

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS ECONÓMICAS Y FINANCIERAS
CARRERA DE CONTADURÍA PÚBLICA



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE
LA ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN
INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN
(PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS

Trabajo Dirigido para la obtención del Grado de Licenciatura

POR: GABY NORCA ARIAS CHAMBI

TUTOR DOCENTE: MG. SC. AUSBERTO CHOQUE MITA

TUTOR PROFESIONAL: LIC. DENNIS MAGNO APAZA GONZALES

LA PAZ – BOLIVIA
2024

UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS ECONÓMICAS Y FINANCIERAS
CARRERA DE CONTADURÍA PÚBLICA

Trabajo Dirigido:

RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA
SOBRE LA ELABORACIÓN E IMPLEMENTACIÓN DEL
PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE
SAN ANDRÉS

Presentado por: Univ. Gaby Norca Arias Chambi

Para Obtener el Grado Académico de Licenciatura en Contaduría Pública

Nota Numeral:

Nota Literal:

Ha sido:

Director de la Carrera de Contaduría Pública: Mg. Sc. Teddy Orlando Catalán Mollinedo

Tutor Docente: Mg. Sc. Ausberto Choque Mita

Tutor Profesional: Lic. Dennis Magno Apaza Gonzales

DEDICATORIA

Dedico este trabajo a Dios, cuya constante presencia y guía han sido mi refugio y fortaleza en cada momento de mi vida.

A mi padre, cuyo incondicional y amoroso apoyo ha sido el motor que ha impulsado mis sueños y aspiraciones; su fe en mí ha sido la fuerza que me ha llevado a superar cada desafío.

A mi madre, por su amor infinito y su incansable dedicación, que han sido mi mayor fuente de inspiración y consuelo.

A todos ellos, expreso mi más profunda gratitud y amor eterno, pues sin su apoyo, este logro no habría sido posible.



AGRADECIMIENTOS

Quiero expresar mi más sincero y profundo agradecimiento al Lic. Dennis Magno Apaza Gonzales, por su invaluable guía, apoyo constante, enseñanzas y comprensión a lo largo de este camino. Su dedicación ha sido esencial para mi crecimiento.

Agradezco de corazón al Mg. Sc. Ausberto Choque Mita, por su confianza en mí y su valiosa orientación, que me han impulsado a seguir adelante con determinación y seguridad.

Mi gratitud se extiende con especial afecto al Departamento de Auditoría Interna de la Universidad Mayor de San Andrés, por haberme acogido y brindado un espacio donde pude desarrollarme profesionalmente y crecer como persona.

A todos ellos, mi más profundo reconocimiento y aprecio, pues su apoyo ha sido fundamental en mi formación y en la realización de este logro.





RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



ÍNDICE GENERAL

PERFIL DEL TRABAJO DIRIGIDO.....	1 al 89
PLAN DE TRABAJO.....	90 al 94
INFORME FINAL.....	95 al 116



UNIVERSIDAD MAYOR DE SAN ANDRÉS
FACULTAD DE CIENCIAS ECONÓMICAS Y FINANCIERAS
CARRERA DE CONTADURÍA PÚBLICA



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE
LA ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN
INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN
(PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS

Trabajo Dirigido para la obtención del Grado de Licenciatura

POR: GABY NORCA ARIAS CHAMBI

TUTOR DOCENTE: MG. SC. AUSBERTO CHOQUE MITA

TUTOR PROFESIONAL: LIC. DENNIS MAGNO APAZA GONZALES

LA PAZ – BOLIVIA
2024



ÍNDICE ESPECÍFICO

CAPÍTULO I.....	1
1 ASPECTOS GENERALES	1
1.1 INTRODUCCIÓN	1
1.2 MODALIDAD DE TITULACIÓN.....	1
1.2.1 ANTECEDENTES GENERALES	1
1.2.2 DESIGNACIÓN DE TUTOR PROFESIONAL Y TUTOR DOCENTE.....	5
CAPÍTULO II	6
2 MARCO INSTITUCIONAL	6
2.1 ANTECEDENTES DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS	6
2.1.1 MISIÓN	8
2.1.2 VISIÓN	9
2.1.3 OBJETIVOS DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS	9
2.1.4 ESTRUCTURA ORGÁNICA	10
2.1.5 NIVELES JERÁRQUICOS.....	11
2.2 ANTECEDENTES DEL DEPARTAMENTO DE AUDITORÍA INTERNA	12
2.2.1 OBJETIVOS DE LA UNIDAD.....	13
2.2.2 FUNCIONES DE LA UNIDAD.....	13
2.2.3 ORGANIGRAMA	15
3 MARCO TEÓRICO.....	16
3.1 AUDITOR.....	16
3.2 AUDITOR INTERNO	16
3.3 AUDITOR GUBERNAMENTAL.....	17
3.4 AUDITORÍA	17
3.5 AUDITORÍA INTERNA	18
3.6 AUDITORÍA GUBERNAMENTAL	18
3.7 RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA	19
3.8 AUDITABILIDAD.....	19
3.9 PRONUNCIAMIENTO DE AUDITABILIDAD.....	19



3.10	ELEMENTOS DE TRABAJO DEL AUDITOR INTERNO	20
3.11	RESPONSABILIDAD DEL AUDITOR GUBERNAMENTAL	21
	CAPÍTULO III	22
4	DISEÑO METODOLÓGICO	22
4.1	PLANTEAMIENTO DEL PROBLEMA	22
4.1.1	IDENTIFICACIÓN DEL PROBLEMA	23
4.2	PLANTEAMIENTO DE OBJETIVOS	24
4.2.1	OBJETIVO GENERAL	24
4.2.2	OBJETIVO ESPECÍFICO	25
4.3	JUSTIFICACIÓN DEL TRABAJO.....	25
4.3.1	JUSTIFICACIÓN TEÓRICA	25
4.3.2	JUSTIFICACIÓN PRÁCTICA.....	26
4.4	MEMORÁNDUM DE ASIGNACIÓN DE TRABAJO	26
4.5	ALCANCE	28
4.6	OBJETO.....	28
4.7	METODOLOGÍA	29
4.8	PROGRAMA DE TRABAJO.....	29
5	MARCO LEGAL Y NORMATIVO.....	40
5.1	MARCO NORMATIVO GENERAL.....	40
5.1.1	CONSTITUCIÓN POLÍTICA DEL ESTADO PLURINACIONAL DE BOLIVIA	40
5.1.2	LEY 1178 DE ADMINISTRACIÓN Y CONTROL GUBERNAMENTALES .	41
5.1.3	DECRETO SUPREMO 23215 REGLAMENTO PARA EL EJERCICIO DE LAS ATRIBUCIONES DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA, ACTUAL CONTRALORÍA GENERAL DE ESTADO	41
5.1.4	DECRETO SUPREMO 23318-A REGLAMENTO DE LA RESPONSABILIDAD POR LA FUNCIÓN PÚBLICA	42
5.1.5	DECRETO SUPREMO 26237 MODIFICACIONES AL REGLAMENTO DE LA RESPONSABILIDAD POR LA FUNCIÓN PÚBLICA.....	42



5.1.6	RESOLUCION N° CGE/094/2012 NORMAS GENERALES DE AUDITORIA GUBERNAMENTAL.....	42
5.1.7	RESOLUCIÓN N° CGE/018/2024 REGLAMENTO PARA LA ELABORACIÓN DE INFORMES DE AUDITORÍA CON INDICIOS DE RESPONSABILIDAD (RE/CE-029) VERSION 3.	43
5.2	MARCO NORMATIVO ESPECIFICO	43
5.2.1	LEY 164 LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.....	43
5.2.2	DECRETO SUPREMO 1793 REGLAMENTO PARA EL DESARROLLO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.....	43
5.2.3	RESOLUCIÓN ADMINISTRATIVA N° AGETIC/RA/0051/2017.....	44
5.2.4	RESOLUCIÓN ADMINISTRATIVA N° AGETIC/RA/0059/2018.....	44
6	DESARROLLO DEL TRABAJO	44
6.1	NOTIFICACIÓN DE LA AGETIC	45
6.2	DESIGNACIÓN DEL RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN DE LA UMSA	45
6.3	CONFORMACIÓN DEL COMITÉ DE SEGURIDAD DE INFORMACIÓN DE LA UMSA.....	48
6.4	ESTRUCTURA Y CONTENIDO DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UMSA	52
6.4.1	ANTECEDENTES Y MARCO NORMATIVO.....	52
6.4.2	ALCANCES DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI).....	53
6.4.3	METODOLOGÍA DE LA GESTIÓN DE RIESGOS	54
6.4.4	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN	55
6.4.5	CONTROLES MÍNIMOS DE LA SEGURIDAD DE LA INFORMACIÓN.....	60
6.4.6	INDICADORES Y MÉTRICAS	61
6.5	CRONOGRAMA DE IMPLEMENTACIÓN DEL PISI - UMSA.....	61
6.6	APROBACIÓN DEL PISI - UMSA	62



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



6.7	IMPLEMENTACIÓN DEL PISI - UMSA.....	62
6.7.1	APLICACIÓN DE CONTROLES.....	62
6.7.2	CAPACITACIÓN E INDUCCIÓN	64
6.7.3	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	64
6.7.4	REVISIÓN Y MEJORA CONTINUA	65
7	COMUNICACIÓN DE RESULTADOS	66
8	CONCLUSIONES	71
9	RECOMENDACIONES	72
10	BIBLIOGRAFÍA	73
11	ANEXOS	75



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



RESUMEN

En cumplimiento a solicitud efectuada mediante nota CGE/GPA2/171-026/2024 del 1 de marzo de 2024, emitida por la Contraloría General del Estado, y en atención a proveído emitido por el Rector de la Universidad Mayor de San Andrés (UMSA) en la Hoja de Ruta VC-5338 del 5 de marzo de 2024, se llevó a cabo el “Relevamiento de Información Específica sobre la Elaboración e Implementación del Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés”.

Este relevamiento, encargado por la Jefatura del Departamento de Auditoría Interna a través del memorándum MEM.T.AUD. No.008/2024 del 14 de marzo de 2024, fue solicitado conforme a los “Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público”, aprobados mediante Resolución Administrativa No. AGETIC/RA/0051/2017. El objetivo principal fue determinar la auditabilidad, evaluar la predisposición de la Máxima Autoridad Ejecutiva y verificar la existencia de información y documentación necesarias para ejecutar la auditoría, según lo estipulado en el Numeral 217 de las Normas Generales de Auditoría Gubernamental.

El Plan Institucional de Seguridad de la Información de la UMSA fue aprobado mediante la Resolución del Honorable Consejo Universitario N°298/2019 del 4 de septiembre de 2019. Sin embargo, desde la gestión 2020 hasta la fecha del presente relevamiento, no se ha designado nuevo personal que conforme el Comité de Seguridad de la Información (CSI) ni un Responsable de Seguridad de la Información (RSI). Esta ausencia de designaciones ha impedido la continuidad en la implementación del Plan Institucional de Seguridad de la Información de la UMSA.

Entre los principales hallazgos del relevamiento destacan la ausencia de designación de personal clave, lo que ha afectado significativamente la implementación continua del Plan Institucional de Seguridad de la Información. Es fundamental que la Máxima Autoridad



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



Ejecutiva de la UMSA realice las designaciones necesarias y tome las medidas pertinentes para asegurar la continuidad y efectividad del PISI. Se recomienda también la revisión y actualización periódica del plan para adaptarse a las necesidades y desafíos actuales en materia de seguridad de la información.



CAPÍTULO I

1 ASPECTOS GENERALES

1.1 INTRODUCCIÓN

En atención a solicitud formalizada mediante la nota CGE/GPA2/171-026/2024, emitida el 1 de marzo de 2024 por la Contraloría General del Estado, y en cumplimiento de lo establecido en el inciso h) del artículo 3 del Reglamento para el Ejercicio de las Atribuciones de la Contraloría General del Estado, así como en el numeral 217.03 de las Normas Generales de Auditoría Gubernamental, aprobada mediante Resolución N° CGE/094/2012 de fecha 27 de agosto de 2012, y mediante proveído del Rector de la Universidad Mayor de San Andrés (UMSA) en Hoja de Ruta VC-5338 de fecha 5 de marzo de 2024, se requirió que la Unidad de Auditoría Interna de la UMSA llevar a cabo el trabajo de relevamiento de información específica sobre la elaboración e implementación del “Plan Institucional de Seguridad de la Información” (PISI). Este trabajo debe de realizarse de acuerdo con los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público, aprobados por la AGETIC mediante Resolución Administrativa No. AGETIC/RA/0051/2017 de fecha 19 de septiembre de 2017.

La ejecución de esta labor fue instruida por Jefatura del Departamento de Auditoría Interna, a través del memorándum MEM.T.AUD. No.008/2024 de fecha 14 de marzo de 2024.

1.2 MODALIDAD DE TITULACIÓN

1.2.1 ANTECEDENTES GENERALES

Mediante Resolución del Honorable Consejo Universitario N°472/2021 de 8 de septiembre de 2021, en su Artículo Primero se resuelve:

“Aprobar el “REGLAMENTO ESPECÍFICO DE LA MODALIDAD DE GRADUACIÓN: TRABAJO DIRIGIDO PARA LA OBTENCIÓN DEL NIVEL



LICENCIATURA EN LA UNIVERSIDAD MAYOR DE SAN ANDRÉS”, en sus V capítulos y 17 Artículos, (...)”, reglamento que, en su contenido entre otros, establece:

Artículo 4. Definición El Trabajo Dirigido es una modalidad de graduación de carácter individual para acceder al nivel académico de Licenciatura, consiste en la realización de prácticas pre profesionales desarrolladas en instituciones externas o dentro la misma Universidad, supervisadas y evaluadas por profesionales en calidad de tutores. Existen dos formas para el desarrollo del Trabajo Dirigido:

1. Trabajo Dirigido Externo
2. Trabajo Dirigido Interno

(...)

Artículo 6. Trabajo Dirigido Interno Es el realizado en las distintas dependencias de la Universidad Mayor de San Andrés bajo la guía de un tutor profesional y un tutor docente, sin necesidad de suscribir Convenios Específicos.

(...)

Artículo 9. Conclusión plan de estudios. El postulante deberá haber aprobado la totalidad de las asignaturas del plan de estudios y cumplir los requisitos estipulados por su Carrera.

Artículo 10. Promedio. El promedio mínimo para acceder a esta modalidad de graduación es de 60 puntos.

Artículo 11. Plazo. La dedicación del postulante en las actividades desarrolladas deberá ser exclusiva, debiendo concluirse el trabajo dirigido en el plazo máximo de 8 (ocho) meses.

(...)

Artículo 14. Evaluación. La evaluación principal estará a cargo del tutor profesional externo debido al vínculo directo con el postulante a trabajo dirigido, mismo que en base al cumplimiento de objetivos emitirá los informes respectivos.

Artículo 15. Informes. Durante la realización del trabajo dirigido el postulante presentará a la Unidad Académica autorizada por su Carrera dos (2) informes trimestrales y uno (1) final elaborado por su tutor profesional”.



En fecha 8 de diciembre de 2021, se Aprueba la Resolución del Honorable Consejo Universitario N°713/2021, que Resuelve:

“Artículo Primero. COMPLEMENTAR el REGLAMENTO ESPECÍFICO DE LA MODALIDAD DE GRADUACIÓN: TRABAJO DIRIGIDO PARA LA OBTENCIÓN DEL NIVEL DE LICENCIATURA EN LA UNIVERSIDAD MAYOR DE SAN ANDRÉS, aprobado con Resolución HCU. No. 472/2021; de acuerdo al siguiente detalle: DISPOSICIONES TRANSITORIAS

PRIMERO. Aquellos estudiantes universitarios que, a la fecha de puesta en vigencia del presente Reglamento, se encuentren en pleno desarrollo de la modalidad de graduación “Trabajo Dirigido” según Reglamentos Específicos de sus Carreras, podrán acogerse al marco regulatorio actual, solicitando expresamente mediante nota dirigida a su Dirección de Carrera acogerse a este Reglamento, cumpliendo todos los requisitos establecidos en esta modalidad de graduación siendo uno de ellos haber obtenido el 60% del promedio general de calificación.

SEGUNDA. Toda vez que la migración al presente Reglamento de los estudiantes que así lo requieran será formalmente solicitada se exime de cualquier responsabilidad administrativa a todas las Autoridades Académicas que se involucren en los trámites que emerjan de la solicitud presentada.

TERCERA La migración de aquellos estudiantes que estuvieran en pleno desarrollo de sus modalidades de graduación (trabajo dirigido) es voluntaria y debe ser expresamente solicitada.

CUARTA. Con fines de evitar observaciones a tiempo de los tramites subsecuentes se deberá acompañar una copia de la presente Resolución en los trámites del solicitante, así como de la Resolución específica e individual del Honorable Consejo de Carrera que autorice esta migración de cada uno de los estudiantes que así lo soliciten.

Artículo Segundo. ENCOMENDAR a las unidades académicas y administrativas dar fiel cumplimiento a la presente Resolución.



Posteriormente, en fecha 11 de mayo de 2022, se Aprueba la Resolución del Honorable Consejo Universitario N°151/2022 que Resuelve:

“Artículo Primero: APROBAR que, para el desarrollo de trabajos Dirigidos como Modalidad de Graduación al Interior de la Universidad Mayor de San Andrés, no será necesaria la suscripción de convenios Individuales entre las Facultades y las unidades académicas y administrativas de destino, al tratarse de una misma institución.

(...)

Artículo Tercero. Las Direcciones de Carrera Adecuaran el desarrollo del Trabajo Dirigido del estudiante de acuerdo a la Reglamentación Vigente”.

Finalmente, en fecha 18 de agosto de 2022, mediante Resolución del Honorable Consejo Universitario N.º 330/2022, se aprueba: “Artículo Primero. Aprobar el “REGLAMENTO ESPECIFICO DE MODALIDAD DE GRADUACIÓN POR TRABAJO DIRIGIDO PARA LA OBTENCIÓN DEL NIVEL DE LICENCIATURA LA UNIVERSIDAD MAYOR DE SAN ANDRÉS” en sus V Capítulos y 20 Artículos...”, documento que, entre otros, dispone:

“Artículo 6° Trabajo Dirigido Interno. Se realiza en las distintas dependencias de la Universidad Mayor de San Andrés, bajo la guía de un Tutor Profesional y un Tutor Docente, sin necesidad de suscribir Convenios Específicos.

Artículo 7° Tutor Docente. Es el Docente designado por la Dirección de Carrera para cada Trabajo Dirigido, siendo sus obligaciones:

- a) Orientar al postulante y efectuar un seguimiento periódico para validar el avance del Trabajo Dirigido.
- b) Realizar la supervisión durante el desarrollo del trabajo dirigido, manteniendo contacto con el tutor profesional y el estudiante.

(...)

Artículo 8° Tutor Profesional (externo). Es el profesional designado por la entidad pública o privada de Convenio o perteneciente a alguna dependencia de la Universidad Mayor de



San Andrés, debe acreditar el grado académico universitario igual o superior al que aspira el postulante y los conocimientos necesarios para realizar una tutela efectiva, siendo sus obligaciones:

- a) Guiar y evaluar el cumplimiento del Trabajo Dirigido.
 - b) Facilitar los medios para el desarrollo del Trabajo Dirigido.
 - c) Organizar las actividades a desarrollar por el postulante durante su estancia en la Institución.
 - d) Supervisar las actividades preprofesionales del postulante garantizando que reciba la formación práctica correspondiente.
 - e) Emitir dos informes trimestrales y uno final, evaluando el desarrollo del Trabajo Dirigido realizado por el postulante en la institución.
- (...)

Artículo 16° Informes. Durante la realización del trabajo Dirigido el postulante presentará a la Dirección de Carrera dos (2) informes trimestrales y un (1) Informe Final, rubricado por el Tutor Profesional y el Tutor Docente. En el Informe Final, el Tutor Profesional debe asignar la calificación cualitativa, misma que debe ser validada por el Tutor Docente con calificación numérica".

1.2.2 DESIGNACIÓN DE TUTOR PROFESIONAL Y TUTOR DOCENTE

Mediante MEM.T.AUD.No.194/2023, de fecha 13 de noviembre de 2023, se designó como Tutor Profesional al Lic. Dennis Magno Apaza Gonzales, Auditor del Departamento de Auditoría Interna.

Asimismo, la Dirección de la Carrera de Contaduría Pública realizó la designación del Mg. Sc. Ausberto Choque Mita, Docente de la Carrera de Contaduría Pública, como Tutor Docente del presente trabajo dirigido.



CAPÍTULO II

2 MARCO INSTITUCIONAL

2.1 ANTECEDENTES DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS

La Universidad Mayor de San Andrés fue denominada inicialmente como Universidad de La Paz y fue creada mediante Decreto Supremo de 25 de octubre de 1830 durante la Presidencia del Mariscal Andrés de Santa Cruz y Calahumana.

La Historia de la Universidad de La Paz consta de tres periodos:

1. La Universidad oficial que comprende desde su fundación hasta la Revolución de junio de 1930.
2. La Universidad semi autónoma o autárquica, que comprende desde la revolución de junio de 1930 hasta el advenimiento al Rectorado de la Universidad de don Héctor Ormachea Zalles en junio de 1936.
3. La Universidad plenamente autónoma que alcanza de este último hecho hasta nuestros días.

El 30 de noviembre de 1830 se verifica la fundación de la Universidad Mayor de San Andrés e inauguración oficial de las faenas universitarias.

El 31 de agosto de 1831 La Asamblea Constituyente dictó la ley que instituye a la Universidad Mayor de San Andrés que funcionó con las siguientes facultades:

- ❖ Facultad de Derecho y Ciencias Políticas
- ❖ Facultad de Medicina y ramas anexas: Farmacia, Odontología, Obstetricia.
- ❖ Facultad de Teología
- ❖ Facultad de Ciencias Económicas y Financieras.
- ❖ Facultad de Ciencias Físicas y Matemáticas
- ❖ Facultad de Filosofía y Humanidades
- ❖ Conservatorio Nacional de Música y
- ❖ Colegio de Artes



El 24 de marzo de 1832, se dio a conocer el Estatuto que regulaba el régimen de la Universidad. En 1901 se conforma la asociación de estudiantes, que después se llamó Federación de Estudiantes. Hoy funciona con el nombre de Federación Universitaria Local (FUL). El 22 de marzo de 1930 se creó la Biblioteca Universitaria.

El 29 de junio de 1930 se emite la Declaratoria de la autonomía universitaria; posteriormente se reforma la Constitución mediante Referéndum popular para consagrar la autonomía. En 1932 el Estatuto Universitario cumple su primer centenario. Posteriormente, en 1936 se promulgan dos decretos históricos para que la UMSA pueda ejercer la autonomía universitaria y el manejo de los recursos, situación que fue gracias al rectorado de Don Héctor Ormachea Zalles y firmado por el Presidente Toro; beneficiándose a todo el sistema universitario, autoridad responsable de la adquisición del edificio del Colegio Militar hoy Monoblock Central.

En 1938 se consagra la autonomía universitaria en la Constitución Política del Estado. El 21 de julio de 1946 El Gobierno Nacional confirió a la UMSA la Gran Cruz de la Orden del Cóndor de los Andes. El 10 de febrero de 1939 se aprueba la Reforma Estatutaria entonces, la UMSA estaba compuesta por 3 Facultades: Ciencias Biológicas, Ciencias Sociales y Ciencias Exactas.

En 1953 se creó la Comisión Nacional de Reforma Educacional. En 1955 se dictó el código de Educación que determinó modificaciones sustanciales en la estructura educativa boliviana. En 1967, en el rectorado del Ing. Hugo Zárate Barrau se realizó una edición definitiva bajo el título “Historia de la Universidad Mayor de San Andrés”.

En abril de 1970 Se desencadenó un proceso de revolución universitaria, protagonizada por jóvenes inspirados en posiciones marxistas, donde los estudiantes exigieron el poder y lo tomaron, solucionando el problema con la inclusión del cogobierno paritario y el veto político.¹

¹ LA RAZON. (1948, 20 de octubre). Historia de la Universidad de La Paz (p. 9-10). Obtenido de <https://www.umsa.bo/historia>



La Universidad Mayor de San Andrés, es la principal universidad pública del Estado Plurinacional de Bolivia, establecida en el departamento de La Paz y desplegada a lo largo del mismo, en la ciudad capital y sus provincias en 4 Centros Regionales Universitarios (CRUs) y diversas Sedes Universitarias Locales (SULs). La UMSA es la segunda universidad más antigua de Bolivia, después de la Universidad San Francisco Xavier de Chuquisaca (1624) y la más representativa del Sistema de la Universidad Boliviana.

En el ámbito del alumnado, hasta el año 2016, la Universidad Mayor de San Andrés tenía en sus aulas alrededor de 74.391 estudiantes, de los cuales 4013 obtuvieron el título de licenciado o su equivalente (pregrado).

En julio del 2021, según el ranking webometrics, es considerada la Primera Mejor Universidad de Bolivia.²

2.1.1 MISIÓN

La Universidad Mayor de San Andrés produce conocimiento científico, tecnológico y cultural, pertinente y relevante, inter y transdisciplinario, que revaloriza los saberes ancestrales y promueve políticas públicas, respondiendo a la demanda y necesidades locales, regionales y nacionales, hacia un desarrollo sostenido.

Forma profesional altamente calificados, con compromiso y responsabilidad social, con reflexión y pensamiento crítico: emprendedores y constructores de una sociedad justa e inclusiva. Promueve la interacción con el Estado, la sociedad y la comunidad científica y académica internacional, promoviendo la transformación y búsqueda conjunta de innovadoras soluciones; impulsando la progresiva mejora de calidad de vida de la población, preservando el medio ambiente y fortaleciendo la identidad cultural.

² UNIVERSIDAD MAYOR DE SAN ANDRES. 2017. Unidad de Transparencia. Obtenido de https://transparencia.umsa.bo/mision_vision.



2.1.2 VISIÓN

Hacia el 2025 la Universidad Mayor de San Andrés es una universidad emprendedora e innovadora, con reconocimiento internacional, valorada por su contribución a la generación de conocimiento y formación de profesionales líderes en la revolución del pensamiento con responsabilidad y compromiso al servicio de la sociedad y la humanidad. Mirando hacia el 2030, en concordancia con las tendencias de la educación superior y la ciencia, tecnología e innovación, en el marco de los Objetivos del Desarrollo Sostenible al 2030, la UMSA se ha trazado los siguientes objetivos en ese horizonte, que coincide con el bicentenario de la creación de la Universidad Mayor de San Andrés:

- ❖ Lograr la acreditación internacional plena de la UMSA.
- ❖ Formar profesionales líderes y conductores del desarrollo regional y nacional, con compromiso por la vida y con responsabilidad social.
- ❖ Generar conocimiento científico promotor del desarrollo social económico, humano y ambiental de Bolivia, consolidándose como entidad estratégica, promotora de políticas públicas que privilegien un futuro digno a las futuras generaciones de manera sostenible.
- ❖ Innovar un modelo de aseguramiento de la calidad de la educación superior, que la sitúe entre las mejores universidades de Latinoamérica.³

2.1.3 OBJETIVOS DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS

Lograr la interdisciplinariedad, concurrencia e interacción de la investigación que desarrolla la Universidad Mayor de San Andrés para aumentar la eficiencia y efectividad de la docencia, la interacción social y la difusión, como base de la gestión del conocimiento.

³ UNIVERSIDAD MAYOR DE SAN ANDRES. Obtenido de <https://www.umsa.bo/web/guest/quienes-somos>



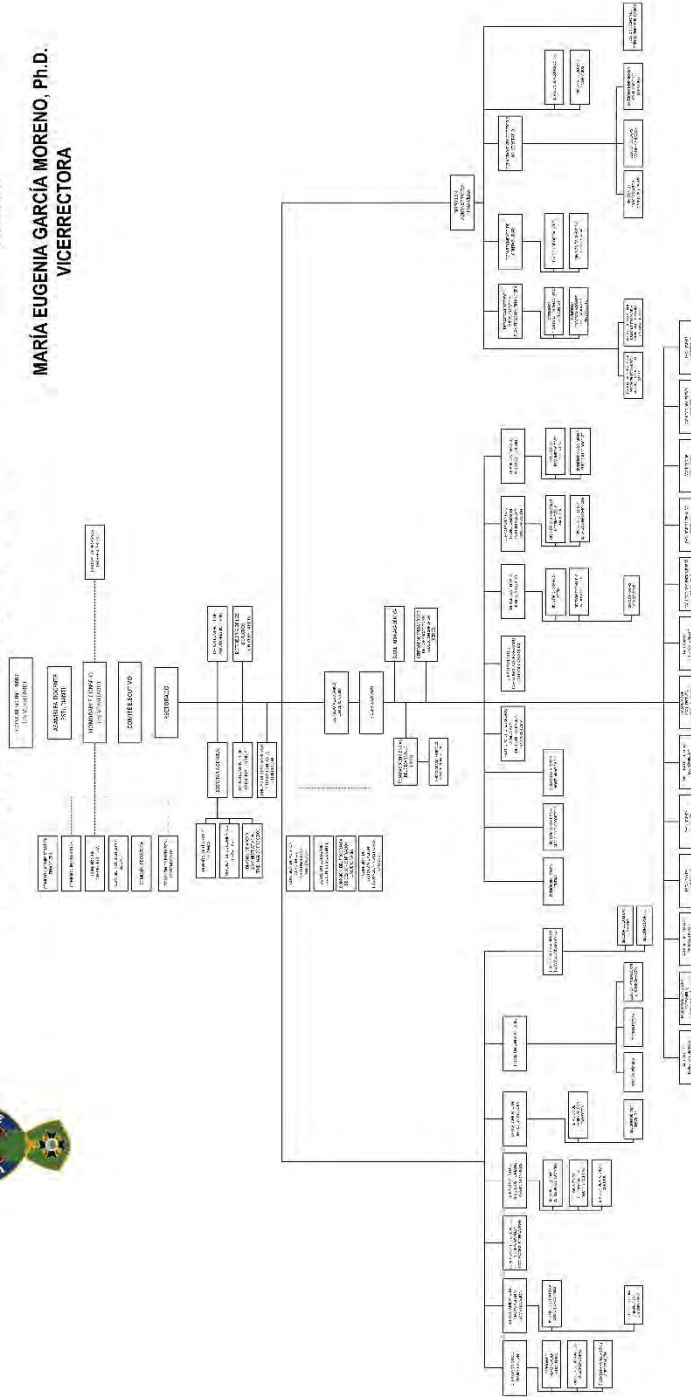
2.1.4 ESTRUCTURA ORGÁNICA

UNIVERSIDAD MAYOR DE SAN ANDRÉS
ESTRUCTURA ORGÁNICA – 2023
RESOLUCIÓN HCU N° 535/2023, de 13/12/2023



M.Sc. OSCAR A. HEREDIA VARGAS
RECTOR

MARIA EUGENIA GARCÍA MORENO, Ph.D.
VICERRECTORA





2.1.5 NIVELES JERÁRQUICOS

El Reglamento Específico del Sistema de Organización Administrativa de la UMSA (RESOA), del 5 de julio de 2017, en su Artículo 15° (Proceso de diseño y/o rediseño organizacional), numeral VI, establece los siguientes niveles jerárquicos de la estructura organizacional de la UMSA:

Nivel Directivo

En el cual se establecen los objetivos, las políticas y las estrategias:

- ❖ Honorable Consejo Universitario
- ❖ Consejo Académico Universitario
- ❖ Honorables Consejos Facultativos
- ❖ Honorables Consejos de Carrera
- ❖ Consejos Técnicos

Nivel Ejecutivo

En el cual se aplican las políticas y la toma de decisiones para el cumplimiento de los planes estratégicos y el funcionamiento de la UMSA de acuerdo con los lineamientos definidos en el nivel directivo:

- ❖ Rectorado
- ❖ Vicerrectorado
- ❖ Decanatos
- ❖ Vicedecanatos
- ❖ Dirección Administrativa Financiera

Nivel Operativo

Donde se ejecutan las tareas y actividades cotidianas de la UMSA:

Área Académica

- ❖ Carreras
- ❖ Unidades de Investigación y/o Posgrado

⁴ UNIVERSIDAD MAYOR DE SAN ANDRES. Obtenido de: <https://www.umsa.bo/web/guest/quienes-somos>



- ❖ Unidades Académicas Facultativas
- ❖ Unidades Administrativas del área académica

Área Administrativa

- ❖ Secretaría General
- ❖ Secretaría Académica
- ❖ Departamentos
- ❖ Divisiones
- ❖ Secciones de la Administración Central⁵

2.2 ANTECEDENTES DEL DEPARTAMENTO DE AUDITORÍA INTERNA

El Departamento de Auditoría Interna de la Universidad Mayor de San Andrés, inicia sus actividades a partir de 1971, figurando, así como Oficina de Auditoría Interna con dependencia del Rectorado. En 1984, se determina en el VI Congreso de Universidades que el DAI figura en la Estructura Orgánica al nivel de Staff, aprobándose bajo la Resolución N°530 del 11 de abril de 1984, referente al Manual de Organización y Funciones, presentadas por el Departamento de Auditoría Interna.

De acuerdo a la Ley N°1178 de los Sistemas de Administración y Control Gubernamentales, promulgada el 20 de julio de 1990, el Departamento de Auditoría Interna (DAI) de la UMSA, forma parte del Sistema de Control Gubernamental cuyo Órgano Rector es la Contraloría General del Estado, como Autoridad Superior del Estado (según Art. 13°, 14°, 15° y 16° de la Ley N°1178 y Art. 1°, 2° y 3° del D.S. 23215 de fecha de 22 de julio de 1992).⁶

⁵ UNIVERSIDAD MAYOR DE SAN ANDRÉS. 2021. Manual de Organizaciones y Funciones 2021. 7p.

⁶ UNIVERSIDAD MAYOR DE SAN ANDRÉS. Departamento de Auditoría Interna. Obtenido de <https://dai.umsa.bo/test-0>



2.2.1 OBJETIVOS DE LA UNIDAD

Los objetivos del Departamento de Auditoría Interna están definidos por los artículos 14° y 15° de la ley 1178, de Administración y control gubernamental:

- ❖ Ejercer el control interno posterior de las actividades realizadas por la UMSA.
- ❖ Evaluar el grado de cumplimiento y eficacia de los sistemas de administración y control gubernamentales.
- ❖ Evaluar los instrumentos de control interno incorporados a los sistemas de administración y control gubernamentales.
- ❖ Determinar la confiabilidad de los registros y estado financiero.
- ❖ Analizar los resultados y la eficiencia de las operaciones que ejecuta la Universidad Mayor de San Andrés.
- ❖ Realizar exámenes de auditoría requeridos por la máxima autoridad ejecutiva de la entidad, Rectorado.
- ❖ Asesorar a la máxima autoridad de la UMSA en asuntos de su competencia.⁷

2.2.2 FUNCIONES DE LA UNIDAD

- a. Elaborar el Plan estratégico del Departamento de Auditoría Interna, sobre la base de los objetivos estratégicos de la Universidad Mayor de San Andrés.
- b. Planificar y elaborar el Plan Operativo Anual del Departamento de Auditoría Interna para remitir a la Contraloría General del Estado Plurinacional de Bolivia previa, aprobación del Rector de la Universidad Mayor de San Andrés. (determinando el requerimiento de los recursos humanos, infraestructura y materiales).
- c. Priorizar la ejecución de cronograma de auditorías a realizar.
- d. Realizar los siguientes exámenes de Auditoría Interna; a) Auditoría Financiera, b) Auditoría Operacional, c) Auditoría Ambiental, d) Auditoría Especial, e) Auditoría

⁷ UNIVERSIDAD MAYOR DE SAN ANDRES. 2021. Manual de Organizaciones y Funciones 2021. 41p.

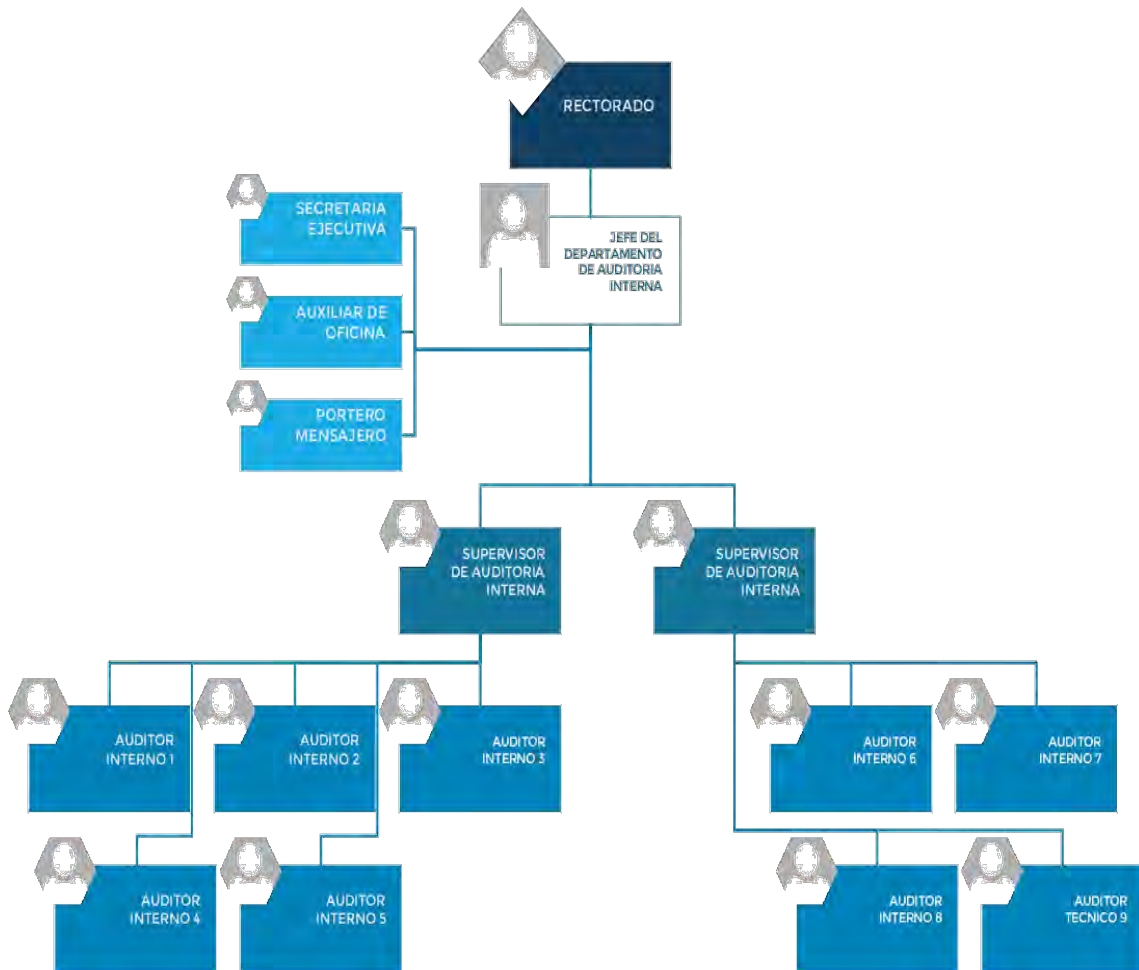


- de Proyectos de Inversión Pública y f) Auditoría de la SAYCO, (Normas de Auditoria Gubernamental NAG Res. CGR – 1/119/2002).
- e. Planificar, ejecutar y comunicar los resultados de las auditorias ejecutadas, así como efectuar la supervisión, el control de calidad de los informes a emitir, y la revisión de los papeles de trabajo emergentes de los exámenes practicados.
 - f. Emitir informes de auditoría independientes y oportunos.
 - g. Promover la capacitación permanente de los auditores internos en coordinación con el CENCAP y el Departamento de Recursos Humanos Administrativos.
 - h. Asesorar a las autoridades de la Administración Central y Académica, a los ejecutivos de la FUL, los centros de estudiantes y apoyara a las jefaturas de las áreas desconcentradas para el mejor cumplimiento de sus responsabilidades institucionales.
 - i. Hacer cumplir las normas de auditoría gubernamental e instructivos emitidos por la Contraloría General del Estado Plurinacional de Bolivia, emergentes de la Ley 1178.
 - j. Emitir opinión sobre la confiabilidad de registros y estados financieros de la UMSA, sobre la base del instructivo emitido por la Contraloría General del Estado Plurinacional de Bolivia.
 - k. Verificar por el cumplimiento de las políticas establecidas en el estatuto orgánico de la UMSA, la normatividad interna de la Universidad Boliviana y de sus principios, fines y objetivos.
 - l. Controlar las actividades del Departamento de Auditoría Interna comprobando la eficiencia de las operaciones conforme a la Ley 1178 de Administración y Control Gubernamentales.
 - m. Cumplir las recomendaciones formuladas por la Contraloría General del Estado Plurinacional de Bolivia y verificar el cumplimiento de las recomendaciones contenidas en informes de auditoría interna y externa, a través de seguimiento de recomendaciones.
 - n. Informar periódicamente al Rector (a) sobre el estado de avance del Programa Anual de Operaciones.



- o. Prepara informes mensuales, semestrales y anuales sobre las actividades que desarrolla el Departamento de Auditoría, para informar a la máxima autoridad.
- p. Realizar la declaración anual de independencia y declaración PAR.⁸

2.2.3 ORGANIGRAMA



9

⁸ UNIVERSIDAD MAYOR DE SAN ANDRES. Departamento de Auditoría Interna. Obtenido de <https://dai.umsa.bo/test-0>

⁹ UNIVERSIDAD MAYOR DE SAN ANDRES. Departamento de Auditoría Interna. Obtenido de <https://dai.umsa.bo/organigrama>



3 MARCO TEÓRICO

Es una estructura que guía la investigación al basarse en teorías previamente desarrolladas y aplicadas a un área específica de estudio. Proporciona una base sólida que justifica la importancia de la investigación y ayuda a definir las variables y las relaciones entre ellas. El marco teórico se fundamenta en una revisión exhaustiva de la literatura existente y en la identificación de las teorías más relevantes para el problema de investigación.¹⁰

3.1 AUDITOR

Un auditor es un profesional independiente que examina de manera sistemática y objetiva la información financiera, operativa y administrativa de una organización para evaluar su precisión, integridad y conformidad con los estándares y regulaciones aplicables.¹¹

3.2 AUDITOR INTERNO

Un auditor interno es un profesional altamente calificado y objetivo que trabaja dentro de una organización para evaluar y mejorar la eficacia de los controles internos, la gestión de riesgos y el gobierno corporativo. Su función principal es asegurar que las operaciones de la empresa se lleven a cabo de manera eficiente, ética y en cumplimiento con las normativas y políticas establecidas.

Este profesional realiza revisiones exhaustivas de los procesos y procedimientos de la organización, identifica posibles riesgos y vulnerabilidades, y proporciona recomendaciones para fortalecer la estructura organizativa y mitigar riesgos. Su trabajo no solo se enfoca en la detección y prevención de fraudes y errores, sino también en mejorar la eficiencia operativa y promover una cultura de cumplimiento y responsabilidad en toda la empresa.

¹⁰ HERNÁNDEZ SAMPIERI, R., FERNÁNDEZ COLLADO, C., & BAPTISTA LUCIO, P. (2014). Metodología de la investigación (6a ed.). McGraw-Hill Interamericana.

¹¹ ARENS, A. A., ELDER, R. J., & BEASLEY, M. S. (2019). Auditing and Assurance Services: An Integrated Approach (17th ed.). Pearson. 3p.



El auditor interno colabora estrechamente con la alta dirección y otras áreas de la empresa para garantizar un ambiente de control adecuado y contribuir al logro de los objetivos estratégicos de la organización.

Además, su independencia y objetividad son fundamentales para garantizar la imparcialidad en sus evaluaciones y asegurar la confianza de las partes interesadas internas y externas en los informes y recomendaciones que proporciona.¹²

3.3 AUDITOR GUBERNAMENTAL

El auditor gubernamental es un profesional especializado en la evaluación de la gestión financiera y administrativa de entidades del sector público. Su labor se enfoca en verificar el cumplimiento de normativas legales y regulatorias, garantizar la transparencia en el uso de los recursos públicos, y promover la eficiencia y eficacia en la gestión de programas y servicios gubernamentales. Este tipo de auditor también tiene la responsabilidad de identificar áreas de riesgo y proponer recomendaciones para mejorar los procesos internos y fortalecer la rendición de cuentas en el sector público.¹³

3.4 AUDITORÍA

Es la acumulación y evaluación objetiva de evidencia para establecer e informar sobre el grado de correspondencia entre la información examinada y los criterios establecidos.¹⁴

La auditoría es un proceso sistemático e independiente mediante el cual se evalúa la información financiera, operativa y administrativa de una organización. Su objetivo es verificar la precisión, integridad y cumplimiento de normativas y estándares establecidos, así como identificar áreas de mejora en los procesos y controles internos.¹⁵

¹² LOUWERS, T. J., RAMSAY, R. J., SINASON, D. H., & STRAWSER, J. R. (2021). *Auditing & Assurance Services* (8th ed.). McGraw-Hill Education. 265p.

¹³ SMITH, J. (2020). *Auditoría Gubernamental: Principios y Prácticas*. Editorial Público y Transparencia. 78p.

¹⁴ BOLIVIA. Contraloría General del Estado Plurinacional de Bolivia. 2012. Resolución CGE/094/2012. Normas Generales de Auditoría Gubernamental, 27 de agosto de 2012. 10p.

¹⁵ ARENS, A. A., ELDER, R. J., & BEASLEY, M. S. (2019). *Auditing and Assurance Services: An Integrated Approach* (17th ed.). Pearson. 23p.



3.5 AUDITORÍA INTERNA

La auditoría interna es una función de control interno posterior de la organización, que se realiza a través de una unidad especializada, cuyos integrantes no participan en las operaciones y actividades administrativas. Su propósito es contribuir al logro de los objetivos de la entidad mediante la evaluación periódica del control interno.¹⁶

La auditoría interna es un proceso sistemático y objetivo llevado a cabo por profesionales independientes dentro de una organización, cuyo propósito es evaluar y mejorar la efectividad de los controles internos, la gestión de riesgos y el gobierno corporativo. Esto se logra mediante la revisión y análisis de las operaciones, los procesos, los sistemas de información y el cumplimiento de políticas y regulaciones internas y externas.¹⁷

3.6 AUDITORÍA GUBERNAMENTAL

La auditoría gubernamental es un proceso sistemático e independiente de evaluación llevado a cabo por profesionales especializados dentro de entidades del sector público. Su objetivo principal es verificar el cumplimiento de normativas legales y regulaciones aplicables al uso de los recursos públicos, así como identificar áreas de mejora en la gestión y control de dichos recursos, con el fin de promover la eficiencia, transparencia y rendición de cuentas en la administración pública.¹⁸

La auditoría gubernamental se concibe como una función esencial dentro de la administración pública, cuyo propósito principal es evaluar la gestión financiera y operativa de entidades gubernamentales. Esta función incluye actividades de control interno, supervisión de procesos, identificación de riesgos y fiscalización del uso de los recursos públicos.

¹⁶ BOLIVIA. Contraloría General del Estado Plurinacional de Bolivia. 2012. Resolución CGE/094/2012. Normas para el Ejercicio de la Auditoría Interna, 27 de agosto de 2012. 7p.

¹⁷ GONZÁLEZ, J. (2021). Auditoría Interna: Conceptos y Prácticas (2ª ed.). Editorial Auditoría Profesional. 45p.

¹⁸ GARCÍA, J. (2021). Auditoría Gubernamental: Fundamentos y Prácticas. Editorial Gobernabilidad y Transparencia. 35p.



Su objetivo es garantizar la transparencia, la eficiencia y la legalidad en la gestión de los asuntos públicos, promoviendo así una mayor confianza y responsabilidad en el uso de los recursos estatales.¹⁹

3.7 RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA

Consiste en la recopilación y evaluación de la información, a fin de tener una apreciación preliminar del área, programa, convenio, contrato, actividad, operación o proceso objeto de la auditoría, a fin de determinar la auditabilidad.²⁰

3.8 AUDITABILIDAD

Condición que debe reunir el sujeto y el objeto de la auditoría para poder ser auditado, es decir contar con la predisposición de la Máxima Autoridad Ejecutiva de someter a la entidad, área, proyecto, proceso, operación u otros, a una auditoría; y la existencia de información y documentación necesaria y suficiente para ejecutar la auditoría.²¹

3.9 PRONUNCIAMIENTO DE AUDITABILIDAD

Documento por el cual el auditor gubernamental, con carácter previo al inicio de la auditoría, y conforme al relevamiento de información, en aplicación a los principios de resultados, economía y de oportunidad, se pronuncia por la auditabilidad de una determinada operación o actividad.²²

El auditor gubernamental, podrá pronunciarse de la siguiente manera:

¹⁹ GONZÁLEZ, A. (2020). La Auditoría Gubernamental como Función de Control y Supervisión. Editorial Gobierno Transparente. 55p.

²⁰ BOLIVIA. Contraloría General del Estado Plurinacional de Bolivia. 2012. Resolución CGE/094/2012. Normas Generales de Auditoría Gubernamental, 27 de agosto de 2012. 24p.

²¹ BOLIVIA. Contraloría General del Estado Plurinacional de Bolivia. 2012. Resolución CGE/094/2012. Normas Generales de Auditoría Gubernamental, 27 de agosto de 2012. 24p.

²² BOLIVIA. Contraloría General del Estado Plurinacional de Bolivia. 2024. Resolución N° CGE/018/2024. Reglamento para la elaboración de Informes de Auditoría Con Indicios De Responsabilidad RE/CE-029 V3, 4 de marzo de 2024. 4p.



- a. Por la auditabilidad inmediata, que implica la decisión de iniciar la auditoría de cumplimiento en la misma gestión o programarla para la siguiente por la relevancia de la operación o actividad.
- b. Por la auditabilidad mediata, que implica la decisión de no inicio de la auditoría de forma inmediata en consideración a la baja relevancia de la operación o actividad analizada. Cuando esta decisión se base en el análisis de importes económicos menores al gasto de la auditoría, se debe exponer y detallar los recursos que se necesitarán para realizar el trabajo de auditoría y/o inicio de acciones legales, como ser el costo que implique las horas laborales, de acuerdo al haber mensual que recibe cada profesional de esa unidad, material de escritorio, notificaciones, entre otros. A objeto de incluir en el pronunciamiento de auditabilidad, se incluirán los recursos que serán invertidos con la participación de otras unidades, como ser legal y técnica, debiendo contarse con la información necesaria.

La decisión de auditabilidad mediata, no se constituye en una decisión final de no realización de la auditoría, pudiendo el auditor gubernamental, en cualquier momento disponer el inicio de la Auditoría de Cumplimiento, siempre que tenga la disponibilidad de recursos humanos y financieros y se hubiera cumplido con la priorización de otros trabajos de auditoría de mayor relevancia para la entidad.

La CGE, podrá instruir a la Unidad de Auditoría Interna, en cualquier momento la realización de una auditoría independientemente del pronunciamiento de auditabilidad inmediata o mediata de la Unidad de Auditoría Interna.²³

3.10 ELEMENTOS DE TRABAJO DEL AUDITOR INTERNO

Los elementos de trabajo del auditor interno son fundamentales para el ejercicio efectivo de su función dentro de una organización. Algunos de estos elementos clave incluyen:

²³ BOLIVIA. Contraloría General del Estado Plurinacional de Bolivia. 2024. Resolución N° CGE/018/2024. Reglamento para la elaboración de Informes de Auditoría Con Indicios De Responsabilidad RE/CE-029 V3, 4 de marzo de 2024. 8-9p.



1. Planificación: El auditor interno debe desarrollar un plan de trabajo detallado que incluya objetivos, alcance, cronograma y recursos necesarios para llevar a cabo las auditorías de manera efectiva.
2. Evaluación de riesgos: Antes de iniciar una auditoría, es importante evaluar los riesgos asociados con los procesos y áreas a auditar para priorizar los esfuerzos y recursos de manera adecuada.
3. Obtención de evidencia: Durante la auditoría, el auditor interno debe obtener evidencia suficiente y competente para respaldar sus hallazgos, conclusiones y recomendaciones.
4. Análisis y pruebas: Se requiere realizar análisis detallados y pruebas de los controles internos, transacciones y operaciones para identificar posibles deficiencias, irregularidades o áreas de mejora.
5. Comunicación: Es fundamental comunicar de manera clara y efectiva los hallazgos, resultados y recomendaciones de la auditoría tanto a nivel interno como a los responsables de la toma de decisiones.
6. Seguimiento: Después de completar la auditoría, se debe realizar un seguimiento para asegurar que las acciones correctivas y mejoras recomendadas se implementen de manera oportuna y efectiva.
7. Informe final: El auditor interno debe preparar un informe final que resuma los hallazgos, conclusiones, recomendaciones y acciones acordadas para abordar los problemas identificados durante la auditoría.²⁴

3.11 RESPONSABILIDAD DEL AUDITOR GUBERNAMENTAL

El auditor gubernamental al estar encargado de realizar el trabajo de campo, es responsable con exclusividad en cuanto a las determinaciones adoptadas en un Informe

²⁴ GONZÁLEZ, J. (2021). "Auditoría Interna: Desarrollo de Competencias para un Desempeño Eficiente" (2ª ed.). Editorial Auditoría Moderna. 75p.



de Auditoría. Es de exclusiva responsabilidad del auditor gubernamental la determinación de limitaciones para sustentar los hallazgos que puedan originar indicios de responsabilidad por la función pública.

La Contraloría General del Estado, se limitará a realizar la evaluación de los Informes de Auditoría en sujeción a la documentación remitida por el auditor gubernamental; sin embargo, puede requerir a la Unidad de Auditoría Interna la remisión de cualquier otra documentación que considere necesaria o requerir la ampliación del análisis sobre aspectos no considerados por el auditor gubernamental.²⁵

CAPÍTULO III

4 DISEÑO METODOLÓGICO

4.1 PLANTEAMIENTO DEL PROBLEMA

El Decreto Supremo N° 2514 del 9 de septiembre de 2015, en su artículo 2, establece la creación de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) como una institución pública descentralizada bajo la tutela del Ministerio de la Presidencia.

La AGETIC tiene el mandato de elaborar, proponer e implementar políticas, planes y estrategias de Gobierno Electrónico y Tecnologías de Información y Comunicación para las entidades del sector público.

Entre las funciones de la AGETIC, en los incisos f) e i) del Artículo 7, se establecen:

“f) Establecer los lineamientos técnicos en seguridad de información para las entidades del sector público.”

²⁵ BOLIVIA. Contraloría General del Estado Plurinacional de Bolivia. 2024. Resolución N° CGE/018/2024. Reglamento para la elaboración de Informes de Auditoría Con Indicios De Responsabilidad RE/CE-029 V3, 4 de marzo de 2024. 23 p.



“i) Elaborar, proponer, promover, gestionar, articular y actualizar el Plan de Implementación de Gobierno Electrónico y el Plan de Implementación de Software Libre y Estándares Abiertos para las entidades del sector público; y otros planes relacionados con el ámbito de gobierno electrónico y seguridad informática.”

En su artículo 8, se crea el Centro de Gestión de Incidentes Informáticos (CGII) como parte de la estructura técnica operativa de la AGETIC. En su párrafo II, se señala que el CGII tiene, entre otras, las siguientes funciones:

“c) Establecer los lineamientos para la elaboración de Planes Institucionales de Seguridad de la Información en las entidades del sector público.”

Asimismo, en su Disposición Transitoria Segunda, se determina que las entidades del nivel central del Estado deberán presentar a la AGETIC, en un plazo no mayor a un (1) año desde la aprobación de las políticas de seguridad de la información por parte de la AGETIC, su Plan Institucional de Seguridad de la Información.

A pesar de la clara normativa y las funciones asignadas a la AGETIC y el CGII, muchas entidades del sector público han encontrado desafíos significativos en la elaboración e implementación y presentación de sus Planes Institucionales de Seguridad de la Información.

Estos desafíos incluyen la falta de recursos técnicos y humanos especializados, la insuficiente capacitación en materia de seguridad de la información, y la necesidad de una mayor coordinación y apoyo técnico por parte de la AGETIC.

4.1.1 IDENTIFICACIÓN DEL PROBLEMA

Mediante Resolución HCU No. 298/2019 de fecha 04 de septiembre de 2019, se aprobó el Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés, según se expone a continuación:

“Artículo Único. Aprobar el “PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS”, cuyo documento se encuentra adjunto a la presente Resolución”.



Adicionalmente, mediante Resolución Rectoral No. 642 de 24 de septiembre de 2018, se designó al Responsable de Seguridad de la Información (RSI) de la Universidad Mayor de San Andrés y representante de la UMSA ante la AGETIC. Sin embargo, la gestión del RSI cesó el 14 de septiembre de 2020, debido al cambio de Jefatura.

Por otro lado, mediante la Resolución del Honorable Consejo Universitario No. 464/2018 de 26 de septiembre de 2018, se conformó el Comité de Seguridad de la Información (CSI) de la Universidad Mayor de San Andrés, la misma que se compuso por autoridades, representantes docentes y estudiantes.

Consecuentemente, desde septiembre de 2020 hasta la fecha de la presente gestión, no se cuenta con la designación de un nuevo Responsable de Seguridad de la Información ni se ha reconstituido el Comité de Seguridad de la Información de la UMSA. Esta falta de designación y reconstitución ha impedido la implementación efectiva del Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés.

4.2 PLANTEAMIENTO DE OBJETIVOS

4.2.1 OBJETIVO GENERAL

El objetivo del presente Relevamiento de Información Específica, es:

Recopilar y evaluar información sobre la elaboración e implementación del Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés, aprobado mediante Resolución del Honorable Consejo Universitario N°298/2019 de 4 de septiembre de 2019, en el marco del Decreto Supremo N°2514 del 9 de septiembre de 2015 y los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, aprobado con Resolución Administrativa N° AGETIC/RA/0051/2017 de 19 de septiembre de 2017.



4.2.2 OBJETIVO ESPECÍFICO

El objetivo específico del presente Relevamiento de Información Específica es:

Determinar la auditabilidad inmediata o mediata, o si no amerita la realización de una auditoría con la debida justificación, según corresponda.

4.3 JUSTIFICACIÓN DEL TRABAJO

4.3.1 JUSTIFICACIÓN TEÓRICA

El Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés se fundamenta en la imperativa necesidad de brindar un nivel adecuado de seguridad para los activos de información, enfocándose en la preservación de su confidencialidad, integridad y disponibilidad.

En este contexto, los Activos de Información comprenden una amplia gama de elementos, como datos sensibles, información crítica, sistemas tecnológicos y recursos asociados que poseen un valor estratégico y operativo significativo para la Universidad.

El PISI no solo busca establecer medidas y controles de seguridad robustos para proteger estos activos, sino también promover una cultura de seguridad informática entre los colaboradores y usuarios de la institución. Esto implica la implementación de políticas claras, procedimientos adecuados, capacitación continua en temas de seguridad de la información y la adopción de tecnologías avanzadas de protección cibernética.

Al asegurar la confidencialidad de la información, se evita el acceso no autorizado y se protege la privacidad de los datos sensibles de la Universidad y de sus miembros. La integridad garantiza que la información no sea alterada o corrompida de manera no autorizada, manteniendo su exactitud y fiabilidad.



Por último, la disponibilidad asegura que los usuarios autorizados puedan acceder a la información cuando lo necesiten, sin interrupciones ni limitaciones indebidas, lo que favorece la continuidad de las operaciones y el cumplimiento de los objetivos institucionales.

4.3.2 JUSTIFICACIÓN PRÁCTICA

El Responsable de la Seguridad de la Información (RSI) y el Comité de Seguridad de la Información (CSI) tienen la importante responsabilidad de llevar a cabo la identificación meticulosa de los activos de información en el marco del Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés.

Su objetivo primordial es preservar la integridad, autenticidad y confidencialidad de la información, asegurando que esta no sea manipulada, alterada ni accedida por personas o procesos no autorizados.

Además, se encargan de establecer y mantener un sistema de acceso seguro y oportuno a la información, garantizando que esté disponible únicamente para el personal autorizado cuando sea necesario y en la forma que se requiera, de manera que se pueda acceder a la información en el momento preciso en que sea requerida, sin comprometer su seguridad ni su exactitud.

4.4 MEMORÁNDUM DE ASIGNACIÓN DE TRABAJO

Mediante MEM.T.AUD. No.008/2024 de 14 de marzo de 2024, se instruye la realización del Relevamiento de Información Específica (RIE) sobre el “Plan Institucional de Seguridad de la Información de la entidad (PISI), como se refleja en la imagen adjunta a continuación.



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



**UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia**

MEMORÁNDUM

**UNIVERSIDAD BOLIVIANA
UNIVERSIDAD MAYOR DE SAN ANDRÉS
DPTO. AUDITORÍA INTERNA**

MEM.T.AUD. No.008/2024

Señor:

Lic. Dennis Magno Apaza Gonzales

AUDITOR INTERNO

Presente. -

La Paz, 14 de marzo de 2024

Licenciado:

En cumplimiento a solicitud de la Contraloría General del Estado efectuada mediante nota CGE/GPA2/171-026/2024 del 1 de marzo de 2024 y proveído del señor Rector con Hoja de Ruta VC-5338; se le instruye la realización del siguiente Relevamiento de Información Específica (RIE), en coordinación con esta Jefatura.

No.	TRABAJO ASIGNADO
1	Relevamiento de Información Específica sobre "Plan Institucional de Seguridad a la Información de la entidad" (PISI) requerido por los "Lineamientos para la elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público" aprobados con la Resolución Administrativa No. AGETIC/RA/0051/2017

El informe de R.I.E. debe cumplir con lo establecido en la Norma 217.04 de las Normas Generales de Auditoría Gubernamental, los Papeles de Trabajo referenciados y correferenciados, los mismos que deben ser entregados hasta el **19 de abril** de la presente gestión.

Para el trabajo encomendado contará con el apoyo de Universitaria Gaby Norca Arias Chambi.

La pertinencia de contar con personal especializado de Sistemas para la labor encomendada, deberá ser comunicada a esta Jefatura en forma oportuna.

Deseándole éxito en la labor encomendada, saludo a usted muy atentamente.

Lic. René Carrasco Condarco
JEFE a.i. DEPARTAMENTO DE AUDITORÍA INTERNA



RCC/mmp
cc: Archivo Auditoría interna



4.5 ALCANCE

El Relevamiento de Información Específica, se efectuó de acuerdo con las "Normas Generales de Auditoría Gubernamental" (NAG), Numeral 217, aprobada con Resolución N°CGE/094/2012 de 27 de agosto de 2012, y Artículo 7 del "Reglamento para la Elaboración de Informes de Auditoría con Indicios de Responsabilidad" aprobado mediante Resolución N° CGE/018/2024 de 4 de marzo de 2024, emitidas por la Contraloría General del Estado (CGE), y comprendió la recopilación y evaluación de la información y documentación generada desde noviembre de 2017 (Notificación a Rectorado de nota AGETIC/NE/3187/2017 de lineamientos del PISI), a la fecha del presente relevamiento de información específica sobre la elaboración e implementación del Plan Institucional de Seguridad de la información de la Universidad Mayor de San Andrés, aprobado mediante Resolución del Honorable Consejo Universitario N°298/2019 de 4 de septiembre de 2019.

4.6 OBJETO

El objeto del Relevamiento de Información Específica lo constituye la integridad de la documentación e información relacionada con la elaboración e implementación del Plan Institucional de Seguridad de la Información de la UMSA, como ser:

- ✓ El Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés, aprobado mediante Resolución del Honorable Consejo Universitario N°298/2019 de 4 de septiembre de 2019.
- ✓ Antecedentes de la Resolución del Honorable Consejo Universitario N°298/2019 de 4 de septiembre de 2019.
- ✓ Reglamentos, Manuales de Procesos y/o Procedimientos de seguridad, emergentes de la Implementación del Plan Institucional de Seguridad de la Información, relacionados a los 11 anexos de los controles mínimos de seguridad de la información, previstos en el numeral 6.2.3.2 de los Lineamientos para la Elaboración e



Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, emitidos por la AGETIC.

- ✓ Documento de designación del Responsable de Seguridad de la Información.
- ✓ Documento de conformación del Comité de Seguridad de la Información.
- ✓ Otra documentación relacionada a la elaboración e Implementación del Plan Institucional de Seguridad de la Información.

4.7 METODOLOGÍA

El trabajo se realizó mediante la aplicación de un programa de trabajo específico que incluye entre otros, los siguientes procedimientos orientados a alcanzar los objetivos del relevamiento de información en los siguientes ámbitos:

- ✓ Evaluación de la información documentada referente a la elaboración e implementación del "Plan Institucional de Seguridad de la Información de la UMSA".
- ✓ Verificación de la normativa aplicable.
- ✓ Emisión de conclusiones y recomendaciones.

4.8 PROGRAMA DE TRABAJO

Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
1.	PROCEDIMIENTOS GENERALES Solicitar la siguiente documentación e información a Rectorado y Departamento de Tecnologías de la Información y Comunicación (DTIC): 1. Documento de designación del Responsable de Seguridad de la Información (RSI) de la Universidad Mayor de San Andrés.			



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
	<ol style="list-style-type: none">2. Documento de conformación del Comité de Seguridad de la Información (CSI) de la UMSA.3. El Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés (Impreso y Medio Magnético).4. Documento de aprobación del Plan Institucional de Seguridad de la Información de la UMSA.5. Informes de evaluación remitidos por el Responsable de Seguridad de la Información, sobre el estado de seguridad de la información y Plan Institucional de Seguridad de la Información de la UMSA.6. Nota AGETIC/NE/3187/2017 emitida por el AGETIC con la integridad de los antecedentes que la misma adjunta y su derivación, según corresponda.7. Documento de presentación del Plan Institucional de Seguridad de la Información de la UMSA al AGETIC.8. Reglamentos, Manuales de Procesos y/o Procedimientos de seguridad, emergentes de la Implementación del Plan Institucional de Seguridad de la Información, relacionados a los 11 anexos de los controles mínimos de seguridad de la información, previstos en el numeral 6.2.3.2 de			



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
	<p>los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, emitidos por la AGETIC:</p> <ul style="list-style-type: none">a) Seguridad en recursos humanos (Véase el punto 1 del Anexo A).b) Gestión de activos de información (Véase el punto 2 del Anexo A).c) Control de accesos (Véase el punto 3 del Anexo A).d) Criptografía (Véase el punto 4 del Anexo A).e) Seguridad física y ambiental (Véase punto 5 del Anexo A)f) Seguridad de las operaciones (Véase punto 6 del Anexo A).g) Seguridad de las comunicaciones (Punto 7 del Anexo A).h) Desarrollo, mantenimiento y adquisición de sistemas (Véase el punto 8 del Anexo A).i) Gestión de incidentes de seguridad de la información (Véase el punto 9 del Anexo A).j) Plan de contingencias tecnológicas (Véase el punto 10 del Anexo A).k) Cumplimiento (Véase el punto 11 del Anexo A).			



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
	9. Información de la capacitación e inducción. 10. Procedimientos de gestión de incidentes.			
2	PROCEDIMIENTOS DE EVALUACIÓN En base a la documentación e información obtenida, efectuar los siguientes procedimientos:			
2.1	Recopile y analice la normativa vigente y aplicable relacionada a la elaboración e implementación del Plan Institucional de Seguridad de la Información.			
2.2	Elabore una cédula analítica y analice si el Plan Institucional de Seguridad de la Información de la UMSA, fue elaborado en el marco de los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, aprobado con Resolución Administrativa N° AGETIC/RA/0051/2017 de 19 de septiembre de 2017. Para el efecto, considere los siguientes atributos: <ul style="list-style-type: none">- Etapa para la elaboración del PISI.- Objetivo de la etapa para la elaboración del PISI.- Actividades de la etapa.- Responsables de las actividades.			



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
	<ul style="list-style-type: none">- Descripción de los “Lineamientos para la Elaboración...” conforme a Resolución Adm. N° AGETIC/RA/0051/2017- Actividades realizadas por la entidad descritas en el PISI UMSA.- Análisis de Auditoría. <p>En relación a las actividades desarrolladas por etapa, considere los siguientes procedimientos:</p> <p>Etapa Inicial – Organización Interna</p> <p>2.3 Verifique que el Rector de la UMSA (MAE) designó y asignó funciones al Responsable de Seguridad de la Información de la UMSA.</p> <p>2.4 Verifique que la MAE conformó el Comité de Seguridad de la Información de la UMSA.</p> <p>Etapa de Desarrollo – Estructura y contenido del Plan Institucional de Seguridad de la Información – PISI</p> <p>2.5 Verifique si el Responsable de Seguridad de la Información (RSI), incorporó en el contenido del Plan Institucional de Seguridad de la Información de la UMSA, los siguientes aspectos definidos en los</p>			



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
	<p>Lineamientos aprobados mediante Resolución Administrativa N° AGETIC/RA/0051/2017:</p> <ul style="list-style-type: none">- La introducción, objetivos y alcance.- La metodología de gestión de riesgos.- La Política de Seguridad de la Información.- Cronograma de Implementación. <p>Etapas de Desarrollo – Aprobación del PISI</p>			
2.6	<p>Verifique que el Plan Institucional de Seguridad de la Información de la UMSA, se encuentre debidamente aprobado por Resolución del Honorable Consejo Universitario previa revisión del Comité de Seguridad de la Información (CSI) y Comisión de Recursos Informativos del HCU.</p>			
2.7	<p>Elabore una cédula analítica y verifique si el Plan Institucional de Seguridad de la Información de la UMSA, fue implementado en el marco de los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, aprobado con Resolución Administrativa N° AGETIC/RA/0051/2017 de 19 de septiembre de 2017. Para el efecto, considere los siguientes atributos:</p>			



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
	<ul style="list-style-type: none">- Etapa para la implementación del PISI.- Objetivo de la etapa para implementación del PISI.- Actividades de la etapa.- Responsables de las actividades.- Descripción de los “Lineamientos para la Elaboración...” conforme a Resolución Adm. N° AGETIC/RA/0051/2017- Actividades realizadas por la entidad para la implementación del PISI de la UMSA.- Análisis de Auditoría. <p>En relación a las actividades desarrolladas por etapa, consideré los siguientes procedimientos:</p> <p>2.8 Etapa Implementación – Aplicación de Controles Verifique que el Responsable de Seguridad de la Información aplicó los controles mínimos contemplados en la etapa de elaboración de acuerdo al cronograma de implementación y aprobación establecido dentro del PISI.</p> <p>2.9 Etapa Implementación – Capacitación e inducción Verifique si se realizaron procesos y actividades de capacitación e inducción al personal que es parte</p>			



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
	<p>integral en la implementación del Plan Institucional de Seguridad de la Información; asimismo, procesos de capacitación e inducción dirigido a la totalidad de servidores públicos (fijos, eventuales y de reciente incorporación) en relación al Plan Institucional de Seguridad de la Información y manuales de procesos y/o procedimientos de seguridad, generados a partir de la Política de Seguridad de la Información.</p> <p>Etapa Implementación – Evaluación y mejora continua</p>			
2.10	<p>Verifique si el RSI promovió la realización de revisiones periódicas a los controles implementados dentro del Plan Institucional de Seguridad de la Información, en relación al cumplimiento y eficacia de procesos y/o procedimientos de la Política de Seguridad de la Información.</p>			
2.11	<p>Etapa Implementación – Gestión de incidentes</p> <p>Verifique que la UMSA elaboró procedimientos para la gestión de incidentes, que establezcan con claridad procesos de planificación y preparación, detección y reporte, valoración y decisión, respuesta y erradicación para la mejora continua ante la</p>			



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
	ocurrencia de incidentes relacionados a la seguridad de la información.			
2.12	Verifique que el RSI es la persona de contacto al interior y exterior de la entidad para la gestión de incidentes, siendo el mismo que tiene la responsabilidad de reportar la ocurrencia de los mismos al CGII de acuerdo a normativa vigente.			
2.13	Verifique que la Entidad reporta sus incidentes y vulnerabilidades identificadas, así como el tratamiento realizado, al Centro de Gestión de Incidentes Informáticos (CGII), de acuerdo al artículo 17 del Decreto Supremo 2514.			
2.14	Identifique, posibles áreas críticas y factores de riesgo, producto del relevamiento de información.			
2.15	Indicios de Responsabilidad por la función pública De identificarse posibles indicios de responsabilidad por la función pública, emitir el informe respectivo, para lo cual deberá considerar el “Reglamento para la elaboración de informes de auditoría con indicios de responsabilidad”, aprobado con Resolución CGE/018/2024 de 04/03/2024:			



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
2.16	<p>Obtener fotocopia legalizada de la documentación de respaldo al hecho observado que genera indicios de responsabilidad por la función pública (evidencia competente y suficiente).</p> <p>Con relación a los posibles hallazgos de control interno, documente y redacte la deficiencia con los atributos: condición, criterio, causa, efecto y recomendación y elabore un informe por separado para reportar dichos hallazgos.</p>			
3	CONCLUSIÓN			
3.1	<p>En base a los resultados obtenidos, elabore informe de relevamiento de información específica, de acuerdo a la estructura establecida en la NAG 217.04, el cual incluya una conclusión sobre la auditabilidad del caso, de conformidad a la Norma de Auditoría NAG 217.03 y Artículo 7 del Reglamento para la elaboración de informes de Auditoría con indicios de responsabilidad aprobado mediante Resolución CGE/018/2024; asimismo, describir los posibles riesgos existentes según el análisis realizado.</p> <p>En función a los riesgos y áreas críticas identificadas, determinar la naturaleza de la auditoría a realizar, si corresponde.</p>			



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
	OTROS PROCEDIMIENTOS			
4.	<p>Previo a la entrega de papeles de trabajo que respalda el relevamiento realizado, asegúrese que estén debidamente diligenciados y que contengan la siguiente información:</p> <ul style="list-style-type: none">• Nombre de la entidad.• Denominación del Relevamiento de Información.• Alcance del Relevamiento de Información.• Fecha de realización, rúbrica e iniciales del auditor que prepara la (s) cédula (s) y fecha e iniciales de supervisión.• Referencias cruzadas (las cédulas y su documentación sustentatoria deberán estar referenciadas y correferenciadas, como resultado de los procedimientos aplicados).• Referencia al paso del programa de trabajo y objetivo de la cédula.• Fuente de información utilizada para el trabajo ejecutado.• Conclusión del trabajo desarrollado.• Descripción del trabajo realizado (aclaración de marcas de auditoría).			



Nº	PROCEDIMIENTOS	REL. CON OBJ.	REF. P/T	HECHO POR
	El presente programa no es limitativo, por lo que el auditor podrá incluir otros procedimientos si fuera necesario.			
Descripción	Nombre	Cargo	Firma	Fecha
Elaborado por:	Lic. Dennis Magno Apaza Gonzales	Auditor		04/2024
Revisado y Aprobado por:	Lic. René Carrasco Condarco	Jefe a.i. Departamento Auditoría Interna		04/2024

5 MARCO LEGAL Y NORMATIVO

El Relevamiento de Información Específica se llevó a cabo con estricta conformidad tanto al Marco Normativo General como al Marco Normativo Específico. A continuación, se procederá una detallada descripción de estos marcos normativos, abarcando las directrices y regulaciones aplicables que orientaron el proceso. Este enfoque garantiza el cumplimiento riguroso de los estándares establecidos y asegura la integridad y precisión de los datos recopilados.

5.1 MARCO NORMATIVO GENERAL

5.1.1 CONSTITUCIÓN POLÍTICA DEL ESTADO PLURINACIONAL DE BOLIVIA

La Constitución Política del Estado de Bolivia, promulgada el 7 de febrero de 2009, establece los fundamentos y la estructura básica de la organización estatal. Define la distribución de poderes, garantiza los derechos individuales y colectivos, reconoce la diversidad cultural y étnica, y asegura la protección de los recursos naturales. Además,



promueve la participación ciudadana y la democracia. En esencia, sirve como el marco normativo fundamental que orienta el funcionamiento y desarrollo del país.

5.1.2 LEY 1178 DE ADMINISTRACIÓN Y CONTROL GUBERNAMENTALES

La Ley 1178 promulgada el 20 de julio de 1990, también denominada Ley de Administración y Control Gubernamental, constituye el marco normativo que regula los principios, normas y procedimientos para la adecuada gestión de los recursos públicos en Bolivia. Su propósito primordial es fomentar la transparencia, eficiencia y responsabilidad en la administración de los fondos estatales. La normativa establece directrices precisas para la planificación, ejecución, monitoreo y evaluación de programas y proyectos gubernamentales, así como para la contratación de bienes y servicios. Además, persigue la prevención y sanción de actos de corrupción y malversación de fondos en la gestión pública.

5.1.3 DECRETO SUPREMO 23215 REGLAMENTO PARA EL EJERCICIO DE LAS ATRIBUCIONES DE LA CONTRALORÍA GENERAL DE LA REPÚBLICA, ACTUAL CONTRALORÍA GENERAL DE ESTADO

El Decreto Supremo 23215 de Bolivia, promulgado el 22 de junio de 1992, establece el Régimen Básico de la Función Pública. Este decreto regula meticulosamente aspectos inherentes al ingreso, permanencia, evaluación, ascensos, sanciones y retiro del personal de la función pública. Asimismo, delinea los derechos y deberes de los funcionarios públicos.

Este marco legal promueve los principios de carrera administrativa, meritocracia, estabilidad laboral y profesionalización del servicio público. En síntesis, el Decreto Supremo 23215 se erige como una herramienta vital para asegurar una gestión pública eficaz y transparente en Bolivia.



5.1.4 DECRETO SUPREMO 23318-A REGLAMENTO DE LA RESPONSABILIDAD POR LA FUNCIÓN PÚBLICA

El Decreto Supremo 23318-A de Bolivia, promulgado el 3 de noviembre de 1992, establece el "Reglamento de la Responsabilidad por la Función Pública". Este reglamento detalla las normas y procedimientos relativos a la responsabilidad de los funcionarios públicos en el ejercicio de sus funciones. Define las acciones y omisiones que constituyen faltas administrativas, así como los mecanismos de investigación, sanción y apelación en caso de incumplimiento. En esencia, el Decreto Supremo 23318-A persigue garantizar la integridad y el cumplimiento ético en el ejercicio de los cargos públicos en Bolivia.

5.1.5 DECRETO SUPREMO 26237 MODIFICACIONES AL REGLAMENTO DE LA RESPONSABILIDAD POR LA FUNCIÓN PÚBLICA

El Decreto Supremo 26237, emitido el 29 de junio de 2001 en Bolivia, presenta modificaciones al Reglamento de Responsabilidad por la Función Pública. Estas enmiendas abordan aspectos clave como la definición de faltas administrativas, los procedimientos de investigación y sanción, así como las medidas disciplinarias aplicables a los funcionarios públicos.

En síntesis, el decreto tiene como objetivo actualizar y mejorar el marco normativo relacionado con la responsabilidad de los servidores públicos en el ejercicio de sus funciones en Bolivia.

5.1.6 RESOLUCION N° CGE/094/2012 NORMAS GENERALES DE AUDITORIA GUBERNAMENTAL.

Las Normas Generales de Auditoría Gubernamental, aprobado por la Contraloría General del Estado mediante Resolución CGE/094/2012 del 27 de agosto de 2012, vigente a partir del 1 de noviembre de 2012. Contiene un conjunto de normas y aclaraciones que permiten asegurar la uniformidad y calidad de la auditoría gubernamental en Bolivia.



5.1.7 RESOLUCIÓN N° CGE/018/2024 REGLAMENTO PARA LA ELABORACIÓN DE INFORMES DE AUDITORÍA CON INDICIOS DE RESPONSABILIDAD (RE/CE-029) VERSION 3.

El Reglamento para la Elaboración de Informes de Auditoría con Indicios de Responsabilidad, aprobado por la Contraloría General del Estado mediante Resolución N° CGE/018/2024, del 4 de marzo de 2024. Tiene por objeto regular las actividades previas para la ejecución y emisión de los Informes de Auditoría de Cumplimiento con indicios de responsabilidad por la función pública, y los Informes de Apoyo Legal y/o Técnico.

5.2 MARCO NORMATIVO ESPECIFICO

5.2.1 LEY 164 LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.

La ley 164 promulgada el 8 de agosto de 2011, tiene por objeto establecer el régimen general de telecomunicaciones y tecnologías de información y comunicación, del servicio postal y el sistema de regulación, en procura del vivir bien garantizando el derecho humano individual y colectivo a la comunicación, con respeto a la pluralidad económica, social, jurídica, política y cultural de la totalidad de las bolivianas y los bolivianos, las naciones y pueblos indígena originario campesinos, y las comunidades interculturales y afrobolivianas del Estado Plurinacional de Bolivia

5.2.2 DECRETO SUPREMO 1793 REGLAMENTO PARA EL DESARROLLO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.

El Decreto Supremo 1793 emitido el 13 de noviembre de 2013, tiene por objeto Reglamentar el acceso, uso y desarrollo de las Tecnologías de Información y Comunicación – TIC, en el marco del Título IV de la Ley N° 164, de 8 de agosto de 2011, General de Telecomunicaciones, Tecnologías de Información y Comunicación.



5.2.3 RESOLUCIÓN ADMINISTRATIVA N° AGETIC/RA/0051/2017

La Resolución Administrativa N° AGETIC/RA/0051/2017 emitida por la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación el 19 de septiembre de 2017, aprueba los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público.

5.2.4 RESOLUCIÓN ADMINISTRATIVA N° AGETIC/RA/0059/2018

La Resolución Administrativa N° AGETIC/RA/0059/2018 emitida de la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación el 1 de agosto de 2018, la misma que modifica la Resolución Administrativa N° AGETIC/RA/0051/2017.

6 DESARROLLO DEL TRABAJO

En cumplimiento a solicitud emitida por la Contraloría General del Estado, mediante la nota CGE/GPA2/171-026/2024, de fecha 1 de marzo de 2024, se procedió con la recopilación y evaluación de la información asociada al relevamiento de información específica sobre la elaboración e implementación del Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés, en estricta conformidad con las Normas Generales de Auditoría Gubernamental de Bolivia.

El proceso de relevamiento se rigió por los siguientes pasos fundamentales:

1. **Recopilación de Información:** Se realizó una exhaustiva recolección de la información documentada, abarcando políticas, procedimientos, manuales y registros inherentes al relevamiento, con el propósito de asegurar la integridad y la totalidad de la compilación documental.
2. **Evaluación de la Información Documentada:** Se efectuó un análisis minucioso de la documentación recopilada, evaluando su coherencia, consistencia y congruencia con los lineamientos normativos.



3. **Elaboración de Informe:** Se elaboró un informe que refleja los resultados obtenidos de la evaluación de la información documentada, identificando tanto las fortalezas como las áreas de mejora en la elaboración e implementación del Plan Institucional de Seguridad de la Información, y ofreciendo recomendaciones concretas para su fortalecimiento.

Teniendo en cuenta lo mencionado anteriormente, se procedió con el relevamiento como se detalla a continuación.

6.1 NOTIFICACIÓN DE LA AGETIC

Mediante nota AGETIC/NE/3187/2017 de 7 de noviembre de 2017, la Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación (AGETIC), notificó al Rector de la Universidad Mayor de San Andrés, sobre la aprobación de los “Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público”, aprobado mediante Resolución Administrativa N° AGETIC/RA/0051/2017 de 19 de septiembre de 2017.

6.2 DESIGNACIÓN DEL RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN DE LA UMSA

Mediante Resolución Rectoral No. 642 de 24 de septiembre de 2018, suscrito por el Rector de la UMSA (MAE), se designó al Jefe del Departamento de Tecnologías de la Información y Comunicación, como Responsable de Seguridad de la Información (RSI) de la Universidad Mayor de San Andrés y representante de la UMSA ante la AGETIC.

El periodo por el cual el RSI, fungió el cargo de Responsable de Seguridad de la Información hasta el 14 de septiembre de 2020.

Respecto la designación del RSI, el Artículo Segundo de la Resolución del Honorable Consejo Universitario N°230/2018, establece: "...la Comisión de Recursos Informativos



del HCU, sugerirá una terna al HCU, con perfil profesional adecuado para el desempeño de este cargo”. Es pertinente hacer notar que la Comisión de Recursos Informativos, puede sugerir a un profesional para la designación de RSI; sin embargo, es atribución de la MAE el nombrar y/o designar al Responsable de Seguridad de la Información.

Por otro lado, se solicitó al DTIC el documento de designación del Responsable de Seguridad de la Información de la UMSA (nota AUD.INT.CARTA N°353/2024 de 26/03/2024), Departamento que mediante NOTA UMSA DTIC N°181/2024 de 3 de abril de 2024, expone lo siguiente:

“Actualmente nuestra institución no cuenta con Responsable de Seguridad de la Información designado.

(...)

... desde la gestión 2020 no se cuenta con el Responsable de Seguridad de la Información”.

Por otro lado, mediante NOTA UMSA DTIC N°189/2024 de 9 de abril de 2024, la Jefatura del DTIC proporcionó un Informe y diferentes notas dirigidas a Rectorado, solicitando se designe un Responsable de Seguridad de la Información.

A continuación, detallamos las notas proporcionadas:

- ❖ INFORME DTIC No.049/2020 de 10 de septiembre de 2020. Nota con la que se le recordó al Rector a.i. de la UMSA, que es función de la MAE nombrar entre otros al Responsable de Seguridad de la Información.
- ❖ NOTA UMSA DTIC N°966/2022 de 1 de septiembre de 2022. Nota con la que la Jefatura del DTIC puso en conocimiento del Rector de la UMSA, de la aprobación del PISI de la UMSA y solicitó la contratación de un profesional, sin especificar la denominación del cargo requerido.
- ❖ NOTA UMSA DTIC N°1363/2022 de 1 de diciembre de 2022. Nota con la que la Jefatura del DTIC, nuevamente solicitó al Rector de la UMSA, la creación de un



ITEM para el Responsable de Seguridad de la Información, con nivel 20, con el fin de que se ejecute el PISI de la UMSA.

- ❖ NOTA DTIC N°214/2023 de 8 de marzo de 2023. Con la que la Jefatura del DTIC solicitó al Rector de la UMSA, se designe a un Oficial de Seguridad de la Información.

Sobre el particular, de las notas descritas precedentemente, solo se obtuvo evidencia de la atención a la nota DTIC N°214/2023, de 8 de marzo de 2023, mediante la cual se solicitó la designación al Jefe de la División de Redes y Sistemas de Información como Oficial de Seguridad de la Información de la Universidad Mayor de San Andrés, hasta la concreción del ítem de RSI, razón por la que se emitió la Resolución Rectoral N°093 de 16 de marzo de 2023; sin embargo, no se tiene definidas las funciones de un Oficial de Seguridad de la Información en el PISI de la UMSA, Manual de Descripción de Puestos y Cargos de la UMSA, Lineamiento para la Elaboración del PISI emitidos por el AGETIC.

Al respecto, la Jefatura del DTIC, respecto las funciones del Oficial de Seguridad de la Información y su relación con el RSI, expone: “Desconozco, sin embargo hago notar que su función principal es la de dirigir la División de Redes y Sistemas de Información, y en caso en que se presentaron incidentes de seguridad bajo su dirección se conformó el equipo de profesionales para dar solución a los mismos”; asimismo, en respuesta del punto 1 del Acta de Reunión N°2 (24/04/2024), respecto a las funciones como Oficial de Seguridad de la Información, expone:

“Actualmente ejerzo como Jefe de la División de Redes y Sistemas de Información, con nivel y cargo de acuerdo a la planilla administrativa vigente.

Entiendo que por necesidad institucional y de contacto, la MAE ha dispuesto designarme en forma adicional y provisional como Oficial de Seguridad de la Información de la UMSA.



No se me ha proporcionado detalle de funciones; sin embargo, en aplicación a los estándares ISO/IEC 27001 - Sistema de Gestión de Seguridad de la Información, en pro de implementar un sistema de gestión de seguridad de la información en forma complementaria al PISI, las funciones que he desarrollado como Oficial de Seguridad de la Información son:

- ✓ Monitorización y Análisis de Seguridad, supervisando constantemente la infraestructura de red y revisando los sistemas de información y redes comunicacionales de la Universidad, para detectar posibles amenazas y vulnerabilidades.
- ✓ Respuesta a Incidentes de Seguridad, coordinando y participando en la respuesta a incidentes de seguridad de la información.
- ✓ Mantenimiento de Documentación y Reportes
- ✓ No se ha designado un Responsable de Seguridad de la Información (RSI), personal clave con rol ejecutivo de quien el Oficial de Seguridad de la Información, debe ser un directo dependiente (OSI), puesto que sus funciones son estrictamente técnicas”.

Por tanto, no se tiene definida las funciones del Oficial de Seguridad de la Información y no responde a las funciones de Responsable de Seguridad de la Información al cual hace referencia el PISI de la UMSA.

Consecuentemente, desde septiembre de la gestión 2020 hasta la fecha del presente Relevamiento de Información Específica, no se designó a un nuevo Responsable de Seguridad de la Información de la UMSA.

6.3 CONFORMACIÓN DEL COMITÉ DE SEGURIDAD DE INFORMACIÓN DE LA UMSA

Mediante Resolución del Honorable Consejo Universitario No. 464/2018 de 26 de septiembre de 2018, suscrita por el Rector de la UMSA (MAE), se conformó el Comité



de Seguridad de la Información (CSI) de la Universidad Mayor de San Andrés, conformado por las siguientes autoridades:

- ✓ Dr. Wilfredo Tavera Llanos, Decano de la Facultad de Ciencias Puras y Naturales.
- ✓ Ing. Miguel Ángel Calla Carrasco, Decano Facultad de Ingeniería.
- ✓ Lic. Víctor Paz Huanca, delegado Docente HCU Facultad de Tecnología.
- ✓ Dr. Martín Villarroel Mareño, delegado Docente HCU. Facultad de Medicina, Enfermería, Nutrición y Tecnología Médica.
- ✓ Univ. Kitzia Jarandina Guamán, delegado Estudiantil HCU. Facultad de Ciencias Facultad de Ciencias Farmacéuticas y Bioquímicas.
- ✓ Univ. Garios Fernando Torrez Alancea, delegado Estudiantil HCU. Facultad de Ciencias Puras y Naturales.
- ✓ Univ. Brian Rojas Mora, delegado Estudiantil HCU. Facultad de Ciencias Geológicas.
- ✓ Lic. Marina Delgado Rodríguez, Jefa a.i. Departamento de Tecnologías de la Información y Comunicación.
- ✓ Lic. Marcelo Germán Aruquipa Chambi, Docente Carrera de Informática.
- ✓ M.Sc. Moisés Martín Silva Choque, Docente Carrera de Informática.
- ✓ Dra. Karina Ingrid Medinaceli Díaz, Directora a.i. Instituto de Investigaciones Seminarios y Tesis Carrera de Derecho – Facultad de Derecho.
- ✓ Lic. Norma Castro Quispe, Coordinadora Plan Maestro TIC – UMSA.
- ✓ M. Sc. Víctor Hugo Chávez Salazar, Docente Carrera de Administración de Empresas.
- ✓ Ing. Marcelo Ramírez Molina, Docente Carrera de Ingeniería Electrónica.

Al respecto, en el detalle precedente, no figura entre los miembros del CSI, el Rector como Máxima Autoridad Ejecutiva en calidad de Presidente de la misma o en su defecto delegar dicha función en su representación, en apego al punto 6.1.3 de los “Lineamientos para la



elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público” emitidos por el AGETIC.²⁶

Asimismo, se solicitó al DTIC el documento de Conformación del Comité de Seguridad de la Información de la UMSA (nota AUD.INT.CARTA N°353/2024 de 26/03/2024), instancia que mediante NOTA UMSA DTIC N°181/2024 de 3 de abril de 2024, expone lo siguiente:

“Actualmente nuestra institución no cuenta con Comité de Seguridad de la Información designado.

(...)

... desde la gestión 2020 no se cuenta con el Comité de Seguridad de la Información...”.

De acuerdo al Plan Institucional de Seguridad de la Información de la UMSA (Res. HCU. N°298/2019 de 04/09/2019), en su punto 1.4.4 “Designación y Funciones del Comité de Seguridad de la Información” establece que la CSI de la UMSA, está conformada por:

“Presidente: Rector o Rectora

Vicepresidente: Presidente de la Comisión de Recursos Informativos del Honorable Consejo Universitario (HCU)

Miembros del Comité: Decanos, delegados docentes y estudiantiles de la comisión de Recursos Informativos del HCU, Jefatura del Departamento de Tecnologías de Información y Comunicación (DTIC) y RSI.

Asesores especializados:

- 1 Docente especializado en Derecho Informático.
- 1 Docente especializado en seguridad Informática.
- 1 Docente especializado en Auditoría Informática”.

Consecuentemente, se ha definido que cargos formaran parte del Comité de Seguridad de la Información; sin embargo, la designación del personal deberá realizarse mediante

²⁶ BOLIVIA. Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación. 2017. Resolución Administrativa N° AGETIC/RA/0051/2017. Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público. 28p.



Resolución Expresa por la MAE, conforme señala el la Resolución Administrativa AGETIC/RA/0059/2018 de 1 de agosto de 2018, en su artículo primero establece: “6.1.3. Mediante Resolución Expresa, la Máxima Autoridad Ejecutiva designará al personal que conformará el Comité de Seguridad de la Información (CSI).”

Por otro lado, respecto la temporalidad de vigencia de los miembros del Comité de Seguridad de la Información, sostenida con la Jefatura del Departamento de Tecnologías de la Información y Comunicación, señala:

“1. Las asignaciones de las comisiones del HCU son anuales y de conformidad a las atribuciones establecidas en el Estatuto Orgánico de la Universidad Mayor de San Andrés, en su Artículo 22 inciso s) y el Reglamento de Constitución de Comisiones del Honorable Consejo Universitario, aprobado mediante Resolución del HCU No. 062/95 que determina la Comisión de Recursos Informativos del Honorable de manera anual. Por ejemplo, la conformación de las comisiones de Recursos Informativos... son establecidas entre las primeras sesiones del HCU, y los miembros que conforman el CSI también son miembros del HCU y de la comisión de Recursos Informativos que son designadas a través de resolución del HCU, por lo que se puede concluir que la temporalidad es similar a la resolución de la comisión”.

Por lo señalado, los miembros de la Comisión de Recursos Informativos designada anualmente en la primera sesión del Honorable Consejo Universitario, son también miembros del Comité de Seguridad de la Información, por lo que su vigencia o temporalidad como miembro del CSI debiera ser anual, al igual que los miembros de la Comisión de Recursos Informativos; sin embargo, respecto la periodicidad y vigencia del personal designado como miembros del CSI, no se tiene formalizada.

Por tanto, desde la gestión 2020 hasta la fecha del presente Relevamiento Información Específica, no se conformó un nuevo Comité de Seguridad de la Información (CSI) de la



UMSA; asimismo, no se tiene definido de manera formal cada que lapso de tiempo (temporalidad) se debe nombrar, designar y/o ratificar a los miembros del CSI.

6.4 ESTRUCTURA Y CONTENIDO DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UMSA

De la revisión y análisis a los antecedentes que dieron origen al Plan Institucional de Seguridad de la Información de la UMSA, se tienen las siguientes consideraciones:

6.4.1 ANTECEDENTES Y MARCO NORMATIVO

Como parte de los antecedentes, el PISI – UMSA, en su punto 1 “ANTECEDENTES Y MARCO NORMATIVO”, hace referencia a lo siguiente:

- ❖ Estatuto Orgánico de la Universidad Mayor de San Andrés.
- ❖ Plan Estratégico Institucional de la Universidad Mayor de San Andrés 2016 -2020, con visión al 2030, aprobado con Resolución de Comité Ejecutivo del Honorable Consejo Universitario N°898/2017, del 5 de diciembre de 2017 y Resolución del Honorable Consejo Universitario N°556/2018 de 31 de octubre de 2018.
- ❖ Plan Maestro TIC de la Universidad Mayor de San Andrés, aprobado el 28 de junio de 2017, a través de Resolución del Honorable Consejo Universitario N°127/2017, expone la Misión, Visión, Plan Estratégico Institucional, Estatuto Orgánico de la UMSA, Plan Maestro TIC de la Universidad Mayor de San Andrés.

De la normativa descrita precedentemente, cabe hacer notar que el Plan Estratégico Institucional no se encuentra vigente, puesto que en la actualidad se cuenta con el PEI 2021-2025 con visión al 2030, aprobado con Resolución del HCU. N°266/2022 de 13 de julio de 2022.



6.4.2 ALCANCES DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI)

El Plan Institución de Seguridad de la Información de la UMSA (PISI), en el marco del Plan Maestro TIC Universidad Mayor de San Andrés, en su punto 2.1 “Alcance del Plan de Seguridad de la Información (PISI)”, define los siguientes alcances:

- a) “Brindar apoyo y orientación a las instancias ejecutivas con respecto a la seguridad de la información, de acuerdo con la normativa de la Universidad y los reglamentos y leyes pertinentes.
- b) Gestionar y mantener la seguridad de la información dentro de la organización, así como de los servicios de procesamiento de información.
- c) Lograr y mantener la protección adecuada de los activos organizacionales.
- d) Asegurar que los docentes, universitarios y personal administrativo de planta, eventuales, consultores, servicios y becarios entiendan sus responsabilidades sobre sus roles asignados, y reducir el riesgo de robo, fraude o uso inadecuado de las instalaciones.
- e) Evitar el acceso físico no autorizado, el daño e interferencia a las instituciones y a la información de la organización.
- f) Asegurar la operación correcta y segura de los servicios de procesamiento de información.
- g) Controlar el acceso a la información.
- h) Garantizar que la seguridad es parte integral de los sistemas de información.
- i) Asegurar que los eventos y las debilidades de la seguridad de la información, asociados con los sistemas de información, se comuniquen de forma tal que permitan tomar las acciones correctivas, oportunamente.
- j) Contrarrestar las interrupciones en las actividades de la universidad y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.



- k) Evitar el incumplimiento de cualquier ley, de obligaciones estatutarias, reglamentarias o contractuales, y de cualquier requisito de seguridad".

El alcance definido en el PISI – UMSA, fue desarrollado en el marco de los Lineamientos para la elaboración del Plan Institucional de Seguridad de la Información.

6.4.3 METODOLOGÍA DE LA GESTIÓN DE RIESGOS

El análisis de riesgos fue definido en el marco de los “Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público”, del Consejo para las Tecnologías de Información y Comunicación, definidos por la AGETIC. Por tanto, se han adoptado las siguientes fases:

- a) Identificación, clasificación y valoración de activos de información

En el punto 2.2.1 “Identificación, clasificación y valoración de activos de Información” del PISI – UMSA, se ha considerado el coordinar el proceso de identificación, clasificación y valoración de activos de información, adoptando la metodología definida en el Anexo B de los Lineamientos emitidos por el AGETIC (Resolución Administrativa N° AGETIC/RA/0051/2017).

- b) Evaluación del riesgo

Se ha considerado en el punto 2.2.2 “Evaluación de Riesgos” del PISI de la UMSA, realizar la identificación, análisis y valoración de los riesgos asociados a los activos de información identificados, clasificados y valorados, situación que permitiría a la Entidad identificar las vulnerabilidades de los activos de información y amenazas a las cuales están expuestas.

- c) Tratamiento del riesgo

En el punto 2.2.3 “Tratamiento del Riesgo” del PISI de la UMSA, se determinó que los responsables de los activos de información, en coordinación con el RSI, tomaran la decisión más apropiada para el tratamiento del riesgo identificado; sin embargo, el mismo aún no fue implementado como se describe más adelante.

- d) Controles implementados y por implementar



El PISI de la UMSA, en su punto 2.2.4 “Controles Implementados y por Implementar” establece que el Responsable de Seguridad de la Información, de manera coordinada con los responsables de activos de información, elaboraran un listado de los controles implementados y por implementar, considerando los siguientes puntos:

- ❖ Seguridad en recursos humanos (Véase el punto 1 del Anexo D).
- ❖ Gestión de activos de la información (Véase el punto 2 del Anexo D).
- ❖ Control de accesos (Véase el punto 3 del Anexo D).
- ❖ Criptografía (Véase el punto 4 del Anexo D).
- ❖ Seguridad física y ambiental (Véase el punto 5 del Anexo D).
- ❖ Seguridad de las operaciones (Véase el punto 6 del Anexo D).
- ❖ Seguridad de las comunicaciones (Véase el punto 7 del Anexo D).
- ❖ Desarrollo, mantenimiento y adquisición de sistemas (Véase el punto 8 del Anexo D).
- ❖ Gestión de incidentes de seguridad de la información (Véase el punto 9 del Anexo D).
- ❖ Plan de contingencias tecnológicas (Véase el punto 10 del Anexo D).
- ❖ Cumplimiento (Véase el punto 11 del Anexo D)”.

El anexo “D” al cual se hace referencia, corresponde a los “Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público” aprobado por Resolución Administrativa N° AGETIC/RA/0051/2017, por lo que el mismo fue adoptado para su aplicación.²⁷

6.4.4 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Respecto la Política de Seguridad de la Información, se tiene:

- Introducción

En el punto 2.3.1 del PISI – UMSA, el contenido describe los antecedentes y contexto de la seguridad de la información en la Universidad Mayor de San Andrés, y las implicancias

²⁷ BOLIVIA. Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación. 2017. Resolución Administrativa N° AGETIC/RA/0051/2017. Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público.



que se tendrían en caso de presentarse fallos, deterioros, modificaciones, ausencias ante accesos no autorizados a la información institucional, por lo que se pretende proporcionar lineamientos generales y claros para una buena administración de la misma.

- Términos y definiciones

El PISI de la UMSA, en su punto 2.3.2 “Términos y Definiciones” expone y desglosa la terminología, acrónimos y palabras propias utilizadas para el desarrollo de la Política de Seguridad de la Información, definiendo los siguientes términos:

- Activo.
- Amenaza.
- Disponibilidad.
- Gestión de riesgo.
- Centro de Procesamiento de Datos (CPD).
- Confidencialidad.
- Control.
- Incidente de seguridad de la información.
- Infraestructura de red de Telecomunicaciones.
- Integridad.
- Internet.
- Lineamientos.
- Medios de Procesamiento de la Información.
- Norma Internacional.
- Política.
- Red de Área Local.
- Red de Perímetro.
- Riesgo.
- Seguridad de la Información.



- Usuario.
- Vulnerabilidad.
- Personal Contratado con SABS.

En contraste con los “Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público” aprobado por Resolución Administrativa N° AGETIC/RA/0051/2017, no se ha considerado en la terminología descrita precedentemente, a los siguientes términos: Activo de Información, Acuerdo de Confidencialidad, Apetito del Riesgo, Comité de Seguridad de la Información, Custodio del Activo de Información, Política de Seguridad de la Información, Responsable del Activo de Información y Seguridad Informática, entre otros.

- Objetivo general

En el punto 2.3.3.1 “Objetivo General”, se define el plan de acción y las políticas relacionadas a la seguridad de la información en la UMSA, garantizando su uso y acceso seguro a las herramientas TIC; sin embargo, no hace énfasis en el resguardo de los activos de información respecto su confidencialidad, integridad y disponibilidad.

- Objetivo Específicos

El punto 2.3.3.2 “Objetivos Específicos”, se han formulado en temas relacionados a la gestión de activos de información, gestión de riesgos, gestión de incidentes, entre otros, relacionados a aspectos de seguridad de la información.

- Alcance

En el punto 2.3.4 “Alcance”, se ha definido el alcance a la integridad de los Sistemas de Información de la Universidad Mayor de San Andrés, con aplicación a los procesos de gestión Académica y Administrativa.



- Roles y responsabilidades

En el punto 3.2.7 “Roles y Responsabilidades”, se han definido los roles y responsabilidades de las siguientes instancias:

- Honorable Consejo Universitario.
- Rector Universidad Mayor de San Andrés (Máxima Autoridad Ejecutiva).
- Responsable de Seguridad de la Información.
- Comité de Seguridad de la Información.
- Departamento de Tecnologías de la Información y Comunicación.
- Jefe de División de Sistemas de Información y Estadística.
- Jefe de División de Redes y Sistemas de Información.

Se han definido roles y responsabilidades acordes a las particularidades que tiene la Universidad Mayor de San Andrés.

- Desarrollo

En el punto 2.3.8.1 “Ámbitos y Lineamientos” del punto 2.3.8 “Desarrollo” del Plan Institucional de Seguridad de la Información de la UMSA, se describe la postura Institucional en materia de lineamientos y reglas generales para el desarrollo de los controles de seguridad, en los siguientes ámbitos de seguridad:

- Protección de la información institucional ante amenazas que se originan de Recursos Humanos.
- Uso y Protección de Activos de Información.
- Control de Accesos a Recursos TIC.
- Protección de la Información transmitida a través de las redes de comunicación.
- Protección de las Áreas e Instalaciones donde se Genera, Procesa, transmite o almacena la Información Sensible y/o Crítica.



- Proporcionar la Seguridad en el Ciclo de Vida de Software y/o Hardware que se Desarrolló y/o Adquiera.
- Proporcionar la Continuidad de las Operaciones y Procesos, Mediante la Gestión de Incidentes en Seguridad de la Información.
- Protección de Información Física Documental.

- Difusión

En el punto 2.6 “Difusión” del PISI de la UMSA, se describe la posición institucional en cuanto a la difusión de toda la documentación generada, así como los medios y mecanismos de su difusión, según se expone a continuación:

- Publicación en sitio Web de la Universidad Mayor de San Andrés (<https://umsa.bo/>).
- Publicación masiva a través del correo electrónico.
- Publicación en las páginas y grupos administrados por la Universidad Mayor de San Andrés en redes sociales.
- Campañas de sensibilización dirigida a los usuarios finales.
- Campañas de capacitación dirigidas a los recursos humanos que gestionan TIC.

- Cumplimiento

En el punto 2.7 “Cumplimiento” del PISI de la UMSA, se establece de forma clara la obligatoriedad del cumplimiento de la Política de Seguridad de Información de la UMSA a los estamentos docentes, estudiantil y administrativo de la Universidad Mayor de San Andrés.

- Sanciones

En el punto 2.8 “Difusión” del PISI de la UMSA, se establece de forma clara que el incumplimiento a la Política de Seguridad de Información y todo lo relacionado a la misma conlleva sanciones en el marco de la normativa vigente.



- Histórico de Cambios

En el punto 2.3.11 “Histórico de Cambios” del PISI de la UMSA, se definen los siguientes parámetros respecto su historial:

“Titulo:	PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS
Versión:	1.2
Fecha dd/mm/aa:	17/06/2019
Resumen:	Documento del Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés.
Palabras Clave:	Plan, estrategia, seguridad.
Autor (es):	Lic. Marina Delgado Rodríguez. Responsable de Seguridad de la Información Lic. Victor Hugo Chávez Salazar Docente Facultad de Ciencias Económicas y Financieras Dra. Karina Medinaceli Díaz Docente Facultad de Derecho y Ciencias Políticas
Revisado por:	Comité de Seguridad de la Información
Aprobado por:	Honorable Consejo Universitario Resolución N°
Información adicional:”	

6.4.5 CONTROLES MÍNIMOS DE LA SEGURIDAD DE LA INFORMACIÓN

En el punto 2.3.9 “Controles Mínimos de Seguridad de la Información”, del PISI de la UMSA, se establecen los siguientes controles mínimos de seguridad de la información:

1. Seguridad en Recursos Humanos.
2. Gestión de Activos de Información.
3. Control de Accesos.



4. Criptografía.
5. Seguridad Física y Ambiental.
6. Seguridad de las Operaciones.
7. Seguridad de las Comunicaciones.
8. Desarrollo, mantenimiento y adquisición de sistemas.
9. Gestión de incidentes de seguridad de la información.
10. Plan de contingencias tecnológicas.
11. Cumplimiento.

6.4.6 INDICADORES Y MÉTRICAS

En el punto 2.3.10 “Indicadores y Métricas” del PISI de la UMSA, se establece que el Responsable de Seguridad de la Información establecerá indicadores y métricas de cumplimiento al momento de elaborar y desarrollar un determinado control de seguridad, indicador y métrica deberá ser:

- a) Específico.
- b) Medible cualitativa o cuantitativamente y/o con indicadores y atributos.
- c) Alcanzable.
- d) Relevante.
- e) Repetible en periodos de tiempo.

6.5 CRONOGRAMA DE IMPLEMENTACIÓN DEL PISI - UMSA

El Plan Institucional de Seguridad de la Información de la UMSA, en su Punto 2.4 “Cronograma de Implantación”, establece lineamientos y contenido mínimo para la elaboración de dicho cronograma, como ser: Fechas, controles a implementarse, roles y responsabilidades, actividades relacionadas a capacitación, seguimiento, revisión y aplicación de controles; sin embargo, desde la aprobación del PISI (04/09/2019), hasta la emisión del presente Relevamiento, no se han elaborado procesos y/o procedimientos



emergentes de la Política de Seguridad de la Información, insumo para la elaboración de dicho cronograma.

Por tanto, no se ha concretado la construcción del Cronograma de Implementación del Plan Institucional de Seguridad de la Información de la UMSA.

6.6 APROBACIÓN DEL PISI - UMSA

El Plan Institucional de Seguridad de la Información de la UMSA, fue aprobado mediante Resolución del Honorable Consejo Universitario N°298/2019 de 4 de septiembre de 2019, según se expone a continuación:

“Artículo Único. Aprobar el “PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS”, cuyo documento se encuentra adjunto a la presente Resolución”.

6.7 IMPLEMENTACIÓN DEL PISI - UMSA

Respecto la implementación del Plan Institucional de Seguridad de la Información de la UMSA, se tiene las siguientes consideraciones:

6.7.1 APLICACIÓN DE CONTROLES

Como procedimiento para verificar si se han aplicado los controles mínimos requeridos por los “Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información en las entidades del Sector Público”, mediante nota AUD.INT.CARTA N°353/2024 de 26 de marzo de 2024, se ha solicitado al DTIC, lo siguiente:

“5. Reglamentos, Manuales de Procesos y/o Procedimientos de seguridad, emergentes de la Implementación del Plan Institucional de Seguridad de la Información, relacionados a los 11 anexos de los controles mínimos de seguridad de la información, previstos en el numeral 6.2.3.2 de los Lineamientos para la Elaboración e Implementación de los Planes



Institucionales de Seguridad de la Información de las Entidades del Sector Público, emitidos por la AGETIC:

- a. Seguridad en recursos humanos
- b. Gestión de activos de información
- c. Control de accesos
- d. Criptografía
- e. Seguridad física y ambiental
- f. Seguridad de las operaciones
- g. Seguridad de las comunicaciones
- h. Desarrollo, mantenimiento y adquisición de sistemas
- i. Gestión de incidentes de seguridad de la información
- j. Plan de contingencias tecnológicas
- k. Cumplimiento.

En atención a nuestro requerimiento, el DTIC mediante NOTA UMSA DTIC N°181/2024 de 3 de abril de 2024, responde lo siguiente:

“Actualmente no se tiene conocimiento de que se hayan aprobado Reglamentos, Manuales de Procesos y/o Procedimientos de seguridad, emergentes de la Implementación del Plan institucional de Seguridad de la Información toda vez que desde la gestión 2020 no se cuenta con el Comité de Seguridad de la Información ni con el Responsable de Seguridad de la Información”.

Por tanto, no se han aplicado los controles mínimos contemplados en el Plan Institucional de Seguridad de la Información de la UMSA, a falta de la designación de un nuevo Responsable de Seguridad de la Información, conformación de un nuevo Comité de Seguridad de la Información, desde la gestión 2020; asimismo, la ausencia de un cronograma de implementación del PISI.



6.7.2 CAPACITACIÓN E INDUCCIÓN

De acuerdo a NOTA UMSA DTIC N°181/2024 de 3 de abril de 2024, emitida por el DTIC, en la gestión 2019 se realizaron 3 cursos de capacitación dirigido a las Autoridades y al personal Administrativo, organizados por el Programa Permanente de Capacitación Administrativa (PPCAD):

- Primer evento desarrollado el 16, 18, 19 y 20 de septiembre de 2019.
- Segundo evento realizado el 30/09/2019 y 1, 2 y 3/10/2019.
- Tercer evento realizado el 28, 29, 30 31 de octubre de 2019.

Sobre el particular, mediante nota RRHH/DIV.DES.RRHH/PPCAD/041/2024 de 18 de abril de 2024, emitido por la División de Desarrollo del Departamento de Recursos Humanos Administrativos, reporta que el Programa Permanente de Capacitación Administrativa (PPCAD), realizó el curso Seguridad de la Información en la gestión 2019, dirigida a personal administrativo de la UMSA y dictada por el Dr. Ivar René Buezo Garcia, desarrollada en la Sala Multipropósito del subsuelo del Edificio Hoy, en las siguientes fechas:

- ❖ Grupo: 1 Desarrollada el 16, 18, 19 y 20 de septiembre 2019.
- ❖ Grupo: 2 Desarrollado el 30 de septiembre, 1, 2 y 3 de octubre de 2019

Asimismo, reporta que el 21 y 22 de octubre de 2021 se desarrolló el Curso de Seguridad de la Información en modalidad virtual, dictada por el Dr. Ruben Pablo Suxo Camacho. Por tanto, se confirma la realización de los cursos de capacitación respecto a temas de seguridad de la información; sin embargo, sin incidencia en la implementación del PISI de la UMSA.

6.7.3 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Conforme lo descrito en el punto 6.7.1 del presente relevamiento, la entidad no elaboró procedimientos para la gestión de incidentes, que establezcan con claridad procesos de planificación y preparación, detección y reporte, valoración y decisión, respuesta y



erradicación para la mejora continua ante la ocurrencia de incidentes relacionados a la seguridad de la información.

Asimismo, a falta de designación de un nuevo Responsable de Seguridad de la Información (desde la gestión 2020), no se cuenta con un contacto al interior y exterior de la entidad para reportar la ocurrencia de gestión de incidentes.

Respecto los incidentes que se presentan a nivel institucional, correspondiente a la reunión sostenida con la Jefatura del Departamento de Tecnologías de la Información y Comunicación se expone: “Oficialmente no se cuenta con el RSI, responsable de incidentes a nivel institucional, sin embargo, ante cualquier notificación por parte del CGII, se arma un equipo de profesionales del DTIC, de acuerdo al área afectada para el análisis e implementación de solución”.

En consecuencia, al no contarse con un RSI, no se ha reportado incidentes informáticos al AGETIC; asimismo, no se ha formalizado procedimientos para la gestión de incidentes.

6.7.4 REVISIÓN Y MEJORA CONTINUA

Como se ha señalado precedentemente, desde la gestión 2020 no se ha designado a un nuevo Responsable de Seguridad de la Información de la UMSA, razón por la cual no se han realizado revisiones periódicas al Plan Institucional de Seguridad de la Información de la UMSA, en relación al cumplimiento y eficacia de procesos y/o procedimientos de la Política de Seguridad de la Información.

Por tanto, no se cuenta con resultados que permitan medir la efectividad y cumplimiento de los controles implementados y en función de los mismos, se realice una mejora continua de la seguridad de la información.



7 COMUNICACIÓN DE RESULTADOS

Mediante Resolución Rectoral No. 642 de 24 de septiembre de 2018, se designó a la Lic. Marina Felicidad Delgado Rodríguez, Jefe a.i. del Departamento de Tecnologías de la Información y Comunicación, como Responsable de Seguridad de la Información (RSI) de la Universidad Mayor de San Andrés y representante de la UMSA ante la AGETIC, cuya gestión cesó el 14 de septiembre de 2020, debido al cambio de Jefatura.

Posteriormente, pese a los recordatorios y solicitudes para la designación de un RSI y creación de un ITEM, efectuada por la Jefatura del DTIC a diferentes gestiones rectorales (INFORME DTIC No.049/2020 10/09/2020, NOTA UMSA DTIC N°966/2022 de 01/09/2022, NOTA UMSA DTIC N°1363/2022 de 01/12/2022), no prospero la designación.

En fecha 16 de marzo de 2023, mediante Resolución Rectoral N°093 se designó al Jefe de la División de Redes y Sistemas de Información como OFICIAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UMSA; sin embargo, no se tiene definidas las funciones de un Oficial de Seguridad de la Información en el PISI de la UMSA y/o Lineamiento para la Elaboración del PISI emitidos por el AGETIC, por lo que no puede considerarse RSI de la UMSA.

Consecuentemente, desde septiembre de 2020 hasta la fecha del presente relevamiento, no se cuenta con la designación de un nuevo Responsable de Seguridad de la Información de la UMSA.

Cabe hacer notar que de acuerdo al Artículo Segundo de la Resolución del Honorable Consejo Universitario N°230/2018 de 11 de julio de 2018, la Comisión de Recursos Informativos del HCU, puede sugerir una terna para la designación del RSI.



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



Mediante Resolución del Honorable Consejo Universitario No. 464/2018 de 26 de septiembre de 2018, se conformó el Comité de Seguridad de la Información (CSI) de la Universidad Mayor de San Andrés, que estuvo compuesta por las siguientes autoridades y representantes docentes y estudiantes:

- ✓ Dr. Wilfredo Tavera Llanos, Decano de la Facultad de Ciencias Puras y Naturales.
- ✓ Ing. Miguel Ángel Calla Carrasco, Decano Facultad de Ingeniería.
- ✓ Lic. Víctor Paz Huanca, delegado Docente HCU Facultad de Tecnología.
- ✓ Dr. Martín Villarroel Mareño, delegado Docente HCU. Facultad de Medicina, Enfermería, Nutrición y Tecnología Médica.
- ✓ Univ. Kitzia Jarandina Guamán, delegado Estudiantil HCU. Facultad de Ciencias Facultad de Ciencias Farmacéuticas y Bioquímicas.
- ✓ Univ. Garios Fernando Torrez Alancea, delegado Estudiantil HCU. Facultad de Ciencias Puras y Naturales.
- ✓ Univ. Brian Rojas Mora, delegado Estudiantil HCU. Facultad de Ciencias Geológicas.
- ✓ Lic. Marina Delgado Rodríguez, Jefa a.i. Departamento de Tecnologías de la Información y Comunicación.
- ✓ Lic. Marcelo Germán Aruquipa Chambi, Docente Carrera de Informática.
- ✓ M.Sc. Moisés Martín Silva Choque, Docente Carrera de Informática.
- ✓ Dra. Karina Ingrid Medinaceli Díaz, Directora a.i. Instituto de Investigaciones Seminarios y Tesis Carrera de Derecho – Facultad de Derecho.
- ✓ Lic. Norma Castro Quispe, Coordinadora Plan Maestro TIC – UMSA.
- ✓ M. Sc. Víctor Hugo Chávez Salazar, Docente Carrera de Administración de Empresas.
- ✓ Ing. Marcelo Ramírez Molina, Docente Carrera de Ingeniería Electrónica.

En el detalle precedente se advierte que no se consigna al Rector como Máxima Autoridad Ejecutiva de la UMSA en calidad de Presidente del Comité de Seguridad de la



Información (CSI), o en su defecto delegar dicha función en su representación, en apego al punto 6.1.3 de los “Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público” emitidos por el AGETIC.

De acuerdo a NOTA UMSA DTIC N°181/2024 de 3 de abril de 2024, se reporta que la UMSA no cuenta con Comité de Seguridad de la Información desde la gestión 2020 designado mediante Resolución Expresa; asimismo, en el Acta de Reunión N°1 de 24 de abril de 2024, la Jefatura del Departamento de Tecnologías de la Información y Comunicación, aclara que los miembros de la Comisión de Recursos Informativos designada anualmente en la primera sesión del Honorable Consejo Universitario, son también miembros del Comité de Seguridad de la Información, por lo que su vigencia o temporalidad como miembro del CSI debiera ser anual, al igual que los miembros de la Comisión de Recursos Informativos; sin embargo, respecto la periodicidad y vigencia del personal designado como miembros del CSI, no se tiene formalizada.

Al respecto, se debe analizar la pertinencia de designar a los miembros de la Comité de Seguridad de la Información de la UMSA, de manera paralela a la conformación de la Comisión de Recursos Informativos del Honorable Consejo Universitario, definiendo que su periodicidad y/o temporalidad de su vigencia sea equivalente.

Por tanto, desde la gestión 2020 hasta la fecha del presente Relevamiento Información Específica, no se designó mediante Resolución Expresa a personal que conforme un nuevo Comité de Seguridad de la Información (CSI) de la UMSA; asimismo, no se tiene definido de manera formal cada que lapso de tiempo (temporalidad) se debe nombrar, designar y/o ratificar a los miembros del CSI.



En el contenido del Plan Institucional de Seguridad de la Información (PISI) de la UMSA (Antecedentes y Marco Normativo, Alcances del PISI, Metodología de la gestión de riesgos, Política de Seguridad de la Información, Controles mínimos de la seguridad de la información, entre otros), se han elaborado en el marco de los “Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público”, aprobado mediante Resolución Administrativa N°AGETIC/RA/0051/2017; sin embargo, se tienen las siguientes consideraciones:

- ✓ El PISI de la UMSA, en sus Antecedentes y Marco Normativo (Punto 1) inserta a la Misión y Visión de la UMSA en extraído del Plan Estratégico Institucional (PEI) 2016-2020 con visión 2030, por lo que corresponde actualizar al PEI 2021-2025 con visión al 2030, aprobado con Resolución del HCU. N°266/2022 de 13 de julio de 2022, vigente.
 - ✓ En el acápite Términos y Definiciones del PISI de la UMSA (punto 2.3.2), expone y desglosa la terminología, acrónimos y palabras propias utilizadas para el desarrollo de la Política de Seguridad de la Información acorde a los Lineamientos para la elaboración del PISI; sin embargo, no se ha considerado las siguientes definiciones: Activo de Información, Acuerdo de Confidencialidad, Apetito del Riesgo, Comité de Seguridad de la Información, Custodio del Activo de Información, Política de Seguridad de la Información, Responsable del Activo de Información y Seguridad Informática, entre otros.
 - ✓ El Objetivo General (punto 2.3.3.1), no hace énfasis en el resguardo de los activos de información respecto su confidencialidad, integridad y disponibilidad.
- Debido a la falta de designación de un nuevo Responsable de Seguridad de la Información y designación de manera expresa por la MAE de un nuevo Comité de Seguridad de la Información desde la gestión 2020, no se ha dado continuidad a la



implementación del Plan Institucional de Seguridad de la Información de la UMSA, por lo que:

- ✓ No se han implementado los siguientes controles mínimos (punto 2.2.4 “Controles Implementados y por Implementar”) contemplados en el Plan Institucional de Seguridad de la Información de la UMSA:
 - “Seguridad en recursos humanos.
 - Gestión de activos de la información.
 - Control de accesos.
 - Criptografía.
 - Seguridad física y ambiental.
 - Seguridad de las operaciones.
 - Seguridad de las comunicaciones.
 - Desarrollo, mantenimiento y adquisición de sistemas.
 - Gestión de incidentes de seguridad de la información.
 - Plan de contingencias tecnológicas.
 - Cumplimiento.

- ✓ Respecto la capacitación e inducción, se realizó el curso Seguridad de la Información en la gestión 2019, dirigida a personal administrativo de la UMSA desarrollada en septiembre y octubre de la gestión 2019 y octubre de 2021; sin embargo, no se dio continuidad a este proceso.

- ✓ La UMSA, al no contar con un RSI, no se ha reportado incidentes informáticos al AGETIC; asimismo, no se ha formalizado procedimientos para la gestión de incidentes.



8 CONCLUSIONES

En base a los aspectos descritos en el punto 6 del presente Trabajo de Relevamiento de Información Específica, sobre la elaboración e implementación del Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés, en el marco del Decreto Supremo N°2514 del 9 de septiembre de 2015 y los “Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público”, aprobado con Resolución Administrativa N° AGETIC/RA/0051/2017 de 19 de septiembre de 2017, se concluye que:

- ✓ El Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés, aprobado mediante Resolución del Honorable Consejo Universitario N°298/2019 de 4 de septiembre de 2019, se ha elaborado en el marco de los “Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público”, aprobado con Resolución Administrativa N° AGETIC/RA/0051/2017 de 19 de septiembre de 2017; sin embargo, el mismo no fue actualizado y/o atravesó por procesos de mejora continua desde la gestión 2020.
- ✓ El Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés, no se ha implementado, debido a que no se ha nombrado a un nuevo Responsable de Seguridad de la Información (RSI) y conformado un nuevo Comité de Seguridad de la Información (CSI) desde la gestión 2020, que dé continuidad a su implementación.

En base al análisis efectuado, y considerando la relevancia e importancia de contar con la implementación del Plan Institucional de Seguridad de la Información, se concluye que se debe ejecutar una Auditoria de Cumplimiento en forma inmediata, para el efecto, se debe programar la misma para la siguiente gestión, toda vez, que a la fecha no se ha



implementado el PISI de la UMSA, por lo que requiere un tiempo adecuado para su implementación, considerando la magnitud de las operaciones de la UMSA.

9 RECOMENDACIONES

Se recomienda al Rector Universidad Mayor de San Andrés:

- a) En el marco del Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés, aprobado mediante Resolución del Honorable Consejo Universitario N°298/2019 de 4 de septiembre de 2019, nombrar a un nuevo Responsable de Seguridad de la Información (RSI) y Conformar un nuevo Comité de Seguridad de la Información (CSI) mediante Resolución Expresa. En este último, a futuro, se analice la pertinencia de nombrar al CSI de manera paralela a la Comisión de Recursos Informativos del Honorable Consejo Universitario.
- b) Cumplida la recomendación a), instruir al Responsable de Seguridad de la Información de la UMSA en Coordinación con el Comité de Seguridad de la Información, en lo que corresponda y considerando lo descrito en el punto 6.7 al 6.7.4 del presente trabajo, actualizar y dar continuidad al proceso de implementación del Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés.



10 BIBLIOGRAFÍA

ARENS, A. A., ELDER, R. J., & BEASLEY, M. S. (2019). Auditing and Assurance Services: An Integrated Approach (17th ed.). Pearson.

BOLIVIA. Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación. 2017. Resolución Administrativa N° AGETIC/RA/0051/2017. Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, 19 de septiembre de 2017.

BOLIVIA. Agencia de Gobierno Electrónico y Tecnologías de la Información y Comunicación. 2018. Resolución Administrativa N° AGETIC/RA/0059/2018. Modificación de la Resolución Administrativa N° AGETIC/RA/0051/2017, 1 de agosto de 2018.

BOLIVIA. Contraloría General del Estado Plurinacional de Bolivia. 2012. Resolución CGE/094/2012. Normas Generales de Auditoría Gubernamental. 27 de agosto de 2012.

BOLIVIA. Contraloría General del Estado Plurinacional de Bolivia. 2012. Resolución CGE/094/2012. Normas para el Ejercicio de la Auditoría Interna, 27 de agosto de 2012.

BOLIVIA. Contraloría General del Estado Plurinacional de Bolivia. 2024. Resolución N° CGE/018/2024. Reglamento para la elaboración de Informes de Auditoría Con Indicios De Responsabilidad RE/CE-029 V3, 4 de marzo de 2024.

BOLIVIA. Presidencia. 1990. Ley 1178. Administración y Control Gubernamental, 20 de julio de 1990.

BOLIVIA. Presidencia. 1992. Decreto Supremo 23215. Reglamento para el Ejercicio de las Atribuciones de la Contraloría General de la República, actual Contraloría General de Estado, 22 de junio de 1992.

BOLIVIA. Presidencia. 1992. Decreto Supremo 23318-A. Reglamento de la Responsabilidad por la Función Pública, 03 de noviembre de 1992.



BOLIVIA. Presidencia. 2009. Decreto Supremo 26237. Modificaciones al Reglamento de la Responsabilidad por la Función Pública, aprobado mediante Decreto Supremo N° 23318-A.

GARCÍA, J. (2021). Auditoría Gubernamental: Fundamentos y Prácticas. Editorial Gobernabilidad y Transparencia.

GONZÁLEZ, A. (2020). La Auditoría Gubernamental como Función de Control y Supervisión. Editorial Gobierno Transparente.

GONZÁLEZ, J. (2021). Auditoría Interna: Conceptos y Prácticas (2ª ed.). Editorial Auditoría Profesional.

GONZÁLEZ, J. (2021). "Auditoría Interna: Desarrollo de Competencias para un Desempeño Eficiente" (2ª ed.). Editorial Auditoría Moderna.

HERNÁNDEZ SAMPIERI, R., FERNÁNDEZ COLLADO, C., & BAPTISTA LUCIO, P. (2014). Metodología de la investigación (6a ed.). McGraw-Hill Interamericana.

LA RAZON. (1948, 20 de octubre). Historia de la Universidad de La Paz. Obtenido de <https://www.umsa.bo/historia>.

LOUWERS, T. J., RAMSAY, R. J., SINASON, D. H., & STRAWSER, J. R. (2021). Auditing & Assurance Services (8th ed.). McGraw-Hill Education.

SMITH, J. (2020). Auditoría Gubernamental: Principios y Prácticas. Editorial Público y Transparencia.

UNIVERSIDAD MAYOR DE SAN ANDRES. Departamento de Auditoría Interna. Obtenido de <https://dai.umsa.bo>

UNIVERSIDAD MAYOR DE SAN ANDRES. 2021. Manual de Organizaciones y Funciones 2021.

UNIVERSIDAD MAYOR DE SAN ANDRES. Obtenido de <https://www.umsa.bo/web/guest/quienes-somos>.

UNIVERSIDAD MAYOR DE SAN ANDRES. 2017. Unidad de Transparencia. Obtenido de https://transparencia.umsa.bo/mision_vision.



11 ANEXOS

ANEXO 1

PAPELES DE TRABAJO



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



INF. AUD. INT. N° _____

AUDITORÍA INTERNA TOMO DE

Legajo de Relevamiento de Información Específica
 Legajo de Planificación
 Legajo Corriente
 Legajo Resumen Auditoría
 Legajo Información Permanente

ARCHIVO DE PAPELES DE TRABAJO

DATOS GENERALES - UNIDAD AUDITADA

FACULTAD Y/O ÁREA: UNIVERSIDAD MAYOR DE SAN ANDRÉS

UNIDAD: _____

DIRECCIÓN: AV. 6 DE AGOSTO Nro. 2170 EDIFICIO HOY - PISO 13

TELEFONOS: (591-2) 2442797

OTROS DATOS: _____

INFORMACIÓN RELATIVA A LA AUDITORÍA

RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI)

TIPO DE AUDITORÍA: _____

PERIODO DE EXAMEN: DEL: 01 / 01 / 2024 AL: 31 / 12 / 2024

MEMORANDUM N° N° 008 / 2024 FECHA: 14 / 03 / 2024

FECHA DE INICIO: 14 / 03 / 2024 FECHA DE CONCLUSIÓN: 29 / 04 / 2024

OTROS DATOS: _____

PERSONAL RESPONSABLE DE LA EJECUCIÓN DEL TRABAJO

CARGO	NOMBRES Y APELLIDOS	INICIALES	RUBRICA
Jefe	<u>Lic. René A. Carrasco Condarco</u>	<u>R / C / C</u>	
Supervisor (1)	_____	<u>/ /</u>	_____
Supervisor (2)	_____	<u>/ /</u>	_____
Auditor (1)	<u>Lic. Dennis Magno Apaza Gonzales</u>	<u>D / A / G</u>	
Auditor (2)	_____	<u>/ /</u>	_____
Ayudante (1)	<u>Egr. Gaby Norca Arias Chambi</u>	<u>G / A / C</u>	
Ayudante (2)	_____	<u>/ /</u>	_____
Especialista y/o Perito	_____	<u>/ /</u>	_____

R.I. 61
12.



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



RI-3.1.1

RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA ELABORACIÓN E IMPLEMENTACIÓN DEL "PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS"
CÉDULA ANALÍTICA: PROCESO DE ELABORACIÓN Y APROBACIÓN DEL PISI

Preámbulo 2, 2.1, 2.2, ..., 2.6 del Programa de Trabajo, Ver en P/T RI-2.1 al RI-2.6

ETAPA	OBJETIVO	ACTIVIDADES	RESPONSABLES	REF. P/T	LINEAMIENTOS PISI ENTIDADES SECTOR PÚBLICO	REF. P/T	ACTIVIDADES REALIZADAS POR LA ENTIDAD SIG PISI - UMSA: HCU No. 293/2019	ANÁLISIS DE AUDITORIA	ACLARACIÓN Y/O OBSERVACIÓN
INICIAL	ORGANIZACIÓN INTERNA	Designación del Responsable de Seguridad de la Información	Maxima Autoridad Ejecutiva	RI - 4 - 79	"6.1 Etapa Inicial" La etapa inicial tiene como objetivo la organización interna en la entidad o institución pública para la elaboración de su PISI y comienza por la designación del Responsable de Seguridad de la Información... por parte de la Máxima Autoridad Ejecutiva (MAE)	RI - 4 - 60	Mediante Resolución Rectoral No. 642 de fecha 24 de septiembre de 2018, firmado por el Rector Waldo Albarrañin, se designó a Lic. Marina Felicidad Delgado Rodríguez, como Responsable de Seguridad de la Información (R.S.I) de la Universidad Mayor de San Andrés ante la AGETIC. De acuerdo al Artículo Segundo de la Resolución del Honorable Consejo Universitario N° 230/2018 de 11 de julio de 2018, se establece: "Aprueba el nombramiento de un Responsable de Seguridad Institucional de nivel ejecutivo, para lo cual previamente la Comisión de Recursos Informativos del HCU, sugerirá una terna al HCU, con perfil profesional adecuado para el desempeño de este cargo."	Mediante Resolución Rectoral No. 642 de fecha 24 de septiembre de 2018, se designó a Lic. Marina Felicidad Delgado Rodríguez, como Responsable de Seguridad de la Información (R.S.I) de la Universidad Mayor de San Andrés ante la AGETIC, con embargo, de acuerdo a NOTA UMSA DTIC N°18/2024 de 3 de abril de 2024, emitida por el Departamento de Tecnologías de la Información y Comunicación (DTIC), expone que desde la gestión 2020 no se cuenta con un PISI. Es pertinente hacer notar que una vez designado el PISI, no se viene definiendo el periodo por el cual el mismo ejecutara con esta designación, de que manera se notifica o designa a nuevos responsables, considerando que las autoridades son susceptibles de extinción su gestión por cambios.	1) Desde la gestión 2020 no se ha notificado (o designado) a un nuevo Responsable de Seguridad de la Información.
		Continuación del Comité de Seguridad de la Información	Maxima Autoridad Ejecutiva	RI - 4 - 79	"6.1 Etapa Inicial" La etapa inicial tiene como objetivo la organización interna en la entidad o institución pública para la elaboración de su PISI y comienza por la conformación del Comité de Seguridad de la Información en la entidad o institución pública por parte de la Máxima Autoridad Ejecutiva (MAE).	RI - 4 - 68	- Con Resolución del Honorable Consejo Universitario No. 464/2018 de fecha 26 de septiembre de 2018, firmado por el Rector Waldo Albarrañin, se conformó el Comité de Seguridad de la Información (C.S.I) de la Universidad Mayor de San Andrés. Dr. Wilfredo Tavera Llanes, DECANO FAC. CIENCIAS PURAS Y NATURALES Ing. Miguel Angel Calla Carrasco, DECANO FAC. INGENIERIA Lic. Victor Paz Huancra, DELEG. DOC. HCU FAC. TECNOLOGIA Dr. Martin Vilmarth Marcano, DELEG. DOC. HCU FAC. MEDICINA, ENFERMERIA, NUT Y TIC MED. Univ. Kizka Jaramanda Guzman, DELEG. ESTUD. HCU FAC. CS. FARMACÉUTICAS Y BIQUÍMICAS Univ. Galeso Fernando Torres Almona, DELEG. ESTUD. HCU FAC. CS. PURAS Y NATURALES Univ. Brian Rojas Mora, DELEG. ESTUD. HCU FAC. CS. GEOLÓGICAS Lic. Marina Delgado Rodríguez, JEFA a.i. DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN. Lic. Marcelo Germán Anquippa Chambo, DOCENTE CARRERA DE INFORMATICA M.Sc. Mónica Martín Silva Choque, DOCENTE CARRERA DE INFORMATICA Dra. Karina Ingrid Medinaceli Diaz, DIRECTORA a.i. INST. DE INV. SEMINARIOS Y TESIS CARRERA DE DERECHO - FAC. DERECHO Lic. Norma Castro Quipe, COORDINADORA PLAN MAESTRO TIC - UMSA M.Sc. Victor Hugo Chavez Salazar, DOCENTE CARRERA DE ADMINISTRACIÓN DE EMPRESAS Ing. Marcelo Ramirez Molina, JEFE CARRERA DE INGENIERIA ELECTRIC.	Mediante Resolución HCU No. 464/2018 de 26 de septiembre de 2018, se conformó el Comité de Seguridad Institucional de la Información (C.S.I) de la Universidad Mayor de San Andrés. De acuerdo a NOTA UMSA DTIC N°19/2024 de 3 de abril de 2024, emitida por el Departamento de Tecnologías de la Información y Comunicación (DTIC), expone que desde la gestión 2020 no se cuenta con C.S.I. Sobre el particular, es pertinente hacer notar que una vez conformado el Comité de Seguridad de la Información, no se viene definiendo el periodo por el cual dicho organismo con esta designación, de que manera se notifica o designa a nuevos responsables, considerando que las autoridades son susceptibles de extinción su gestión por cambios.	2) Desde la gestión 2020 no se ha notificado (o designado) a un nuevo Comité de Seguridad de la Información.
		Introducción, objetivos y alcance de la Información	Responsable de Seguridad de la Información	RI - 4 - 81	6.2 Etapa de desarrollo del PISI Tiene como objetivo establecer las actividades para la elaboración y aprobación del PISI 6.2.1 Definición de los alcances del PISI La entidad o institución pública definirá, dentro de su PISI, los alcances relacionados a proyectos, procesos y operaciones considerados prioritarios para cumplir con la misión, visión y objetivos estratégicos de la entidad.	RI - 4 - 43 - 1 RI - 4 - 43 - 2 RI - 4 - 43 - 3	PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS 7. ANTECEDENTES Y MARCO NORMATIVO 7.1 Misión La Universidad Mayor de San Andrés produce conocimiento científico, tecnológico y cultural pertinente y relevante, inter y transdisciplinario, que revoluciona los saberes ancestrales y promueve políticas públicas, respondiendo a la demanda y necesidades locales, regionales y nacionales, hacia un desarrollo sustentable. Formar profesionales altamente calificados, con compromiso y responsabilidad social, con reflexión y pensamiento crítico. 7.2 Visión Hacia el 2020 la Universidad Mayor de San Andrés es una Universidad emprendedora e innovadora, con reconocimiento internacional, valorada por su contribución a la generación de conocimiento y formación de profesionales líderes en la revolución del pensamiento con responsabilidad y compromiso al servicio de la sociedad y la humanidad. 7.3 Marco normativo de la Universidad Mayor de San Andrés El Estatuto Orgánico de la Universidad Mayor de San Andrés define que los fines y objetivos principales de la Universidad Mayor de San Andrés son: a) Los fines y objetivos generales señalados en el Estatuto Orgánico de la Universidad Boliviana. b) Formar profesionales líderes en todas las áreas del quehacer científico, tecnológico y cultural, los que deberán responder a las necesidades de la transformación y el desarrollo nacional y regional. (...) En el área de Tecnologías de Información y Comunicación, resea al interior de la Universidad Mayor de San Andrés las siguientes disposiciones: - Plan estratégico Institucional de la Universidad Mayor de San Andrés 2016-2020, con visión al 2030, aprobado con resolución de Comité Ejecutivo del Honorable Consejo Universitario N° 699/2017, del 5 de diciembre de 2017 y Resolución del Honorable Consejo Universitario N° 559/2018 del 31 de octubre de 2018. - Plan Maestro TIC de la Universidad Mayor de San Andrés, aprobado en fecha 28 de junio de 2017, a través de Resolución del Honorable Consejo Universitario W 127/2017. De forma complementaria, se aplican las disposiciones normativas vigentes en el Estado Plurinacional en el área de telecomunicaciones y TIC.	De la normativa descrita precedentemente, cabe hacer notar que el Plan Estratégico Institucional no se encuentra vigente, puesto que en la actualidad no cuenta con el PEI 2021-2025 con visión al 2030, aprobado con Resolución del HCU, N° 296/2022, de 13 de julio de 2022.	3) El PISI de la UMSA, cuenta en su contenido el PEI 2021-2025 con visión 2030, por lo que corresponde actualizar el PEI 2021-2025 con visión 2030.

SUBSCRITO POR
R.C.C.
D.M.A.G.

Ver Fuente, objetivo y conclusión en P/T RI-3.1.9



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



RI-3.1.2

SEGÚN RESOLUCIÓN ADMINISTRATIVA N° AGETIC/RA/0051/2017					ACTIVIDADES REALIZADAS POR LA ENTIDAD		ANÁLISIS DE AUDITORÍA		
ETAPA	OBJETIVO	ACTIVIDADES	RESPONSABLES	REF: P/T	REF: P/T	REF: P/T	REF: P/T	REF: P/T	
DESARROLLO	ESTRUCTURA Y CONTENIDO DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI)					<p>2. ETAPA DE DESARROLLO PLAN INSTITUCIONAL DE SEGURIDAD DE INFORMACIÓN</p> <p>2.1. Alcances del Plan Institucional de Seguridad de la Información</p> <p>Queda cumplimiento el Plan Maestro TIC Universidad Mayor de San Andrés, el Plan Institucional de Seguridad de la Información formará los objetivos establecidos en el Proyecto de Sistema de Gestión de Seguridad de la Información por lo que se definen los siguientes alcances:</p> <p>a) Brindar apoyo y orientación a las instancias ejecutivas con respecto a la seguridad de la información, de acuerdo con la normativa de la Universidad y los reglamentos y leyes pertinentes.</p> <p>b) Gestionar y mantener la seguridad de la información dentro de la organización, así como de los servicios de procesamiento de información.</p> <p>c) Lograr y mantener la protección adecuada de los activos organizacionales.</p> <p>d) Asegurar que los docentes, universitarios y personal administrativo de planta, eventuales, consultores, servicios y becarios entiendan sus responsabilidades sobre sus roles asignados, y reducir el riesgo de robo, fraude o uso indebido de los instalaciones.</p> <p>e) Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.</p> <p>f) Asegurar la operación correcta y segura de los servicios de procesamiento de información.</p> <p>g) Controlar el acceso a la información.</p> <p>h) Garantizar que la seguridad es parte integral de los sistemas de información.</p> <p>i) Asegurar que los eventos y las actividades de la seguridad de la información, asociados con los sistemas de información, se comuniquen de forma tal que permitan tomar las acciones correctivas, oportunamente.</p> <p>j) Contratar las informaciones en las actividades de la universidad y proteger sus procesos críticos contra los efectos de fallos importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.</p> <p>k) Evitar el incumplimiento de cualquier ley, de disposiciones estatutarias, reglamentarias o contractuales, y de cualquier requisito de seguridad.</p>			<p>Si se elabora dentro de el PISI -UMSA, se detallado en el marco de los Lineamientos para la elaboración del Plan Institucional de Seguridad de la Información.</p>
		Metodología de Gestión de Riesgos	Responsable de Seguridad de la Información	<p>6.2.2 Adopción de una metodología de gestión de riesgos</p> <p>El PISI contempla la gestión de riesgos en el ámbito de la seguridad de la información. Para esto, la entidad o institución pública deberá adoptar un estándar o metodología de gestión de riesgos dentro de los alcances del PISI, con el objetivo de implementar controles de seguridad e mejorar la eficacia de los controles ya existentes.</p> <p>La adopción de dicha metodología deberá incorporar los siguientes aspectos:</p> <p>a) Identificación, clasificación y valoración de activos de información.</p> <p>b) El PISI, de forma conjunta con los responsables de los procesos identificados dentro de los alcances del Plan Institucional de Seguridad de la Información, coordinará el proceso de identificación, clasificación y valoración de activos de información. Para esta parte, se recomienda usar la que se indica en el Anexo B.</p>	RI-4-46-1	<p>7.2. Metodología de la Gestión del Riesgo</p> <p>Para el tratamiento del análisis de riesgos, se seguirá los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, del Consejo para las Tecnologías de Información y Comunicación, definidos por el AGETIC, de acuerdo a la solicitud emitida al Rector de la Universidad Mayor de San Andrés a través de nota AGETIC/NO/1870/2017. En fecha 07/11/2017, se recibió la nota proveniente de la AGETIC en la cual el Rector fue notificado de la aprobación por unanimidad el documento "Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público" por el Pleno del Consejo para las Tecnologías de Información y Comunicación del Estado Plurinacional de Bolivia (CETIC-EPB) a través de Resolución Administrativa AGETIC/RA/0051/2017.</p> <p>Teniendo presente que, Seguridad es la capacidad de las redes o los sistemas de información para resistir con un determinado nivel de confianza, los accidentes o acciones (fuerza o malintencionadas) que comprometen la disponibilidad, integridad y confidencialidad de los datos almacenados e transmitidos y de los servicios que dichos redes y sistemas ofrecen a los usuarios, en este entendido la metodología adoptada para la gestión de riesgos, está basada la Metodología de Análisis y Gestión de Riesgos MAGERIT, y el Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés trabajará en las siguientes fases:</p> <ul style="list-style-type: none"> Identificación, clasificación y valoración de activos de información Evaluación del riesgo Tratamiento del riesgo Controles implementados y por implementar. 		<p>Mediante los Lineamientos para la elaboración e implementación del PISI emitidos por el AGETIC, menciona en el punto 6.2.2 que la entidad deberá adoptar metodología de gestión de riesgos dentro de los alcances del PISI, con el objetivo de implementar medidas de seguridad, de acuerdo con lo indica el, menciona que se elaborará un listado de servicios, los cuales se estructuran en el punto 6.2.2.2. Controles críticos de seguridad de la información, cuando encuentre lo mencionado, estos controles implementados y por implementar de seguridad se encuentran en el Anexo D. LINEAMIENTOS PARA LA ELABORACIÓN E IMPLEMENTACIÓN DE LOS PLANES INSTITUCIONALES DE SEGURIDAD DE LA INFORMACIÓN DE LAS ENTIDADES DEL SECTOR PÚBLICO, PUBLICADO POR EL CONSEJO PARA LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN Y EL CENTRO DE GESTIÓN DE TECNOLOGÍAS INFORMATICAS.</p>	
						RI-4-47-1	<p>7.2.1. Identificación, clasificación y valoración de activos de información</p> <p>7.2.1.1. Identificación</p> <p>La identificación y el inventario de activos de información de la Universidad Mayor de San Andrés permitirá clasificar y valorar el activo en términos cuantitativos o cualitativos, para brindar un mejor tratamiento y protección se debe identificar, especificar claramente sus características y la función al interior de los procesos alineados con los objetivos y a los alcances definidos en este documento.</p> <p>La clasificación de los activos de información se realizará con los siguientes criterios:</p> <ul style="list-style-type: none"> Datos e información Claves criptográficas Software, como sistemas de información de apoyo a la gestión académica, financiera, administrativa, Equipamiento informático, como computadores, servidores, periféricos, routers, y otros. Servicios, como correo electrónico, servicios web, DNS, DHCP, entre otros. Recursos humano: personal docente, universitarios, personal administrativo, que este directamente relacionados con los procesos de gestión del riesgo y por sus conocimientos y habilidades se considera un activo de información. <p>La identificación, clasificación y valoración de activos de información, permitirá identificar los activos de información claves de la Universidad Mayor de San Andrés, por lo que serán clasificados de acuerdo a su tipo y se los valorará según su disponibilidad, integridad y confidencialidad.</p> <p>Este análisis se realizará:</p> <ul style="list-style-type: none"> De manera anual en el Departamento de Tecnologías de Información y Comunicación (DTIC) y las Unidades TIC facultadas, que estarán encargadas de realizar esta clasificación. Al efecto, deberán comunicarse al Responsable de Seguridad de la Información (RSI) el nombre del docente, administrativo o personal contratado bajo SABS que lo designe como responsable de esta tarea. Actualización al proceso al que pertenece el activo. Inclusión de nuevos procesos y procedimientos. Inclusión de un nuevo activo. Ocupación de una unidad organizacional, proceso o cargo, de los responsables o custodios de los activos de información. Correos o migraciones de sistemas de información en donde se almacenan los activos de la ubicación ya inventariados. Cambios físicos de la ubicación de activos de información. Bajas/eliminación/suspensión de un activo de información. 		<p>En el punto 7.2.1 "Identificación, clasificación y valoración de activos de información" del PISI -UMSA, se ha considerado el coordinar el proceso de identificación, clasificación y valoración de activos de información, adoptando la metodología definida en el Anexo B de los Lineamientos emitidos por el AGETIC (Resolución Administrativa N° AGETIC/RA/0051/2017).</p>



Ver Fuente, objetivo y conclusión en P/T RI-3.1.9



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



RI-3.1.9

SEGUN RESOLUCIÓN ADMINISTRATIVA N° AGETIC/RA/0051/2017					REF. PIT	ACTIVIDADES REALIZADAS POR LA ENTIDAD SIG PISI- UMSA- HCU No. 288/2019	ANÁLISIS DE AUTORÍA	ACLARACIÓN Y/O OBSERVACIÓN
ETAPA	OBJETIVO	ACTIVIDADES	RESPONSABLES	REF. PIT				
		Programa de implementación de la Información	Responsable de Seguridad de la Información	<p>3.3 Cronograma de implementación</p> <p>En el marco del Plan Institucional de Seguridad de la Información, la entidad o institución pública deberá elaborar un cronograma de implementación de los controles definidos. Para esto, todos los procesos y procedimientos que se desprenden de la Política de Seguridad de la Información deberán estar previamente elaborados para su aplicación. El cronograma de implementación deberá contemplar mínimamente:</p> <p>a) Fechas b) Controles a implementarse c) Roles y responsabilidades. d) Actividades relacionadas a capacitación, seguimiento, revisión y aplicación de controles.</p> <p>La implementación del Plan Institucional de Seguridad de la Información estará sujeta al cronograma y no debería exceder el plazo de un año desde su aprobación por parte de la entidad o institución pública. De acuerdo al contrato de cada institución y sus recursos, este plazo podrá ser ampliado previa justificación escrita por la MAE y la documentación de respaldo elaborada por el PISI indicando las causas del retraso.</p> <p>La disposición transitoria segunda del Decreto Supremo 2514 de 9 de septiembre de 2015, establece que "las entidades del nivel central del Estado deberán presentar a la AGETIC, en un plazo no mayor a un (1) año desde la aprobación de las políticas de seguridad de la información por la AGETIC, su Plan Institucional de Seguridad de la Información".</p>	<p>3.4 Cronograma de implementación</p> <p>En el marco del Plan Institucional de Seguridad de la Información, la entidad o institución pública deberá elaborar un cronograma de implementación de los controles definidos. Para esto, todos los procesos y procedimientos que se desprenden de la Política de Seguridad de la Información deberán estar previamente elaborados para su aplicación. El cronograma de implementación deberá contemplar mínimamente:</p> <p>a) Fechas b) Controles a implementarse c) Roles y responsabilidades. d) Actividades relacionadas a capacitación, seguimiento, revisión y aplicación de controles.</p>	<p>En el Decreto Supremo N° 2514 en la Disposición Transitoria Segunda, determina que las entidades del nivel central del Estado deberán presentar a la AGETIC, en un plazo no mayor a un año, desde la aprobación por la AGETIC, su Plan Institucional de Seguridad de la Información.</p> <p>El Plan Institucional de Seguridad de la Información de la UMSA, en su Punto 2.4 "Cronograma de implementación" establece lineamientos y controles como para la elaboración de dicho cronograma, como ser Fechas, controles a implementarse, roles y responsabilidades, actividades relacionadas a capacitación, seguimiento, revisión y aplicación de controles, sin embargo desde la aprobación del PISI (2019/2019), a la fecha no se han elaborado procesos y/o procedimientos emergentes de la Política de Seguridad de la Información, mismo para la elaboración de dicho cronograma.</p>	<p>3) A la fecha no se ha concluido la elaboración del Cronograma de implementación del Plan Institucional de Seguridad de la Información de la UMSA.</p>	
APROBACIÓN DEL PISI	Revisión y aprobación del PISI		Comité de Seguridad de la Información Máxima Autoridad Ejecutiva	<p>3.4 Aprobación del PISI</p> <p>El PISI deberá ser revisado por el CSI que impulsará su aprobación ante la Máxima Autoridad Ejecutiva de la entidad o institución pública.</p> <p>El PISI deberá ser flexible a actualizaciones periódicas en función de la mejora continua de la seguridad de la información.</p>	<p>3.1 Aprobación del Plan Institucional de Seguridad de la Información (PISI)</p> <p>El presente documento fue aprobado por el Comité de Seguridad de la Información y el Honorable Consejo Universitario a través de Resolución N° 288/2019</p>	<p>Mediante Resolución HCU No. 028/2019 de fecha 04 de septiembre de 2019 firmado por el Rector Wálter Albornoz, se aprueba el "Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés".</p>	<p>6) El documento "Plan Institucional de Seguridad de la Información (PISI)" de la Universidad Mayor de San Andrés a la fecha de escritura no está actualizado.</p>	

Fuente: Documentación e información proporcionada por Rectorado y Departamento de Tecnologías de la Información y Comunicación.

Objetivo: Verificar si el Plan Institucional de Seguridad de la Información de la UMSA, fue elaborado en el marco de los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, aprobado con Resolución Administrativa N° AGETIC/RA/0051/2017 de 19 de septiembre de 2017.

Conclusión: De la verificación efectuada se concluye que, excepto por los aspectos observados, el Plan Institucional de Seguridad de la Información de la UMSA, fue implementado en el marco de los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, aprobado con Resolución Administrativa N° AGETIC/RA/0051/2017 de 19 de septiembre de 2017.





RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



RI-3.2.1



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORIA INTERNA

RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA ELABORACIÓN E IMPLEMENTACIÓN DEL "PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS"
CÉDULA ANALÍTICA: PROCESO DE IMPLEMENTACIÓN DEL PISI

Procedimiento 2.7.2.8... 2.14 del Programa de Trabajo Ver en P/T RI-2.1 al RI-2.6

ETAPA	OBJETIVO	ACTIVIDADES	RESPONSABLES	REF: P/T	LINEAMIENTOS PISI ENTIDADES SECTOR PÚBLICO	REF: P/T	ACTIVIDADES REALIZADAS POR LA ENTIDAD SIG PISI - UMSA: HCU No. 258/2019	ANÁLISIS DE AUDITORIA	ACLARACIÓN Y/O OBSERVACIÓN
IMPLEMENTACIÓN	IMPLEMENTACIÓN DEL PISI	Activación de controles	Responsable de Seguridad de la Información Comité de Seguridad de la Información	RI - 4.85	7.1 Aplicación de controles La entidad o institución pública deberá aplicar los controles mínimos contemplados en la etapa de elaboración de acuerdo al programa de implementación y aprobación establecido dentro del PISI.			Como procedimiento para verificar si se han aplicado los controles mínimos requeridos por los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información en las entidades del Sector Público, mediante nota AUD/INT CARTA N°363/2024 de 25 de marzo de 2024, se ha solicitado al DTIC, lo siguiente: - Registros, Manuales de Procesos y/o Procedimientos de seguridad, emergentes de la implementación del Plan Institucional de Seguridad de la Información, relacionados a los 11 aspectos de los controles mínimos de seguridad de la información, presentados en el numeral 6.2.3.2 de los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, emitidos por la AGETIC. a) Seguridad en recursos humanos (Véase el punto 1 del Anexo A). b) Gestión de activos de información (Véase el punto 2 del Anexo A). c) Control de accesos (Véase el punto 3 del Anexo A). d) Continuidad (Véase el punto 4 del Anexo A). e) Seguridad Física y ambiental (Véase el punto 5 del Anexo A). f) Seguridad de las operaciones (Véase el punto 6 del Anexo A). g) Seguridad de las comunicaciones (Véase el punto 7 del Anexo A). h) Descubrimiento, mantenimiento y eliminación de sistemas (Véase el punto 8 del Anexo A). i) Gestión de incidentes de seguridad de la información (Véase el punto 9 del Anexo A). j) Plan de contingencia tecnológica (Véase el punto 10 del Anexo A). k) Cumplimiento (Véase el punto 11 del Anexo A). En atención a nuestro requerimiento, el DTIC mediante NOTA UMSA DTIC N°191/2024 de 3 de abril de 2024, respondió lo siguiente: "Actualmente no se tiene conocimiento de que se hayan aprobado Registros, Manuales de Procesos y/o Procedimientos de seguridad, emergentes de la implementación del Plan Institucional de Seguridad de la Información toda vez que desde la gestión 2020 no se cuenta con el Comité de Seguridad de la Información ni con el Responsable de Seguridad de la Información". Por tanto, no se han aplicado los registros mínimos contemplados en el Plan Institucional de Seguridad de la Información de la UMSA, a falta de la designación de un nuevo Responsable de Seguridad de la Información, conformado de un nuevo Comité de Seguridad de la Información, desde la gestión 2020, existiendo la cuenta de un programa de implementación del PISI.	El Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés, no se ha implementado, debido a que no se ha nombrado a un nuevo Responsable de Seguridad de la Información (RSI) y conformado un nuevo Comité de Seguridad de la Información (CSI) desde la gestión 2020, que de continuidad a su implementación.
		Capacitación e inducción	Responsable de Seguridad de la Información Comité de Seguridad de la Información	RI - 4.85	7.2 Capacitación e Inducción La capacitación e inducción al personal es parte integral en la implementación del Plan Institucional de Seguridad de la Información. El Área de Recursos Humanos, en coordinación con el RSI, planificará actividades de capacitación calificadas y la totalidad de los servidores públicos (fijos, eventuales y de reciente incorporación) en relación al Plan Institucional de Seguridad de la Información y manuales de procesos y/o procedimientos de seguridad, generados a partir de la Política de Seguridad de la Información. Para esta fin, se deberán establecer mecanismos de formación continua en relación al PISI.		De acuerdo a NOTA UMSA DTIC N°191/2024 de 3 de abril de 2024, emitida por el DTIC, en la gestión 2019 se realizaron 3 cursos de capacitación dirigidos a las Autoridades y al personal Administrativo, organizados por el Programa Recurso de Capacitación Administrativa (PPCAD). - Primer evento desarrollado el 18, 19 y 20 de septiembre de 2019. - Segundo evento realizado el 30/09/2019 y 1, 2 y 3/10/2019. - Tercer evento realizado el 28, 29, 30 y 31 de octubre de 2019. Deben el particular, mediante nota RRHH/DIV DES RRHH/PPCAD/SAN/024 de 19 de abril de 2024, emitida por la División de Desarrollo del Departamento de Recursos Humanos Administrativos, reporta que el Programa Recurso de Capacitación Administrativa (PPCAD), realizó el curso Seguridad de la Información en la gestión 2019, dirigida al personal administrativo de la UMSA y dictada por el Dr. Iván René Buazo García, desarrollado en la Sala Multipropósito del subsuelo del Edificio Hey, en las siguientes fechas: Grupo 1 Desarrollado el 18, 19 y 20 de septiembre 2019. Grupo 2 Desarrollado el 30 de septiembre, 1, 2 y 3 de octubre de 2019. Adicionalmente, reporta que el 21 y 22 de octubre de 2021 se desarrolló el Curso de Seguridad de la Información en modalidad virtual, dictada por el Dr. Rubén Pablo Saco Camacho. Por tanto, se confirma la realización de los cursos de capacitación respecto a temas de seguridad de la información sin embargo, sin incidencia en la implementación del PISI de la UMSA.		
		Evaluación y mejora continua	Responsable de Seguridad de la Información Comité de Seguridad de la Información	RI - 4.86	7.4 Revisión y mejora continua El RSI deberá promover la realización de revisiones periódicas a los controles implementados dentro del Plan Institucional de Seguridad de la Información, en relación al cumplimiento y eficacia de procesos y/o procedimientos de la Política de Seguridad de la Información. Los resultados de la revisión permitirán medir la efectividad y cumplimiento de los controles implementados para que, en función de los mismos, se realice la mejora continua de la seguridad de la información.		Como se ha señalado precedentemente, desde la gestión 2020 no se ha designado a un nuevo Responsable de Seguridad de la Información de la UMSA, razón por la cual no se han realizado revisiones periódicas al Plan Institucional de Seguridad de la Información de la UMSA, en relación al cumplimiento y eficacia de procesos y/o procedimientos de la Política de Seguridad de la Información. Por tanto no se cuenta con resultados que permitan medir la efectividad y cumplimiento de los controles implementados y en función de los mismos, se realice una mejora continua de la seguridad de la información.		

CC
RCC
D.M.A.G.

Ver Fuente, objetivo y conclusión en P/T

RI-3.1.2



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



RI-3.2.2

SEGUN RESOLUCIÓN ADMINISTRATIVA N° AGETIC/RA/0051/2017					REF. PIT	ACTIVIDADES REALIZADAS POR LA ENTIDAD SIG PISI - UMSA: HCU No. 298/2019	ANÁLISIS DE AUDITORÍA	ACLARACIÓN Y/O OBSERVACIONES
ETAPA	OBJETIVO	ACTIVIDADES	RESPONSABLES	REF. PIT	LINEAMIENTOS PISI ENTIDADES SECTOR PÚBLICO			
		Gestión de incidentes	Responsable de Seguridad de la Información Comité de Seguridad de la Información	RI - 4.85	<p>7.3 Gestión de incidentes de seguridad de la información</p> <p>La entidad o institución pública elaborará procedimientos para la gestión de incidentes, que establezcan con claridad procesos de planificación y preparación, detección y reporte, valoración y decisión, respuesta y erradicación para la mejora continua ante la ocurrencia de incidentes relacionados a la seguridad de la información.</p> <p>El RSI será la persona de contacto al interior y exterior de la entidad o institución pública para la gestión de incidentes y tendrá la responsabilidad de reportar la ocurrencia de los mismos al CGI de acuerdo a normativa vigente.</p> <p>Las entidades o instituciones públicas que tengan conformados equipos de respuesta ante incidentes informáticos (CSIRT, CERT o similares) deberán reportar sus incidentes y vulnerabilidades identificadas, así como el tratamiento realizado, al Comité de Gestión de Incidentes Informáticos (CGII), de acuerdo al artículo 17 del Decreto Supremo 2514.</p> <p>El Anexo C contiene una guía para la gestión de incidentes de seguridad de la información.</p>		<p>Conforme lo descrito en el punto 3.7.1 del presente informe, la entidad no elaboró procedimientos para la gestión de incidentes, que establezcan con claridad procesos de planificación y preparación, detección y reporte, valoración y decisión, respuesta y erradicación para la mejora continua ante la ocurrencia de incidentes relacionados a la seguridad de la información.</p> <p>Asimismo, a falta de designación de un nuevo Responsable de Seguridad de la Información (desde la gestión 2020), no se cuenta con un contacto al interior y exterior de la entidad para reportar la ocurrencia de incidentes.</p> <p>Respecto los incidentes que se presentaron a nivel institucional, el punto 3 del Acta de Razonamiento N° 14 de 20 de abril de 2023, correspondiente a la reunión sostenida con la oficina del Departamento de Tecnologías de la Información y Comunicación de respuesta: "Oscurecimiento no se cuenta con el RSI, responsable de incidentes a nivel institucional, con embargo, esta cuestión verificación por parte del CGI), se arma un equipo de profesionales del OTIC, de acuerdo a una directiva para el estudio e implementación de solución".</p> <p>En consecuencia, si no contare con un RSI, no se ha reportado incidentes informáticos al AGETIC, además, no se ha formalizado procedimientos para la gestión de incidentes.</p>	

Fuente: Documentación e información proporcionada por Rectorado y Departamento de Tecnologías de la Información y Comunicación.

Objetivo: Verificar si el Plan Institucional de Seguridad de la Información de la UMSA, fue implementado en el marco de los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, aprobado con Resolución Administrativa N° AGETIC/RA/0051/2017 de 19 de septiembre de 2017.

Conclusión: De la verificación efectuada se concluye que, el Plan Institucional de Seguridad de la Información de la UMSA, no fue implementado debido a que desde la gestión 2020 no se ha designado a un nuevo Responsable de Seguridad de la Información y conformado un nuevo Comité de Seguridad de la Información, que den continuidad al proceso de implementación del PISI de la UMSA.



5-4-2023
D.M.A.3.



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



P.P.F.

RI-4

UNIVERSIDAD MAYOR DE SAN ANDRÉS
HONORABLE CONSEJO UNIVERSITARIO
La Paz - Bolivia

RESOLUCIÓN

HONORABLE CONSEJO UNIVERSITARIO No. 298/2019

La Paz, 04 de septiembre de 2019

VISTOS Y CONSIDERANDO:

Que, el Honorable Consejo Universitario, en sesión ordinaria de la fecha, ha tomado conocimiento de la nota COM.REC.INF No. 04/2019 de fecha 25 de junio de 2019, enviada por el Dr. Wilfredo Tavera Llanos, Decano de la Facultad de Ciencias Puras y Naturales y Presidente de la Comisión de Recursos Informativos del HCU, referida al "PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS".

Que, a través de la citada nota señala que el documento "PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS", ha sido considerado, revisado y complementado en la Comisión de Recursos Informativos del HCU, recomendando que el mismo sea aprobado en la máxima instancia.

Que, se comprende por seguridad como la capacidad de las redes o los sistemas de información para resistir con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometen la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hace accesibles, en ese entendido la metodología adoptada para la gestión de riesgos está basada en la Metodología de Análisis y Gestión de Riesgos.

Que, el Honorable Consejo Universitario, en consideración a los antecedentes del caso, ha determinado emitir la presente Resolución.

POR TANTO
SE RESUELVE:

Artículo Único. Aprobar el "PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS", cuyo documento se encuentra adjunto a la presente Resolución.

Regístrese, comuníquese, archívese.

2019
D.M.A.G.

Dr. Waldo Albarracín Sánchez
RECTOR

Ing. Pamela V. Rodríguez
SECRETARÍA GENERAL UMISA

Ver Fuente, objetivo
y conclusión en P/T

RI-4 1

UNIVERSIDAD MAYOR DE SAN ANDRÉS
RECTORADO
DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y
COMUNICACIÓN



PLAN INSTITUCIONAL DE SEGURIDAD
DE LA INFORMACIÓN DE LA
UNIVERSIDAD MAYOR DE SAN ANDRÉS

La Paz - Bolivia
2019



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



R1-4.12

P.P.F.F.
ÍNDICE

CONTENIDO

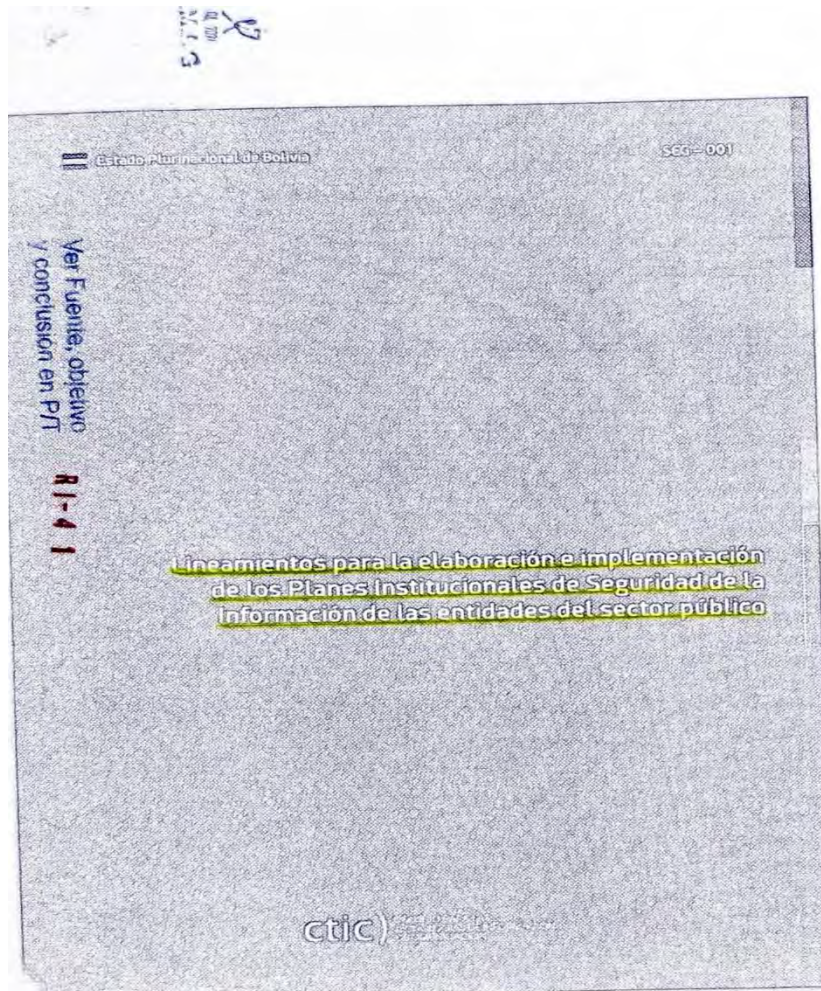
1. ANTECEDENTES Y MARCO NORMATIVO	1
1.1 Misión	1
1.2 Visión	1
1.3 Marco normativo de la Universidad Mayor de San Andrés	3
1.4 Definición de roles y responsabilidades	3
1.4.1 Responsabilidades del Honorable Consejo Universitario Respecto a la Seguridad de la Información	3
1.4.2 Responsabilidades del (la) Rector(a) Máxima Autoridad Ejecutiva (MAE) respecto a la Seguridad de la Información	4
1.4.3 Responsabilidades del Responsable de Seguridad de la Información	6
1.4.4 Designación y Funciones del Comité de Seguridad de la Información	5
2. ETAPA DE DESARROLLO	7
PLAN INSTITUCIONAL DE SEGURIDAD DE INFORMACION	7
2.1 Alcances del Plan Institucional de Seguridad de la Información (PISI)	7
2.2 Metodología de la Gestión del Riesgo	8
2.2.1 Identificación, clasificación y valoración de activos de información.	9
2.2.2 Evaluación del Riesgo.	13
2.2.3 Tratamiento del Riesgo.	16
2.2.4 Controles Implementados y por Implementar.	16
2.2.5 Indicadores y métricas.	17
2.3 Política de Seguridad de la Información	17
2.3.1 Introducción	17
2.3.2 Términos y Definiciones	19
2.3.3 Objetivos	21
2.3.4 Alcance	22
2.3.5 Justificación	22
2.3.6 Antecedentes	23
2.3.7 Roles y Responsabilidades	25
2.3.8 Desarrollo	29
2.3.9 Controles Mínimos de Seguridad de la Información	35
2.3.10 Indicadores y Métricas	35
2.3.11 Histórico de Cambios	36

ver Fuente, objetivo y conclusión en P/T R1-4.1

2.4 Cronograma de Implementación	36
2.5 Aprobación del Plan Institucional de Seguridad de la Información (PISI)	37
✓ 2.6 Difusión	37
✓ 2.7 Cumplimiento	37
✓ 2.8 Sanciones	38
ANEXOS	39
INDICE DE TABLAS	
Tabla 1 Conceptualización de las Características de la información	11
Tabla 2 Escala de criterios de valoración de los activos de información	11
Tabla 3 Clasificación de Activos de información	12
Tabla 4 Escala de vulnerabilidad	14
Tabla 5 Probabilidad de ocurrencia	14
Tabla 6 Escala de Impacto	14
Tabla 7 Relación Probabilidad - impacto	15



RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS



Consejo para las Tecnologías de Información y Comunicación

Contenido

1 Antecedentes	13
2 Marco normativo referencial	18
3 Objetivo	21
4 Alcance y ámbito de aplicación	21
5 Términos y definiciones	22
6 Lineamientos para la elaboración del PISI	24
6.1 Etapa inicial	25
6.1.1 Responsabilidades de la Máxima Autoridad Ejecutiva (MAE) respecto a la seguridad de la información.....	25
6.1.2 Designación y funciones del Responsable de Seguridad de la Información (RSI)	26
6.1.3 Conformación y funciones del Comité de Seguridad de la Información (CSI).....	28
6.2 Etapa de desarrollo del PISI.....	29
6.2.1 Definición de los alcances del PISI	29
6.2.2 Adopción de una metodología de gestión de riesgos.....	29
6.2.3 Contenido de la Política de Seguridad de la Información (PSI).....	31
6.2.3.1 Estructura de la Política de Seguridad de la Información.....	32
6.2.3.2 Controles mínimos de seguridad de la información.....	34
6.2.3.3 Indicadores y métricas.....	35
6.3 Cronograma de implementación.....	35
6.4 Aprobación del PISI.....	35
7 Lineamientos para la implementación del PISI	37
7.1 Aplicación de controles	38
7.2 Capacitación e inducción.....	38
7.3 Gestión de incidentes de seguridad de la información.....	38
7.4 Revisión y mejora continua	39
8 Auditoría al PISI	40
9 Presentación del PISI	40

R1-470



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



Consejo para las Tecnologías de Información y Comunicación

<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Ver Fuente, objetivo y conclusión en P/T</p> <p style="color: red; font-weight: bold; font-size: 1.2em;">R1-41</p>	<p style="text-align: right;">10 Revisión de los lineamientos40</p> <p style="text-align: right;">ANEXO A41</p> <p style="text-align: right;">Controles de seguridad de la información.....41</p> <p style="text-align: right;">1. Seguridad en recursos humanos.....41</p> <p style="text-align: right;">1.1. Términos y condiciones de la relación laboral.....41</p> <p style="text-align: right;">1.1.1 Acuerdo de confidencialidad.....41</p> <p style="text-align: right;">1.2 Concientización, educación y formación en seguridad de la información.....42</p> <p style="text-align: right;">1.2.1 Capacitación y formación42</p> <p style="text-align: right;">1.3 Sanciones o amonestaciones a consecuencia del incumplimiento del PISI institucional.....43</p> <p style="text-align: right;">1.4 Desvinculación de personal o cambio de cargo.....43</p> <p style="text-align: right;">2. Gestión de activos de información44</p> <p style="text-align: right;">2.1. Identificación y responsables de los activos de información44</p> <p style="text-align: right;">2.1.1. Inventario de activos de información44</p> <p style="text-align: right;">2.1.2. Responsabilidad y custodia de los activos de información.....45</p> <p style="text-align: right;">2.1.3. Uso aceptable de los activos de información.....46</p> <p style="text-align: right;">2.1.4. Devolución de los activos de información47</p> <p style="text-align: right;">2.2. Clasificación de la información.....47</p> <p style="text-align: right;">2.2.1. Clasificación.....48</p> <p style="text-align: right;">2.2.2. Etiquetado y manejo48</p> <p style="text-align: right;">2.2.3. Protección del archivo.....49</p> <p style="text-align: right;">2.3. Gestión de medios de almacenamiento removibles.....49</p> <p style="text-align: right;">2.3.1. Gestión de medios removibles50</p> <p style="text-align: right;">2.3.2. Eliminación segura de información.....50</p> <p style="text-align: right;">2.3.3. Traslado físico de los medios de almacenamiento51</p> <p style="text-align: right;">3. Control de accesos51</p> <p style="text-align: right;">3.1. Documentos normativos y operativos para el control de accesos.....51</p> <p style="text-align: right;">3.1.1. Normativa de control de acceso.....52</p> <p style="text-align: right;">3.2. Administración de accesos52</p> <p style="text-align: right;">3.2.1. Administración de accesos, cancelación y privilegios de usuarios...52</p> <p style="text-align: right;">3.2.2. Responsabilidades de los usuarios para la autenticación53</p> <p style="text-align: right;">3.2.3. Revisión, eliminación o ajuste de los derechos de acceso54</p>	<p style="text-align: right;">3.3. Control de acceso a redes y servicios de red.....55</p> <p style="text-align: right;">3.3.1. Acceso remoto55</p> <p style="text-align: right;">3.3.2. Acceso por redes inalámbricas56</p> <p style="text-align: right;">3.3.3. Acceso de dispositivos móviles56</p> <p style="text-align: right;">4. Criptografía.....57</p> <p style="text-align: right;">4.1. Controles criptográficos57</p> <p style="text-align: right;">4.1.1. Uso de criptografía.....57</p> <p style="text-align: right;">5. Seguridad física y ambiental.....58</p> <p style="text-align: right;">5.1. Áreas e instalaciones seguras.....58</p> <p style="text-align: right;">5.1.1. Seguridad física en áreas e instalaciones.....60</p> <p style="text-align: right;">5.1.2. Trabajo en áreas e instalaciones seguras.....60</p> <p style="text-align: right;">5.2. Equipamiento.....60</p> <p style="text-align: right;">5.2.1. Seguridad del equipamiento61</p> <p style="text-align: right;">5.2.2. Escritorio y pantalla limpia.....61</p> <p style="text-align: right;">5.3. Seguridad física y ambiental en el centro de procesamiento de datos62</p> <p style="text-align: right;">5.3.1. Condiciones operativas62</p> <p style="text-align: right;">6. Seguridad de las operaciones64</p> <p style="text-align: right;">6.1. Responsabilidad de las operaciones64</p> <p style="text-align: right;">6.1.1. Documentación de procedimientos operacionales.....64</p> <p style="text-align: right;">6.1.2. Gestión de cambios.....65</p> <p style="text-align: right;">6.1.3. Gestión de la capacidad65</p> <p style="text-align: right;">6.2. Respaldos.....66</p> <p style="text-align: right;">6.2.1. Respaldos de información.....66</p> <p style="text-align: right;">7. Seguridad de las comunicaciones.....67</p> <p style="text-align: right;">7.1. Gestión de la seguridad en redes67</p> <p style="text-align: right;">7.1.1. Gestión de la red68</p> <p style="text-align: right;">7.1.2. Seguridad en servicios de red69</p> <p style="text-align: right;">7.1.3. Seguridad en la red perimetral.....69</p> <p style="text-align: right;">7.1.4. Segmentación de la red70</p> <p style="text-align: right;">7.1.5. Seguridad en redes WiFi71</p> <p style="text-align: right;">7.2. Seguridad del servicio de mensajería electrónica.....71</p> <p style="text-align: right;">7.2.1. Mensajería y correo electrónico.....71</p>
---	--	--



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



Ver Fuente, objetivo y conclusión en P/T

RI-4

7.3. Control sobre información transferida	72
7.3.1. Transferencia de información	72
8. Desarrollo, mantenimiento y adquisición de sistemas	73
8.1. Desarrollo y mantenimiento de sistemas	73
8.1.1. Elaboración de la normativa de desarrollo	73
8.1.2. Identificación de requisitos de seguridad	74
8.1.3. Seguridad en el desarrollo y mantenimiento de sistemas	75
8.1.4. Interoperabilidad de sistemas	76
8.1.5. Pruebas de seguridad	77
8.1.6. Seguridad en bases de datos	77
8.2. Seguridad para la adquisición de sistemas	79
8.2.1. Requisitos de seguridad	79
9. Gestión de incidentes de seguridad de la información	79
9.1. Gestión de incidentes de seguridad de la información	80
9.1.1. Gestión de incidentes	80
10. Plan de contingencias tecnológicas	81
10.1. Implementación del plan de contingencias tecnológicas	81
10.1.1. Elaboración del plan de contingencias tecnológicas	82
10.1.2. Pruebas y mantenimiento del plan de contingencias tecnológicas	83
11. Cumplimiento	83
11.1. Revisión de controles	84
11.1.1. Revisión	84
11.1.2. Verificación del cumplimiento técnico	85
11.2. Auditoría al Plan Institucional de Seguridad de la Información	85
11.2.1. Evaluación de cumplimiento del plan Institucional de seguridad de la información	85
ANEXO B	87
Guía para la metodología de gestión de riesgos	87
1. Introducción	87
2. Objetivo	87

10

Consejo para las Tecnologías de Información y Comunicación

3. Referencias	88
4. Documentos relacionados	88
5. Términos y definiciones	88
6. Identificación, clasificación y valoración de activos de información	89
6.1. Identificación	90
6.2. Valoración	91
6.2.1. Ejemplo	93
6.2.2. Matriz de inventario y valoración	94
6.3. Revisión y actualización	95
6.4. Reserva	96
7. Evaluación del riesgo	96
7.1. Identificación	97
7.2. Análisis y valoración	103
7.3. Ejemplo de evaluación del riesgo	104
7.3.1. Matriz de valoración del riesgo	105
8. Tratamiento del riesgo	106
9. Controles implementados y por implementar	106
ANEXO C	108
Guía para la gestión de incidentes de seguridad de la información	108
1. Introducción	108
2. Objetivo	108
3. Referencias	108
4. Documentos relacionados	108
5. Términos y definiciones	109
6. Gestión de incidentes	109
6.1. Planificación y preparación	112
6.2. Detección y reporte	112
6.3. Valoración y decisión	115
6.4. Respuesta y erradicación	117
6.5. Mejora continua	117

RI-4/12



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



UNIVERSIDAD MAYOR DE SAN ANDRÉS
RECTORADO
La Paz - Bolivia

La Paz, 24 de septiembre de 2018

RESOLUCIÓN
RECTORAL No. 0642

P.P.E.

VISTOS:

La NOTA DTIC N° 406/18 enviada por la Lic. Marina F. Delgado Rodríguez Jefa a.i. del Departamento de Tecnologías de Información y Comunicación, solicitando su designación como Responsable de Seguridad de la Información ante la AGETIC, para trabajar en el Plan Institucional de Seguridad de la Información.

CONSIDERANDO:

Que, la nota AGETIC/NE/0735/2018 enviado por Nicolás Laguna Ouyroga, Director General Ejecutivo de la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) refrenda a los avances del Plan Institucional de Seguridad de la Información y Responsable de Seguridad de la Información.

Que, de la misma forma se solicita se ratifique o designe a un Responsable de Seguridad de la Información, en cumplimiento al D.S. 2514 en su Disposición Transitoria Primera, inciso a) indica: "Las entidades del sector público remitirán a la AGETIC, en un plazo no mayor a treinta (30) días calendario la designación de un Responsable de Seguridad de la Información" a partir de la publicación del Decreto Supremo.

Que, en consideración a los antecedentes y con el fin de coadyuvar con las actividades y cumplimiento de los objetivos de dicha Unidad se determina emitir la presente Resolución.

POR TANTO SE RESUELVE:

Artículo Único. DESIGNAR a la Lic. MARINA FELICIDAD DELGADO RODRÍGUEZ como RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN de la Universidad Mayor de San Andrés ante la Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC) dependiente del Ministerio de la Presidencia del Estado Plurinacional de Bolivia.

Regístrese, comuníquese y archívese.

C.c Arch

Waldo Albarrocin Sánchez
RECTOR
Universidad Mayor de San Andrés

Ing. Alberto Rojas Velazco
SECRETARIO GENERAL
Universidad Mayor de San Andrés

Ver Fuente, objetivo y conclusión en PIT RI-41

UNIVERSIDAD MAYOR DE SAN ANDRÉS
HONORABLE CONSEJO UNIVERSITARIO
La Paz - Bolivia

RI - 4.68

RESOLUCIÓN

HONORABLE CONSEJO UNIVERSITARIO No. 464/2018

La Paz, 26 de septiembre de 2018

P.P.E.

VISTOS:

La Resolución del Honorable Consejo Universitario No. 230/2018, que resuelve en su Artículo Primero conformar el Comité de Seguridad Institucional de la Información (C.S.I.) de la Universidad Mayor de San Andrés, integrada por los miembros de la Comisión de Recursos Informativos del Honorable Consejo Universitario, los cuales contarán con el asesoramiento de un profesional en derecho informático, un profesional en temas financieros y dos profesionales del área informática con especialidad en seguridad de la información.

CONSIDERANDO:

Que, el Honorable Consejo Universitario en su sesión ordinaria de la fecha, ha tomado conocimiento de las nominaciones realizadas de los profesionales que conformarán el Comité de Seguridad Institucional de la Información de la Universidad Mayor de San Andrés (C.S.I.).

Que, es importante que el Comité de Seguridad Institucional de la Información - UMSA, inicie sus labores de manera tal que podamos ir avanzando en cuanto a esta temática que es prioritaria toda vez que se cada día nos vemos más inmersos en una dinámica continua con las Tecnologías de la Información.

Que, el Honorable Consejo Universitario, luego de conocer la solicitud y en atención a las conclusiones arribadas del debate, ha determinado emitir la presente Resolución.

POR TANTO SE RESUELVE:

Artículo Único. CONFORMAR el COMITÉ de SEGURIDAD INSTITUCIONAL de la INFORMACIÓN (C.S.I.) de la UNIVERSIDAD MAYOR SAN ANDRÉS, que estará integrada por:

- Dr. Wilfredo Tavera Llanos
DECANO FAC. CIENCIAS PURAS Y NATURALES
- Ing. Miguel Ángel Calla Carrasco
DECANO FAC. INGENIERÍA
- Lic. Víctor Paz Huancá
DELEG. DOC. HCU. FAC. TECNOLOGÍA
- Dr. Martín Villarreal Mareño
DELEG. DOC. HCU. FAC. MEDICINA, ENFERMERÍA, NUT Y TEC. MED.
- Univ. Kitzo Jaramilla Guaman
DELEG. ESTUD. HCU. FAC. CS. FARMACÉUTICAS Y BIOQUÍMICAS
- Univ. Carlos Fernando Tarrez Alanoca
DELEG. ESTUD. HCU. FAC. CS. PURAS Y NATURALES
- Univ. Brian Rojas Mora
DELEG. ESTUD. HCU. FAC. CS. GEOLÓGICAS
- Lic. Marina Delgado Rodríguez
JEFA a.i. DEPARTAMENTO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN.
- Lic. Marcelo German Arquipa Chambi
DOCENTE CARRERA DE INFORMÁTICA
- M.Sc. Moisés Martín Silva Choque
DOCENTE CARRERA DE INFORMÁTICA
- Dra. Karina Ingrid Medinaceli Díaz
DIRECTORA a.i. INST. DE INVEST., SEMINARIOS Y TESIS CARRERA DE DERECHO - FAC. DERECHO
- Lic. Norma Castro Quispe
COORDINADORA PLAN MAESTRO TIC - UMSA
- M.Sc. Víctor Hugo Chavez Salazar
DOCENTE CARRERA DE ADMINISTRACIÓN DE EMPRESAS
- Ing. Marcelo Ramirez Molina
DOCENTE CARRERA DE INGENIERÍA ELECTRÓNICA

Regístrese, comuníquese y archívese.

Dr. Waldo Albarrocin Sánchez
RECTOR

Ing. Alberto Rojas Velazco
SECRETARIO GENERAL UMSA

Ver Fuente, objetivo y conclusión en PIT RI-41



ANEXO 2
MEMORÁNDUM DE DESIGNACIÓN



**RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA
ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA
INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS**



**UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia**

MEMORÁNDUM

**UNIVERSIDAD BOLIVIANA
UNIVERSIDAD MAYOR DE SAN ANDRÉS
DPTO. AUDITORÍA INTERNA**

MEM.T.AUD. No.008/2024

Señor:

Lic. Dennis Magno Apaza Gonzales

AUDITOR INTERNO

Presente. -

La Paz, 14 de marzo de 2024

Licenciado:

En cumplimiento a solicitud de la Contraloría General del Estado efectuada mediante nota CGE/GPA2/171-026/2024 del 1 de marzo de 2024 y proveído del señor Rector con Hoja de Ruta VC-5338; se le instruye la realización del siguiente Relevamiento de Información Específica (RIE), en coordinación con esta Jefatura.

No.	TRABAJO ASIGNADO
1	Relevamiento de Información Específica sobre "Plan Institucional de Seguridad a la Información de la entidad" (PISI) requerido por los "Lineamientos para la elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las entidades del Sector Público" aprobados con la Resolución Administrativa No. AGETIC/RA/0051/2017

El informe de R.I.E. debe cumplir con lo establecido en la Norma 217.04 de las Normas Generales de Auditoría Gubernamental, los Papeles de Trabajo referenciados y correferenciados, los mismos que deben ser entregados hasta el **19 de abril** de la presente gestión.

Para el trabajo encomendado contará con el apoyo de Universitaria Gaby Norca Arias Chambi.

La pertinencia de contar con personal especializado de Sistemas para la labor encomendada, deberá ser comunicada a esta Jefatura en forma oportuna.

Deseándole éxito en la labor encomendada, saludo a usted muy atentamente.



Lic. René Carrasco Condarco
JEFE a.i. DEPARTAMENTO DE AUDITORÍA INTERNA



RCC/mmp
cc: Archivo Auditoría interna

ANEXO 3
PLAN DE TRABAJO

PLAN DE TRABAJO

MODALIDAD DE TITULACIÓN: TRABAJO DIRIGIDO
DEPARTAMENTO DE AUDITORÍA INTERNA DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS
UNIVERSITARIA: GABY NORCA ARIAS CHAMBI
CÉDULA DE IDENTIDAD.: 8336449 L.P.
REGISTRO UNIVERSITARIO: 1728196

1. ANTECEDENTES.

En fecha 08 de septiembre de 2021, se emitió la **Resolución del Honorable Consejo Universitario N°472/2021** que aprueba el *"Reglamento Específico de la Modalidad de Graduación; Trabajo Dirigido para la obtención del nivel licenciatura en la Universidad Mayor de San Andrés.*

En fecha 18 de agosto de 2022 el Honorable Consejo Universitario, emite la Resolución N° **330/2022**, en la que resuelve en su **Artículo Primero**; **"Aprobar el "REGLAMENTO ESPECÍFICO DE MODALIDAD DE GRADUACIÓN POR TRABAJO DIRIGIDO PARA LA OBTENCIÓN DEL NIVEL LICENCIATURA EN LA UNIVERSIDAD MAYOR DE SAN ANDRÉS", en sus V capítulos y 20 Artículos, (...)", de la cual en su artículo 14 se requiere presentar el Plan de Trabajo"**.

Bajo el marco normativo señalado es que el Departamento de Auditoría Interna, en consideración a que acoge a estudiantes egresados de la Carrera de Contaduría Pública para que realicen Trabajos Dirigidos, es que ha elaborado el siguiente Plan de Trabajo que fue preparado en observancia al Programa Operativo Anual (POA) de la gestión 2023 y de la gestión 2024 y otras actividades no programadas requeridas por el Señor Rector (MAE) o por la Contraloría General del Estado.

2. OBJETIVO

Establecer el Plan de Trabajo correspondiente a las actividades (programadas y no programadas gestión 2023 y gestión 2024) a ser desarrolladas en el Departamento de Auditoría Interna de la UMSA por la estudiante egresada de la Carrera de Contaduría Pública de la Facultad de Ciencias Económicas y Financieras de la Universidad Mayor de San Andrés, que accedió a la modalidad de titulación de Trabajo Dirigido, para poner en práctica los conocimientos teóricos adquiridos en sus actividades académicas como universitaria y adquirir nuevas competencias en el ámbito de la Auditoría Gubernamental.

3. ACTIVIDADES A REALIZAR

De acuerdo al Plan Operativo Anual 2023 y 2024 del Departamento de Auditoría Interna de la UMSA, y otras actividades no programadas requeridas por el Señor Rector (MAE) o por la Contraloría General del Estado, se desarrolló el presente PLAN DE TRABAJO, considerando la ejecución de las siguientes actividades durante las gestiones 2023 y 2024:

- Auditoría de Confiabilidad de los Registros y Estados Financieros de la Universidad Mayor De San Andrés al 31 de diciembre de 2023.
- Auditoría Operacional sobre el Cumplimiento del Plan Operativo Anual, Uso y Destino de los recursos provenientes del Impuesto Directo a los Hidrocarburos (IDH) de la Universidad Mayor De San Andrés, correspondiente a la gestión 2023.
- Relevamiento de Información Específica sobre la Elaboración e Implementación del Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés.
- Relevamiento de Información Específica sobre el "Incidente de Seguridad – Filtración CPU SIA producido en la Universidad mayor de San Andrés.

POA 2023/2024	GESTIÓN 2023			GESTIÓN 2024					
	OCT.	NOV.	DIC.	ENE.	FEB.	MAR.	ABR.	MAY.	JUN.
1. Auditoría de Confiabilidad de los Registros y Estados Financieros de la Universidad Mayor De San Andrés al 31 de diciembre de 2023.									
2. Auditoría Operacional sobre el Cumplimiento del Plan Operativo Anual, Uso y Destino de los recursos provenientes del Impuesto Directo a los Hidrocarburos (IDH) de la UMSA, correspondiente a la gestión 2023.									

POA 2023/2024	GESTIÓN 2023			GESTIÓN 2024					
	OCT.	NOV.	DIC.	ENE.	FEB.	MAR.	ABR.	MAY.	JUN.
3. Relevamiento de Información Específica sobre la Elaboración e Implementación del Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés".									
4. Relevamiento de Información Específica sobre el "Incidente de Seguridad – Filtración CPU SIA producido en nuestra Institución.									

4. PROCEDIMIENTOS PARA LA EJECUCIÓN

Para el logro del cumplimiento de las actividades mencionadas anteriormente, con el apoyo del Tutor Profesional las mismas serán ejecutadas en función de los procedimientos establecidos en los programas de trabajo diseñados para tal efecto.

5. RECURSOS NECESARIOS

Para la ejecución y cumplimientos de las actividades se proporciona un equipo de computación, escritorio, materiales de escritorio, entre otros; asimismo, para su movilización por las distintas unidades académicas sujetas a evaluación se le otorgará y cubrirá el costo de los pasajes.

6. CONCLUSIÓN

Se ha establecido el Plan de Trabajo correspondiente a las actividades (programadas y no programadas gestión 2023 y 2024) a ser desarrolladas en los ocho meses (23 de octubre de 2023 al 23 de junio de 2024) en el Departamento de Auditoría Interna de la UMSA por la estudiante egresada de la Carrera de Contaduría Pública de la Facultad de Ciencias Económicas y Financieras de la Universidad Mayor de San Andrés, que accedió a la modalidad de titulación de Trabajo Dirigido, que pondrá en práctica los conocimientos teóricos adquiridos en sus actividades académicas como universitaria y adquirirá nuevas competencias en el ámbito de la Auditoría Gubernamental, mismo que será desarrollado bajo la guía del Tutor Profesional asignado para tal cometido.

Sin otro particular, saludo a usted con las consideraciones más distinguidas.


Lic. Dennis Magno Apaza Gonzales
AUDITOR
TUTOR PROFESIONAL


Mg. Sc. Ausberto Choque Mita
TUTOR DOCENTE


Egr. Gaby Norca Arias Chambi
TRABAJO DIRIGIDO

C.C.Arch.AG

ANEXO 4
INFORME FINAL



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

INFORME FINAL – TRABAJO DIRIGIDO

A: M. Sc. Teddy Orlando Catalán Mollinedo
DIRECTOR DE LA CARRERA DE CONTADURÍA PÚBLICA

VÍA: Lic. Adolfo Balboa Mamani
JEFE DEPARTAMENTO DE AUDITORÍA INTERNA

VÍA: Mg. Sc. Ausberto Choque Mita
TUTOR DOCENTE

DE: Lic. Dennis Magno Apaza Gonzales
TUTOR INSTITUCIONAL (AUDITOR INTERNO)

REF.: **INFORME FINAL (PERIODO 23/10/2023 AL 23/06/2024) DE LA EGRESADA GABY NORCA ARIAS CHAMBI, TRABAJO DIRIGIDO DEL DEPARTAMENTO DE AUDITORÍA INTERNA – UMSA**

FECHA : La Paz, 24 de junio de 2024

1. ANTECEDENTES.

1.1. Antecedentes de la Modalidad de Titulación Trabajo Dirigido

Mediante Resolución del Honorable Consejo Universitario N° **472/2021** de 8 de septiembre de 2021 (Ver **Anexo 1**), en su Artículo Primero se aprueba: "**Aprobar el 'REGLAMENTO ESPECÍFICO DE LA MODALIDAD DE GRADUACIÓN: TRABAJO DIRIGIDO PARA LA OBTENCIÓN DEL NIVEL LICENCIATURA EN LA UNIVERSIDAD MAYOR DE SAN ANDRÉS'**", en sus V capítulos y 17 Artículos, (...)", reglamento que, en su contenido entre otros, establece:

*"**Artículo 4. Definición** El Trabajo Dirigido es una modalidad de graduación de carácter individual para acceder al nivel académico de Licenciatura, consistente en la realización de prácticas pre profesionales desarrolladas en instituciones externas o dentro la misma Universidad, supervisadas y evaluadas por profesionales en calidad de tutores. Existen dos formas para el desarrollo del Trabajo Dirigido:*

1. Trabajo Dirigido Externo
 2. Trabajo Dirigido Interno
- (...)

***Artículo 6. Trabajo Dirigido Interno** Es el realizado en las distintas dependencias de la Universidad Mayor de San Andrés bajo la guía de un tutor profesional y un tutor docente, sin necesidad de suscribir Convenios Específicos.*

(...)

Página 1 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

Artículo 9. Conclusión plan de estudios El postulante deberá haber aprobado la totalidad de las asignaturas del plan de estudios y cumplir los requisitos estipulados por su Carrera.

Artículo 10. Promedio El promedio mínimo para acceder a esta modalidad de graduación es de 60 puntos.

Artículo 11. Plazo La dedicación del postulante en las actividades desarrolladas deberá ser exclusiva, debiendo concluirse el trabajo dirigido en el plazo máximo de 8 (ocho) meses.

(...)

Artículo 14. Evaluación La evaluación principal estará a cargo del tutor profesional externo debido al vínculo directo con el postulante a trabajo dirigido, mismo que en base al cumplimiento de objetivos emitirá los informes respectivos.

Artículo 15. Informes Durante la realización del trabajo dirigido el postulante presentará a la Unidad Académica autorizada por su Carrera dos (2) informes trimestrales y uno (1) final elaborados por su tutor profesional".

En fecha 8 de diciembre de 2021, se Aprueba la Resolución del Honorable Consejo Universitario N° 713/2021 (Ver Anexo 2), que Resuelve:

"Artículo Primero. COMPLEMENTAR el REGLAMENTO ESPECÍFICO DE LA MODALIDAD DE GRADUACIÓN: TRABAJO DIRIGIDO PARA LA OBTENCIÓN DEL NIVEL DE LICENCIATURA EN LA UNIVERSIDAD MAYOR DE SAN ANDRÉS, aprobado con Resolución HCU. No. 472/2021; de acuerdo al siguiente detalle:

DISPOSICIONES TRANSITORIAS

PRIMERO Aquellos estudiantes universitarios que, a la fecha de puesta en vigencia del presente Reglamento, se encuentren en pleno desarrollo de la modalidad de graduación "Trabajo Dirigido" según Reglamentos Específicos de sus Carreras, podrán acogerse al marco regulatorio actual, solicitando expresamente mediante nota dirigida a su Dirección de Carrera acogerse a este Reglamento, cumpliendo todos os requisitos establecidos en esta modalidad de graduación siendo uno de los haber obtenido el 60% del promedio general de calificación.

SEGUNDA Toda vez que la migración al presente Reglamento de los estudiantes que así lo requieran será formalmente solicitada se exime de cualquier responsabilidad administrativa a todas las Autoridades Académicas que se involucren en los trámites que emerjan de la solicitud presentada.

TERCERA La migración de aquellos estudiantes que estuvieran en pleno desarrollo de sus modalidades de graduación (trabajo dirigido) es voluntaria y debe ser expresamente solicitada.

CUARTA. Con fines de evitar observaciones a tiempo de los trames subsecuentes se deberá acompañar una copia de la presente Resolución en los trámites de le solicitantes, así como de la Resolución específica e individual del Honorable Consejo de Carrera que autorice esta migración de cada uno de los estudiantes que así lo soliciten.

Página 2 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

Artículo Segundo. ENCOMENDAR a las unidades académicas y administrativas dar fiel cumplimiento a la presente Resolución."

Posteriormente, en fecha 11 de mayo de 2022, se Aprueba la Resolución del Honorable Consejo Universitario N° 151/2022 (Ver **Anexo 3**), que **Resuelve**:

Artículo Primero: APROBAR que, para el desarrollo de trabajos Dirigidos como Modalidad de Graduación al Interior de la Universidad Mayor de San Andrés, no será necesaria la suscripción de convenios Individuales entre las Facultades y las unidades académicas y administrativas de destino, al tratarse de una misma institución.

(...)

Artículo Tercero. Las Direcciones de Carrera Adecuaran el desarrollo del Trabajo Dirigido del estudiante de acuerdo a la Reglamentación Vigente".

Finalmente, en fecha 18 de agosto de 2022, mediante Resolución del Honorable Consejo Universitario N.º 330/2022 (Ver **Anexo 4**), se aprueba: "**Artículo Primero. Aprobar** el "REGLAMENTO ESPECIFICO DE MODALIDAD DE GRADUACIÓN POR TRABAJO DIRIGIDO PARA LA OBTENCIÓN DEL NIVEL DE LICENCIATURA LA UNIVERSIDAD MAYOR DE SAN ANDRÉS" en sus V Capítulos y 20 Artículos...", documento que, entre otros, dispone:

Artículo 6º Trabajo Dirigido Interno. Se realiza en las distintas dependencias de la Universidad Mayor de San Andrés, bajo la guía de un Tutor Profesional y un Tutor nte, sin necesidad de suscribir Convenios Específicos.

Artículo 7º Tutor Docente. Es el Docente designado por la Dirección de Carrera para cada Trabajo Dirigido, siendo sus obligaciones:

- a) Orientar al postulante y efectuar un seguimiento periódico para validar el avance del Trabajo Dirigido.
- b) Realizar la supervisión durante el desarrollo del trabajo dirigido, manteniendo contacto con el tutor profesional y el estudiante.

(...)

Artículo 8º Tutor Profesional (externo). Es el profesional designado por la entidad pública o privada de Convenio o perteneciente a alguna dependencia de la Universidad Mayor de San Andrés, debe acreditar el grado académico universitario igual o superior al que aspira el postulante y los conocimientos necesarios para realizar una tutela efectiva, siendo sus obligaciones:

- a) Guiar y evaluar el cumplimiento del Trabajo Dirigido.
- b) Facilitar los medios para el desarrollo del Trabajo Dirigido.
- c) Organizar las actividades a desarrollar por el postulante durante su estancia en la Institución.
- d) Supervisar las actividades pre-profesionales del postulante garantizando que reciba la formación práctica correspondiente.
- e) Emitir dos informes trimestrales y uno final, evaluando el desarrollo del Trabajo Dirigido realizado por el postulante en la institución.

(...)

Página 3 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS

DEPARTAMENTO DE AUDITORÍA INTERNA

La Paz - Bolivia

AUD.INT.INF.ID.Nº 22/2024

Artículo 16º Informes. Durante la realización del trabajo Dirigido el postulante presentará a la Dirección de Carrera dos (2) informes trimestrales y un (1) Informe Final, rubricado por el Tutor Profesional y el Tutor Docente. En el Informe Final, el Tutor Profesional debe asignar la calificación cualitativa, misma que debe ser validada por el Tutor Docente con calificación numérica”.

1.2. Objetivo

Emitir el informe final de actividades del trabajo realizado por la Univ. Gaby Norca Arias Chambi, Trabajo Dirigido del Departamento de Auditoría Interna, egresada de la Carrera de Contaduría Pública de la Facultad de Ciencias Económicas y Financieras de la Universidad Mayor de San Andrés; asimismo, calificar de manera cualitativa el desarrollo del Trabajo Dirigido.

1.3. Autorización de acceso a la Modalidad de Titulación de Trabajo Dirigido

En cumplimiento al marco normativo expuesto, en fecha 15 de septiembre de 2023, mediante nota sin número (Ver **Anexo 5**), la Egresada **Gaby Norca Arias Chambi**, solicitó al Mg. Sc. Teddy Orlando Catalán Mollinedo, Director de la Carrera de Contaduría Pública, **AUTORIZACIÓN** para acceder a la **Modalidad de Titulación de Trabajo Dirigido**.

En atención a la solicitud efectuada, el Director de la Carrera de Contaduría Pública, mediante nota FCEF/CARR/CONT/PUBL. Nº1783/23 de 16 de octubre de 2023 (Ver **Anexo 6**), **AUTORIZÓ** a la Egresada Gaby Norca Arias Chambi, **el inicio del proceso de titulación bajo la Modalidad de Trabajo Dirigido** a desarrollarse en el Departamento de Auditoría Interna de la Universidad Mayor de San Andrés, quien cumple con los requisitos exigidos para acceder a esta modalidad de titulación establecidos en el **“REGLAMENTO ESPECÍFICO DE LA MODALIDAD DE GRADUACIÓN: TRABAJO DIRIGIDO PARA LA OBTENCIÓN DEL NIVEL DE LICENCIATURA EN LA UNIVERSIDAD MAYOR DE SAN ANDRÉS”**, aprobado mediante Resolución del Honorable Consejo Universitario Nº 330/2022 de 18 de agosto de 2022.

1.4. Designación de Tutor Institucional

Mediante **MEM.T.AUD.No. 194/2023**, de fecha 13 de noviembre de 2023 (Ver **Anexo 7**), se designó como Tutor Institucional al Lic. Dennis Magno Apaza Gonzales, Auditor del Departamento de Auditoría Interna.

1.5. Designación de Tutor Docente

La Dirección de la Carrera de Contaduría Pública realizó la designación del Mg. Sc. Ausberto Choque Mita, Docente de la Carrera de Contaduría Pública, como Tutor Académico del presente trabajo dirigido.

2. PERFIL DEL TUTOR PROFESIONAL

Mi persona, Dennis Magno Apaza Gonzales, con grado académico de Licenciatura en Auditoría Financiera, obtenido en la Universidad Mayor de San Andrés de la Ciudad de La

Página 4 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

Paz; cuento con 16 años de servicio en el Sector Público, ocupando cargos administrativos y de Auditor Interno.

Actualmente, cumpla funciones como Auditor Interno del Departamento de Auditoría Interna de la Universidad Mayor de San Andrés desde octubre de 2018.

En cuanto a la formación Posgradual, cuento Diplomado realizado en el CEPIES y en proceso de Desarrollo de la Tesis de Grado de la Maestría Auditoría y Control Financiero, entre otros cursos y programas de especialización realizados en el CENCAP de la Contraloría General del Estado (Se adjunta en **Anexo 8**, la documentación que acredita el grado académico y perfil profesional).

3. DESARROLLO DE ACTIVIDADES.

A continuación, se describen las actividades asignadas a la Egr. Gaby Norca Arias Chambi, en el marco del Plan Operativo Anual del Departamento del Auditoría Interna de la Universidad Mayor de San Andrés y Plan de Trabajo definido para el desarrollo del Trabajo dirigido, mismas que en su desarrollo fueron objeto de supervisión por el Tutor Institucional.

3.1 ACTIVIDADES REALIZADAS

3.1.1 TRABAJO ASIGNADO: AUDITORÍA DE CONFIABILIDAD DE REGISTROS Y ESTADOS FINANCIEROS DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS AL 31 DE DICIEMBRE DE 2023.

Memorándum de designación: MEM.T.AUD. No. 182/2023 del 26 de octubre de 2023. (Ver Anexo 9)
--

Auditor Responsable: Lic. Rubén Pablo Sossa Mamani

ACTIVIDADES DESARROLLADAS

Para tal efecto, se procedió con la inducción respecto las Normas de Auditoría de Confiabilidad de Registros y Estados Financieros, aprobadas por la Contraloría General del Estado mediante Resolución CGE/073/2021 de 28 de octubre de 2021.
--

Posteriormente, revisó y analizó documentación presentada por la Unidad de Administración Desconcentrada de la Facultad de Ingeniería (DA 30), según se describe a continuación:
--

- | |
|---|
| <ul style="list-style-type: none">- Se procedió con la revisión y análisis de los Registros de Ejecución de Gastos (C-31) y documentación de respaldo de procesos de contratación en sus diferentes modalidades, considerando los siguientes aspectos:<ul style="list-style-type: none">• Que la documentación de respaldo, no contengan tachaduras, borrones, enmiendas o alteraciones que den indicios de alguna irregularidad.• Que el respaldo documentario tenga coherencia de fechas y que todas las operaciones registradas, correspondan a la Universidad Mayor de San Andrés. |
|---|

Página 5 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

- Que los procesos de contratación se encuentren adecuadamente registrados, respaldados, expuestos y correspondan a operaciones generadas durante la gestión 2021, cumpliendo así con las afirmaciones de Integridad, existencia y exposición.
 - Que los Registros de Ejecución de Gasto correspondan a gastos propios de la entidad, según la naturaleza de sus operaciones, cumpliendo con ello el principio de Propiedad
 - Que los registros se encuentran adecuadamente valuados y autorizados cumpliendo los principios de Valuación y legalidad.
 - Que las acciones de control interno se encuentran adecuadamente diseñadas y funcionan, verificando: la autorización, aprobación, exactitud, oportunidad, salvaguarda y la competencia, según corresponda.
- Se elaboró planillas Analíticas para el análisis de los procesos de contratación, tomando en cuenta que se elaboraron mediante los programas de trabajo de:
- CONTRATACIÓN MENOR (COMPRAS MENORES hasta Bs 20.000)
 - CONTRATACIÓN MENOR (COMPRAS MENORES de Bs 20.001 hasta Bs 50.000)
 - CONTRATACIÓN MODALIDAD ANPE (de Bs 50.001 hasta Bs 1.000.000)
 - PARTIDA 26990 OTROS
- Se procedió con la revisión de los papeles de respaldo de:

DA	FACULTAD	PARTIDA	PROG.	No. COMPR.	RESPONSABLE
30	INGENIERIA	26990	100-101-102	19	Gaby Norca Arias Chambi

100-0-14 ING – CURSO PREFACULTATIVO
101-0-25 ING – CARRERA DE INGENIERIA CIVIL
101-0-26 ING – CARRERA DE INGENIERIA ELECTRONICA
101-0-27 ING – CARRERA DE INGENIERIA ELECTRICA
101-0-29 ING – CARRERA DE INGENIERIA MECANICA Y ELECTROMECHANICA
101-0-33 ING – CURSO BÁSICO
102-0-89 ING – PG MAESTRIA EN CS. DE GESTIÓN INDUSTRIAL Y EMPRESARIAL

Al respecto, se realizaron las siguientes tareas:

CONTRATACIONES PARTIDA 26990 (OTROS)

- ✓ Comprobante
- ✓ Importe
- ✓ Número de Contrato
- ✓ Objeto del Contrato
- ✓ Plazo
- ✓ Inicio de servicio
- ✓ Conclusión de servicio

Página 6 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

- ✓ Formulario de compatibilidad horaria
- ✓ Declaración de parentesco

Proceso de Contratación

Atributo de pruebas de Control (Cumplimiento de Controles Clave Identificados)

- ✓ Solicitud de Compra de Bienes o Servicios
- ✓ Certificación presupuestaria
- ✓ Diploma Académico en Fotocopia Legalizada
- ✓ Título en provisión Nacional en Fotocopia Legalizada
- ✓ Certificado de Diplomado en Educación Superior en Fotocopia Legalizada
- ✓ Resolución de Designación/ memorándum
- ✓ Contrato/ Orden de Compra – servicio

Pagos

- ✓ Cumplimiento del Objeto de Contrato
- ✓ Informe Final de Actividades con Vo Bo. de Inmediato superior.
- ✓ Factura emitida a nombre y con NIT de la Universidad Mayor de San Andrés
- ✓ Retenciones impositivas

- Se elaboró papeles de trabajo, con las características de auditoría (informativos, marcas de auditoría, fuente, comentario, rúbrica, fecha, etc.)
- Se realizó la referencia y correferencia de los papeles de trabajo realizados.
- Se procedió a realizar el armado de los legajos de auditoría.
- Otras tareas instruidas por el Auditor y/o Jefatura del Departamento de Auditoría Interna.

Memorándum de designación: MEM.T.AUD. No. 183/2023 del 26 de octubre de 2023. (Ver **Anexo 10**)

Auditor Responsable: Lic. Dennis Magno Apaza Gonzales

- Se revisó y analizó la documentación presentada por la DA-80 PROGRAMAS CENTRALES ACADÉMICOS CEPIES, según se describe a continuación:
- Se colaboró con la revisión y análisis de los Registros de Ejecución de Gastos (C-31) y documentación de respaldo de procesos de contratación en sus diferentes modalidades, considerando los siguientes aspectos:
 - Que la documentación de respaldo, no contengan tachaduras, borrones, enmiendas o alteraciones que den indicios de alguna irregularidad.
 - Que el respaldo documentario tenga coherencia de fechas y que todas las operaciones registradas, correspondan a la Universidad Mayor de San Andrés.

Página 7 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

- Que los procesos de contratación se encuentren adecuadamente registrados, respaldados, expuestos y correspondan a operaciones generadas durante la gestión 2021, cumpliendo así con las afirmaciones de Integridad, existencia y exposición.
 - Que los Registros de Ejecución de Gasto correspondan a gastos propios de la entidad, según la naturaleza de sus operaciones, cumpliendo con ello el principio de Propiedad
 - Que los registros se encuentran adecuadamente valuados y autorizados cumpliendo los principios de Valuación y legalidad.
 - Que las acciones de control interno se encuentran adecuadamente diseñadas y funcionan, verificando: la autorización, aprobación, exactitud, oportunidad, salvaguarda y la competencia, según corresponda.
- Se colaboró con el análisis de los procesos de contratación, tomando en cuenta que se elaboraron mediante los programas de trabajo de:
- CONTRATACIÓN MENOR (COMPRAS MENORES hasta Bs 20.000)
 - CONTRATACIÓN MENOR (COMPRAS MENORES de Bs 20.001 hasta Bs 50.000)
 - CONTRATACIÓN MODALIDAD ANPE (de Bs 50.001 hasta Bs 1.000.000)
 - PARTIDA 25220 CONSULTORES INDIVIDUALES DE LINEA.
- Se colaboró con la revisión de los papeles de respaldo de:
- DA 80 PROGRAMAS CENTRALES ACADÉMICOS – CEPIES**
- PAGO DE HONORARIOS A CONSULTORES INDIVIDUALES DE LÍNEA.
- Al respecto, se realizaron las siguientes tareas:
- CONTRATACIONES PARTIDA 25220 (CONSUTORES INDIVIDUALES DE LINEA)**
- Proceso de Contratación*
Atributo de pruebas de Control (Cumplimiento de Controles Clave Identificados)
- ✓ Solicitud de Compra de Bienes o Servicios
 - ✓ Certificación presupuestaria
 - ✓ Diploma Académico en Fotocopia Legalizada (Según objeto de contratación)
 - ✓ Título en provisión Nacional en Fotocopia Legalizada (Según objeto de contratación)
 - ✓ Certificado de Diplomado en Educación Superior en Fotocopia Legalizada (Según objeto de contratación)
 - ✓ Resolución de Designación/ memorándum
 - ✓ Contrato/ Orden de Compra – servicio
- Se colaboró con los papeles de trabajo, con las características de auditoría (informativos, marcas de auditoría, fuente, comentario, rúbrica, fecha, etc.)

Página 8 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.N° 22/2024

- Se realizó la referencia y correferencia de los papeles de trabajo realizados.
- Se procedió a realizar el armado de los legajos de auditoría.
- Otras tareas instruidas por el Auditor y/o Jefatura del Departamento de Auditoría Interna.

Memorándum de designación: MEM.T.AUD. No. 005-A/2024 del 17 de enero de 2024. (Ver **Anexo 11**)

Auditor Responsable: Lic. Mayra Torrico Maldonado

- Se coadyuvo en la revisión del Rubro del Balance: Cuentas de Orden, gestión 2023.
- Se revisó y analizó la documentación proporcionada por archivo del departamento de Contabilidad.
- Se realizó el análisis de la siguiente subcuenta:

818 Deudores de Gastos a Rendir

En base a la documentación proporcionada por la DA 1 y DA 60 corresponde a registros de pasajes y viáticos que no fueron descargados y fueron clasificados en la cuenta 81800 Deudores de Gastos a Rendir, aplicando para el efecto el Reglamento Interno de Pasajes y Viáticos aprobado con Resolución del Honorable Consejo Universitario N° 095/2018 del 09/05/2018, respecto el cual se verificó la siguiente documentación:

- ✓ Invitación, Convocatoria o documento que respalde el viaje en comisión
- ✓ Formulario original de "Entrega de fondos con cuenta por viajes, pasajes y viáticos"
- ✓ Formulario original de "Entrega de fondos con cuenta por viajes, pasajes y viáticos" con Certificación y aprobación del descargo
- ✓ Informe de viaje presentado en el plazo de 8 días hábiles desde la fecha de retorno
- ✓ Aprobación del informe de viaje por parte de autoridad competente

Pasajes

- ✓ Orden de compra o servicio
- ✓ Factura o recibo a nombre y NIT de la UMSA
- ✓ Pases a bordo, si el viaje ha sido por vía aérea

Viáticos

- ✓ Nota de solicitud de viáticos que adjunta la invitación, Convocatoria u otro documento que respalde la necesidad de realizar el viaje.

Página 9 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

- ✓ Recalculo conforme a la escala de viáticos aprobados por el Honorable Consejo Universitario Honorable Consejo Universitario N°095/2018 aprobado el 9 de mayo de 2018 y por los días solicitados.
- ✓ Cheque a nombre del cuentadante
- Se elaboró planillas Analíticas sobre la muestra seleccionada de la cuenta 81000 "Cuentas de Orden Deudoras"
- Se colaboró con los papeles de trabajo, tomando en cuenta las características de auditoría (informativos, marcas de auditoría, fuente, comentario, rúbrica, fecha, etc.) en función al orden establecido para el armado de papeles de trabajo.
- Se realizó la referencia y correferencia de los papeles de trabajo (Planillas de Analíticas y documentación de respaldo), en función al orden establecido para el armado de papeles de trabajo.
- Se colaboró en la realización del armado del legajo corriente de Cuentas de Orden.
- Otras tareas instruidas por el Auditor y/o Jefatura del Departamento de Auditoría Interna.

Memorándum de designación: SIN MEMORANDUM POR INSTRUCCIÓN DE JEFATURA

Auditor Responsable: Lic. Sara Limachi Huallpa

En fecha 11/12/2023 al 12/01/2024 se realizó las siguientes actividades:

- Se participó en la Verificación física de 76 activos fijos de las siguientes facultades:
 - DA 30 FACULTAD DE INGENIERÍA
 - DA 45 FACULTAD DE ARQUITECTURA, ARTES, DISEÑO Y URBANISMO
- Se elaboró el informe con sustento fotográfico correspondiente a la Verificación Física de Activos Fijos.
- Se procedió con la revisión de los papeles de respaldo de las siguientes facultades:
 - DA 1 ADMINISTRACIÓN CENTRAL INSTITUCIONAL
 - DA 55 FACULTAD DE CIENCIAS SOCIALES
 - DA 75 POST GRADO MULTIDISCIPLINARIO – CIDES
 - DA 80 PROGRAMAS CENTRALES ACADÉMICOS – CEPIES
 - DA 85 COMUNICACIÓN Y DIFUSIÓN UNIVERSITARIA
- Se elaboró y analizó planillas Analíticas de las partidas:
 - PARTIDA 436 EQUIPO EDUCACIONAL Y RECREATIVO
 - PARTIDA 4311 EQUIPO DE OFICINA Y MUEBLES

Página 10 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

- PARTIDA 4312 EQUIPO DE COMPUTACIÓN
- PARTIDA 435 EQUIPO DE COMUNICACIÓN
- PARTIDA 437 OTRA MAQUINARIA Y EQUIPO

Se tomó en cuenta para el análisis de los procesos de contratación, el Programa de Trabajo respecto a:

- CONTRATACIÓN DE COMPRA MENOR (COMPRAS MENORES hasta Bs 20.000)
- CONTRATACIÓN DE COMPRA MENOR (COMPRAS MENORES de Bs 20.001 hasta Bs 50.000)
- CONTRATACIÓN MODALIDAD ANPE (de Bs 50.001 hasta Bs 1.000.000)

Memorándum de designación: SIN MEMORANDUM POR INSTRUCCIÓN DE JEFATURA

Auditor Responsable: Lic. Valeria Mistas Moya

En fecha 26/01/2024 se participó en la Comisión de Activos Fijos, realizando las siguientes actividades:

- Se realizó la verificación física de 13 activos fijos de la DA 1- Administración Central Institucional.
- Se verificó que el activo se encuentre en el predio, edificio, piso y ambiente con indica el formulario.
- Se cotejó el Formulario de Verificación Física con las placas y las series en caso de equipos de computación.
- Se verificó que el activo este con el responsable como indica el formulario.
- se hizo el sustento fotográfico de los activos fijos.
- Se realizó el acta de verificación, con el llenado correspondiente y firmado por el inventariador designado.
- Se elaboró el informe con sustento fotográfico correspondiente a la Verificación Física de Activos Fijos.
- Se realizó el llenado de las marcas de auditoria en los respectivos Formularios de Verificación Física proporcionado por el inventariador designado.

Página 11 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

3.1.2 TRABAJO ASIGNADO: AUDITORÍA OPERACIONAL SOBRE EL CUMPLIMIENTO DEL PLAN OPERATIVO ANUAL, USO Y DESTINO DE LOS RECURSOS PROVENIENTES DEL IMPUESTO DIRECTO A LOS HIDROCARBUROS (IDH) DE LA UMSA, CORRESPONDIENTE A LA GESTIÓN 2023.

Memorándum de designación: MEM.T.AUD. No. 001/2024 del 16 de enero de 2024. (Ver Anexo 12)

Auditor Responsable: Lic. Dennis Magno Apaza Gonzales
Lic. Mayra G. Torrico Maldonado

Para tal efecto se procedió con la inducción respecto las Normas Básicas de Auditoría Operacional, aprobadas mediante Resolución N° CGE/093/2022 de 9 de noviembre de 2022 por la Contraloría General del Estado; asimismo, sobre lo dispuesto en el Artículo 2 del Decreto Supremo No.28421, del 21 de octubre de 2005, que establece que "Los beneficiarios presentarán de acuerdo a normativa legal vigente, Estados Financieros auditados sobre la ejecución de los recursos institucionales y auditorias operativas sobre el cumplimiento de sus Programas Operativos Anuales, con pronunciamiento expreso sobre la utilización y destino de los recursos provenientes del IDH.

Asimismo, el objeto del examen, comprendió las operaciones referidas al cumplimiento del Plan Operativo Anual de los proyectos y actividades de la UMSA financiadas con recursos provenientes del Impuesto Directo a los Hidrocarburos (IDH) para la gestión 2023 y documentación relacionada a la utilización y destino de los mismos.

Posteriormente, revisó y analizó documentación presentada por las Unidades Desconcentrada de los siguientes Proyectos:

DA 1 ADMINISTRACIÓN CENTRAL INSTITUCIONAL

- 01401 APOYO GENERACIÓN PROY. PRODUC. Y DE INVEST. P/ DESARROLLO ECO. SOCIAL Y MEDIOAMBIENTAL NORTE AMAZ. DPTO. L.P

DA 50 FACULTAD DE TECNOLOGÍA

- 50113 CONST. TALLERES Y LABORATORIOS CARRERA DE ELECTRICIDAD INDUSTRIAL COTA COTA

DA 95: CONVENIOS PARA PROYECTOS DE INVESTIGACIÓN ASDI - BRC – TB

- 300 ANALISIS INMUNOGENICIDAD DE LAS VACUNAS COVID 19 QUE SE ADMINISTRA A LA POBLACION MUNICIPIO DE LA PAZ
- 301 ANALISIS VARIANTES DE PREOCUPACION E INTERES DE SARSCOV2 POR CARACTERIZACIÓN GENÉTICA MUNICIPIO DE LA PAZ

Página 12 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

- 303 INVESTIGACIÓN EFECTIVIDAD DE LAS VACUNAS CONTRA SARS-COV2 MUNICIPIO DE LA PAZ
- 304 ANALISIS DEL SUJETO EN RELACION CON EL COVID-19 Y LA VACUNACION MUNICIPIO DE LA PAZ

- Se procedió con la revisión y análisis de los Registros de Ejecución de Gastos (C-31) y documentación de respaldo de los proyectos y actividades de la muestra seleccionada, considerando el Programa de Trabajo – Uso y Destino de Recursos IDH, cuyo objetivo es:

Determinar que la ejecución presupuestaria de Proyectos y Actividades con recursos provenientes del Impuesto Directo a los Hidrocarburos (IDH) correspondientes a la gestión 2023, fueron utilizados en el marco de las competencias establecidas en el Decreto Supremo Nº 28421 de 21 de octubre de 2005, Decreto Supremo Nº961 de 18 de agosto de 2011 y Reglamento Interno para la Administración de Recursos del IDH de la Universidad Mayor de San Andrés, aprobado mediante Resolución del Honorable Consejo Universitario Nº 611/2013 de 28 de noviembre de 2013, vigente en la gestión 2022; y si fueron destinados a los fines previstos.

- Se elaboró planillas Analíticas de Uso y Destino de los recursos IDH en base a la documentación de respaldo obtenida, tomando en cuenta los siguientes procedimientos de auditoría:

USO DE LOS RECURSOS IDH

Verificar que:

- Los recursos IDH sean utilizados únicamente en los siguientes tipos de gasto, según corresponda:
 - a) Gasto corriente.
 - b) Gasto en inversión universitaria.
- El gasto corriente sea efectuado de acuerdo a las siguientes competencias:

(Art. 22 del Reglamento Interno de Administración de Recursos IDH, aprobado por RHCU Nº611/2013 de 28/11/2013)

- a) Gastos centrales institucionales, por compensación por la eliminación de ingresos en títulos de bachiller.
- b) Gastos de la administración central, por la compensación por la extensión gratuita del Diploma Académico y Título en Provisión nacional a los graduados por excelencia.
- c) Transferencias corrientes al Seguro Social Universitario a objeto de financiar el Programa Médico Estudiantil.

Página 13 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.N° 22/2024

- d) Transferencias corrientes para financiar el Fondo de Fomento a la Educación Cívico Patriótica
 - e) Transferencia corriente para financiar becas otorgadas a los estudiantes universitarios.
 - f) Gastos para el financiamiento del Programa de Extensión Universitaria, Cultura y Deporte.

 - g) Gastos de Operación y funcionamiento de la Desconcentración Académica Universitaria.
- Los gastos de inversión universitaria correspondan a programas y proyectos, considerados en los siguientes componentes:
- (Art. 23 del Reglamento Interno de Administración de Recursos IDH, aprobado por RHCU N°611/2013 de 28/11/2013).
- a) Infraestructura.
 - b) Equipamiento.
 - c) Investigación científica, tecnológica e innovación.
 - d) Interacción social.
 - e) Programa de evaluación, acreditación y gestión de calidad

A efecto de verificar el cumplimiento de las disposiciones legales en los procesos de contratación y adquisición, así como verificar que los pagos efectuados con recursos IDH correspondan a partidas presupuestarias asignadas, cuenten con la documentación de respaldo suficiente y pertinente, seleccione una muestra de registros contables mínimamente del 50% de la ejecución por proyecto o actividad que forman parte de la muestra y efectúe los siguientes procedimientos de auditoría:

PROCESOS DE CONTRATACIÓN

- ✓ CONTRATACIÓN MENOR (COMPRAS MENORES hasta Bs 20.000)
- ✓ CONTRATACIÓN MENOR (COMPRAS MENORES de Bs 20.001 hasta Bs 50.000)
- ✓ CONTRATACIÓN MODALIDAD ANPE (de Bs 50.001 hasta Bs 1.000.000)
- ✓ PASAJES Y VIÁTICOS, para el recalcule se consideró la Escala de Viáticos aprobada mediante Res.HCU N° 741/2021.
- ✓ MANUAL DE OPERACIONES DEL SICOES, para los procedimientos, plazos y condiciones.
- ✓ PARTIDA 22210 VIÁTICOS POR VIAJES AL INTERIOR DEL PAÍS
- ✓ PARTIDA 25810 CONSULTORIA POR PRODUCTO
- ✓ PARTIDA 24120 MANTENIMIENTO Y REPARACIÓN DE VEHÍCULOS, MAQUINARIA Y EQUIPO
- ✓ PARTIDA 42230 OTRAS CONSTRUCCIONES Y MEJORAS DE BIENES PUBLICOS DE DOMINIO PRIVADO

Página 14 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

- Realizó la exposición de aclaraciones, informativos y marcas de auditoría en los papeles de trabajo; asimismo, verificar que los mismos cumplan los atributos de un papel de trabajo (Fuente, objetivo, conclusión, rubrica e iniciales del auditor, fecha, exponer si corresponde a documentación proporcionado por la Entidad, etc.).
- Se realizó la referencia y correferencia de los papeles de trabajo (Planillas de Analíticas y documentación de respaldo), en función al orden establecido para el armado de papeles de trabajo.
- Se procedió a realizar el armado del legajo de auditoría.

Los resultados de los objetivos de gestión específicos deberán ser evaluados anualmente por las instancias superiores correspondientes, contemplando aspectos cuantitativos y cualitativo, en base a la información obtenida de la verificación de la ejecución de los indicadores de eficacia, eficiencia y otros aspectos que permita medir el grado de cumplimiento de los resultados y el logro de los objetivos.

A fin de contar con criterios uniformes sobre la interpretación de los resultados que se obtengan en el seguimiento y evaluación del POA, se consideró la siguiente tabla de calificaciones:

**PARÁMETROS DE MEDICIÓN ENTIDAD RES.
HCU 1190/2019**

Niveles	Rango	Conclusiones
1 nivel	=100%	Eficaz
2 nivel	>50% y <100%	Aceptable
3 nivel	<= 50%	No eficaz

**PARÁMETROS DE MEDICIÓN
RES.NºCGE/93/2022 DE 09/11/2022**

Niveles	Rango	Conclusiones
1 nivel	De 0 a 69%	No eficaz
2 nivel	>69% y <=100%	Eficaz

Teniendo en cuenta lo mencionado se realizó lo siguiente:

- Elaboró la Cédula Analítica de cumplimiento del POA con datos extraídos del Sistema Leo V.2 y documentación proporcionada las Unidades Desconcentrada.
- Otras tareas instruidas por el inmediato superior y jefatura del Departamento de Auditoría Interna.

Página 15 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

3.1.3 TRABAJO ASIGNADO: RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE LA ELABORACIÓN E IMPLEMENTACIÓN DEL PLAN INSTITUCIONAL DE SEGURIDAD DE LA INFORMACIÓN (PISI) DE LA UNIVERSIDAD MAYOR DE SAN ANDRÉS.

Memorándum de designación: MEM.T.AUD. No. 008/2024 del 14 de marzo de 2024. (Ver Anexo 13)

Auditor Responsable: Lic. Dennis Magno Apaza Gonzales

ACTIVIDADES DESARROLLADAS

Para tal efecto, se procedió con la inducción respecto a las Normas Generales de Auditoría Gubernamental, numeral 217, aprobada mediante Resolución Nº CGE/094/2012 del 27 de agosto de 2012, referente al numeral 217 Relevamiento de Información Específica, Reglamento para la elaboración de Informes de Auditoría con Indicios de Responsabilidad aprobado mediante Resolución Nº CGE/018/2024 de 4 de marzo de 2024, emitida por la Contraloría General del Estado, Decreto Supremo Nº2514 de 9 de septiembre de 2015, correspondiente a la creación del AGETIC y Resolución Administrativa Nº AGETIC/RA/0051/2017 de 19 de septiembre de 2017, que aprueba los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público.

El objetivo definido para el Relevamiento de Información Específica, es recopilar y evaluar información sobre la elaboración e implementación del Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés, aprobado mediante Resolución del Honorable Consejo Universitario Nº298/2019 de 4 de septiembre de 2019, en el marco del Decreto Supremo Nº2514 del 9 de septiembre de 2015 y los Lineamientos para la Elaboración e Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, aprobado con Resolución Administrativa Nº AGETIC/RA/0051/2017 de 19 de septiembre de 2017, a fin de determinar la auditabilidad.

Asimismo, el objeto del Relevamiento lo constituye la integridad de la documentación e información relacionada con la elaboración e implementación del Plan Institucional de Seguridad de la Información de la UMSA, como ser:

- o El Plan Institucional de Seguridad de la Información de la Universidad Mayor de San Andrés, aprobado mediante Resolución del Honorable Consejo Universitario Nº298/2019 de 4 de septiembre de 2019.
- o Antecedentes de la Resolución del Honorable Consejo Universitario Nº298/2019 de 4 de septiembre de 2019.
- o Reglamentos, Manuales de Procesos y/o Procedimientos de seguridad, emergentes de la Implementación del Plan Institucional de Seguridad de la Información, relacionados a los 11 anexos de los controles mínimos de seguridad de la información, previstos en el numeral 6.2.3.2 de los Lineamientos para la Elaboración e

Página 16 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

Implementación de los Planes Institucionales de Seguridad de la Información de las Entidades del Sector Público, emitidos por la AGETIC.

- o Documento de designación del Responsable de Seguridad de la Información.
- o Documento de conformación del Comité de Seguridad de la Información.

Teniendo en cuenta lo mencionado se realizó las siguientes actividades:

- Analizó los Lineamientos para la elaboración e implementación de los Planes Institucionales de Seguridad de la Información de las entidades del sector público, aprobado por la AGETIC mediante Resolución Administrativa No. AGETIC/RA/0051/2017 de fecha 19 de septiembre de 2017.
- Participó en las reuniones con el Departamento de Tecnologías de Información y Comunicación (DTIC), para informar sobre el Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés.
- Analizó el documento Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés, aprobado mediante Resolución HCU No. 298/2019 de fecha 04 de septiembre de 2019.
- Coadyuvo en la elaboración de la Cédula Analítica contrastando los lineamientos para la elaboración e implantación del PISI para las entidades del sector público respecto el Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés.
- Armado legajos de papeles de trabajo, conforme a índice establecido.
- Referencia y correferencia los papeles de trabajo de acuerdo a código de referencia asignada.
- Realizó la exposición de aclaraciones, informativos y marcas de auditoría en los papeles de trabajo; asimismo, verificar que los mismos cumplan los atributos de un papel de trabajo (Fuente, objetivo, conclusión, rubrica e iniciales del auditor, fecha, exponer si corresponde a documentación proporcionado por la Entidad, etc.).

Página 17 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

3.1.4 TRABAJO ASIGNADO: RELEVAMIENTO DE INFORMACIÓN ESPECÍFICA SOBRE EL INCIDENTE DE SEGURIDAD – FILTRACIÓN CPU SIA PRODUCIDO EN LA UNIVERSIDAD MAYOR DE SAN ANDRÉS.

Memorándum de designación: MEM.T.AUD. No. 031/2024 del 22 de abril de 2024. (Ver Anexo 14)
Auditor Responsable: Lic. Dennis Magno Apaza Gonzales
ACTIVIDADES DESARROLLADAS
<p>Para tal efecto, se procedió con la inducción respecto a las Normas Generales de Auditoría Gubernamental, numeral 217, aprobada mediante Resolución Nº CGE/094/2012 del 27 de agosto de 2012, referente al numeral 217 Relevamiento de Información Específica y de acuerdo al Capítulo II, artículo 7 Relevamiento de Información del Reglamento para la elaboración de Informes de Auditoría con Indicios de Responsabilidad aprobado mediante Resolución Nº CGE/018/2024 de 4 de marzo de 2024, emitida por la Contraloría General del Estado.</p> <p>El objetivo definido para el Relevamiento de Información Específica, es recopilar y evaluar información sobre el Incidente de Seguridad – Filtración CPU SIA producido en la Universidad Mayor de San Andrés, a fin de determinar la auditabilidad.</p> <p>Asimismo, el objeto del Relevamiento lo constituye la integridad de la documentación e información relacionada al Sistema de Información Académica y Base de Datos de matriculación de la Universidad Mayor de San Andrés, como ser:</p> <ol style="list-style-type: none">1. En qué sistema o sistemas se encuentra la base de datos de los registros de matriculación de los estudiantes de pregrado y postgrado de la Universidad Mayor de San Andrés y que tipo de información personal se registra en la misma.2. Información si se cuenta con la integridad de la información del Sistema de Información Académica a la fecha del incidente de seguridad; así como de los demás sistemas integrados y/o vinculados a dicho sistema.3. Informar y documentar si a la fecha, se han reportado denuncias, quejas y/o reclamos por parte de estudiantes de pregrado y postgrado u otros como consecuencia del incidente de seguridad y filtración de información personal expuesta en el SIA.4.Cuál es la razón por la que se produjo el incidente de seguridad y filtración de información y que sistemas fueron vulnerados. <p>Al respecto se analizó la documentación proporcionada por el Departamento de Tecnología de la Información y Comunicación (DTIC) y División de Sistemas de Información y Estadística – UMSA.</p> <p>Teniendo en cuenta lo mencionado se realizó las siguientes actividades:</p>

Página 18 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

- Se participó en las reuniones con el Departamento de Tecnologías de Información y Comunicación (DTIC), para informar sobre el Sistema de Información Académica y Base de Datos de matriculación de la Universidad Mayor de San Andrés.
- Se coadyuvo en la elaboración de la Cédula Analítica Incidente de Seguridad – Filtración CPU SIA de la Universidad Mayor de San Andrés.
- Armado de legajos de papeles de trabajo, conforme a índice establecido.
- Referencia y correferencia los papeles de trabajo de acuerdo a código de referencia asignada.
- Se realizó la exposición de aclaraciones, informativos y marcas de auditoria en los papeles de trabajo; asimismo, verificó que los mismos cumplan los atributos de un papel de trabajo (Fuente, objetivo, conclusión, rubrica e iniciales del auditor, fecha, exponer si corresponde a documentación proporcionado por la Entidad, etc.).

Todos los trabajos descritos anteriormente, se encuentran sustentados en los informes mensuales presentados por la Egresada Gaby Norca Arias Chambi, a la Jefatura del Departamento de Auditoría Interna de la Universidad Mayor de San Andrés.

Por lo señalado, en cumplimiento al "Reglamento Especifico de Modalidad de Graduación de Trabajo Dirigido para la obtención del nivel de licenciatura en la Universidad Mayor de San Andrés" aprobado por Resolución del Honorable Consejo Universitario N°330/2022 de 18 de agosto de 2022, la Egr. Gaby Norca Arias Chambi, elaboró para su exposición el proceso correspondiente al Relevamiento de Información Especifica sobre la Elaboración e Implementación del Plan Institucional de Seguridad de la Información (PISI) de la Universidad Mayor de San Andrés.

4. EVALUACIÓN DEL TRABAJO DIRIGIDO

En cumplimiento al **Artículo 16 y 18** del Reglamento Especifico de Modalidad de Graduación por Trabajo Dirigido para la Obtención del Nivel de Licenciatura en la Universidad Mayor de San Andrés, aprobado mediante Resolución del Honorable Consejo Universitario N° 330/2022 de fecha 18 de agosto de 2022, mismos que citan lo siguiente:

"Artículo 16° Informes. Durante la realización del Trabajo Dirigido el postulante presentará a la Dirección de carrera dos (2) Informes Trimestrales y un (1) Informe Final, rubricado por el Tutor Profesional y el Tutor Docente.

En el Informe Final, el Tutor Profesional debe asignar la calificación cualitativa misma que debe ser validada por el Tutor Docente con calificación numérica.

Artículo 18° La escala de calificaciones cualitativa y cuantitativa es la siguiente:

Página 19 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

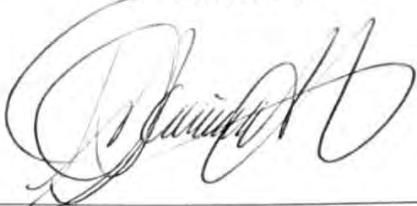
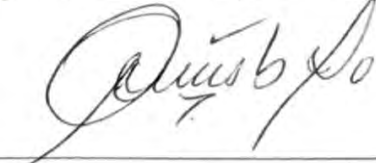
QUALITATIVA	CUANTITATIVA
Reprobado	0-50
Aprobado-Buena	51-70
Sobresaliente-Con recomendación de Publicación	71-89
Excelente - con mención honorífica y recomendación de Publicación.	90-100"

El tutor profesional realiza la calificación a la Egresada Gaby Norca Arias Chambi, considerando para ello la escala establecida en el Artículo 18 del Reglamento anteriormente citado, calificación que será validada por el Tutor Docente asignando una calificación numérica.

En mérito al apoyo y desempeño en el desarrollo de los diferentes trabajos realizados por parte de la Egresada Gaby Norca Arias Chambi en el Departamento de Auditoria Interna de la Universidad Mayor de San Andrés, en el cual adquirió conocimientos teóricos y prácticos sobre la realización de diferentes actividades de Auditoria, como ser:

- Auditoría de Confiabilidad de Registros y Estados Financieros de la Universidad Mayor de San Andrés al 31 de diciembre de 2023.
- Auditoria Operacional sobre el Cumplimiento del Plan Operativo Anual, Uso y Destino de los recursos provenientes del Impuesto Directo a los Hidrocarburos (IDH) de la UMSA.
- Procesos de Relevamiento de Información Especifica.

En consideración a lo anteriormente mencionado, se le asigna a la Egresada Gaby Norca Arias Chambi, la siguiente calificación:

EVALUACIÓN QUALITATIVA TUTOR PROFESIONAL Ute. Dennis Magno Apeza Gonzales	EVALUACIÓN CUANTITATIVA TUTOR DOCENTE Mg. Sc. Ausberto Choque Mita
Sobresaliente - Con recomendación de Publicación 	75 (setenta y cinco) 

Página 20 de 21



UNIVERSIDAD MAYOR DE SAN ANDRÉS
DEPARTAMENTO DE AUDITORÍA INTERNA
La Paz - Bolivia

AUD.INT.INF.TD.Nº 22/2024

5. CONCLUSIÓN.

Por todo lo antes mencionado se concluye que, las actividades desarrolladas de los ocho meses (23 de octubre de 2023 al 23 de junio de 2024) por la Univ. Gaby Norca Arias Chambi, Trabajo Dirigido del Departamento de Auditoría Interna, egresada de la Carrera de Contaduría Pública de la Facultad de Ciencias Económicas y Financieras de la Universidad Mayor de San Andrés, mismas que fueron desarrolladas de conformidad al Plan de Trabajo definido para el desarrollo del Trabajo dirigido, que incluyó procedimientos de inducción normativa para la aplicación de procedimientos de auditoría establecidos en los programas de trabajo, para cumplimiento de criterios de calidad del trabajo; asimismo, la egresada aplicó conocimientos teóricos adquiridos en el desarrollo de sus actividades académicas como universitaria y adquirió nuevas competencias en el ámbito de la Auditoría Gubernamental en el desarrollo del Trabajo Dirigido, demostrando proactividad, responsabilidad, disciplina y adaptabilidad en los trabajos realizados en equipo.

Asimismo, se ha evaluado el trabajo Dirigido de la Egr. Gaby Norca Arias Chambi, alcanzando una calificación cualitativa de: **Sobresaliente-Con recomendación de Publicación** y cuantitativa de:

En cuanto informamos a su autoridad para los fines consiguientes, saludo a usted con las consideraciones más distinguidas.


Lic. Dennis Magno Apaza Gonzales
**TUTOR PROFESIONAL
AUDITOR INTERNO**


Mg. Sc. Ausberto Choque Mita
TUTOR DOCENTE - UMSA


Lic. Adolfo Balboa Mamani
**JEFE DEPARTAMENTO DE
AUDITORÍA INTERNA**

C.c Arch. DAI.
Adj. Anexo N° 1 al 14

Página 21 de 21