la Organización?
4	¿Cuantas personas están dentro de los procesos que hacen parte del alcance del SGSI? ¿Dónde están ubicadas físicamente?
5	¿Cuantas oficinas tiene la Organización? Mencionar número y ubicación. ¿Cuántas de estas hacen parte del alcance?
6	¿Está previsto que el proyecto se desarrolle en diferentes ciudades?
	Se han realizado proyectos o la Organización tiene avances en los siguientes aspectos: • Políticas de seguridad • Procedimientos de seguridad • Aseguramiento tecnológico / Hardening • Gestión de activos • Gestión de incidentes de seguridad • Clasificación de información • Definición de objetivos e indicadores de seguridad • Análisis de riesgos • Pruebas de vulnerabilidad y/o Ethical hacking • Capacitación y sensibilización en seguridad • Otros proyectos sobre seguridad de la información. (Mencionar fecha, avance y/o breve alcance de los proyectos)
7	¿La Organización cuenta con un plan de continuidad de negocio (BCP) y/o un plan de contingencia (DRP)?

	¿Estos planes están documentados y aprobados formalmente por la alta gerencia?
8	La gestión de continuidad de negocio de la Organización aborda los siguientes aspectos: • Gobierno de continuidad • Análisis de impacto en el negocio • Estrategias de recuperación • Planes de recuperación de los procesos críticos • Manejo de crisis
9	¿Cuándo se realizaron las dos últimas pruebas a los planes de continuidad y/o contingencia?
10	¿La Organización cuenta con un centro alternativo de trabajo y/o un centro alternativo de procesamiento de información?
11	¿La Organización cuenta con un área o cargo responsable para la gestión de seguridad de la información?
12	¿La Organización cuenta con un área o cargo responsable para la gestión de continuidad del negocio?
13	¿La Organización está certificada en alguna otra norma ISO?
14	¿La Organización ha avanzado en la implementación de responsabilidades de seguridad derivadas de las regulaciones o buenas prácticas relacionadas con protección de datos personales? Mencionar los principales avances.
15	¿Existe alguna ley nacional o regulación para un sector específico sobre seguridad de la información?
16	¿La Organización cuenta con alguno de los siguientes procedimientos?: • Auditorías internas sobre seguridad de la información • Acciones preventivas y correctivas para aspectos relacionados con seguridad de la información
17	¿La Organización ha realizado auditorías internas al SGSI? En caso afirmativo: ¿Ya se implementaron todas las acciones correctivas?

Anexo 12. Formulario para gestión de contactos del área.

Nro.	Rol	Apellido y Nombre	Área	Teléfono/Celular	Email
1					
2					

Anexo 13. Dominios del Anexo A de la Norma ISO 27001:2013.

Nro.	Dominio	Descripción
A5	Políticas de seguridad de la Información	Su propósito es desarrollar e instaurar directivas en la Organización que permitirán facilitar el soporte y la orientación para salvaguardar la información adicional, sirve para realzar el compromiso de la Gerencia para la puesta en marcha del SGSI.
A6	Organización de la seguridad de la información	Su propósito es instituir métodos y procedimientos para establecer el SGSI mediante la asignación de responsables y roles, el acercamiento con autoridades y agrupaciones especiales de interés en el ámbito de seguridad, etc. También permite visualizar como se encuentra estructurada la organización.
A7	Seguridad de los recursos humanos	Su propósito es disponer procedimientos formales sobre todo el personal que labora en la organización (empleados, clientes, proveedores, partes externas) para que realicen un buen uso de la información que va acorde a sus funciones, a través de campañas de concientización, directivas disciplinarias, etc.
A8	Gestión de activos	Su propósito es proveer el uso adecuado de todos los activos de la organización, para ello se debe realizar inventarios, catálogos de clasificación, niveles de uso admisibles, etc. Además, brinda asistencia sobre cómo establecer mecanismos en dispositivos cuyo manejo puede poner en riesgo la información de la organización.
A9	Control de acceso	Su propósito es desplegar directivas de derechos de acceso sobre la información que

		se encuentran en los distintos sistemas de la organización, así como también en las aplicaciones, y otras fuentes que puedan existir. Del mismo modo, brinda soporte sobre la administración de usuarios, contraseñas, pautas para un inicio seguro, etc.
A10	Criptografía	Su propósito es definir e implantar procedimientos para usar tecnologías de seguridad criptográfica. Con esto definido, proporciona métodos para contar con un sistema de administración de claves adecuado acorde a los riesgos que se pueda presentar.
A11	Seguridad física y ambiental	Su propósito es suministrar protección a los departamentos donde se almacena y/o procesa información mediante la creación de zonas de seguridad física. Por otro lado, tiene la intención de proteger a los equipos y todo aquello que proporciona su funcionamiento para garantizar su integridad.
A12	Seguridad de las comunicaciones	Su propósito es declarar en documentos todos los procedimientos a nivel operativo, los cambios que tiene, la capacidad que posee, y como se deben separar los entornos ante variaciones. Así mismo, provee mecanismos para proteger a las distintas herramientas y tecnologías que están involucradas con las operaciones del negocio.
A13	Seguridad de las comunicaciones	Su propósito es proporcionar acceso a los distintos recursos de la red solo a los usuarios autorizados. Para ello es necesario establecer niveles para hacer uso de los servicios de red. Del mismo modo, otorga métodos para proteger la información durante la transferencia en diversos medios. Por último, infiere en el acto de realizar acuerdos sobre confidencialidad.
A14	Adquisición, desarrollo y mantenimiento de Sistemas	Su propósito es definir aquellos requerimientos que posee una organización que cuenta con un departamento de desarrollo de aplicaciones (software), para luego hacer uso de éstas en sus diferentes actividades relacionadas al negocio. De igual manera es para aquellas

		empresas que contratan a un tercero para la producción de sus aplicativos.
	Relaciones con los proveedores	Su propósito es precisar el argumento que se incluirá en los acuerdos que se estipulan con los proveedores, de esta forma se podrá plantear controles de seguridad para todas las actividades en las que se encuentren vinculados.

Fuente: https://www.ijcaonline.org/archives/volume158/number7/aldhahri-2017-ijca-912851.pdf

Anexo 14. Formulario de aplicabilidad de controles del Anexo A de la norma ISO/IEC 27001:2013.

A.5. **Políticas de seguridad**			
A.5.1 Política de seguridad de la información: Orientación de la dirección para la gestión de la seguridad de la información			
ID	Control	Aplicable	Implementación
A.5.1.1	Políticas para la seguridad de la información		
A.5.1.2	Revisión de las políticas para la seguridad de la información		

A.6. **Organización de la seguridad de la información**			
A.6.1 Organización interna			
ID	Control	Aplicable	Implementación
A.6.1.1	Roles y responsabilidades para la seguridad de la información		
A.6.1.2	Separación de deberes		
A.6.1.3	Contacto con las autoridades		
A.6.1.4	Contacto con grupos de interés especial		
A.6.1.5	Seguridad de la información en la gestión de proyectos		

A.6.2	**Dispositivos móviles y teletrabajo**		
A.6.2.1	Política para dispositivos móviles		
A.6.2.2	Teletrabajo		

A.7. **Seguridad de los recursos humanos**			
A.7.1 Antes de asumir el empleo			
ID	Control	Aplicable	Implementación
A.7.1.1	Selección		
A.7.1.2	Términos y condiciones del empleo		
A.7.2	**Durante la ejecución del empleo**		
A.7.2.1	Responsabilidades de la dirección		
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información		
A.7.2.3	Proceso disciplinario		
A.7.3	**Terminación y cambio de empleo**		
A.7.3.1	Terminación o cambio de responsabilidades de empleo		.

A.8. **Gestión de activos**			
A.8.1 Responsabilidad por los activos			
ID	Control	Aplicable	Implementación
A.8.1.1	Inventario de activos		
A.8.1.2	Propiedad de los activos		
A.8.1.3	Uso aceptable de los activos		
A.8.1.4	Devolución de los activos		
A.8.2	**Clasificación de la información**		
A.8.2.1	Clasificación de la información		
A.8.2.2	Etiquetado de la información		

A.8.2.3	Manejo de activos		
A.8.3	**Manejo de medios**		
A.8.3.1	Gestión de medios removibles		
A.8.3.2	Disposición de los medios		
A.8.3.3	Transferencia de medios físicos		

A.9. **Control de acceso**			
A.9.1 Requisitos del negocio para control de acceso			
ID	Control	Aplicable	Implementación
A.9.1.1	Políticas de control de acceso		
A.9.1.2	Acceso a redes y a servicios en red		
A.9.2	**Gestión de acceso de usuarios**		
A.9.2.1	Registro y cancelación de registro de usuarios		
A.9.2.2	Clasificación de la información		
A.9.2.3	Gestión de derechos de acceso privilegiado		
A.9.2.4	Gestión de información de autenticación secreta de usuarios		
A.9.2.5	Revisión de los derechos de acceso de usuarios		
A.9.2.6	Retiro o ajuste de los derechos de acceso		
A.9.3	**Responsabilidades de los usuarios**		
A.9.3.1	Uso de información de autenticación secreta		
A.9.4	**Control de acceso a sistemas y aplicaciones**		
A.9.4.1	Restricción de acceso a la información		
A.9.4.2	Procedimiento de ingreso seguro		
A.9.4.3	Sistema de gestión de contraseñas		

A.9.4.4	Uso de programas utilitarios privilegiados		
A.9.4.5	Control de acceso a códigos fuente de programas		

A.10. **Criptografía**			
A.10.1 Controles criptográficos			
ID	Control	Aplicable	Implementación
A.10.1.1	Política sobre el uso de controles criptográficos		
A.10.1.2	Gestión de llaves		

A.11. **Seguridad física y del entorno**			
A.11.1 Áreas seguras			
A.11.1.1	Perímetro de seguridad física		
A.11.1.2	Controles de acceso físicos		
A.11.1.3	Seguridad de oficinas, recintos e instalaciones		
A.11.1.4	Protección contra amenazas externas y ambientales		
A.11.1.5	Trabajo en áreas seguras		
A.11.1.6	Áreas de despacho y carga		
A.11.2	**Equipos**		
A.11.2.1	Ubicación y protección de los equipos		
A.11.2.2	Servicios de suministro		
A.11.2.3	Seguridad del cableado		
A.11.2.4	Mantenimiento de equipos		
A.11.2.5	Retiro de activos		
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		

A.11.2.7	Disposición segura o reutilización de equipos		
A.11.2.8	Equipos de usuario desatendido		
A.11.2.9	Políticas de escritorio limpio y pantalla limpia		

A.12. **Seguridad de las operaciones**			
A.12.1 Procedimientos operacionales y responsabilidades			
ID	Control	Aplicable	Implementación
A.12.1.1	Procedimientos de operación documentados		
A.12.1.2	Gestión de cambios		
A.12.1.3	Gestión de capacidad		
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		
A.12.2	**Protección contra códigos maliciosos**		
A.12.2.1	Controles contra códigos maliciosos		.
A.12.3	**Copias de respaldo**		
A.12.3.1	Respaldo de la información		
A.12.4	**Registro y seguimiento**		
A.12.4.1	Registro de eventos		
A.12.4.2	Protección de la información de registro		
A.12.4.3	Registros del administrador y del operador		
A.12.4.4	Sincronización de relojes		
A.12.5	**Control de software operacional**		
A.12.5.1	Instalación de software en los sistemas operativos		
A.12.6	**Gestión de la vulnerabilidad técnica**		

A.12.6.1	Gestión de las vulnerabilidades técnicas		
A.12.6.2	Restricciones sobre la instalación de software		
A.12.7	**Consideraciones sobre auditorías de sistemas de información**		
A.12.7.1	Controles de auditorías de sistemas de información		

A.13. **Seguridad de las comunicaciones**			
A.13.1 Gestión de la seguridad de las redes			
ID	Control	Aplicable	Implementación
A.13.1.1	Controles de redes		
A.13.1.2	Seguridad de los servicios de red		
A.13.1.3	Separación en las redes		
A.13.2	**Transferencia de la información**		
A.13.2.1	Políticas y procedimientos de transferencia de información		
A.13.2.2	Acuerdos sobre transferencia de información		
A.13.2.3	Mensajería electrónica		
A.13.2.4	Acuerdos de confidencialidad o de no divulgación		

A.14 **Adquisición, desarrollo y mantenimiento de sistemas**			
A.14.1 Requisitos de seguridad de los sistemas de información			
ID	Control	Aplicable	Implementación
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información		
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas		

A.14.1.3	Protección de las transacciones de los servicios de las aplicaciones		
A.14.2	**Seguridad en los procesos de desarrollo y soporte**		
A.14.2.1	Política de desarrollo seguro		
A.14.2.2	Procedimientos de control de cambios en sistemas		
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		
A.14.2.4	Restricciones en los cambios a los paquetes de software		
A.14.2.5	Principios de construcción de los sistemas seguros		
A.14.2.6	Ambiente de desarrollo seguro		
A.14.2.7	Desarrollo contratado externamente		
A.14.2.8	Pruebas de seguridad de sistemas		
A.14.2.9	Pruebas de aceptación de sistemas		
A.14.3	Datos de prueba		

A.15 **Relaciones con los proveedores**			
A.15.1 Seguridad de la información en las relaciones con los proveedores			
ID	Control	Aplicable	Implementación
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores		
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		
A.15.2	**Gestión de la prestación de servicios de proveedores**		
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		

A.15.2.2	Gestión de cambios en los servicios de 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			
ID	Control	Aplicable	Implementación
A.16.1.1	Responsabilidades y procedimientos		
A.16.1.2	Reporte de eventos de seguridad de la información		
A.16.1.3	Reporte de debilidades de seguridad de la información		
A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos		
A.16.1.5	Respuesta a incidentes de seguridad de la información		
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información		
A.16.1.7	Recolección de evidencia		

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			
ID	Control	Aplicable	Implementación
A.17.1.1	Planificación de la continuidad de la seguridad de la información		
A.17.1.2	Implementación de la continuidad de la seguridad de la información		
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información		
A.17.2	**Redundancias**		

A.17.2.1	Disponibilidad de instalaciones de procesamiento de información		

A.18 Cumplimiento			
A.18.1 Cumplimiento de los requisitos legales y contractuales			
ID	Control	Aplicable	Implementación
A.18.1.1	Identificación de la legislación aplicable a los requisitos contractuales		
A.18.1.2	Derechos de propiedad intelectual		
A.18.1.3	Protección de registros		
A.18.1.4	Privacidad y protección de información de datos personales		
A.18.1.5	Reglamentación de controles criptográficos		
A.18.2	**Revisiones de seguridad**		
A.18.2.1	Revisión independiente de la seguridad de la información		
A.18.2.2	Cumplimiento con las políticas y normas de seguridad		
A.18.2.3	Revisión del cumplimiento técnico		

Anexo 15. Tabla de identificación y valoración de amenazas del área TI de la DGLH

[D] Datos / Información

Bases de Datos de SIU Mapuche

Amenazas	Frecuencia	Degradación o Impacto
5.3.10. [E.15] Alteración accidental de la información	1	0%
5.3.11. [E.18] Destrucción de información	1	50%
5.4.13. [A.15] Modificación deliberada de la información	1	0%
5.4.14. [A.18] Destrucción de información	1	100%
5.4.15. [A.19] Divulgación de información	1	0%
5.4.4. [A.6] Abuso de privilegios de acceso	1	100%
5.4.9. [A.11] Acceso no autorizado	1	0%

Código fuente de aplicaciones

Amenazas	Frecuencia	Degradación o Impacto
5.3.10. [E.15] Alteración accidental de la información	2	100%
5.3.11. [E.18] Destrucción de información	2	100%
5.3.12. [E.19] Fugas de información	2	100%
5.3.4. [E.4] Errores de configuración	2	100%
5.3.9. [E.14] Escapes de información	5	100%
5.4.13. [A.15] Modificación deliberada de la información	2	100%
5.4.14. [A.18] Destrucción de información	2	100%
5.4.15. [A.19] Divulgación de información	2	100%
5.4.4. [A.6] Abuso de privilegios de acceso	2	100%
5.4.9. [A.11] Acceso no autorizado	2	100%

Copias de seguridad de sistemas

Amenazas	Frecuencia	Degradación o Impacto
5.3.1. [E.1] Errores de los usuarios	1	100%
5.3.10. [E.15] Alteración accidental de la información	1	100%
5.3.11. [E.18] Destrucción de información	1	100%
5.3.12. [E.19] Fugas de información	1	100%
5.3.2. [E.2] Errores del administrador	1	100%
5.3.9. [E.14] Escapes de información	1	100%
5.4.13. [A.15] Modificación deliberada de la información	1	100%
5.4.14. [A.18] Destrucción de información	1	100%
5.4.15. [A.19] Divulgación de información	1	100%

5.4.4. [A.6] Abuso de privilegios de acceso	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

Históricos de SIU Mapuche

Amenazas	Frecuencia	Degradación o Impacto
5.3.11. [E.18] Destrucción de información	1	100%
5.3.12. [E.19] Fugas de información	1	100%
5.3.9. [E.14] Escapes de información	1	100%
5.4.13. [A.15] Modificación deliberada de la información	1	100%
5.4.14. [A.18] Destrucción de información	1	100%
5.4.15. [A.19] Divulgación de información	1	100%
5.4.3. [A.5] Suplantación de la identidad del usuario	1	100%
5.4.4. [A.6] Abuso de privilegios de acceso	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

Sistema SIU Mapuche Producción

Amenazas	Frecuencia	Degradación o Impacto
5.3.11. [E.18] Destrucción de información	1	100%
5.3.12. [E.19] Fugas de información	1	100%
5.3.9. [E.14] Escapes de información	1	100%
5.4.13. [A.15] Modificación deliberada de la información	1	100%
5.4.14. [A.18] Destrucción de información	1	100%
5.4.15. [A.19] Divulgación de información	1	100%
5.4.3. [A.5] Suplantación de la identidad del usuario	1	100%
5.4.4. [A.6] Abuso de privilegios de acceso	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

Registros y Logs

Amenazas	Frecuencia	Degradación o Impacto
5.3.11. [E.18] Destrucción de información	1	100%
5.3.12. [E.19] Fugas de información	1	100%
5.3.3. [E.3] Errores de monitorización (log)	1	100%
5.4.1. [A.3] Manipulación de los registros de actividad (log)	1	100%
5.4.13. [A.15] Modificación deliberada de la información	1	100%
5.4.14. [A.18] Destrucción de información	1	100%

[S] SERVICIOS

Portal de inicio

Amenazas	Frecuencia	Degradación o Impacto
5.3.10. [E.15] Alteración accidental de la información	1	100%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	2	100%
5.4.14. [A.18] Destrucción de información	1	100%
5.4.18. [A.24] Denegación de servicio	1	100%

Correo electrónico

Amenazas	**Frecuencia**	**Degradación o Impacto**
5.3.1. [E.1] Errores de los usuarios	3	0%
5.3.10. [E.15] Alteración accidental de la información	2	0%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	0%
5.3.9. [E.14] Escapes de información	2	0%
5.4.11. [A.13] Repudio	2	0%
5.4.13. [A.15] Modificación deliberada de la información	1	100%
5.4.14. [A.18] Destrucción de información	1	100%
5.4.15. [A.19] Divulgación de información	1	100%
5.4.18. [A.24] Denegación de servicio	2	0%

Sistema de Usuarios

Amenazas	**Frecuencia**	**Degradación o Impacto**
5.3.10. [E.15] Alteración accidental de la información	1	100%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	1	100%
5.3.9. [E.14] Escapes de información	1	100%
5.4.11. [A.13] Repudio	1	100%
5.4.13. [A.15] Modificación deliberada de la información	1	100%
5.4.14. [A.18] Destrucción de información	1	100%
5.4.15. [A.19] Divulgación de información	1	100%
5.4.18. [A.24] Denegación de servicio	1	100%
5.4.3. [A.5] Suplantación de la identidad del usuario	2	100%
5.4.4. [A.6] Abuso de privilegios de acceso	1	100%
5.4.9. [A.11] Acceso no autorizado	2	100%

[SW] Software

Base de Datos

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

Programas de oficina

Amenazas	Frecuencia	Degradación o Impacto
5.2.6. [I.5] Avería de origen físico o lógico	3	0%
5.3.1. [E.1] Errores de los usuarios	2	50%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	3	50%
5.3.6. [E.8] Difusión de software dañino	3	0%
5.4.5. [A.7] Uso no previsto	1	0%
5.4.6. [A.8] Difusión de software dañino	2	50%
5.4.9. [A.11] Acceso no autorizado	2	0%

Sistemas Operativos

Amenazas	Frecuencia	Degradación o Impacto
5.2.6. [I.5] Avería de origen físico o lógico	1	100%
5.3.1. [E.1] Errores de los usuarios	2	100%
5.3.10. [E.15] Alteración accidental de la información	1	100%

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

Antivirus

Amenazas	Frecuencia	Degradación o Impacto
5.2.6. [I.5] Avería de origen físico o lógico	2	50%
5.3.1. [E.1] Errores de los usuarios	1	50%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	1	50%
5.3.6. [E.8] Difusión de software dañino	1	100%
5.4.5. [A.7] Uso no previsto	1	50%
5.4.6. [A.8] Difusión de software dañino	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

Software desarrollo propio

Amenazas	Frecuencia	Degradación o Impacto
5.2.6. [I.5] Avería de origen físico o lógico	1	100%
5.3.1. [E.1] Errores de los usuarios	2	100%
5.3.10. [E.15] Alteración accidental de la información	2	100%
5.3.11. [E.18] Destrucción de información	1	100%
5.3.12. [E.19] Fugas de información	1	100%
5.3.13. [E.20] Vulnerabilidades de los programas (software)	1	100%
5.3.2. [E.2] Errores del administrador	2	100%
5.3.6. [E.8] Difusión de software dañino	1	100%
5.3.9. [E.14] Escapes de información	1	100%

5.4.13. [A.15] Modificación deliberada de la información	1	100%
5.4.14. [A.18] Destrucción de información	1	100%
5.4.15. [A.19] Divulgación de información	1	100%
5.4.16. [A.22] Manipulación de programas	1	100%
5.4.3. [A.5] Suplantación de la identidad del usuario	2	100%
5.4.4. [A.6] Abuso de privilegios de acceso	1	100%
5.4.5. [A.7] Uso no previsto	1	100%
5.4.6. [A.8] Difusión de software dañino	1	100%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	1	100%
5.4.8. [A.10] Alteración de secuencia	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

Software SIU Mapuche

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

[H] HARDWARE
Servidores

Amenazas	Frecuencia	Degradación o Impacto
5.2.1. [I.1] Fuego	1	100%
5.2.2. [I.2] Daños por agua	1	100%

5.2.6. [I.5] Avería de origen físico o lógico	1	100%
5.2.7. [I.6] Corte del suministro eléctrico	3	100%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	1	100%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipo hardware	1	100%
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	1	100%
5.3.17. [E.25] Pérdida de equipos	1	100%
5.3.2. [E.2] Errores del administrador	1	100%
5.4.17. [A.23] Manipulación de los equipos	1	100%
5.4.18. [A.24] Denegación de servicio	1	100%
5.4.19. [A.25] Robo	1	100%
5.4.4. [A.6] Abuso de privilegios de acceso	1	100%
5.4.5. [A.7] Uso no previsto	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

Impresoras

Amenazas	Frecuencia	Degradación o Impacto
5.2.1. [I.1] Fuego	1	100%
5.2.2. [I.2] Daños por agua	1	100%
5.2.6. [I.5] Avería de origen físico o lógico	1	100%
5.2.7. [I.6] Corte del suministro eléctrico	1	100%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	1	100%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos hardware	1	100%
5.3.17. [E.25] Pérdida de equipos	1	100%
5.4.19. [A.25] Robo	1	100%

Computadoras de escritorio

Amenazas	Frecuencia	Degradación o Impacto
5.2.1. [I.1] Fuego	1	100%
5.2.2. [I.2] Daños por agua		100%
5.2.6. [I.5] Avería de origen físico o lógico	1	100%
5.2.7. [I.6] Corte del suministro eléctrico	1	100%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	1	100%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos hardware	1	100%

5.3.16. [E.24] Caída del sistema por agotamiento de recursos	1	100%
5.3.17. [E.25] Pérdida de equipos	1	100%
5.3.2. [E.2] Errores del administrador	1	100%
5.4.17. [A.23] Manipulación de los equipos	1	100%
5.4.18. [A.24] Denegación de servicio	1	100%
5.4.19. [A.25] Robo	1	100%
5.4.4. [A.6] Abuso de privilegios de acceso	1	100%
5.4.5. [A.7] Uso no previsto	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

Routers

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

[COM] COMUNICACIONES

Internet

Amenazas	Frecuencia	Degradación o Impacto
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	1	100%
5.3.2. [E.2] Errores del administrador	1	100%
5.3.7. [E.9] Errores de [re-]encaminamiento	1	100%
5.4.10. [A.12] Análisis de tráfico	1	100%
5.4.12. [A.14] Interceptación de información (escucha)	1	100%
5.4.18. [A.24] Denegación de servicio	1	100%

5.4.7. [A.9] [Re-]encaminamiento de mensajes	1	100%
5.4.8. [A.10] Alteración de secuencia	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

Conectividad inalámbrica

Amenazas	Frecuencia	Degradación o Impacto
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	1	0%
5.3.2. [E.2] Errores del administrador	1	100%
5.3.7. [E.9] Errores de [re-]encaminamiento	1	100%
5.4.10. [A.12] Análisis de tráfico	1	100%
5.4.12. [A.14] Interceptación de información (escucha)	1	100%
5.4.18. [A.24] Denegación de servicio	1	100%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	1	100%
5.4.8. [A.10] Alteración de secuencia	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

Red de área local

Amenazas	Frecuencia	Degradación o Impacto
5.3.16. [E.24] Caída del sistema por agotamiento de recursos	3	100%
5.3.2. [E.2] Errores del administrador	2	100%
5.3.7. [E.9] Errores de [re-]encaminamiento	1	100%
5.4.10. [A.12] Análisis de tráfico	1	100%
5.4.12. [A.14] Interceptación de información (escucha)	1	100%
5.4.18. [A.24] Denegación de servicio	1	100%
5.4.7. [A.9] [Re-]encaminamiento de mensajes	1	100%
5.4.8. [A.10] Alteración de secuencia	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

[AUX] EQUIPOS AUXILIARES

Racks

Amenazas	Frecuencia	Degradación o Impacto
5.2.1. [I.1] Fuego	1	100%
5.2.2. [I.2] Daños por agua	1	100%
5.2.6. [I.5] Avería de origen físico o lógico	1	100%
5.2.7. [I.6] Corte del suministro eléctrico	1	100%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	1	100%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos hardware	1	100%

5.4.19. [A.25] Robo	1	100%
5.4.20. [A.26] Ataque destructivo	1	100%

Sistema de alimentación Ininterrumpida (UPS)

Amenazas	Frecuencia	Degradación o Impacto
5.2.1. [I.1] Fuego	1	100%
5.2.2. [I.2] Daños por agua	1	100%
5.2.6. [I.5] Avería de origen físico o lógico	1	100%
5.2.7. [I.6] Corte del suministro eléctrico	1	100%
5.2.8. [I.7] Condiciones inadecuadas de temperatura o humedad	1	100%
5.3.15. [E.23] Errores de mantenimiento / actualización de equipos hardware	1	100%
5.4.19. [A.25] Robo	1	100%
5.4.20. [A.26] Ataque destructivo	1	100%

[L] INSTALACIONES
Oficina administrativa y técnica

Amenazas	Frecuencia	Degradación o Impacto
5.1.3. [N.*] Desastres Naturales	2	100%
5.2.12. [I.11] Emanaciones electromagnéticas	1	100%
5.3.10. [E.15] Alteración accidental de la información	1	100%
5.3.11. [E.18] Destrucción de información	1	100%
5.3.12. [E.19] Fugas de información	1	100%
5.4.13. [A.15] Modificación deliberada de la información	1	100%
5.4.14. [A.18] Destrucción de información	1	100%
5.4.15. [A.19] Divulgación de información	1	100%
5.4.20. [A.26] Ataque destructivo	1	100%
5.4.5. [A.7] Uso no previsto	1	100%
5.4.9. [A.11] Acceso no autorizado	1	100%

[P] PERSONAL
Directora de DGLH

Amenazas	Frecuencia	Degradación o Impacto
5.3.12. [E.19] Fugas de información	1	100%
5.3.18. [E.28] Indisponibilidad del personal	1	100%
5.3.5. [E.7] Deficiencias en la organización	1	100%
5.4.22. [A.28] Indisponibilidad del personal	1	100%

Personal administrativo

Amenazas	Frecuencia	Degradación o Impacto
5.3.12. [E.19] Fugas de información	1	50%
5.3.18. [E.28] Indisponibilidad del personal	1	50%
5.3.5. [E.7] Deficiencias en la organización	1	50%
5.4.22. [A.28] Indisponibilidad del personal	1	50%

Personal técnico

Amenazas	Frecuencia	Degradación o Impacto
5.3.12. [E.19] Fugas de información	1	100%
5.3.18. [E.28] Indisponibilidad del personal	1	100%
5.3.5. [E.7] Deficiencias en la organización	1	100%
5.4.22. [A.28] Indisponibilidad del personal	1	100%