PROYECTO

GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO NORMAS ISO/IEC 27001

UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ					
CONVOCATORIA GESTIÓN DE LA CIENCIA 2018					
FORMULARIO PARA LA PRESENTACIÓN DE PROYECTOS DE INVESTIGACIÓN					
CARRERA/FACULTAD: Ingeniería en Sistemas / Ciencias Informáticas					
1.- DATOS GENERALES					
Título del proyecto de Investigación: **Sistema de Gestión de la Seguridad de la Información bajo Normas ISO/IEC 27001**			**Tipología del Proyecto de Investigación**		
			Investigación Básica		
			Investigación Aplicada	**X**	
			Desarrollo Tecnológico	**X**	
ÁREAS DE CONOCIMIENTO					
	Ciencias de la Vida y Salud				
X	Ciencias Sociales				
	Ciencias Exactas				
X	Ciencias Técnicas				
Duración del Proyecto (en meses)			**12**		
Fecha de Inicio:	Diciembre /2018		**Fecha de terminación (estimada):**	Diciembre/2019	
Financiamiento: UNIVERSIDAD LAICA ELOY ALFARO DE MANABÍ					
Monto Total $USD:	**$9.670,80**			**Financiamiento Externo:**	
Estado del Proyecto de Investigación:	**Propuesta Nueva**			**Unidad Responsable de ejecución (Facultad, Extensión, Campus):**	Facultad de Ciencias Informáticas, Manta
	Propuesta de Continuación	**X**			
2.- OBJETIVO GENERAL					

Diseñar e Implementar un Sistema de Gestión de la Seguridad de la Información bajo la Norma ISO/IEC 27001 en la Facultad de Ciencias Informáticas, que permita establecer políticas de seguridad y disminuir el riesgo de la información ante un eventual ataque informático o desastre natural.

3.- OBJETIVOS ESPECÍFICOS

- Identificar riesgos de seguridad en el área informática a los que está expuesta la Facultad de Ciencias Informática.
- Definir las medidas de seguridad más apropiadas a aplicarse en este caso.
- Definir las políticas de seguridad encaminadas a minimizar los riesgos a los que está expuesta la información.
- Plantear un Sistema de Gestión de la Seguridad de la Información (SGSI) bajo la norma ISO/IEC 27001 para la Facultad de Ciencias Informáticas que permita obtener confidencialidad, integridad y disponibilidad de la información.
- Implementar un SGSI para la Facultad de Ciencias Informáticas que permita proteger los recursos informáticos más valiosos; cómo la información el hardware y el software.

4.- HIPÓTESIS PRINCIPAL

Un sistema de gestión de la seguridad de la información (SGSI) mitigaría los riesgos informáticos, identificando las amenazas informáticas (fuga de información, phishing, virus, suplantación de identidad, etc.) y desastres naturales (terremotos, tsunamis, etc.) que existen en el entorno aplicando políticas que harán a los usuarios más responsables con la información que manejan.

5.- DESCRIPCIÓN DETALLADA DEL PROYECTO

1. Introducción

En la sociedad del conocimiento que vivimos hoy, las innovaciones tecnológicas han influenciado en la manipulación de la información y las comunicaciones, donde el incremento en la transferencia de la información modificó en muchos sentidos la forma en que desarrollan muchas actividades en la sociedad moderna. Estas actividades han dejado expuesta nuestra información sin tener la precaución de determinar que es confidencial y que es público.

La implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) es una opción fundamental cuando se trata de proteger la información, ya que este tiene como objetivo esencial proteger dicho activo a través de controles y políticas de seguridad que deben ser aplicadas en una organización empresarial o académica.

La Facultad de Ciencias Informáticas, a través del diseño e implementación de un SGSI busca minimizar los riesgos a los que se encuentra expuesta la información de la Facultad, proceso que se documenta paso a paso.

Para el desarrollo de la primera etapa se aplica la metodología Magerit con la cual se realiza el análisis de riesgos que es una de las principales actividades a cumplir ya que permite identificar y analizar cada uno de los procesos y determinar los riesgos a los cuales estamos expuestos identificando amenazas y vulnerabilidades.

Para el análisis de riesgos se realiza un inventario actualizado de activos, una valoración cualitativa de dichos activos, identificación de amenazas, definición de salvaguardas. También se atacará diversos entornos con la intención de descubrir fallos, vulnerabilidades, etc.

Una vez identificado claramente los activos que se encuentra en un riesgo inminente y que generaría mayor impacto en caso de que sufrieran un ataque, o con una alta probabilidad de que una amenaza informática o natural se materializara, se procede a definir políticas de seguridad, la declaración y aplicabilidad de los controles considerados en la Norma ISO/IEC 27001, de este proceso puede nacer la creación de planes integrales de prevención y mitigación de riesgo, como un plan de continuidad de los servicios y un plan de contingencia los cuales ayudaran a volver a la operatividad de las labores académicas si se concretara una amenaza natural.

Las políticas y controles creados deben ser aceptadas y aprobadas por las Autoridades de la Facultad, en un Consejo de Facultad se determinará su aplicación en todas las áreas vinculadas con el manejo de la información y los recursos informáticos. Se recomendarán la creación de una Comisión de Seguridad la cual monitoreará el cumplimiento de las políticas y controles, su actualización en el caso de que sea necesario, así en conjunto se cumplirá con el objetivo fundamental del SGSI que es proteger la información y disminuir los riesgos, garantizando la continuidad del negocio.

Sabemos que este tipo de cambios en hábitos es muy chocante para las personas por tal motivo se creará un plan de sensibilización para capacitar a la comunidad académica en la adecuada aplicación de las políticas implementadas con sus respectivas sanciones, amenazas informáticas, atención y respuesta a incidentes de seguridad de la información, etc.

Cuando las organizaciones han llevado con éxito la ejecución de todas estas actividades su mayor objetivo, el más ambicioso es el de la Certificación, el nuestro será certificar la Facultad de Ciencias Informáticas en la Norma ISO/IEC 27001 y porque no en un futuro cercano la Universidad.

2. Marco Teórico

¿Qué es un SGSI?:

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Información Security Management System.

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

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información[1]:

- **Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Figura 1. SGSI

[1] ISO 27001. (2005). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/iso27000.html

Fuente: www.iso27000.es

¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial y académica necesarios para lograr los objetivos de la organización y asegurar beneficios deseados.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo. Los virus informáticos, el "hacking" o los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones[2].

Figura 2. Utilidad de un SGSI

Fuente: www.iso27000.es

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la Facultad, sus

[2] IBID., ISO 27001.

autoridades al frente, tomando en consideración también a docentes, estudiantes y personal administrativo.

¿Cuáles son los componentes de un SGSI?:

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma[3].

Figura 3. Componentes de un SGSI

Fuente: www.iso27000.es

3. Preguntas de Investigación

La propuesta presentada se enmarca en la línea de investigación de gestión de sistemas específicamente dentro de la auditoría de sistemas que hacen referencia a:

- **Gestión de sistemas:** Se ocupa de integrar, planificar y controlar los aspectos técnicos, humanos, organizativos, comerciales y sociales del proceso completo empezando con el análisis del dominio del problema, continuando con el diseño de alternativas de solución y finalizando con la operatividad de un sistema. La gestión de sistema incluye también procesos que abarcan la planificación de actividades, metas, responsables, indicadores de eficiencia eficacia y efectividad.
- **Auditoría de sistemas:** Incluye control de información, calidad de procesos, seguridad informática, que son vitales para asegurar la validez y veracidad de la información.

4. Justificación

Proteger la información en una Institución de Educación Superior consiste en poner barreras de protección para bloquear posibles ataques, es necesario resguardar todos los medios de acceso a la institución debido a que las últimas décadas el uso del internet y los sistemas de información es más común lo que convierte a una institución cualquiera que sea su razón social en vulnerable frente a los atacantes.

Tal vez nos preguntaremos, que es preciado en nuestra institución proteger, pues nuestros procesos de matriculación, notas, asistencias, tareas, proyectos integradores; así como los datos de nuestros docentes, estudiantes, personal administrativo, proveedores de servicios y contratistas.

[3] IBID., ISO 27001.

La Facultad de Ciencias Informáticas busca un mejoramiento continuo prestando un mejor servicio a la comunidad universitaria, adoptando herramientas de optimización, basadas en nuevas tecnologías y estableciendo políticas de seguridad de la información a fin de ir innovando en la calidad de la educación con la colaboración tanto de las autoridades como de los docentes, estudiantes y administrativos.

La información se ha denominado como uno de los activos más preciados en una organización por lo tanto definir políticas de seguridad en el manejo de la información y en el uso de las herramientas tecnológicas es vital, porque permite evitar incidentes que afecten el buen desempeño de las actividades académicas.

Hasta el momento se han presentados ataques leves al aula virtual, por lo que sabemos que el riesgo es inminente y estas falencias pueden traer inconvenientes desastrosos, que estamos a tiempo para prevenir, mitigar y controlar.

Teniendo en consideración que nuestra Facultad pertenece a una Institución de Educación Superior Pública y nos rigen las leyes del Estado Ecuatoriano, el 19 de septiembre de 2013 se emitió el Acuerdo Ministerial No. 166, que dispone que las entidades de la Administración Pública Central, Institucional y Dependiente de la Función Ejecutiva (APCID), la implementación del "Esquema Gubernamental de Seguridad de la Información EGSI", Norma Técnica Ecuatoriana INEN ISO/IEC 27002. Por tal motivo las leyes ecuatorianas también nos facultan para el desarrollo de este proyecto ambicioso pero necesario.

5. Metodología

a. Diseño del Estudio

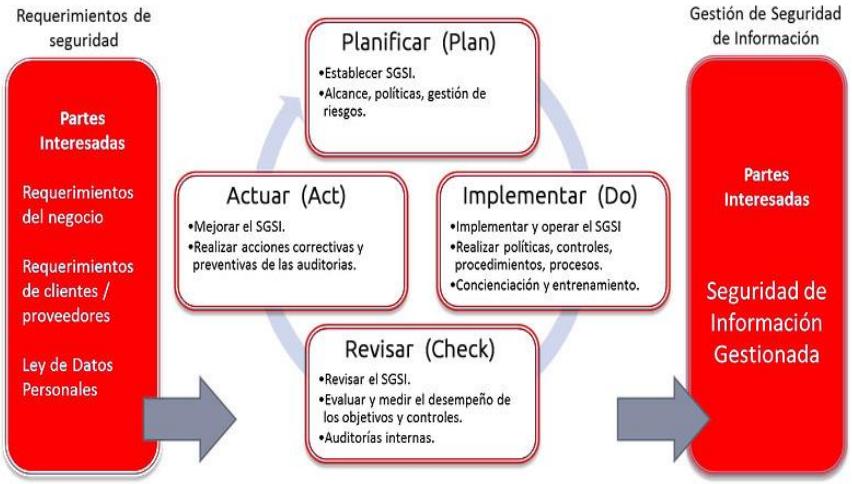
La metodología que vamos a utilizar para el desarrollo del proyecto será el de Plan/Do/Check/Act que es una serie de actividades documentadas ampliamente probadas en este campo, por parte de profesionales expertos, auditores de sistemas informáticos, peritos informáticos, informáticos forenses, oficiales de seguridad, etc.

Este modelo incluye la estructura, políticas, actividades, responsabilidades, prácticas, procedimientos, procesos y recursos.

- Plan – Planificación
- Do – Hacer
- Check – Monitorear
- Act - Actuar

En la siguiente figura podemos observar la metodología mencionada y sus componentes.

Figura 4. Metodología de la ISO/IEC 27001



Fuente: www.iso27000.es

b. Definición de Variables

Variables independientes se tiene:

- Estudiantes involucrados en procesos académicos con manejo de información.
- Recursos informáticos, hardware, software, talento humano.

Variables dependientes:

- Estimación de número de ataques informáticos a los recursos informáticos.
- Tiempo de concurrencia de los ataques informáticos.

c. Medición de Variables y Procedimientos

Las variables son medibles y verificables mediante la aplicación de las metodologías antes expuestas y a través del análisis de riesgo informático.

6. Consideraciones Éticas

Como nuestro campo de acción es una Institución de Educación Superior Pública, nos debemos someter a los reglamentes que la rigen, así tenemos que con la creación del "Esquema Gubernamental de Seguridad de la Información EGSI", Norma Técnica Ecuatoriana INEN ISO/IEC 27002, nos proponen la obligatoriedad del *"Código de Buenas Prácticas para la Gestión de la Seguridad de la Información"*. El cual regirá nuestro accionar de manera ética.

7. Resultados Esperados

a. Productos esperados

- Dos publicaciones científicas para dos congresos regionales.
- Un artículo científico para una revista científica, en un Q3.

6.- REFERENCIAS BIBLIOGRAFICAS

- AMUTIO, Miguel y CANDAU, Javier. MAGERIT. Versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I. Método. Ministerio de Hacienda y Administraciones Pública. España, 2012.
- Ciclo PDCA. Sistemas de Gestión de Seguridad de la Información. Obtenido de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-14-agosto-2013/135_ciclo_pdca__edward_deming.htmll
- ISO 27001. (2005). El portal de ISO 27001 en Español. Obtenido de http://www.iso27000.es/iso27000.html.
- ISO 27001. (2013). Statement of Applicability of ISO/IEC 27001 Annex A controls. Obtenido de www.ISO27001security.com.
- ISO 27001. (2013). Plan de tratamiento de riesgos, Obtenido de http://www.iso27001standard.com/es/documentacion/Plan-de-tratamiento-de- riesgos.
- UNIVERSIDAD JAVERIANA. Manual del sistema de gestión de la seguridad de la información, Obtenido: http://pegasus.javeriana.edu.co/~CIS0830IS12/documents/Anexo%20K%20MG-05%20Manual%20del%20Sistema%20de%20Gestion%20de%20Seguridad%20de%20la%20Informacion.pdf.

7. RESUMEN EJECUTIVO: Este es un breve análisis de los aspectos más importantes del proyecto. Incluye Introducción, objetivo general, métodos y resultados esperados

La Secretaría Nacional de Administración Pública (SNAP) dispone de leyes y decretos que las instituciones públicas deben de tener un aseguramiento de su información cumpliendo con objetivos fundamentales como la confidencialidad, la integridad y la disponibilidad de la data. Teniendo en consideración que todas las atribuciones otorgadas a la SNAP en el decreto 5 del nuevo Mandato Presidencial fueron transferidas a la Secretaría General de la Presidencia.

Por lo tanto, la Facultad de Ciencias Informáticas que forma parte de una IES en donde se maneja grandes volúmenes de información en los procesos académicos, pretende implementar políticas y controles de seguridad para protegerla; incrementando la confiabilidad en los softwares de administración de información, brindándoles eficiencia y calidad.

El presente proyecto tiene como objetivo fundamental, diseñar un SGSI para la Facultad de Ciencias Informáticas bajo la Norma ISO/IEC 27001 con el fin de clasificar la información, identificar las vulnerabilidades y amenazas; valorar los riesgos y con base en estos definir controles y políticas de seguridad que deben ser de conocimiento y aceptación de todo el personal que labora en la facultad, instrucciones de los procedimientos a realizarse y la documentación que se debe desarrollar en todo el proceso para la posterior implementación del SGSI, aplicando el modelo PDCA (Plan/Do/Check/Act).

Como primera actividad se ha recolectado información a través de la observación, que se espera contrastar con encuestas y una prueba de tráfico de la red que permiten una idea general del manejo de la seguridad en la organización.

Seguidamente se realiza un análisis de riesgos paso a paso desarrollando el inventario de activos, la valoración cualitativa de los activos, identificación de las amenazas, identificación de salvaguardas para los activos y evaluación del riesgo y el informe de calificación del riesgo, que permiten identificar los riesgos más relevantes a los que está expuesta la facultad.

Finalmente se definen políticas y controles de seguridad, que tienen como objetivo mitigar el riesgo y fortalecer la seguridad con medidas que se verán reflejadas en el accionar de todo el personal docente y administrativo que maneja información. De la misma manera los estudiantes tendrán responsabilidades que cumplir en el proceso académico que manejan de acuerdo con los recursos informáticos involucrados en ellos.

Lo innovador del proyecto es que este tipo de implementación se ha hecho con gran éxito en el Ecuador en instituciones públicas y privadas como es el caso del Banco Guayaquil, Telconet y CNTEP siendo parte fundamental de su crecimiento financiero y en el caso de CNTEP salvándola de la quiebra.

Sabemos que el objetivo principal de una Institución de Educación Superior (IES) no es el auge financiero, pero si la estabilidad económica que lo da la confianza del Estado en la IES, confianza que es valorada por la acreditación. IES acreditadas como la Pontificia Universidad Católica del Ecuador (PUCE), la Escuela Superior Politécnica del Litoral (ESPOL) y la Universidad Politécnica Salesiana están implementando proyectos similares al nuestro en busca de la mejora continua que les pide como requisito la acreditación y un SGSI les permite mantenerse en el sitial de calidad otorgado.

8.- DESCRIBIR LOS IMPACTOS DE ACUERDO AL OBJETIVO DEL PROYECTO.

El impacto esperado por nosotros es el de concientizar a la comunidad académica en el correcto manejo de la información y de los recursos informáticos que nos ayudan a manipularla, de esta forma se incrementará la confiabilidad en los procesos académicos, dándole seguridad a los usuarios de la fidelidad de la información.

Si bien es cierto los ataques informáticos son un riesgo residual, que subsiste después de haber implementado controles y aumentando este riesgo están las amenazas naturales y antrópicas, que por la ubicación geográfica en la que se encuentra la Facultad de Ciencias Informáticas (FACCI) la hace vulnerable a estos incidentes tanto naturales como informáticos.

Siendo así la materialización del proyecto contribuirá a tener un plan de continuidad y plan de contingencia que nos permita recuperar la operatividad académica luego de un siniestro.

9.- BENEFICIARIOS DE LOS RESULTADOS DEL PROYECTO

Beneficiarios Directos	731			**Beneficiarios Indirectos**	1500
Empleo Directo	Hombres 584 Mujeres 147			**Empleo Indirecto**	Hombres 450 Mujeres 1050
% Insumos Nacionales	100 %			**% Insumos Importados**	0%

11.- PARTICIPANTES EN LA EJECUCIÓN DEL PROYECTO			
LIDER DEL PROYECTO (PROFESOR TITULAR O NO TITULAR A TIEMPO COMPLETO)			
APELLIDOS	VERA NAVARRETE	**NOMBRES**	DENISE SORAYA
NÚMERO DE CÉDULA DE IDENTIDAD	1308400249	**DIRECCIÓN DOMICILIARIA**	10 DE AGOSTO Y GARCÍA MORENO
TITULO TERCER NIVEL	INGENIERA EN SISTEMAS INFORMÁTICO	**TITULO CUARTO NIVEL**	MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA
CATEGORÍA Y NIVEL DE TITULARIDAD	NO TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	INGENIERÍA EN SISTEMAS / CIENCIAS INFORMÁTICAS
TELÉFONO FIJO	05-2631-191	**TELÉFONO MÓVIL**	098-722-4890
CORREO ELECTRÓNICO PERSONAL	DENISSE.VERA09@GMAIL.COM	**CORREO ELECTRÓNICO INSTITUCIONAL**	DENISE.VERA@LIVE.ULEAM.EDU.EC
CO-LÍDER (PROFESOR TITULAR)			
APELLIDOS	BAZURTO ROLDÁN	**NOMBRES**	JOSÉ ANTONIO
NÚMERO DE CÉDULA DE IDENTIDAD	1305063958	**DIRECCIÓN DOMICILIARIA**	AVENIDA 108 Y CALLE 109
TITULO TERCER NIVEL	INGENIERO ELÉCTRICO	**TITULO CUARTO NIVEL**	MÁSTER BUSINESS ADMINISTRACIÓN (MBA)
CATEGORÍA Y NIVEL DE TITULARIDAD	TITULAR	**TIEMPO DE DEDICACIÓN**	COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	INGENIERÍA EN SISTEMAS / CIENCIAS INFORMÁTICAS
TELÉFONO FIJO	052384435	**TELÉFONO MÓVIL**	099-961-7002
CORREO ELECTRÓNICO PERSONAL	BAZURTO.JOSE@GMAIL.COM	**CORREO ELECTRÓNICO INSTITUCIONAL**	JOSE.BAZURTO@LIVE.ULEAM.EDU.EC

PROFESORES E INVESTIGADORES			
APELLIDOS	MENDOZA RODRÍGUEZ	**NOMBRES**	HOMERO RENÁN
NÚMERO DE CÉDULA DE IDENTIDAD	1306984632	**DIRECCIÓN DOMICILIARIA**	PORTOVIEJO, ANDRÉS DE VERA
TITULO TERCER NIVEL		**TITULO CUARTO NIVEL**	MASTER OF ARTS, MATH
CATEGORÍA Y NIVEL DE TITULARIDAD	NO TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	INGENIERÍA EN SISTEMAS - FACULTAD DE CIENCIAS INFORMÁTICAS
NIVEL DE TITULARIDAD	NO TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
TELÉFONO FIJO	052933346	**TELÉFONO MÓVIL**	0980383831
CORREO ELECTRÓNICO PERSONAL	HOMER3680@GMAIL.COM	**CORREO ELECTRÓNICO INSTITUCIONAL**	HOMERO.MENDOZA@LIVE.ULEAM.EDU.EC

PROFESORES E INVESTIGADORES			
APELLIDOS	LARREA PLÚA	**NOMBRES**	JOHNNY JAVIER
NÚMERO DE CÉDULA DE IDENTIDAD	1303801532	**DIRECCIÓN DOMICILIARIA**	CIUDADELA UNIVERSITARIA, CALLE 3 AVENIDA U2
TITULO TERCER NIVEL	INGENIERO EN SISTEMAS	**TITULO CUARTO NIVEL**	MAGISTER EN DOCENCIA UNIVERSITARIA E INVESTIGACIÓN EDUCATIVA
CATEGORÍA Y NIVEL DE TITULARIDAD	TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	INGENIERÍA EN SISTEMAS - FACULTAD DE CIENCIAS INFORMÁTICAS
NIVEL DE TITULARIDAD	TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
TELÉFONO FIJO	052626641	**TELÉFONO MÓVIL**	0984496002
CORREO ELECTRÓNICO PERSONAL	JHONNYLARREA@HOTMAIL.COM	**CORREO ELECTRÓNICO INSTITUCIONAL**	JOHNNY.LARREA@LIVE.ULEAM.EDU.EC

PROFESORES E INVESTIGADORES			
APELLIDOS	MACHUCA AVALOS	**NOMBRES**	MIKE PAOLO
NÚMERO DE CÉDULA DE IDENTIDAD	1307673911	**DIRECCIÓN DOMICILIARIA**	CALLE 110 Y AVENIDA 111
TITULO TERCER NIVEL	INGENIERO ELÉCTRICO	**TITULO CUARTO NIVEL**	MAGISTER EN FINANZAS Y COMERCIO INTERNACIONAL
CATEGORÍA Y NIVEL DE TITULARIDAD	NO TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	INGENIERÍA EN SISTEMAS - FACULTAD DE CIENCIAS INFORMÁTICAS
NIVEL DE TITULARIDAD	NO TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
TELÉFONO FIJO	052384545	**TELÉFONO MÓVIL**	0993419854
CORREO ELECTRÓNICO PERSONAL	MIKE@PROSERBICORP.COM	**CORREO ELECTRÓNICO INSTITUCIONAL**	MIKE.MACHUCA@LIVE.ULEAM.EDU.EC

PROFESORES E INVESTIGADORES			
APELLIDOS	GONZÁLEZ LÓPEZ	**NOMBRES**	OSCAR ARMANDO
NÚMERO DE CÉDULA DE IDENTIDAD	1307613727	**DIRECCIÓN DOMICILIARIA**	AVENIDA 27 Y CALLE 17
TITULO TERCER NIVEL	ANALISTA DE SISTEMAS	**TITULO CUARTO NIVEL**	MAESTRÍA EJECUTIVA EN INFORMÁTICA DE GESTIÓN Y NUEVAS TECNOLOGÍAS
CATEGORÍA Y NIVEL DE TITULARIDAD	NO TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	INGENIERÍA EN SISTEMAS - FACULTAD DE CIENCIAS INFORMÁTICAS
NIVEL DE TITULARIDAD	NO TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
TELÉFONO FIJO	056051749	**TELÉFONO MÓVIL**	0985723603
CORREO ELECTRÓNICO PERSONAL	AS_OSCAR@HOTMAIL.COM	**CORREO ELECTRÓNICO INSTITUCIONAL**	OSCAR.GOZALEZ@LIVE.ULEAM.EDU.EC

PROFESORES E INVESTIGADORES			
APELLIDOS	GARCÍA MACÍAS	NOMBRES	VIVIANA KATIUSKA
NÚMERO DE CÉDULA DE IDENTIDAD	1310391691	**DIRECCIÓN DOMICILIARIA**	PORTOVIEJO, VÍA SANTA ANA CALLE PARAÍSO
TITULO TERCER NIVEL	INGENIERA EN SISTEMAS INFORMÁTICOS	**TITULO CUARTO NIVEL**	MAGISTER EN INFORMÁTICA EMPRESARIAL
CATEGORÍA Y NIVEL DE TITULARIDAD	NO TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	INGENIERÍA EN SISTEMAS - FACULTAD DE CIENCIAS INFORMÁTICAS
NIVEL DE TITULARIDAD	NO TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
TELÉFONO FIJO	052417272	**TELÉFONO MÓVIL**	0996238349
CORREO ELECTRÓNICO PERSONAL	VIVIANAKATIUSKAGARCIAMACIAS@GMAIL.COM	**CORREO ELECTRÓNICO INSTITUCIONAL**	VIVIANA.GARCIA@LIVE.ULEAM.EDU.EC

PROFESORES E INVESTIGADORES			
APELLIDOS	GARCÍA VÉLEZ	**NOMBRES**	WALTER COLÓN
NÚMERO DE CÉDULA DE IDENTIDAD	1304078742	**DIRECCIÓN DOMICILIARIA**	URBANIZACIÓN CIELITO LINDO MZ. D11 VILLA 9
TITULO TERCER NIVEL	INGENIERO CIVIL	**TITULO CUARTO NIVEL**	EDUCACIÓN DE COMPETENCIAS UNIVERSITARIA
CATEGORÍA Y NIVEL DE TITULARIDAD	TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	INGENIERÍA EN SISTEMAS - FACULTAD DE CIENCIAS INFORMÁTICAS
NIVEL DE TITULARIDAD	AGREGADO	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
TELÉFONO FIJO	052567033	**TELÉFONO MÓVIL**	0988010079
CORREO ELECTRÓNICO PERSONAL	WALTERGARCIAFISICA@HOTMAIL.COM	**CORREO ELECTRÓNICO INSTITUCIONAL**	WALTER.GARCIA@LIVE.ULEAM.EDU.EC

PROFESORES E INVESTIGADORES			
APELLIDOS	MUÑOZ VERDUGA	**NOMBRES**	DOLORES
NÚMERO DE CÉDULA DE IDENTIDAD	1306796366	**DIRECCIÓN DOMICILIARIA**	CONDOMINIOS TERRAZAS DEL CONDE VILLA 5
TITULO TERCER NIVEL	LICENCIADA EN CIENCIAS DE LA EDUCACIÓN ESPECIALIDAD FÍSICO-MATEMÁTICO	**TITULO CUARTO NIVEL**	DOCTORA EN CIENCIAS PEDAGÓGICAS
CATEGORÍA Y NIVEL DE TITULARIDAD	PRINCIPAL	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DECANA	**CARRERA-FACULTAD**	FACULTAD DE CIENCIAS INFORMÁTICAS
NIVEL DE TITULARIDAD	PRINCIPAL	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
TELÉFONO FIJO	052554060	**TELÉFONO MÓVIL**	0999891195
CORREO ELECTRÓNICO PERSONAL	SILVIA_DOLORES72@YAHOO.ES	**CORREO ELECTRÓNICO INSTITUCIONAL**	DOLORES.MUÑOZ@LIVE.ULEAM.EDU.EC

PROFESORES E INVESTIGADORES			
APELLIDOS	ZAMORA MERO	**NOMBRES**	WILLIAN JESÚS
NÚMERO DE CÉDULA DE IDENTIDAD	1308526456	**DIRECCIÓN DOMICILIARIA**	ESPAÑA
TITULO TERCER NIVEL	INGENIERO EN SISTEMAS	**TITULO CUARTO NIVEL**	MAGISTER EJECUTIVO EN INFORMÁTICA DE GESTIÓN EN NUEVAS TECNOLOGÍAS
CATEGORÍA Y NIVEL DE TITULARIDAD	TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	INGENIERÍA EN SISTEMAS - FACULTAD DE CIENCIAS INFORMÁTICAS
NIVEL DE TITULARIDAD	TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
TELÉFONO FIJO		**TELÉFONO MÓVIL**	0034653330276
CORREO ELECTRÓNICO PERSONAL	WZAMORA@GMAIL.COM	**CORREO ELECTRÓNICO INSTITUCIONAL**	WILLIAN.ZAMORA@LIVE.ULEAM.EDU.EC

PROFESORES E INVESTIGADORES			
APELLIDOS	AYOVÍ RAMÍREZ	**NOMBRES**	MARCO WELLINGTON
NÚMERO DE CÉDULA DE IDENTIDAD	0800631152	**DIRECCIÓN DOMICILIARIA**	CIUDADELA UNIVERSITARIA
TITULO TERCER NIVEL	INGENIERO EN SISTEMAS	**TITULO CUARTO NIVEL**	MAGISTER EJECUTIVO EN INFORMÁTICA DE GESTIÓN Y NUEVAS TECNOLOGÍAS
CATEGORÍA Y NIVEL DE TITULARIDAD		**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	INGENIERÍA EN SISTEMAS - FACULTAD DE CIENCIAS INFORMÁTICAS
NIVEL DE TITULARIDAD		**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
TELÉFONO FIJO	052612915	**TELÉFONO MÓVIL**	0958988015
CORREO ELECTRÓNICO PERSONAL	CONSULTMAR@YAHOO.ES	**CORREO ELECTRÓNICO INSTITUCIONAL**	MARCO.AYOVI@LIVE.ULEAM.EDU.EC

PROFESORES INVESTIGADORES			
APELLIDOS	SANTAMARIA PHILCO	**NOMBRES**	ALEX
NÚMERO DE CÉDULA DE IDENTIDAD	0603073776	**DIRECCIÓN DOMICILIARIA**	CIUDADELA UNIVERSITARIA
TITULO TERCER NIVEL	INGENIERO EN SISTEMAS	**TITULO CUARTO NIVEL**	MASTER UNIVERSITARIO EN INGENIERIA DEL SOFTWARE, METODOS FORMALES Y SISTEMAS DE INFORMACION EN LA ESPECILIDAD INGENIERIA DE SOFTWARE
CATEGORÍA Y NIVEL DE TITULARIDAD	TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
CARGO ACTUAL	DOCENTE	**CARRERA-FACULTAD**	
NIVEL DE TITULARIDAD	TITULAR	**TIEMPO DE DEDICACIÓN**	TIEMPO COMPLETO
TELÉFONO FIJO	052612915	**TELÉFONO MÓVIL**	34634271406
CORREO ELECTRÓNICO PERSONAL		**CORREO ELECTRÓNICO INSTITUCIONAL**	

ESTUDIANTES EN TITULACIÓN

ESTUDIANTE EN TITULACIÓN 1			
APELLIDOS	RODRÍGUEZ ZAMBRANO	**NOMBRES**	JOSELYNE ELIZABETH
NÚMERO DE CÉDULA DE INDENTIDAD	131214296-9	**DIRECCIÓN**	CDLA. 15 DE ABRIL (CALLE 325 AVE. 215)
TELÉFONO FIJO/MOVIL	0995923599	**FACULTAD**	FACULTAD DE CIENCIAS INFORMÁTICAS
CARRERA	INGENERIA EN SISTEMAS	**SEMESTRE**	DÉCIMO

ESTUDIANTE EN TITULACIÓN 2			
APELLIDOS	SÁNCHEZ MONTES	**NOMBRES**	DIANA FERNANDA
NÚMERO DE CÉDULA DE INDENTIDAD	131698344-2	**DIRECCIÓN**	CIUDADELA URBIRRIOS II
TELÉFONO FIJO/MOVIL	0990761958	**FACULTAD**	FACULTAD DE CIENCIAS INFORMÁTICAS
CARRERA	INGENIERÍA EN SISTEMAS	**SEMESTRE**	DÉCIMO

ESTUDIANTE EN TITULACIÓN 3			
APELLIDOS	DELGADO DELGADO	**NOMBRES**	YULEIKA MARICELA
NÚMERO DE CÉDULA DE INDENTIDAD	131341707-1	**DIRECCIÓN**	BARRIO LA PAZ CALLE 117 AV 203
TELÉFONO FIJO/MOVIL	0988341392	**FACULTAD**	CIENCIAS INFORMÁTICAS

CARRERA	INGENIERIA EN SISTEMAS	**SEMESTRE**	DÉCIMO
ESTUDIANTE EN TITULACIÓN 4			
APELLIDOS	GUERRERO GARCÍA	**NOMBRES**	MARÍA JOSÉ
NÚMERO DE CÉDULA DE INDENTIDAD	085024364-3	**DIRECCIÓN**	CIUDADELA BELLA VISTA
TELÉFONO FIJO/MOVIL	0986058044	**FACULTAD**	CIENCIAS INFORMÁTICAS
CARRERA	INGENIERIA EN SISTEMAS	**SEMESTRE**	DECIMO

ESTUDIANTE EN TITULACIÓN 5			
APELLIDOS	FLORES	**NOMBRES**	MICHAEL BRYAN
NÚMERO DE CÉDULA DE INDENTIDAD	131401100-6	**DIRECCIÓN**	MONTECRISTI "LA PAOLA"
TELÉFONO FIJO/MOVIL	0980075397	**FACULTAD**	FACULTAD DE CIENCIAS INFORMÁTICAS
CARRERA	INGENIERÍA EN SISTEMAS	**SEMESTRE**	DECIMO
ESTUDIANTE EN TITULACIÓN 6			
APELLIDOS	DELGADO LUCAS	**NOMBRES**	KIMBERLY NAYESKA
NÚMERO DE CÉDULA DE INDENTIDAD	131252313-5	**DIRECCIÓN**	CALLE 105 AV 102 TARQUI
TELÉFONO FIJO/MOVIL	0979034814	**FACULTAD**	CIENCIAS INFORMÁTICAS
CARRERA	INGENIERIA EN SISTEMAS	**SEMESTRE**	DECIMO

ESTUDIANTE EN TITULACIÓN 7			
APELLIDOS	CASTILLO PALMA	**NOMBRES**	ADRIAN ABEL
NÚMERO DE CÉDULA DE INDENTIDAD	1314950484	**DIRECCIÓN**	MONTECRISTI, AVENIDA MANTA, CDLA SORAYA
TELÉFONO FIJO/MOVIL	0994838180	**FACULTAD**	CIENCIAS INFORMÁTICAS
CARRERA	INGENIERIA EN SISTEMAS	**SEMESTRE**	DÉCIMO

ESTUDIANTE EN TITULACIÓN 8			
APELLIDOS	DELGADO SUÁREZ	**NOMBRES**	EVELYN ELIZABETH
NÚMERO DE CÉDULA DE INDENTIDAD	1310185200	**DIRECCIÓN**	MONTECRISTI, CALLE 9 DE JULIO
TELÉFONO FIJO/MOVIL	0987587368	**FACULTAD**	FACULTAD DE CIENCIAS INFORMÁTICAS
CARRERA	INGENIERÍA EN SISTEMAS	**SEMESTRE**	DÉCIMO

ESTUDIANTE EN TITULACIÓN 9			
APELLIDOS	PELÁEZ SÁNCHEZ	**NOMBRES**	RICARDO DAVID
NÚMERO DE CÉDULA DE INDENTIDAD	131250878-9	**DIRECCIÓN**	VILLAS DEL IESS MZ E # 17
TELÉFONO FIJO/MOVIL	0985655412	**FACULTAD**	FACULTAD DE CIENCIAS INFORMÁTICAS
CARRERA	INGENIERÍA EN SISTEMAS	**SEMESTRE**	DÉCIMO

ESTUDIANTE EN TITULACIÓN 10			
APELLIDOS	DELGADO	**NOMBRES**	KERLY
NÚMERO DE CÉDULA DE INDENTIDAD		**DIRECCIÓN**	
TELÉFONO FIJO/MOVIL		**FACULTAD**	CIENCIAS INFORMÁTICAS
CARRERA	INGENIERIA EN SISTEMAS	**SEMESTRE**	DÉCIMO

ESTUDIANTE EN TITULACIÓN 11			
APELLIDOS	ARIOSTO MUENTES	**NOMBRES**	
NÚMERO DE CÉDULA DE INDENTIDAD		**DIRECCIÓN**	
TELÉFONO FIJO/MOVIL		**FACULTAD**	CIENCIAS INFORMÁTICAS
CARRERA	INGENIERIA EN SISTEMAS	**SEMESTRE**	DÉCIMO

CRONOGRAMA VALORADO														
Actividad	**Descripción**	**Responsable**	**Presupuesto**	**Duración: tiempo/mes (puede variar)**										
				1	2	3	4	5	6	7	8	9	10	11	12
Identificar riesgos de seguridad en el área informática a los que está expuesta la Facultad de Ciencias Informática.	*Ejecutar un análisis de riesgo informático basado en la metodología Magerit. *Evaluar los riesgos informáticos encontrados.	**Docente:** Ing. Denise Vera, **Estudiantes:** Srta. Evelin Mera Srta. Gema Guerrero	500												
Definir las medidas de seguridad más apropiadas a aplicarse.	*Definir medidas de seguridad físicas y lógicas que permitan mitigar los riesgos informáticos evaluados.	**Docente:** Ing. Mike Machuca Ing. Viviana García **Estudiantes:** Srta. María José Guerrero. Sr. Michael Flores	500												
Definir las políticas de seguridad encaminadas a minimizar los riesgos a los que está expuesta la información	*Elaborar una Declaración de Aplicabilidad con las políticas que aplican a la FACCI. * Definir los motivos de la elección de los controles, los objetivos que se lograrán con los controles y describir cómo se implementarán.	**Docente:** Ing. Denise Vera **Estudiantes:** Srta. Kerly Delgado	500												

Plantear un Sistema de Gestión de la Seguridad de la Información (SGSI) bajo la norma ISO/IEC 27001 para la Facultad de Ciencias Informáticas que permita obtener confidencialidad, integridad y disponibilidad de la información.	*Redactar las políticas y procedimientos obligatorios para el aseguramiento de la información. *Elaborar Plan de Continuidad y Plan de Contingencia *Presentar la documentación (Políticas y Planes) al Consejo de Facultad para su aprobación y poderlos implementar en la FACCI.	**Docentes:** Ing. José Bazurto Ing. Walter García Ing. Oscar González **Estudiantes:** Sr. Ariosto Muentes Srta. Yuleika Delgado Sr. Armando Domínguez	1000												
Implementar un SGSI para la Facultad de Ciencias Informáticas que permita proteger los recursos informáticos más valiosos; cómo la información el hardware y el software.	*Auditorías Internas (Planes de MTT Preventivo y Correctivo). *Creación de Comisión de Seguridad (evaluación de riesgo periódico, seguimiento y control de las políticas). *Diseño de un modelo para la supervisión y monitoreo del SGSI	**Docentes:** Ing. Oscar González Ing. Marco Ayoví Ing. Denise Vera Lcda. Dolores Muñoz Ing. Johnny Larrea **Estudiantes:** Srta. Kimberly Delgado Srta. Evelyn Delgado Sr. Adrián Castillo Sr. Ricardo Peláez Srta. Elizabeth Rodríguez Srta. Diana Sánchez	7000												

	*Plataforma web para el seguimiento y control de las políticas. *Plan de Sensibilización.														

FORMULARIO PARA PRESENTACIÓN DE GRUPOS DE INVESTIGACIÓN.

1. **CARRERA:**
Nombre de la carrera proponente del grupo de investigación.

Ingeniería En Sistemas

2. **FACULTAD, EXTENSIÓN, CAMPUS:**
Nombre de la Facultad proponente del grupo de investigación.

Facultad De Ciencias Informáticas

3. **NOMBRE DEL GRUPO DE INVESTIGACIÓN** (Máximo 100 caracteres que caracterice lo esencial del contenido de las tareas del grupo).

Seguridad Informática

4. **LÍDER DEL GRUPO DE INVESTIGACIÓN** (deberán tener prioritariamente el título de 4to nivel en el área de conocimiento de la temática de estudio).

Mg. Denise Soraya Vera Navarrete.

5. **PROFESORES DEL GRUPO DE INVESTIGACIÓN**.

- Denise Soraya Vera Navarrete (Líder)
- José Antonio Bazurto Roldan (Co-Líder)
- Alex Santamaría Philco
- Dolores Muñoz Verduga
- Homero Mendoza Rodríguez
- Johnny Larrea Plúa
- Marco Ayoví Ramírez
- Mike Machuca Avalos
- Oscar González López
- Patricia Quiroz Palma
- Viviana García Macías
- Walther García Vélez
- Willian Zamora Mero

Facultad de Ciencias Administrativas

- Gonzalo Farfán
- Cesar Diomedes Moreira

Facultad de Contabilidad Pública y Auditoría

- Luis Simón Cedeño

- Sayonara Reyna

Universidades Nacionales

- Mg. Albert Espinal (ESPOL)
- Mg. Karina Astudillo (ESPOL)
- Ing. Edison Simbaña (EPN)
- Dr. Ramiro García (FLACSO)
- Ing. Ernesto Pérez Estévez (REDCEDIA)
- Mg. Alberto Balda (USGP)
- Mg. Luis Oyarzun (UTM)

Universidades Internacionales

- Dr. Ernesto Cuadros (Perú)
- Dra. Regina Ticona (Francia)
- Dr. Vladimir Cobarrubias (Chile)

6. **ESTUDIANTES DEL GRUPO DE INVESTIGACIÓN**.

- Elizabeth Rodríguez (10mo. Semestre)
- Diana Sánchez (10mo. Semestre)
- Kimberly Delgado (10mo. Semestre)
- Kerly Delgado (10mo. Semestre)
- Ariosto Muentes (10mo. Semestre)
- Yuleika Delgado (10mo. Semestre)
- Ricardo Peláez (10mo. Semestre)
- Adrián Castillo (10mo. Semestre)
- Evelyn Delgado (10mo. Semestre)
- María José Guerrero (10mo. Semestre)
- Michael Flores (10mo. Semestre)

7. **DESCRIPCIÓN DEL GRUPO DE INVESTIGACIÓN: PROBLEMÁTICA LOCAL O REGIONAL DE ESTUDIO.** Debe estar alineado al proyecto, programa y línea de investigación de la Universidad.

Grupo de profesionales con conocimientos técnicos de seguridad informática.