CEHANI E.S.E.

VIGILADO Supersalud

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-2026-CEHANÍ E.S.E

AMANDA LILIANA VIVEROS ORDOÑEZ
Gerente

COPIA CONTROLADA

No.
COPIA

COPIA NO CONTROLADA

CICLO DE EVALUACIÓN Y MEJORAMIENTO			
REVISIÓN	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACIÓN**	**MEJORAMIENTO**
Revisión del documento	Enero de 2020	Se actualizó el cronograma para la vigencia 2020.	Mejoramiento continuo
Revisión del documento	Junio de 2021	Se articula documento con la Guía básica de riesgos y oportunidades GU-CDG-001, Procedimiento de Gestión de riesgos y oportunidades PR-CDG-003 y Matriz de riesgos y oportunidades MA-CDG-003	Mejoramiento Continuo
Revisión del documento	Enero de 2022	Se actualiza nombres de procesos y oficinas en el documento para la vigencia 2022	Mejoramiento continuo
Revisión del documento	Enero de 2023	Se ajustan los códigos de los documentos referenciados	Mejoramiento continuo
Revisión del documento	Enero de 2024	En el Numeral 3.1 FASE 1: Planeación para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información (Definición de Estrategias) se actualizan las referencias de los documentos MA-SIG-007 por MA-GSI-002, se actualiza el numeral 4. Cronograma y el 5. Presupuesto.	Mejoramiento continuo
Revisión del documento	Enero de 2025	Se registra en la Introducción el dominio MGGTI en su componente de Seguridad de la Información, Se realiza actualización de listado de activos de Información por proceso, dueños y custodios de la información, Se actualizan los niveles de criticidad, se actualiza actividades, cronograma y presupuesto.	Mejoramiento continuo
Revisión del documento	Enero 2026	Se actualiza el cronograma de actividades para la vigencia 2026. Se procede con la eliminación de Paso 1: Listar los activos de información por cada proceso. Paso 2: Identificar el dueño y custodio de los activos Paso 3: Clasificar los activos Paso 4: Clasificar la información d. Clasificación de los Activos Según las Normas	Mejoramiento continuo

INTRODUCCIÓN

Uno de los objetivos del Sistema de Gestión de la Seguridad y Privacidad de la Información en las entidades es garantizar que los riesgos asociados a la seguridad de la información sean conocidos, gestionados y tratados por la Entidad y además de que estos deben quedar soportados en un documento, para que sea un ejercicio de gestión, sistemático, estructurado, repetible y eficiente, en este orden de ideas es fundamental que la entidad identifique y valore los riesgos que pueden afectar la seguridad y privacidad de la información y por consiguiente establecer los mecanismos más convenientes para darle protección.

La información que genera constantemente el CEHANI E.S.E. es crucial para su correcto desempeño y cumplimiento de los objetivos organizacionales, es por ello que la seguridad y privacidad de la información se convierte en prioridad para evitar cualquier posibilidad de ataque a la integridad, disponibilidad y/o confidencialidad entre otros eventos, los cuales pueden incidir en el normal funcionamiento y por ende redundar en la prestación de los servicios de salud.

Teniendo en cuenta lo anterior y tal como se establece desde el dominio MGGTI en su componente Gestión de seguridad y también desde el Modelo de Seguridad y Privacidad de la información –MSPI del Min Tic, un tema decisivo, es la Gestión de riesgos asociados a la seguridad y privacidad de la información, la cual puede ser utilizada para la toma de decisiones en todos los niveles.

Es importante resaltar que para la evaluación de riesgos en seguridad y privacidad de la información un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación que se describirán en el presente plan.

1. OBJETIVOS

1.1 General

Definir un marco regulatorio interno que permita identificar, medir, controlar, monitorear y comunicar los riesgos asociados a la seguridad y privacidad de la información y que puedan afectar el cumplimiento de los objetivos estratégicos, minimizando las pérdidas para la entidad.

1.2 Específicos

Establecer los lineamientos y principios que lleven a la unificación de criterios para la gestión adecuada de los riesgos de seguridad y privacidad de la información.

Fortalecer el sistema de gestión de riesgos de la Entidad incorporando controles y medidas para la seguridad y privacidad de la información.

Contribuir para que se minimice la posibilidad de que un evento produzca determinado impacto bien sea en la información o cualquier otro activo de información asociado, a través de la gestión adecuada de los riesgos de la seguridad y privacidad de la información.

Dar pautas para que la implementación de controles sea adecuada y que el nivel de probabilidad e impacto se encuentren en niveles aceptables para la entidad.

2. CONCEPTOS BÁSICOS

Administración del riesgo: Conjunto de elementos de control que al Interrelacionarse brindan a la entidad la capacidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales y protegerla de los efectos ocasionados por su ocurrencia.

Análisis de riesgos: Es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado.

Amenaza: Es la causa potencial de una situación de incidente y no deseada por la organización

Activo de Información: Se considera principalmente a cualquier conjunto de datos creado o utilizado por un proceso de la organización, así como el hardware y el software utilizado para su procesamiento o almacenamiento, los servicios utilizados para su transmisión o recepción y las herramientas y/o utilidades para el desarrollo y soporte de sistemas de información. En casos particulares, se puede considerar como un activo de información a personas que manejen datos, transacciones o un conocimiento específico muy importante para la organización.

Causa: Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Confidencialidad: La confidencialidad es la garantía de que la información será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información. Cada individuo tiene derecho a proteger su información personal.

Consecuencia: Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

Disponibilidad: Una vez que la información ha sido capturada en un sistema de cómputo, debe ser almacenada de manera segura y estar disponible para los usuarios cuando la necesiten. La información también debe ser mantenida y utilizada de tal forma que su integridad no se vea comprometida.

Evento: Un incidente o situación, que ocurre en un lugar particular durante un intervalo de tiempo específico.

Estimación del riesgo. Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Evitación del riesgo. Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Factores de Riesgo: Situaciones, manifestaciones o características medibles u observables asociadas a un proceso que generan la presencia de riesgo o tienden a aumentar la exposición, pueden ser internos o externos a la entidad.

Gestión del Riesgo: Proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Integridad: Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es decir, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Impacto: Se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Probabilidad: Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la

soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo Inherente: Es el nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles.

Riesgo Residual: El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Reducción del riesgo. Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo. Aceptación de la pérdida o ganancia proveniente de un riesgo particular

Seguimiento: Mesa de trabajo semestral, en el cual se revisa el cumplimiento del plan de acción, indicadores y metas de riesgo y se valida la aplicación de los controles de seguridad de la información sobre cada uno de los procesos.
Tratamiento del Riesgo: Proceso para modificar el riesgo" (Icontec Internacional, 2011).

Valoración del Riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.

Vulnerabilidad: Es aquella debilidad de un activo o grupo de activos de información.

3. PROCESO DE GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

3.1 FASE 1: Planeación para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información (Definición de Estrategias)

Para el desarrollo de esta fase se aplican básicamente la Guía básica para la administración de riesgos y oportunidades GU-SIG-007 y el procedimiento Gestión de riesgos y oportunidades PR-SIG-013, los pasos 1,2 y 3 de la guía para la Administración de los Riesgo de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, emitida por la Función Pública, lo que implica las siguientes actividades con las cuales se busca profundizar en lo concerniente a riesgos de seguridad digital.

El adecuado manejo de los riesgos favorece el desarrollo y crecimiento de la entidad, con el fin de asegurar dicho manejo es importante que se establezca el entorno y ambiente organizacional de la entidad, la identificación, análisis, valoración y definición de las alternativas de acciones de mitigación de los riesgos, esto en desarrollo de los siguientes elementos:

- Contexto estratégico – MA-DRE-003
- Identificación de riesgos y oportunidades – MA-GSI-002
- Análisis de riesgos y oportunidades – MA-GSI-002
- Valoración de riesgos - MA-GSI-002

a. Alcance

El tratamiento de riesgos asociados a la Seguridad y Privacidad de la Información es extensible y aplicable a todos los procesos de la entidad por tratarse de riesgos transversales y que se enmarcarán dentro de los criterios del Modelo de Seguridad y Privacidad de la Información, que es el habilitador, en materia de seguridad digital, de la Estrategia de Gobierno Digital expedida por el MINTIC.

b. Política de tratamiento de riesgos de seguridad y privacidad de la información

En este aspecto la entidad cuenta con la Política de Riesgos DI-DRE-012, de una manera integral, más, sin embargo, no incluye el compromiso para la gestión de riesgos de seguridad y privacidad de la información en todos los niveles.

c. Roles y responsabilidades

La entidad cuenta con la Matriz de roles, responsabilidades y autoridades del sistema integrado de gestión MA-DRE-005, el cual se encuentra enfocado hacia el Sistema de Sistemas Integrados de gestión, Sistema de Gestión Ambiental y Sistema de Gestión de Seguridad y Salud en el trabajo. Para que el mismo se enfoque hacia el Sistema de Gestión de Seguridad de la información debe delegar la responsabilidad en una persona o funcionario que haga parte de la línea estratégica o de la alta dirección, quien tendrá como responsabilidades las siguientes:

- Definir el procedimiento para la Identificación y Valoración de Activos.

- Adoptar o adecuar el procedimiento formal para la gestión de riesgos de seguridad digital (Identificación, Análisis, Evaluación y Tratamiento).

- Asesorar y acompañar a la primera línea de defensa en la realización de la gestión de riesgos de seguridad digital y en la recomendación de controles para mitigar los riesgos.

- Apoyar en el seguimiento a los planes de tratamiento de riesgo definidos.

- Informar a la línea estratégica sobre cualquier variación importante en los niveles o valoraciones de los riesgos de seguridad digital.

Es importante tener presente la Guía 4: Roles y responsabilidades definida por el MSPI y que hace parte de la política Gobierno Digital para complementar el tema anterior.

d. Asignación de recursos:

La entidad debe disponer de los recursos suficientes para el tratamiento de riesgos de seguridad y privacidad de la información, estos recursos requeridos son capital, tiempo, personal, procesos, sistemas y tecnologías, con el fin de apoyar a los responsables en la implementación de controles y seguimiento de los riesgos.

e. Identificación de activos de seguridad y privacidad de la información

Para la entidad un activo es cualquier elemento que tenga valor, pero aplicado al contexto de seguridad y privacidad de la información hace referencia a elementos tales como aplicaciones de la entidad, servicios Web, redes, información física o digital, Tecnologías de la Información -TI- o Tecnologías de la Operación -TO que utiliza la organización para su funcionamiento.

Establecer este inventario de activos de información es importante ya que así se podrá saber lo que se debe proteger para garantizar tanto su funcionamiento interno como su funcionamiento de cara al ciudadano, lo que redundará en el aumento de su confianza en el uso del entorno digital.

Para la entidad es importante determinar los riesgos asociados a seguridad y confidencialidad de la información por tanto se realizó valoración de activos de información de manera generalizada desde la Primera Línea de Defensa – Líderes de Proceso.

Para la generación de este inventario, la entidad pública debe tener en cuenta los siguientes pasos:

Paso 3: Clasificar los activos

TIPO DE ACTIVO	DESCRIPCIÓN
INFORMACIÓN	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
SOFTWARE	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
HARDWARE	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.
SERVICIOS	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales

	organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).
INTANGIBLES	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el Good Will, entre otros.
COMPONENTES DE RED	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.
PERSONAS	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
INSTALACIONES	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

Paso 4: Clasificar la información

a. **Según la confidencialidad**: Se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, Esta se debe definir de acuerdo con las características de los activos que se manejan en la entidad, para el caso de CEHANI E.S.E. Se definen tres (3) niveles alineados con los tipos de información declarados en la ley 1712 del 2014.

INFORMACIÓN PÚBLICA RESERVADA	Información disponible sólo para un proceso de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.
INFORMACIÓN PÚBLICA CLASIFICADA	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
INFORMACIÓN PÚBLICA	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de INFORMACIÓN PÚBLICA RESERVADA.

b. **Según la integridad**: Se refiere a la exactitud y completitud de la información (ISO 27000) esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. Para el caso de CEHANI E.S.E se utilizará el siguiente esquema de clasificación de tres (3) niveles.

A **(ALTA)**	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
M **(MEDIA)**	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderada a funcionarios de la entidad.
B **(BAJA)**	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de integridad ALTA.

c. **Según la disponibilidad**: Es la propiedad de la información que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona entidad o proceso autorizado cuando así lo requiera está, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. Para el caso de CEHANI E.S.E. es recomendable utilizar el siguiente esquema de clasificación de tres (3) niveles

A **(ALTA)**	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
M **(MEDIA)**	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.
B	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no

(BAJA)	conlleva implicaciones legales, económicas o de pérdida de imagen.
NO CLASIFICADA	Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como activos de información de disponibilidad ALTA.

Paso 5: Determinar la criticidad del activo

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	**ALTA (A)**	**ALTA (1)**
INFORMACIÓN PÚBLICA CLASIFICADA	**MEDIA (M)**	**MEDIA (2)**
INFORMACIÓN PÚBLICA	**BAJA (B)**	**BAJA (3)**
NO CLASIFICADA	**NO CLASIFICADA**	**NO CLASIFICADA**

Para determinar el nivel de criticidad se utiliza los siguientes criterios:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

3.1.1 Metodología para la identificación de riesgos Identificación de riesgos a la seguridad y privacidad de la información – MA-GDC-003

Para identificar los riesgos relacionados a seguridad y privacidad de la información, es necesario previamente identificar las amenazas que pueden materializarse. Los tipos de amenazas se han clasificado en 2: amenazas comunes y amenazas dirigidas por el hombre.

Amenazas Comunes

TIPO	AMENAZA	ORIGEN
Daño físico	Fuego	F, D, A
	Agua	F, D, A
Eventos naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
Pérdidas de los servicios esenciales	Fallas en el sistema de suministro de agua	E
	Fallas en el suministro de aire acondicionado	F, D, A
Perturbación debida a la radiación	Radiación electromagnética	F, D, A
	Radiación térmica	F, D, A
Compromiso de la información	Interceptación de servicios de señales de interferencia comprometida	D
	Espionaje remoto	D
Fallas técnicas	Fallas del equipo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información	D, F
	Mal funcionamiento del software	D, F
	Incumplimiento en el mantenimiento del sistema de información	D, F
Acciones no autorizadas	Uso no autorizado del equipo	D, F
	Copia fraudulenta del software	D, F
Compromiso de las funciones	Error en el uso o abuso de derechos	D, F
	Falsificación de derechos	D

F: Fortuito
D: Deliberada
A: Ambiental

Escala de Probabilidades, Impacto y Metodología de Valoración

La escala de probabilidades o frecuencias en que se puede presentar la materialización del riesgo, el impacto o consecuencias que se pueden presentar y la metodología establecida para su análisis y valoración se encuentran definidos en la Guía básica de gestión de riesgos y oportunidades de CEHANI ESE GU-SIG-007.

3.1.2 Indicadores para la gestión de los riesgos

En los planes operativos anuales de la vigencia 2025 se tiene establecido el indicador de cumplimiento de la evaluación de riesgos por proceso.

3.2 FASE 2: Ejecución

Fase que corresponde a la implementación de los controles del cuadro anterior, conservando los tiempos de ejecución y llevar a cabo lo planeado.

En esta fase es importante el compromiso de la Alta dirección de brindar los recursos necesarios para iniciar con el tratamiento de los riesgos y por otra parte el liderazgo del responsable del proceso de GSI.

3.3 FASE 3: Monitoreo y Revisión

La entidad y sus Tres Líneas de defensa definidas en el MIPG deben hacer un seguimiento a los planes de tratamiento para determinar su efectividad, según lo siguiente:

- Realizar monitoreo de los riesgos y controles tecnológicos.
- Efectuar la evaluación del plan de acción y realizar nuevamente la valoración de los riesgos de seguridad digital para verificar su efectividad.
- Verificar que los controles están diseñados e implementados de manera efectiva y operen como se pretende para controlar los riesgos.
- Suministrar recomendaciones para mejorar la eficiencia y eficacia de los controles.

3.4 FASE 4: Mejoramiento Continuo

La Entidad garantiza la mejora continua de la gestión de los riesgos de seguridad y privacidad de la información, estableciendo las acciones de mejora según lo definido en el Procedimiento de Mejora Continuo PR-SIG-005 el cual aplica para cuando existan hallazgos, falencias o incidentes de seguridad y privacidad de la información, se identifica la fuente de la no conformidad, se mitiga el impacto de su existencia y se toman acciones para controlarlos y prevenirlos.

4. CRONOGRAMA

ACTIVIDAD	RESPONSABLE	FECHA MAXIMA DE IMPLEMENTACION	PRODUCTO
Revisión de la normatividad vigente y actualización del plan de acuerdo a los lineamientos normativos y realidad institucional	Líder GSI Coordinador GD	30-04-2026	Documento elaborado, codificado, socializado e implementado
Revisión de la matriz de riesgos del proceso GSI	Líder GSI Coordinador GD Jefe Oficina Control Interno	28-05-2026	Matriz de riesgos verificada y/o ajustada
Análisis de controles establecidos para los riesgos de seguridad y privacidad de la información	Líder GSI jefe Oficina Control Interno	30-06-2026	Informe
Monterero de Riesgos de Seguridad y privacidad de la Información	Líder GSI Jefe Oficina Control Interno	30-09-2026	Informe

ORIGINAL FIRMADO

	Elaborado por:	Revisado por:	Aprobado por:
Firma			
Nombre	WILSON PAZ DELGADO	NIDIAN MENDOZA	AMANDA LILIANA VIVEROS
Cargo / Rol	Profesional Universitario – Líder Proceso GSI	Subgerente Administrativo y Financiero	Gerente

	Visto Bueno.
Firma	
Nombre	ANA MILENA ARROYO
Cargo/ Rol	Profesional Universitario