VICERRECTORADO DE INVESTIGACIÓN INNOVACIÓN Y TRANSFERENCIA TECNOLÓGICA

DIRECCIÓN DE POSTRAGOS

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE MAGÍSTER EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS DE TECNOLOGÍA

TEMA: EVALUACIÓN TECNICA DE LA SEGURIDAD DE INFORMACIÓN DE LA UNIVERSIDAD DE LA FUERZAS ARMADAS ESPE SEDE PRINCIPAL

AUTOR: CAJAMARCA PAUL, GUANOTASIG DIEGO

DIRECTOR: ING. NANCY VELASQUEZ, MSc

SANGOLQUI

2015

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLÓGICA
CENTRO DE POSGRADO
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRIA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

CERTIFICADO DE CUMPLIMIENTO DE LA TESIS.

Sangolquí, 18/05/2015

Señor
Ing. Ruben Arroyo
COORDINADOR DE LA MAESTRIA
Presente.-

Yo, Nancy Guadalupe Velásquez Villagrán, Directora de Tesis, certifico que los mencionados maestrantes los Ing. Fredy Paul Cajamarca Llive y Diego Armando Guanotasig Chiluisa, egresados del Programa de Maestría Evaluación y Auditoria de Sistemas de Tecnología, V Promoción, han presentado la tesis Titulada Evaluación Técnica de la seguridad de la información de la Universidad ESPE Sede Principal – Quito", la misma que ha sido revisada en su totalidad en forma y fondo, la cual reúne las condiciones de calidad para ser presentado en la defensa y el empastado entregado a biblioteca, por lo que solicito se digne disponer el trámite correspondiente.

El presente trabajo es fruto de su investigación, el cual ha sido orientado durante su ejecución por los suscritos.

Atentamente.-

.....

DOCENTE DIRECTOR DE TESIS

Ing. Velásquez Villagrán Nancy Guadalupe, MSc.

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLÓGICA
CENTRO DE POSGRADO
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE MAESTRIA EN EVALUACIÓN Y AUDITORIA DE SISTEMAS TECNOLÓGICOS

CERTIFICADO DE CUMPLIMIENTO DE LA TESIS.

Sangolquí, 18/05/2015

Señor
Ing. Ruben Arroyo
COORDINADOR DE LA MAESTRIA
Presente.-

Yo, Carlos Oswaldo Caizaguano Chimbo, Oponente de Tesis, certifico que los mencionados maestrantes los Ing. Fredy Paul Cajamarca Llive y Diego Armando Guanotasig Chiluisa, egresados del Programa de Maestría Evaluación y Auditoria de Sistemas de Tecnología, V Promoción, han presentado la tesis Titulada "Evaluación Técnica de la seguridad de la información de la Universidad ESPE Sede Principal – Quito", la misma que ha sido revisado en su totalidad en forma y fondo, la cual reúne las condiciones de calidad para ser presentado en la defensa y el empastado entregado a biblioteca, por lo que solicito se digne disponer el trámite correspondiente.

El presente trabajo es fruto de su investigación, el cual ha sido orientado durante su ejecución por los suscritos.

Atentamente.-

.....

OPONENTE DE TESIS

Ing. Caizaguano Chimbo Carlos Oswaldo

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLÓGICA
CENTRO DE POSGRADO
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

DECLARACIÓN DE RESPONSABILIDAD

Nosotros, Fredy Paul Cajamarca Llive y Diego Armando Guanotasig Chiluisa

Declaramos que

El proyecto de maestría denominado "**Evaluación Técnica de la seguridad de la información de la Universidad ESPE Sede Principal – Quito**", ha sido realiza en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en el trabajo correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

En virtud de esta declaración nos responsabilizamos del contenido, veracidad y alcance científico del proyecto de maestría en mención.

Sangolquí, Mayo del 2015

Ing. Fredy Paul Cajamarca Llive

Ing. Diego Armando Guanotasig Chiluisa

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y TRANSFERENCIA DE TECNOLÓGICA
CENTRO DE POSGRADO
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

AUTORIZACIÓN DE PUBLICACIÓN

Nosotros, Fredy Paul Cajamarca Llive y Diego Armando Guanotasig Chiluisa

Autorizamos a la Universidad de las fuerzas armadas ESPE la publicación, en la biblioteca virtual de la institución, del trabajo "**Evaluación Técnica de la seguridad de la información de la Universidad ESPE Sede Principal – Quito**", cuyo contenido, ideas y criterio son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, 18 de Mayo del 2015

Ing. Fredy Paul Cajamarca Llive

Ing. Diego Armando Guanotasig Chiluisa

AGRADECIMIENTO

A mi familia por siempre brindarme su sabiduría confianza y el apoyo en todo momento.

A las autoridades de la Universidad de las Fuerzas Armadas que apoyaron en la consecución del presente proyecto desde el inicio.

A Dios, por permitirme alcanzar una meta más en este largo camino llamado vida.

Ing. Fredy Paul Cajamarca Llive.

Al personal que conforma el área de postgrados de la Universidad de las Fuerzas Armadas ESPE, que nos supieron guiar con su experiencia para la finalización de este documento.

A Dios, por brindarnos la fortaleza en momentos complicados en el desarrollo de este documento, por darnos la sabiduría para tomar las decisiones correctas con mi compañero/amigo Paúl que ha sido un apoyo fundamental en la consecución de este objetivo.

Ing. Diego Armando Guanotasig Chiluisa.

DEDICATORIA

Dedico todo este trabajo realizado a mi familia, a mi padre Hugo Cajamarca que aunque no lo tenga físicamente sus enseñanzas me han permitido salir adelante y alcanzar metas.

Una dedicatoria especial a mi madre María Elena Llive cuyo cariño, templanza, coraje y fuerza las he asimilado como ejemplo para mi vida.

Ing. Fredy Paul Cajamarca Llive

A todas las personas que pasaron en este proceso con sus enseñanzas, su paciencia, su dedicación, su motivación, de manera especial para mis padres y hermano que siempre han sido un pilar fundamental en cada meta que me he propuesto.

Ing. Diego Armando Guanotasig Chiluisa.

INDICE DE CONTENIDO

CAPITULO IV

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

El presente trabajo contempla la evaluación del sistema de seguridad de información de la universidad de las fuerzas armadas ESPE sede principal, como apoyo a los proyectos que la universidad actualmente se encuentra ejecutando. La seguridad de información es impulsada por entidades como la ISO (International Standard Organization) e ISACA (Information Systems Audit and Control Association) las cuales han publicado estándares y marcos de referencia para implementarse en organizaciones que requieren mejorar su nivel de seguridad y emprender acciones de mejora. Así, como actividad inicial en el camino de mejoramiento, en la universidad se realiza el presente trabajo utilizando los marcos de referencia COBIT 5, ISO/IEC 27001:2013 e ISO/IEC 27002:2013. Adaptar los actuales procesos de la universidad con estos marcos de referencia ayudará a mejorar dichos procesos, y permitirá que la seguridad de la información sea tratada como un concepto esencial y parte integral de sus actividades diarias. Aspectos organizacionales de seguridad de la información, el personal interno, los procesos y la tecnología constituyen el enfoque de la presente evaluación, considerando nivel estratégico (nivel de gobierno) y gerencial (nivel de gestión). Se describen los hallazgos encontrados en el análisis y finalmente las conclusiones y recomendaciones que la universidad debe aplicar para elevar el nivel de seguridad e implementar la Gestión de Seguridad de la Información. La presente evaluación pretende ser un paso más para apoyar a la universidad en su misión y objetivos estratégicos.

PALABRAS CLAVES:

- **SEGURIDAD DE INFORMACION**
- **ISACA**
- **COBIT 5**
- **ISO 27001:2013 E ISO 27002:2013**
- **NIVEL DE GOBIERNO Y NIVEL DE GESTION**

ABSTRACT

The current document contemplates the Evaluation of System of Information Security System that belongs to Army University, ESPE, headquarters, as support the projects currently university is executing. Information Security is boosted by entities like ISO (International Standard Organization) and ISACA (Information Systems Audit and Control Association) which have published standards and frameworks to implement them in organizations that require to improve the information security for executing improvement actions. So, as initial activity in the way of improvement, in the university is done this current work using the frameworks COBIT5, ISO/IEC 27001:2013 and ISO/IEC 27002:2013. Adapting the current processes of the university with these frameworks is going to support the improvement of these processes and procedures and is going to permit the security information is treated like an essential concept, and as integral part of their daily activities. Organizations aspects of information security, staff, processes and technology constituted the focusing of this evaluation, considering a strategic level (government level) and managerial level (management level). Also are described the findings detected in the analysis and finally the conclusions and recommendations university must apply to increase the security level and to implement the Information Security Management. This evaluation pretends to be a one more step for supplying university in its mission and strategic objectives.

KEY WORDS:

- **INFORMATION SECURITY**
- **ISACA**
- **COBIT 5**
- **ISO 27001:2013 e ISO 27002:2013**
- **GOVERNMENT LEVEL AND MANAGEMENT LEVEL.**

CAPITULO I

ANTECEDENTES Y SITUACIÓN ACTUAL DE LA SEGURIDAD DE INFORMACIÓN EN LA ESPE

1.1 Antecedentes

Según (Ron, 2014), en el **Proyecto para realizar Evaluación Técnica Informática de la Universidad de las Fuerzas Armadas ESPE** se indica:

- La Universidad de las Fuerzas Armadas ESPE, desde hace algunos años, ha venido ejecutando varios proyectos relacionados con el área informática, con el objeto de apoyar a las diferentes actividades que desarrolla la Universidad.
- Se han implementado algunos servicios informáticos y otros se encuentran en desarrollo, para lo que se han adquirido equipos, instalado redes y contratado otros servicios adicionales.
- La Universidad de las Fuerzas Armadas ESPE, como una Institución Educativa de prestigio que brinda servicios académicos de alta calidad, cuenta con una Unidad de Tecnología de Información y Comunicación (UTIC) que centraliza la administración y gestión de las actividades de TI, es decir se encarga del análisis, desarrollo e implantación de los sistemas requeridos en la ESPE y se preocupa por el adecuado funcionamiento de las aplicaciones existentes, de las redes y las comunicaciones. Adicional brinda soporte a los usuarios finales y ejecuta proyectos de implementación de soluciones tecnológicas encaminados a automatizar los procesos de la ESPE.
- Cada proyecto ha sido ejecutado para cumplir con requerimientos necesarios y brindar mejores herramientas TI a los clientes internos.

Por su importancia, la seguridad de la información ha sido considerada en los planes y proyectos que se ejecutan en la universidad, para mejorar el esquema ya existente.

1.2 Justificación e importancia

Estado del arte a nivel mundial y local

Conforme la tecnología ha avanzado en los últimos años, los sistemas de información y comunicación se han convertido en un elemento muy importante en las instituciones y empresas. La información que años atrás era registrada y custodiada en elementos físicos como hojas de papel, los cuales conformaban expedientes o carpetas, han sido reemplazados por el registro electrónico de dicha información en bases de datos, a través de sistemas y aplicaciones que operan sobre elementos de hardware, como servidores, con sus respectivos dispositivos de almacenamiento y transmitidos mediante equipos de comunicación e interconectados a nivel mundial.

Cada organización otorga diferente importancia a la información; para la ESPE la información es considerada como un activo sensible. Considerando su misión de formar estudiantes que sean responsables con el país, ser una institución que promueve la investigación, ser un organismo que ofrece empleo a docentes, gestiona información de varios tipos con su debida importancia. Por ejemplo, las notas debidamente registradas constituyen los títulos profesionales que acreditan a los estudiantes el ejercicio de su vida profesional. Los documentos formales, tesis, trabajos de investigación, publicados en el portal web y aula virtual constituyen un patrimonio de la universidad a nivel de investigación. El rol de pagos de los docentes conlleva información salarial, de compensaciones (de ser el caso) y a la vez los procesos de cumplimiento de las remuneraciones ligados a los contratos del personal.

Por ello es importante la clasificación de los activos de información y la administración de su seguridad a través de procedimientos de control de acceso que comprenden creación, modificación y eliminación de usuarios con acceso a la información para funcionarios de la universidad de acuerdo con el cargo (roles y responsabilidades) que desempeñan. A su vez que cada funcionario posee un perfil para acceder a un determinado tipo de información, con el propósito es brindar seguridad a la misma.

El principal objetivo de la ESPE es implementar la seguridad de información para su protección y a su vez para garantizar:

- Autenticación: Acceso a los sistemas de información solo por las personas autorizadas.
- Confidencialidad: Solo usuarios autorizados pueden acceder a determinado tipo de información.
- Disponibilidad: Que se tenga acceso a la información el momento que se requiera.
- Integridad: Mantener la información tal como fue ingresada/generada. Su modificación será posible con la respectiva autorización.

Con la finalidad de estar preparado para prevenir incidentes de seguridad de la información.

Un evento en la seguridad en la información puede pasar en cualquier momento. Continuamente se ha visto que la información, en especial la considerada sensible, puede ser sujeta a ataques de Intrusos Informáticos, los cuales intentan obtenerla de manera fraudulenta para beneficio individual o de otros. En cualquier caso, directa o indirectamente, dicha intromisión causará impacto sobre las personas y sobre las organizaciones.

En una empresa pueden existir diferentes sistemas y aplicaciones informáticas que pueden ser el blanco de ataques informáticos y vulnerar su seguridad. Lo principal es determinar el proceso crítico y realizar un análisis de riesgos para determinar los controles de seguridad a aplicar, estableciendo prioridades.

Como lo menciona (Muñoz & Ulloa, 2011): Las empresas y los gobiernos dependen hoy en día de las tecnologías de información (TI) para su funcionamiento y desarrollo. Hacen enormes esfuerzos e inversiones en TI con el objetivo de ser más eficientes, más seguras, cumplir con su misión y con los aspectos claves de su planeación estratégica.

Las empresas han tomado medidas de control elaborando esquemas de seguridad basados en experiencias y hábitos profesionales de sus funcionarios. Adicional han ido apareciendo estándares, métodos, protocolos, reglas, herramientas, leyes y marcos de referencia como COBIT 5, ISO 27001:2013, ISO 27002:2013, trabajos realizados por entidades y colaboradores a nivel mundial para:

- Ejecutar proyectos en materia de seguridad de la información y,
- Para minimizar la ocurrencia de un evento en la Seguridad de la Información.

Asimismo en cada país se han publicado legislaciones para regular la seguridad de la información y para sancionar a los implicados en un evento de seguridad. Ecuador no ha sido la excepción y actualmente existe artículos en el Código de Procedimiento Penal y en el Código Penal los cuales definen claramente un delito y las sanciones respectivas. Se considera que queda mucho por hacer respecto a este tema principalmente por el continuo avance de la tecnología y las herramientas de software que se difunden en la red global

internet, que facilitan a los intrusos informáticos vulnerar la seguridad de la información.

Actualmente en Ecuador se está avanzando en el uso de los estándares citados para proveer una efectiva seguridad a la información, recurso calificado como patrimonio de una organización. Pero conforme avanza la tecnología, también aparecen nuevas vulnerabilidades lo que implica realizar revisiones continuas en una infraestructura existente.

En seguridad de la información cualquier nuevo aporte es considerado como mejora en beneficio de las instituciones.

1.3 Planteamiento del problema

La Universidad de las Fuerzas Armadas, ESPE, por ser una institución de educación superior posee información sensible que debe ser custodiada y asegurada con el mayor rigor mediante el uso de sistemas y aplicaciones que garanticen su confidencialidad, integridad y disponibilidad. Una intromisión o mal manejo de esta información podría resultar en un problema muy grave a nivel institucional tanto para la ESPE como para sus funcionarios, estudiantes y todas las personas en su entorno.

Por ejemplo, el historial académico de un estudiante determina si éste ha aprobado sus materias en un determinado período. Si esa información es modificada injustificadamente generaría inconsistencias de datos en los sistemas y aplicaciones y por supuesto malestar y problemas al estudiante. El rol de pagos de un docente de la universidad contiene información de su salario y del pago realizado. Cualquier modificación de esa información provocará una molestia al funcionario y por supuesto le ocasionará inconvenientes. Ambos casos son muy probables si la seguridad de información no es debidamente gestionada.

Por tanto es indispensable verificar y asegurar procedimientos internos ya existentes, mediante la aplicación de controles de seguridad, su mejora si es necesario y concatenarlos con las herramientas de tecnología, aplicativos, y sistemas. La evaluación técnica de la seguridad de la información de la ESPE sede principal pretende cubrir y cumplir con lo indicado en beneficio de la institución.

1.4 Formulación del problema a resolver

En el Ecuador muchas instituciones del sector público y privado, conscientes de la importancia, regulan sus procedimientos de gestión de la información basada en estándares y marcos de referencia, utilizándolos de manera estricta. Asimismo utilizan herramientas de hardware y software como su complemento para permitir que los controles antes mencionados puedan ser ejecutados e integrados con procedimientos generales.

El presente trabajo pretende realizar una evaluación sobre la seguridad de la información considerando lo siguiente:

- En la actualidad, son los procedimientos utilizados por la ESPE en el manejo de la seguridad de la información los más adecuados acordes a estándares y marcos de referencia usados a nivel nacional y mundial?
- Es conocido el nivel de riesgo de los activos de información del Macroproceso de la Universidad de las Fuerzas Armadas ESPE?
- Se cumplen los procedimientos de seguridad de la información existentes en la ESPE? Cuál es el impacto de no cumplimiento?
- Están identificados los responsables de la seguridad de la información para garantizar su correcta gestión?,

- Los roles y responsabilidades están acorde a cada uno de sus responsables?

1.5 Objetivo General

Realizar la evaluación técnica de la seguridad del sistema de información de la ESPE Sede Principal, alineado al estándar COBIT 5, ISO/IEC 27001:2013 e ISO/IEC 27002:2013, con la finalidad de identificar debilidades y emitir recomendaciones que permitan minimizar los riesgos.

1.6 Objetivos Específicos

- Establecer el nivel de cumplimiento de los procedimientos formales de la ESPE en comparación con los lineamientos del marco de referencia COBIT 5 y de las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013.
- Ejecutar la Evaluación Técnica de la Seguridad de la Información de la ESPE.

1.7 Actividades

- Investigar el marco de referencia COBIT 5 y las normas ISO/EC 27001:2013, ISO 27002:2013.
- Levantar información tanto de los procedimientos formales de la seguridad de la información, así como del hardware y software que soportan los procedimientos en materia de seguridad de la información.
- Revisar y analizar los procedimientos formales obtenidos en el levantamiento de la información de la ESPE según el marco de referencia COBIT 5 y las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013.

- Elaborar el informe de evaluación con toda la información recopilada y las acciones indicadas en los objetivos precedentes.
- Definir la hoja de ruta para establecer el SGSI en la ESPE
- Emitir conclusiones y recomendaciones.

CAPITULO II

MARCO TEORICO, METODOLOGIAS ISO/IEC 27001:2013, ISO/IEC 27002:2013, COBIT 5

La presente evaluación será realizada basado en los marcos de referencia COBIT 5, ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

2.1 ISO/IEC 27001:2013, ISO/IEC 27002:2013

La Norma ISO/IEC 27001:2013 detalla un modelo para gestionar los sistemas de gestión de seguridad de la información (SGSI) mediante un enfoque del proceso para establecer, implementar, monitorear, operar, revisar, mantener y mejorar dicho SGSI en una organización.

Como lo menciona la (ISO, 2014), la última edición, 2013, no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua.

Así mismo la versión ISO/IEC 27001:2013 toma muchos lineamientos de su predecesor, la versión 2005. La Figura 1 muestra un diagrama de relación de la reorganización de las cláusulas principales de la versión 2005 a la publicada en 2013. Tomado de (ISO, 2014).

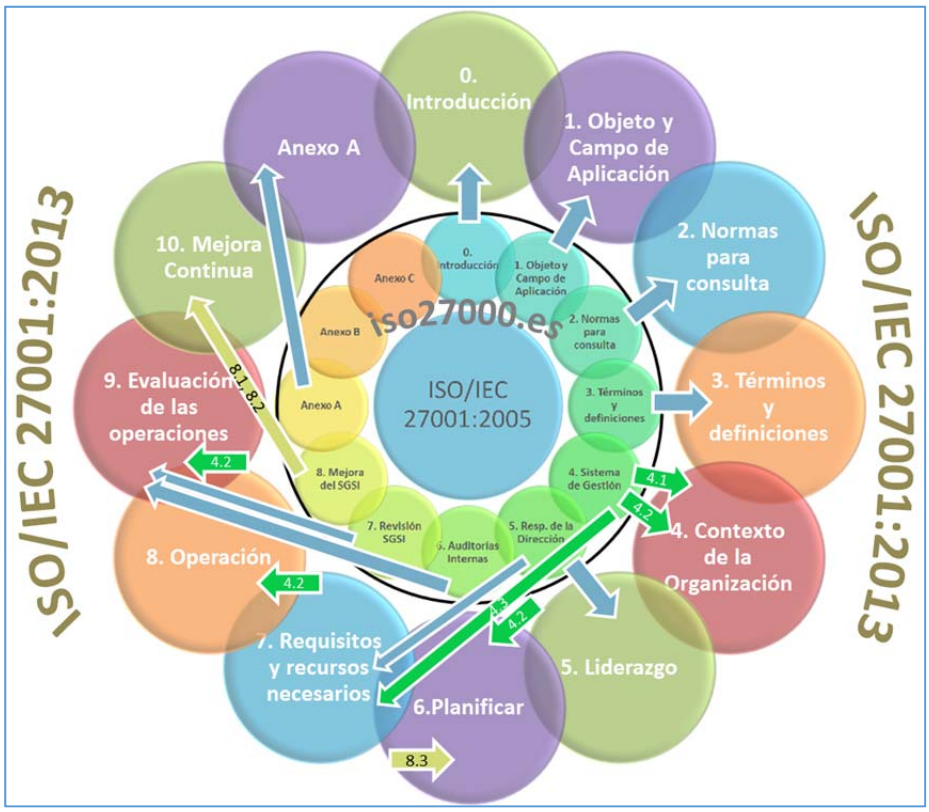


Figura 1. Diagrama de relación de la reorganización de las cláusulas principales de la versión 2005 a la publicada en 2013, Tomado de (ISO, 2014).

Adicional, (Miranda, 2014) menciona en su publicación: *Mapeo de controles del Anexo A ISO 27001:2013, Comparación con ISO 27001:2005* que en dicho Anexo A de la ISO/IEC 27001:2013 hay una lista de controles que permanecen, otras que se han reubicado y finalmente aquellos controles que se han retirado, teniendo en cuenta que el Anexo A de ISO/IEC 27001 enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO/IEC 27002. A continuación se registra el mapeo de algunos controles en relación a las ediciones 2013 y 2005.

27001:2013	27001:2005
A.5 Orientación de la Dirección para la seguridad de la información	**A.5 Política de seguridad**
A.5.1 Directrices de Gestión para la Seguridad de la Información *Objetivo:* Proporcionar orientación y apoyo de la Dirección para la seguridad de la información, en concordancia con los requisitos del negocio, las leyes y las regulaciones pertinentes.	
A.5.1.1 Políticas de seguridad de la información	A.5.1.1 Documento de política de seguridad de la información
A.5.1.2 Revisión de las políticas de seguridad de la información	A.5.1.2 Revisión de la política de seguridad de la información
A.6 Organización de seguridad de la información	**A.6 Organización de seguridad de la información**
A.6.1 Organización Interna *Objetivo:* Establecer un marco de trabajo de la Dirección para iniciar y controlar la implementación y el funcionamiento de la seguridad de la información dentro de la organización.	
A.6.1.1 Responsabilidades y roles de seguridad información	A.6.1.3 Asignación de responsabilidades para la seguridad de información
A.6.1.2 Segregación de funciones	A.10.1.3 Segregación de tareas
A.6.1.3 Contacto con autoridades	A.6.1.6 Contacto con autoridades
A.6.1.4 Contacto con grupos de interés especial	A.6.1.7 Contacto con grupos de interés especial
A.6.1.4 Seguridad de la información en la gestión de proyectos (**NUEVO**)	
A.6.2 Dispositivos móviles y teletrabajo *Objetivo:* Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles	
A.6.2.1 Política de dispositivo móvil	A.11.7.1 Ordenadores portátiles y comunicaciones móviles
A.6.2.2 Teletrabajo	A.11.7.2 Teletrabajo

Figura 2. Mapeo de controles en relación a las ediciones 2013 y 2005. Tomado de (Miranda, 2014), publicación: Mapeo de controles del Anexo A ISO 27001:2013.

Finalmente se debe tener en cuenta la publicación de la (ISO, 2014), en su sección certificaciones menciona:

2.1.1 Certificaciones ya Emitidas

Para organizaciones ya certificadas en el momento de la publicación de ISO/IEC 27001:2013 pueden mantener sus auditorías periódicas de seguimiento en la versión de 2005 hasta un período orientativo máximo de 24 meses, aunque siempre se debe preguntar a su entidad de certificación sobre los plazos concretos establecidos para efectuar la migración.

2.1.2 Certificaciones iniciales

Para las organizaciones que tengan previsto certificarse en ISO/IEC 27001 después de la publicación de ISO/IEC 27001:2013 podrán pasar su auditoría inicial de certificación en la versión del 2005 sin problemas y durante un período máximo orientativo de 12 meses (confirmar con la entidad de certificación elegida) desde la publicación de la nueva norma (hasta Octubre 2014). Después de Octubre 2014, sólo se podrán desarrollar auditorías iniciales de certificación según ISO/IEC 27001:2013.

2.2 COBIT 5

Como lo indica (ISACA, COBIT 5 AN ISACA FRAMEWORK, 2012), COBIT 5 provee un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando completamente al negocio de principio a fin y las áreas funcionales de responsabilidad de T, considerando los intereses relacionados con TI de las partes interesadas internas y externas.

COBIT 5 divide procesos de gobierno y de gestión de la TI empresarial conformando en total 37 procesos, 5 procesos de gobierno y 32 de gestión, distribuidos de la siguiente manera:

Gobierno, dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión (EDM)

Gestión, contiene 4 dominios, relacionados con las áreas de responsabilidad de:

- Alinear, Planificar y Organizar (Align, Plan and Organise, APO)
- Construir, Adquirir e Implementar (Build, Acquire and Implement, BAI)
- Entregar, dar servicio y soporte (Deliver, Service and Support, DSS)
- Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, MEA).

La Figura 3 muestra el conjunto completo de los 37 procesos de gobierno y de gestión. Tomado de (ISACA, COBIT 5 AN ISACA FRAMEWORK, 2012).

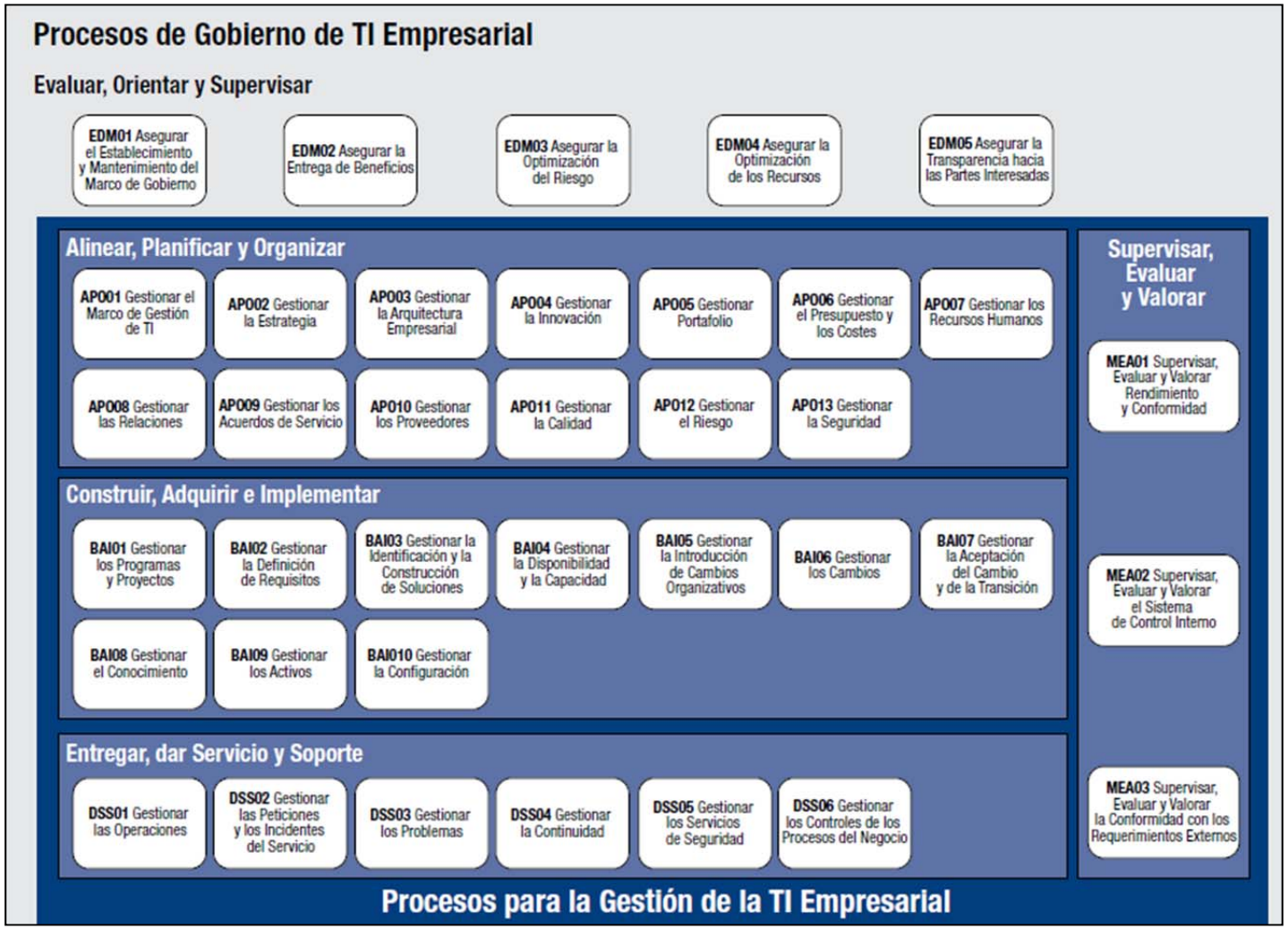


Figura 3. Procesos COBIT de gobierno y gestión. Tomado de (ISACA, COBIT 5 AN ISACA FRAMEWORK, 2012)

2.3 Marco conceptual

2.3.1 Gobierno de TI

El Gobierno de TI es un conjunto de acciones que el área de TI realiza en conjunto con la alta gerencia para habilitar a la organización con las herramientas necesarias para la toma de decisiones óptimas respecto a la realización de inversiones en tecnología considerando la dirección, requerimientos del negocio y su comportamiento financiero.

2.3.2 Análisis y evaluación de riesgos

Es la actividad de identificar eventos que podrían afectar a la organización, los daños potenciales que puedan ocasionar tales eventos, y las medidas preventivas (controles) que deben mitigar las probabilidades de que estos eventos ocurran.

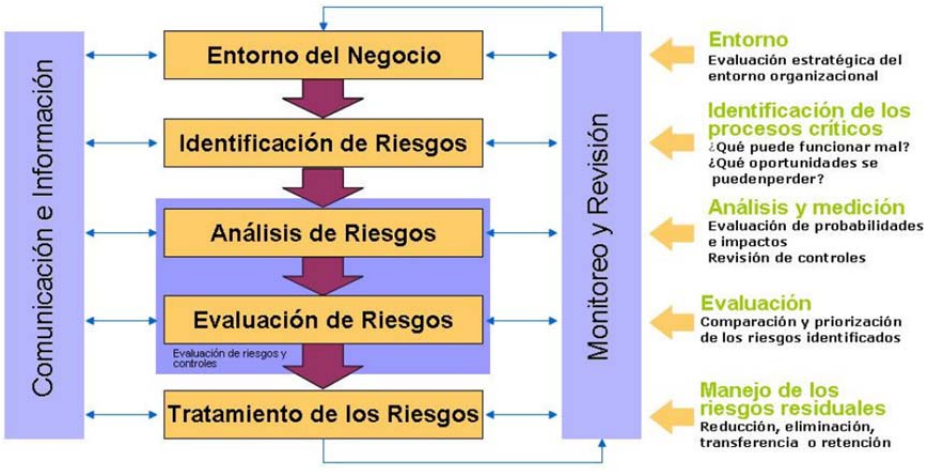


Figura 4. Grafico conceptual de Análisis de Riesgos

2.3.3 COBIT 5

COBIT 5 es el marco de gestión y de negocio global para gestión de las TI y del gobierno de la organización.

COBIT 5 proporciona herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y riesgos del negocio y permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización. Como lo indica (ISACA, COBIT 5 AN ISACA FRAMEWORK, 2012), COBIT 5 realiza una clara distinción entre gobierno y gestión. Estas 2 disciplinas engloban diferentes tipos de actividades, requieren estructuras organizativas diferentes y sirven para diferentes propósitos. La principal distinción entre ellas es:

- El Gobierno asegura que se evalúen las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcancen las metas corporativas equilibradas y acordadas, estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y cumplimiento respecto a la dirección y a las metas acordadas.
- La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.

El objetivo de gobierno es la creación de valor en la organización lo cual significa obtener beneficios mediante la optimización del riesgo y la optimización de recursos.

Asimismo (ISACA, COBIT 5 AN ISACA FRAMEWORK, 2012) presenta la cascada de metas u objetivos, mostrado en la Figura 5. En ella se puede apreciar como las necesidades de las partes interesadas concluyen en los

objetivos de los catalizadores, que no son otra cosa que los procesos formales de COBIT 5.

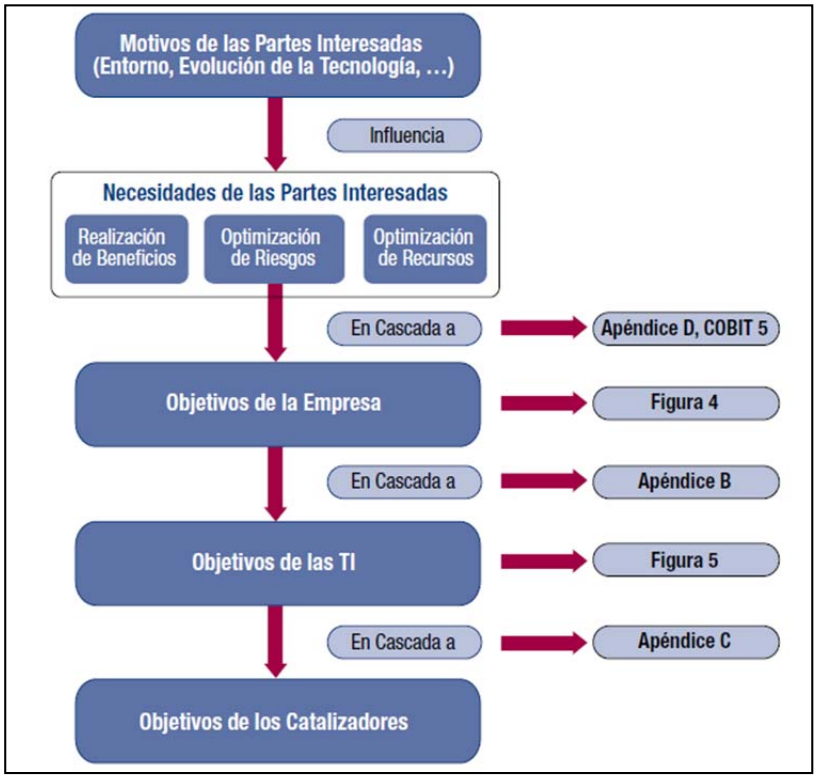


Figura 5. Cascada de Metas u objetivos de COBIT 5. Tomado de (ISACA, COBIT 5 AN ISACA FRAMEWORK, 2012)

En el presente trabajo, el análisis que se realiza será basado en la Cascada de Objetivos COBIT 5 indicada.

2.3.4 ISO/IEC 27001:2013

ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar mantener y mejorar continuamente un Sistema de Gestión de la Seguridad de la Información SGSI, dentro del contexto de la organización. Además incluye los requerimientos para la evaluación y tratamiento de los riesgos de la seguridad de la información adoptados a las necesidades de la

empresa. Los requerimientos en ISO/IEC 27001:2013 se exponen como genéricos para que sean aplicables a todas las organizaciones, sin importar el tipo, tamaño o naturaleza.

2.4 Estado del arte

Las organizaciones a nivel mundial han ido adoptando estándares y modelos de referencia existentes como COBIT 5, ISO/IEC 27001:2013 e ISO/IEC 27002:2013 dentro de sus procesos y procedimientos con el fin de garantizar la seguridad en los sistemas de información.

Según (ISACA, 2014), el HDFC Bank (con 3042 sucursales y 10743 cajeros) han priorizado su compromiso con la tecnología e internet como unos de sus responsabilidades más importantes, mediante COBIT, inicialmente con COBIT 4.1 y en este año con la migración a COBIT 5, en los procesos de la entidad. De igual forma, en casos meritorios y de acuerdo al artículo, HDFC Bank ha cruzado a COBIT con ISO 27001 en un documento de política integral.

Así mismo, de acuerdo al mismo artículo, GlaxoSmithKline (GSK, empresa que desarrolla productos farmacéuticos para tratar una variedad de afecciones incluyendo enfermedades respiratorias, cáncer, etc, con presencia en más de 115 países), la cual depende ampliamente de la TI, está iniciando su transición a COBIT 5, específicamente en su gestión del soporte de TI.

Por otro lado la integración de normas y/o estándares facilita la aplicación de procedimientos adecuados. Según (GOVERNANCE INSTITUTE IT, 2008), las mejores prácticas adoptadas e implementadas deben ser compatibles con un marco de control de riesgos y control idóneo para la organización, integrándolas con métodos y prácticas vigentes.

El mismo artículo indica que el proceso COBIT para la gestión de riesgo y la aplicación de marco de control y los criterios de información ayudarán a asegurar en la identificación y asignación de los riesgos, y la norma ISO/IEC 27002 clarifica los riesgos de seguridad de la siguiente manera:

En apoyo a la gobernabilidad:

- Proporcionar políticas de gestión y marcos de control.
- Asignación de roles y responsabilidades claras con la asignación de recursos respectiva.
- Asegurar la identificación de riesgos significativos.
- Alinear objetivos TI con objetivos del negocio.

Definición de requisitos de los servicios y definiciones del proyecto

- Establecimiento de objetivos claros de TI y sus métricas relacionadas al negocio.
- Definición de servicios y proyectos en términos del usuario final.
- Elaborar y monitorear acuerdos de niveles de servicios.

Verificar capacidad profesional y demostrar competencia.

- Mediante evaluaciones y auditorias independientes de terceros.
- Compromisos contractuales.
- Constancias y certificaciones.

Para entregar mejora continua

- Evaluaciones de madurez.

- Análisis de brechas.
- Planificación de la mejora.

Como marco para la auditoria, evaluación y una visión externa.

- Criterios objetivos y entendidos.
- Brenchmarking para justificar las debilidades.

También podemos indicar que a nivel mundial las empresas han incrementado su disposición para acceder a las certificaciones ISO 27001 como demostración de interés hacia la protección de la información. Como lo indica (ISO, 2012) a través de la Tabla 1, en los últimos años las certificaciones han ido en aumento en sectores de la industria. Tecnología de información se ubica en primer lugar, claro indicador que permite justificar el presente trabajo.

Tabla 1.

Sectores de la industria certificados ISO por año. **Tomado de (ISO, 2012)**

Sectores de la Industria Certificados ISO/IEC 27001		2009	2010	2011	2012
1	Tecnología de Información	2086	3217	3588	4557
2	Otros servicios	380	579	564	755
3	Construcción	127	266	350	411
4	Equipamiento eléctrico y óptico	135	221	280	342
5	Transporte, almacenamiento y comunicación	170	184	241	288

Las universidades del Ecuador como toda institución educativa gestionan información sensible de sus estudiantes, docentes y funcionarios. Se indica en el sitio web (EPN, 2015) de la Escuela Politécnica Nacional que al momento existe el proyecto REDU, Red de universidades para investigación y postgrados, fundada en 2012 e integrada por varias universidades entre ellas la Escuela Politécnica Nacional EPN, Escuela Politécnica del litoral ESPOL,

Pontificia Universidad Católica del Ecuador PUCE, Universidad San Francisco de Quito USFQ, entre otras con el fin de unir esfuerzos en conjunto en investigación y postgrados. Lastimosamente mediante consulta en los sitios web, ni REDU ni tampoco las universidades y escuelas politécnicas hacen mención relacionada a proyectos de seguridad de información ni a acceder a certificaciones de seguridad. Es posible que dichas instituciones se encuentren elaborando o avanzado en proyectos de seguridad de la información pero no se ha encontrado información formal que lo respaldo.

La situación es diferente en empresas de telecomunicaciones. Como lo menciona (PPElVerdadero, 2014), AENOR entregó a CNT EP en el 2014 la certificación ISO 27001:2005. Situación similar ocurre con la empresa Telconet, en cuyo portal web, (Telconet, 2015), menciona su verificación ISO/IEC 27001:2005, mostrando claramente su interés por la información. Claramente esta es una oportunidad de captar clientes y estar a la vanguardia en servicios de data center.

La universidad de las fuerzas armadas ESPE a través del programa de maestría Evaluación y Auditoria de Sistemas de Tecnología, ha permitido a los maestrantes desarrollar temas de tesis relacionadas a la seguridad de la información. Tal es el caso de (Aguirre Freire & Palacios Cruz, 2014), que ejecutaron una evaluación de seguridades del data center del municipio de Quito, basado en la ISO/IEC 27001 y 27002 versión 2005.

Por consiguiente el presente trabajo es un aporte más para mejorar el tema de seguridades en las instituciones.

CAPITULO III

EJECUCION DE LA EVALUACION TECNICA INFORMATICA DE LOS SISTEMAS DE SEGURIDAD DE INFORMACION DE LA ESPE, SEDE PRINCIPAL

3.1 Metodología y Técnicas de investigación

El presente trabajo está basado en la Auditoria por Análisis de Riesgos y las técnicas a utilizar son todas aquellas actividades que derivan de la investigación de campo como son: observación, entrevistas, encuestas, análisis, elaboración de informes.

Adicional la investigación teórica inicial relacionada con los estándares y buenas prácticas a utilizar en correlación con las actividades planteadas en cada capítulo del proyecto.

Asimismo serán utilizadas las matrices COBIT 5 de Metas Corporativas, Metas relacionadas con las TI y procesos COBIT, las mismas que serán mencionadas conforme el avance del análisis.

3.2 Situación Actual de la Universidad de las fuerzas armadas ESPE en relación a seguridad de información.

Para iniciar la presente evaluación se solicitó a la ESPE información formal, documentos aprobados por la universidad respecto a seguridad de la información. Es así que se realizó una solicitud requiriendo a la ESPE documentación que incluya:

- Plan estratégico tecnológico institucional ESPE 2015 o el más actualizado.

- Manual de operación y procedimientos del sistema de gestión de seguridad de información.
- Informes de estado del sistema de gestión de seguridad de información
- Documentación de roles y responsabilidades del personal de seguridad de información
- Documento de acuerdo de niveles de servicio, SLAs, OLAs.
- Manuales de Ética y comportamiento para el personal de tecnología de la ESPE
- Informes de auditoría y evaluaciones periódicas realizadas a la ESPE.
- Documento de plan de seguridad de información
- Documento de plan de capacitación y desarrollo profesional relacionadas a la seguridad de la información y sistemas
- Documento de requerimientos de base de conocimiento relacionado con RRHH para enrolamiento de nuevo personal para el sistema de seguridad de información.
- Manuales de inventarios de configuración y líneas base de dispositivos, herramientas y aplicaciones.
- Documento de inventario de equipamiento, programas y aplicaciones operativas en la ESPE relativos a la seguridad de información
- Planes de concientización respecto al uso y protección de herramientas y aplicaciones de la ESPE
- Documento de análisis de riesgos relacionados al sistema de seguridad de la información de la ESPE
- Documento de gestión de cambios al hardware, programas, herramientas y aplicaciones de la ESPE.
- Documento de inventario de documentos e información sensible en la ESPE
- Manual de gestión de incidentes y problemas relacionados con los sistemas de gestión de seguridad de información.

- Manuales relacionados a la gestión de configuración y cambios del sistema de información en la ESPE.
- Plan de Análisis de Impacto del Negocio y recuperación de desastres de los sistemas de información de la ESPE.

Mediante respuesta enviada por el departamento de UTIC, la ESPE entrega los documentos que se indican a continuación:

- Resultados de encuestas de servicios TICs
- Procesos de Negocio ESPE 2014
- Planificación UTIC 2014
- Plan de Contingencia 2014
- Plan estratégico institucional ESPE 2014-2017
- Plan de desarrollo UTIC 2012-2016
- Plan de capacitación UTIC 2014
- Inventario de Aplicaciones
- Estructura de UTIC 2015
- Contrato Antivirus
- Catálogo de servicios TICs 2014
- Catálogo de proveedores contratados.
- Características técnicas aplicaciones

La entrega formal de los documentos se muestra en el Anexo 1 y los mismos serán citados más adelante en el documento en caso de ser necesario.

3.3 Caracterización actual en la Universidad de las Fuerzas Armadas, ESPE, respecto a seguridad de información.

La Universidad de las Fuerzas Armadas ESPE tiene aprobado y en ejecución (ESPE, 2014), indicado en el Anexo 1, el cual presenta los objetivos

institucionales más significativos para el período en mención, los cuales se indica a continuación:

- Fortalecer las capacidades y potencialidades de la ciudadanía.
- Impulsa la transformación de la matriz productiva.
- Asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica.
- Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas - ESPE como una institución referente en educación superior.
- Incrementar la calidad de los profesionales y postgraduados.
- Incrementar la producción científica - tecnológica y su calidad.
- Incrementar el impacto social de los programas de vinculación.
- Incrementar la eficiencia y eficacia del sistema formativo de grado y postgrado.
- Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.
- Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo.
- Incrementar las capacidades de sustentación institucional. (Talento Humano- Finanzas- Recursos Físicos y Tecnológicos).

3.2.1 Listado de Objetivos Institucionales priorizados con mayor importancia.

La presente evaluación se enfocará en los objetivos más relevantes en relación a la seguridad de la información. Para ello se toma en cuenta la calificación a dar en cada caso de acuerdo a la Tabla 2:

Tabla 2.

Escala de Importancia de Objetivos Institucionales (desde el enfoque de seguridad de información)

Valor	Importancia de Objetivo Institucional
3	Importante
2	Importancia moderada
1	Menos importante

Adicional en la Tabla 3 se considera un intervalo de importancia en relación a enfoque de seguridad de información para determinar la importancia primaria o secundaria de los objetivos.

Tabla 3.

Intervalo de importancia para los Objetivos COBIT 5

Intervalo	Valor
Mayores de 25%	P
Entre 20% y 25%	S

Por tanto se realiza la correlación entre los objetivos institucionales de la Universidad de las Fuerzas Armadas, ESPE con los Objetivos Corporativos formales de COBIT 5, el cual se presenta la Tabla 4. La tabla fue desarrollada mediante el enfoque de seguridad de la información de la Tabla 2.

Posteriormente con el resultado de la Tabla 4, y usando el intervalo de importancia de la Tabla 3, se prioriza a los objetivos corporativos más relevantes para el presente análisis, el mismo que se presenta en la Tabla 5.

Tabla 4.

Objetivos Institucionales ESPE vs Objetivos Corporativos COBIT5

		METAS/OBJETIVOS CORP COBIT 5			
		1. Valor para las partes interés de las inver. de negocio	2. Cartera de producto y servicios competitivos	3. Riesgos de negocio gestión (salvaguarda de activos)	4. Cumplimiento de leyes y regulaciones externas
METAS CORPERATIVAS UNIVERSIDAD DE LAS FUERZAS ARMADAS	Fortalecer las capacidades y potencialidades de la ciudadanía	3	2	1	2
	Impulsar la transformación de la matriz productiva	3	2	2	2
	Asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica.	3	1	3	2
	Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas - ESPE como una institución referente en educación superior	3	2	3	3
	Incrementar la calidad de los profesionales y postgraduados	3	1	1	3
	Incrementar la producción científica - tecnológica y su calidad.	3	2	1	2
	Incrementar el impacto social de los programas de vinculación	3	3	1	2
	Incrementar la eficiencia y eficacia del sistema formativo de grado y postgrado	3	1	2	3
	Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.	3	1	1	2
	Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo	3	2	2	1
	Incrementar las capacidades de sustentación institucional. (Talento Humano Finanzas- Recursos Físicos y Tecnológicos).	3	3	3	1

Continua

		METAS/OBJETIVOS CORPORATIVOS COBIT 5			
		5. Transparencia financiera	6.Cultura de servicio orientada al cliente	7.Continuidad y disponibilidad del servicio de negocio	8.Respuestas ágiles a un entorno de negocio cambiante
METAS CORPERATIVAS UNIVERSIDAD DE LAS FUERZAS ARMADAS	Fortalecer las capacidades y potencialidades de la ciudadanía	1	2	1	2
	Impulsar la transformación de la matriz productiva	1	1	1	2
	Asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica.	1	1	3	2
	Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas - ESPE como una institución referente en educación superior	3	1	3	2
	Incrementar la calidad de los profesionales y postgraduados	1	1	1	2
	Incrementar la producción científica - tecnológica y su calidad.	2	2	1	2
	Incrementar el impacto social de los programas de vinculación	2	3	1	2
	Incrementar la eficiencia y eficacia del sistema formativo de grado y postgrado	2	1	1	2
	Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.	2	2	1	2
	Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo	1	3	2	2
	Incrementar las capacidades de sustentación institucional. (Talento Humano Finanzas- Recursos Físicos y Tecnológicos).	2	3	3	3

Continua

		METAS/OBJETIV CORP COBIT 5			
		9. Toma estratégica de decisiones basadas en info.	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de proceso de negocio	12. Optimización de los costes de los proceso de negocio
METAS CORPERATIVAS UNIVERSIDAD DE LAS FUERZAS ARMADAS	Fortalecer las capacidades y potencialidades de la ciudadanía	2	1	1	1
	Impulsar la transformación de la matriz productiva	3	2	2	2
	Asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica.	3	2	2	2
	Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas - ESPE como una institución referente en educación superior	3	1	2	2
	Incrementar la calidad de los profesionales y postgraduados	1	1	2	2
	Incrementar la producción científica - tecnológica y su calidad.	1	1	2	3
	Incrementar el impacto social de los programas de vinculación	1	2	2	2
	Incrementar la eficiencia y eficacia del sistema formativo de grado y postgrado	2	2	3	2
	Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.	3	2	3	3
	Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo	2	1	2	2
	Incrementar las capacidades de sustentación institucional. (Talento Humano Finanzas-Recursos Físicos y Tecnológicos).	3	3	2	2

Continua

		METAS/OBJETIVOS CORP COBIT 5				
		13. Programas gestionados de cambio en negocio	14. Productiv oper. y de empleados	15. Cumplir. con las políticas internas	16. Personal entrenado/motivado	17. Cultura de innovación del producto y del negocio
METAS CORPERATIVAS UNIVERSIDAD DE LAS FUERZAS ARMADAS	Fortalecer las capacidades y potencialidades de la ciudadanía	2	1	1	1	2
	Impulsar la transformación de la matriz productiva	2	1	2	2	2
	Asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica.	2	2	2	1	2
	Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas - ESPE como una institución referente en educación superior	1	3	3	3	1
	Incrementar la calidad de los profesionales y postgraduados	2	3	3	3	3
	Incrementar la producción científica - tecnológica y su calidad.	2	3	2	3	3
	Incrementar el impacto social de los programas de vinculación	2	2	2	2	3
	Incrementar la eficiencia y eficacia del sistema formativo de grado y postgrado	2	3	3	3	3
	Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.	2	2	2	2	2
	Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo	2	1	2	1	2
	Incrementar las capacidades de sustentación institucional. (Talento Humano Finanzas- Recursos Físicos y Tecnológicos).	2	2	3	3	2

Tabla 5.

Calificación de objetivos corporativos COBIT 5 de acuerdo a intervalo de importancia en Tabla 2

	METAS/OBJETIVOS CORPORATIVOS COBIT 5							
	1. Valor para las partes interesadas de las inversiones de negocio	2. Cartera de productos y servicios competitivos	3. Riesgos de negocio gestionados (salvaguarda de activo)	4. Cumplimiento de leyes y regulaciones externas	5. Transparencia financiera	6. Cultura de servicio orientada al cliente	7. Continuidad y disponibilidad del servicio de negocio	8. Respuestas ágiles a un entorno de negocio cambiante
TOTAL	33	20	20	23	18	20	18	23
PRIORIDAD TOTAL	P			S				S

	METAS/OBJETIVOS CORPORATIVOS COBIT 5				METAS/OBJETIVOS CORPORATIVOS COBIT 5				
	9. Toma estratégica de Decisiones basadas en información	10. Optimización de costes de entrega del servicio	11. Optimización de la funcionalidad de los procesos de negocio	12. Optimización de los costes de los procesos de negocio	13. Programas gestionados de cambio en el negocio	14. Productividad operacional y de los empleados	15. Cumplimiento con las políticas internas	16. Personal entrenado y motivado	17. Cultura de innovación del producto y del negocio
TOTAL	24	18	23	23	21	23	25	24	25
PRIORIDAD TOTAL	P		S	S	S	S	P	P	P

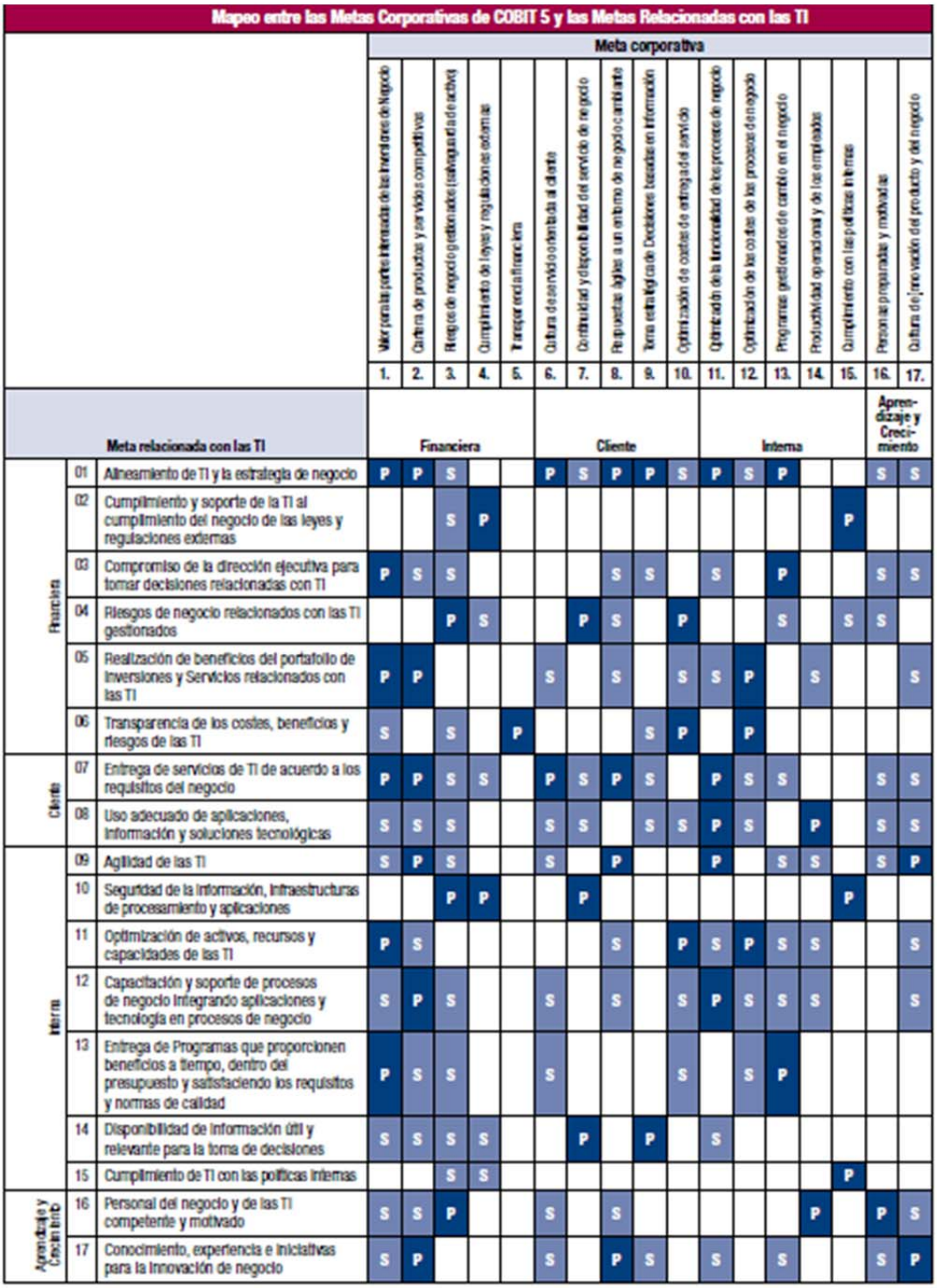
Como resultado del análisis anterior se tiene que los objetivos corporativos a considerar son:

a) Primarios
    - Valor para las partes interesadas de las inversiones del negocio.
    - Toma estratégica de decisiones basadas en información.
    - Cumplimiento con las políticas internas
    - Personal entrenado y motivado.
    - Cultura de innovación del producto y del negocio.

b) Secundarios
    - Cumplimiento de leyes y regulaciones internas.
    - Respuestas ágiles a un entorno de negocio cambiante.
    - Optimización de la funcionalidad de los procesos del negocio.
    - Programas gestionados de cambio en el negocio.
    - Productividad operacional y de los empleados.

3.2.2 Listado de Objetivos de TI priorizados con mayor importancia.

Utilizando (ISACA, COBIT 5 AN ISACA FRAMEWORK, 2012), **Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI COBIT 5**, Figura 6, se realiza un mapeo entre los objetivos institucionales con mayor prioridad de la Universidad de las Fuerzas Armadas ESPE y los Metas u Objetivos de TI formales de COBIT 5.



Mapeo entre las Metas Corporativas de COBIT 5 y las Metas Relacionadas con las TI																				
			Meta corporativa																	
			Valor para las partes interesadas de las inversiones de Negocio	Cartera de productos y servicios competitivos	Riesgos de negocio gestionados (salvaguarda de activos)	Cumplimiento de leyes y regulaciones externas	Transparencia financiera	Cultura de servicio orientada al cliente	Continuidad y disponibilidad del servicio de negocio	Respuestas ágiles a un entorno de negocio cambiante	Toma estratégica basada en información	Optimización de costes de entrega del servicio	Optimización de la funcionalidad de los procesos de negocio	Optimización de los costes de los procesos de negocio	Programas gestionados de cambio en el negocio	Productividad operacional y de los empleados	Cumplimiento con las políticas internas	Personas preparadas y motivadas	Cultura de innovación del producto y del negocio
			1.	2.	3.	4.	5.	6.	7.	8.	9.	10.	11.	12.	13.	14.	15.	16.	17.
		Meta relacionada con las TI	Financiera					Cliente					Interna					Aprendizaje y Crecimiento	
Financiera	01	Alineamiento de TI y la estrategia de negocio	P	P	S			P	S	P	P	S	P	S	P			S	S
	02	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas			S	P											P		
	03	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	P	S	S					S	S		S		P			S	S
	04	Riesgos de negocio relacionados con las TI gestionados			P	S			P	S		P			S		S	S	
	05	Realización de beneficios del portafolio de inversiones y Servicios relacionados con las TI	P	P				S		S		S	S	P		S			S
	06	Transparencia de los costes, beneficios y riesgos de las TI	S		S		P				S	P		P					
Cliente	07	Entrega de servicios de TI de acuerdo a los requisitos del negocio	P	P	S	S		P	S	P	S		P	S	S			S	S
	08	Uso adecuado de aplicaciones, información y soluciones tecnológicas	S	S	S			S	S		S	S	P	S		P		S	S
Interna	09	Agilidad de las TI	S	P	S			S		P			P		S	S		S	P
	10	Seguridad de la información, infraestructuras de procesamiento y aplicaciones			P	P			P								P		
	11	Optimización de activos, recursos y capacidades de las TI	P	S						S		P	S	P	S	S			S
	12	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	S	P	S			S		S		S	P	S	S	S			S
	13	Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	P	S	S			S				S		S	P				
	14	Disponibilidad de información útil y relevante para la toma de decisiones	S	S	S	S			P		P		S						
	15	Cumplimiento de TI con las políticas internas			S	S											P		
Aprendizaje y Crecimiento	16	Personal del negocio y de las TI competente y motivado	S	S	P			S		S						P		P	S
	17	Conocimiento, experiencia e iniciativas para la innovación de negocio	S	P				S		P	S		S		S			S	P

Figura 6. Mapeo entre las Metas/Objetivos Corporativos y las Metas/Objetivos Relacionadas con las TI, COBIT 5. Tomado de (ISACA, COBIT 5 AN ISACA FRAMEWORK, 2012)

El mapeo se realiza tomando en cuanta la Tabla 6 mostrada a continuación.

Tabla 6.

Escala de Importancia de Objetivos de TI

Índice	Valor	Descripción	Importancia de Objetivo de TI
P	**3**	**Principal**	Importante
S	**1**	**Secundario**	Menos Importante

A continuación se determina el porcentaje o peso de cada Objetivo de TI como resultado del mapeo, mostrado en la Tabla 7. Finalmente se califica el valor obtenido de porcentaje de acuerdo a la tabla indicada.

Tabla 7.

Intervalos de Importancia para los Objetivos de TI

Intervalo	Valor
Mayores de 45%	P
Entre 35% y 45%	S

El resultado del Análisis se lo presenta en la Tabla 8.

Tabla 8

Mapeo Metas Corporativas más relevantes de la ESPE vs Metas de TI COBIT 5

				METAS RELACIONADAS CON LAS TI					
				1. Alineamiento de TI y la estrategia de negocio	2. Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	4. Riesgos de negocio relacionados con las TI gestionados	5. Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	6. Transparencia de los costes, beneficios y riesgos de las TI
1	Valor para las partes interesadas de las inversiones de negocio	P	3	P		P		P	S
2	Cartera de productos y servicios competitivos	0	0	P		S		P	
3	Riesgos de negocio gestionados (salvaguarda de activo)	0	0	S	S	S	P		S
4	Cumplimiento de leyes y regulaciones externas	S	1		P		S		
5	Transparencia financiera	0	0						P
6	Cultura de servicio orientada al cliente	0	0	P				S	
7	Continuidad y disponibilidad del servicio de negocio	0	0	S			P		
8	Respuestas ágiles a un entorno de negocio cambiante	S	1	P		S	S	S	
9	Toma estratégica de Decisiones basadas en información	P	3	P		S			S
10	Optimización de costes de entrega del servicio	0	0	S			P	S	P
11	Optimización de la funcionalidad de los procesos de negocio	S	1	P		S		S	
12	Optimización de los costes de los procesos de negocio	S	1	S				P	P
13	Programas gestionados de cambio en el negocio	S	1	P		P	S		
14	Productividad operacional y de los empleados	S	1					S	
15	Cumplimiento con las políticas internas	P	3		P		S		
16	Personal entrenado y motivado	P	3	S		S	S		
17	Cultura de innovación del producto y del negocio	P	3	S		S		S	

Continua

				METAS RELACIONADAS CON LAS TI					
				7. Entrega de servicios de TI de acuerdo a los requisitos del negocio	8. Uso adecuado de aplicaciones, información y soluciones tecnológicas.	9. Agilidad de las TI	10. Seguridad de la información, infraestructura de procesamiento y aplicaciones	11. Optimización de activos, recursos y capacidades de las TI	12. Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio
1	Valor para las partes interesadas de las inversiones de negocio	P	3	P	S	S		P	S
2	Cartera de productos y servicios competitivos	0	0	P	S	P		S	P
3	Riesgos de negocio gestionados (salvaguarda de activo)	0	0	S	S	S	P		S
4	Cumplimiento de leyes y regulaciones externas	S	1	S			P		
5	Transparencia financiera	0	0						
6	Cultura de servicio orientada al cliente	0	0	P	S	S			S
7	Continuidad y disponibilidad del servicio de negocio	0	0	S	S		P		
8	Respuestas ágiles a un entorno de negocio cambiante	S	1	P		P		S	S
9	Toma estratégica de Decisiones basadas en información	P	3	S	S				
10	Optimización de costes de entrega del servicio	0	0		S			P	S
11	Optimización de la funcionalidad de los procesos de negocio	S	1	P	P	P		S	P
12	Optimización de los costes de los procesos de negocio	S	1	S	S			P	S
13	Programas gestionados de cambio en el negocio	S	1	S		S		S	S
14	Productividad operacional y de los empleados	S	1		P	S		S	S
15	Cumplimiento con las políticas internas	P	3				P		
16	Personal entrenado y motivado	P	3	S	S	S			
17	Cultura de innovación del producto y del negocio	P	3	S	S	P		S	S

Continua

				METAS RELACIONADAS TI				
				13. Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	14. Disponibilidad de información útil y relevante para la toma de decisiones	15. Cumplimiento de las políticas internas por parte de las TI	16. Personal del negocio y de las TI competente y motivado	17. Conocimiento, experiencia e iniciativas para la innovación de negocio
1	Valor para las partes interesadas de las inversiones de negocio	P	3	P	S		S	S
2	Cartera de productos y servicios competitivos	0	0	S	S		S	P
3	Riesgos de negocio gestionados (salvaguarda de activo)	0	0	S	S	S	P	
4	Cumplimiento de leyes y regulaciones externas	S	1		S	S		
5	Transparencia financiera	0	0					
6	Cultura de servicio orientada al cliente	0	0	S			S	S
7	Continuidad y disponibilidad del servicio de negocio	0	0		P			
8	Respuestas ágiles a un entorno de negocio cambiante	S	1				S	P
9	Toma estratégica de Decisiones basadas en información	P	3		P			S
10	Optimización de costes de entrega del servicio	0	0	S				
11	Optimización de la funcionalidad de los procesos de negocio	S	1		S			S
12	Optimización de los costes de los procesos de negocio	S	1	S				
13	Programas gestionados de cambio en el negocio	S	1	P				S
14	Productividad operacional y de los empleados	S	1				P	
15	Cumplimiento con las políticas internas	P	3			P		
16	Personal entrenado y motivado	P	3				P	S
17	Cultura de innovación del producto y del negocio	P	3				S	P

El porcentaje obtenido para cada Objetivo de TI así como su importancia se indica a continuación en la Tabla 9.

Tabla 9.

Metas de TI más significativas a tener en cuenta en la ESPE en relación al mapeo realizado

METAS RELACIONADAS CON LAS TI							
1. Alineamiento de TI y la estrategia de negocio	2. Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	4. Riesgos de negocio relacionados con las TI gestionados	5. Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	6. Transparencia de los costes, beneficios y riesgos de las TI	7. Entrega de servicios de TI de acuerdo a los requisitos del negocio	8. Uso adecuado de aplicaciones, información y soluciones tecnológicas.
27	7	13	14	15	12	23	16
11	4	7	2	5	2	8	6
40,74%	57,14%	53,85%	14,29%	33,33%	16,67%	34,78%	37,50%
S	**P**	**P**					**S**

METAS RELACIONADAS CON LAS TI								
9. Agilidad de las TI	10. Seguridad de la información, infraestructura de procesamiento y aplicaciones	11. Optimización de activos, recursos y capacidades de las TI	12. Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	13. Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas	14. Disponibilidad de información útil y relevante para la toma de decisiones	15. Cumplimiento de las políticas internas por parte de las TI	16. Personal del negocio y de las TI competente y motivado	17. Conocimiento, experiencia e iniciativas para la innovación de negocio
18	12	15	15	11	11	5	14	15
7	4	5	3	4	4	3	6	7
38,89%	33,33%	33,33%	20,00%	36,36%	36,36%	60,00%	42,86%	46,67%
S				**S**	**S**	**P**	**S**	**P**

3.2.3 Listado de los procesos de COBIT 5 priorizados con mayor importancia.

Utilizando (ISACA, COBIT 5 AN ISACA FRAMEWORK, 2012), **Mapeo Detallado de las Metas Relacionadas con las TI y los Procesos Relacionados con las TI**, Figura 7, se realiza un mapeo entre los objetivos relacionados con las TI de mayor importancia en la Universidad de las Fuerzas Armadas ESPE y los procesos relacionados de TI formales de COBIT 5.

		Metas relacionadas con las TI							
		1. Alineamiento de TI y la estrategia de negocio	2. Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	4. Riesgos de negocio relacionados con las TI gestionados	5. Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	6. Transparencia de los costes, beneficios y riesgos de las TI	7. Entrega de servicios de TI de acuerdo a los requisitos del negocio	8. Uso adecuado de aplicaciones, información y soluciones tecnológicas.
	Procesos de COBIT 5								
Evaluar, Orientar, Supervisar	EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P	S	P	S	S	S	P	
	EDM02 Asegurar Entrega de Beneficios	P		S		P	P	P	S
	EDM03 Asegurar Optimización del Riesgo	S	S	S	P		P	S	S
	EDM04 Asegurar Optimización de Recursos	S		S	S	S	S	S	S
	EDM05 Asegurar la Transparencia hacia las partes interesadas	S	S	P			P	P	
Alinear, Planificar y Organizar	APO01 Gestionar el Marco Gestión de TI	P	P	S	S			S	
	APO02 Gestionar la Estrategia	P	S	S	S		P	S	S
	APO03 Gestionar la Arquitectura Empresarial	P		S	S	S	S	S	S
	APO04 Gestionar la Innovación	S			S	P			P
	APO05 Gestionar el portafolio	P		S	S	P	S	S	S
	APO06 Gestionar Presupuesto y Costes	S		S	S	P	P	S	S
	APO07 Gestionar los Recursos Humanos	P	S	S	S			S	
	APO08 Gestionar las Relaciones	P		S	S	S	S	P	S
	APO09 Gestionar Acuerdos de Servicio	S			S	S	S	P	S
	APO10 Gestionar los Proveedores		S		P	S	S	P	S
	APO11 Gestionar la Calidad	S	S		S	P		P	S
	APO12 Gestionar el Riesgo		P		P		P	S	S
	APO13 Gestionar la Seguridad		P		P		P	S	S

Continua

		Metas relacionadas con las TI								
		9. Agilidad de las TI	10. Seguridad de la información, infraestructura de procesamiento y aplicaciones	11. Optimización de activos, recursos y capacidades TI	12. Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	13. Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	14. Disponibilidad de información útil y relevante para la toma de decisiones	15. Cumplimiento de las políticas internas por parte de las TI	16. Personal del negocio y de las TI competente y motivado	17. Conocimiento, experiencia e iniciativas para la innovación de negocio
	Procesos de COBIT 5									
Evaluar, Orientar, Supervisar	EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	S	S	S	S	S	S	S	S	S
	EDM02 Asegurar Entrega de Beneficios			S	S	S	S		S	P
	EDM03 Asegurar Optimización del Riesgo		P			S	S	P	S	S
	EDM04 Asegurar Optimización de Recursos	P		P		S			P	S
	EDM05 Asegurar la Transparencia hacia las partes interesadas					S	S	S		S
Alinear, Planificar y Organizar	APO01 Gestionar el Marco Gestión de TI	P	S	P	S	S	S	P	P	P
	APO02 Gestionar la Estrategia			S	S	S	S	S	S	P
	APO03 Gestionar la Arquitectura Empresarial	P	S	P	S	S	S			S
	APO04 Gestionar la Innovación	P		P	S		S			P
	APO05 Gestionar el portafolio	S		S		P				S
	APO06 Gestionar Presupuesto y Costes			S		S				
	APO07 Gestionar los Recursos Humanos	S	S	P		P		S	P	P
	APO08 Gestionar las Relaciones			S	P	S		S	S	P
	APO09 Gestionar Acuerdos de Servicio	S	S	S		S	P	S		
	APO10 Gestionar los Proveedores	P	S	S		S	S	S		S
	APO11 Gestionar la Calidad	S		S		P	S	S	S	S
	APO12 Gestionar el Riesgo	S	P			P	S	S	S	S
	APO13 Gestionar la Seguridad		P				P			

Continua

		Metas relacionadas con las TI							
		1. Alineamiento de TI y la estrategia de negocio	2. Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	4. Riesgos de negocio relacionados con las TI gestionados	5. Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	6. Transparencia de los costes, beneficios y riesgos de las TI	7. Entrega de servicios de TI de acuerdo a los requisitos del negocio	8. Uso adecuado de aplicaciones, información y soluciones tecnológicas.
	Procesos de COBIT 5								
Construcción, Adquisición e Implementación	BAI01 Gestión Programas y Proyectos	P		S	P	P	S	S	S
	BAI02 Gestionar Definición de Requisitos	P	S	S	S	S		P	S
	BAI03 Gestionar la Identificación y la Construcción de Soluciones	S			S	S		P	S
	BAI04 Gestionar Disponibilidad y la Capacidad				S	S		P	S
	BAI05 Gestionar la introducción de Cambios Organizativos	S		S		S		S	P
	BAI06 Gestionar los Cambios			S	P	S		P	S
	BAI07 Gestionar la Aceptación del Cambio y de la Transición				S	S		S	P
	BAI08 Gestionar el Conocimiento	S				S		S	S
	BAI09 Gestionar los Activos		S		S		P	S	
	BAI10 Gestionar la Configuración		P		S		S		S
Entrega, Dar servicio y Soporte	DSS01 Gestionar las Operaciones		S		P	S		P	S
	DSS02 Gestionar las Peticiones y los Incidentes del Servicio				P			P	S
	DSS03 Gestionar los Problemas		S		P	S		P	S
	DSS04 Gestionar la Continuidad	S	S		P	S		P	S
	DSS05 Gestión Servicios de Seguridad	S	P		P			S	S
	DSS06 Gestionar los Controles de los Procesos del Negocio		S		P			P	S
Supervisión, Evaluación y Verificación	MEA01 Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	S	P	S	S	P	S
	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno		P		P		S	S	S
	MEA03 Supervisar, Evaluar y Valorar la Conformidad con Requerimientos Externos		P		P	S		S	

Continua

		Metas relacionadas con las TI								
		9. Agilidad de las TI	10. Seguridad de la información, infraestructura de procesamiento y aplicaciones	11.Optimización de activos recursos capacidad TI	12. Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	13. Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	14. Disponibilidad de información útil y relevante para la toma de decisiones	15. Cumplimiento de las políticas internas por parte de las TI	16. Personal del negocio y de las TI competente y motivado	17. Conocimiento, experiencia e iniciativas para la innovación de negocio
	Procesos de COBIT 5									
Construcción, Adquisición e Implementación	BAI01 Gestión Programas y Proyectos			S		P			S	S
	BAI02 Gestión Definición de Requisitos	S	S	S	P	S	S			S
	BAI03 Gestionar la Identificación y la Construcción de Soluciones			S	S	S	S			S
	BAI04 Gestionar Disponibilidad y la Capacidad	S		P		S	P			S
	BAI05 Gestionar la introducción de Cambios Organizativos	S		S	S	P				P
	BAI06 Gestionar los Cambios	S	P	S	S	S	S	S		S
	BAI07 Gestionar la Aceptación del Cambio y de la Transición	S			P	S	S	S		S
	BAI08 Gestionar el Conocimiento	P	S	S			S		S	P
	BAI09 Gestionar los Activos	S	S	P			S	S		
	BAI10 Gestionar la Configuración	S	S	P			P	S		
Entrega, Dar servicio y Soporte	DSS01 Gestionar las Operaciones	S	S	P			S	S	S	S
	DSS02 Gestionar las Peticiones y los Incidentes del Servicio		S				S	S		S
	DSS03 Gestionar los Problemas	S		P	S		P	S		S
	DSS04 Gestionar la Continuidad	S	S	S	S		P	S	S	S
	DSS05 Gestión Servicios de Seguridad		P	S	S		S	S		
	DSS06 Gestionar los Controles de los Procesos del Negocio		S	S	S		S	S	S	S
Supervisión, Evaluación y Verificación	MEA01 Supervisar, Evaluar y Valorar Rendimiento y Conformidad	S	S	P		S	S	P	S	S
	MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno		S				S	P		S
	MEA03 Supervisar, Evaluar y Valorar la Conformidad Requerimientos Externos		S					S		S

Figura 7. Mapeo entre los procesos de COBIT 5 y las Metas Relacionadas con las TI. Tomado de (ISACA, COBIT 5 AN ISACA FRAMEWORK, 2012).

El mapeo se realiza tomando en cuenta la Tabla 10 mostrada a continuación.

Tabla 10.

Escala de Importancia de procesos de TI

Índice	Valor	Descripción	Importancia de Procesos de TI
P	**3**	**Principal**	Importante
S	**1**	**Secundario**	Menos Importante

A continuación se obtiene el porcentaje o peso de cada Proceso de TI como resultado del mapeo. Finalmente se califica el valor obtenido de porcentaje de acuerdo a la Tabla 11.

Tabla 11.

Intervalos de importancia de los procesos de TI

Intervalo	Valor
Mayores de 40%	P
Entre 30% y 40%	S

Mediante el uso de la escala de importancia de la Tabla 10 se presenta el resultado del mapeo en la Tabla 12.

Tabla 12.

Mapeo Detallado de las Metas Relacionadas con las TI y los Procesos Relacionados con las TI

Metas Relacionadas con las TI de la empresa	1. Alineamiento de TI y la estrategia de negocio	2. Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	3. Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	4. Riesgos de negocio relacionados con las TI gestionados	5. Realización de beneficios del portafolio de Inversiones y Servicios relacionados con las TI	6. Transparencia de los costes, beneficios y riesgos de las TI	7. Entrega de servicios de TI de acuerdo a los requisitos del negocio	8. Uso adecuado de aplicaciones, información y soluciones tecnológicas.	9. Agilidad de las TI	10. Seguridad de la información, infraestructura de procesamiento y aplicaciones	11. Optimización de activos, recursos y capacidades de las TI	12. Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	13. Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad.	14. Disponibilidad de información útil y relevante para la toma de decisiones	15. Cumplimiento de las políticas internas por parte de las TI	16. Personal del negocio y de las TI competente y motivado	17. Conocimiento, experiencia e iniciativas para la innovación de negocio
	S	P	P					S	S				S	S	P	S	P
	1	3	3					1	1				1	1	3	1	3

El porcentaje obtenido para cada Objetivo de TI así como su importancia se indica a continuación en la Tabla 13.

Tabla 13.

Porcentaje obtenido en los procesos TI evaluados en la ESPE.

Procesos de COBIT 5	Puntaje Posible	Puntaje Obtenido	Porcent	Calif
EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	22	7	31,82%	S
EDM02 Asegurar la Entrega de Beneficios	22	5	22,73%	
EDM03 Asegurar la Optimización del Riesgo	21	6	28,57%	
EDM04 Asegurar la Optimización de los Recursos	18	4	22,22%	
EDM05 Aseg. Transparencia hacia part interesadas	15	6	40,00%	P
APO01 Gestionar el Marco de Gestión de TI	28	13	46,43%	P
APO02 Gestionar la Estrategia	20	7	35,00%	S
APO03 Gestionar la Arquitectura Empresarial	20	4	20,00%	
APO04 Gestionar la Innovación	19	5	26,32%	
APO05 Gestionar el portafolio	17	4	23,53%	
APO06 Gestionar el Presupuesto y los Costes	13	1	7,69%	
APO07 Gestionar los Recursos Humanos	22	9	40,91%	P
APO08 Gestionar las Relaciones	21	6	28,57%	
APO09 Gestionar los Acuerdos de Servicio	16	2	12,50%	
APO10 Gestionar los Proveedores	19	4	21,05%	
APO11 Gestionar la Calidad	19	4	21,05%	
APO12 Gestionar el Riesgo	22	6	27,27%	
APO13 Gestionar la Seguridad	17	4	23,53%	P
BAI01 Gestionar los Programas y Proyectos	19	4	21,05%	
BAI02 Gestionar la Definición de Requisitos	20	4	20,00%	
BAI03 Gestionar la Identificación y la Construcción de Soluciones	12	1	8,33%	
BAI04 Gestionar la Disponibilidad y la Capacidad	15	2	13,33%	
BAI05 Gestionar introducción de Cambios Organizativos	16	6	37,50%	S
BAI06 Gestionar los Cambios	19	3	15,79%	
BAI07 Gestión Aceptación del Cambio y Transición	14	3	21,43%	
BAI08 Gestionar el Conocimiento	14	4	28,57%	
BAI09 Gestionar los Activos	13	2	15,38%	
BAI10 Gestionar la Configuración	15	5	33,33%	S
DSS01 Gestionar las Operaciones	18	3	16,67%	
DSS02 Gestionar las Peticiones y los Incidentes del Servicio	11	2	18,18%	
DSS03 Gestionar los Problemas	19	4	21,05%	
DSS04 Gestionar la Continuidad	20	4	20,00%	
DSS05 Gestionar los Servicios de Seguridad	16	4	25,00%	P
DSS06 Gestionar los Controles de los Procesos del Negocio	15	3	20,00%	
MEA01 Supervisar, Evaluar y Valorar Rendimiento y Conformidad	24	6	25,00%	
MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	15	7	46,67%	P
MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	11	5	45,45%	P

En la Tabla 13 se tiene 2 casos particulares: El Proceso APO13 GESTIONAR LA SEGURIDAD y el proceso DSS05 GESTIONAR LOS SERVICIOS DE SEGURIDAD obtuvieron calificaciones de 23,53% y 25%, ambos valores fuera del intervalo mostrado en la Tabla 11.

La calificación obtenida no ha tomado en cuenta a estos procesos para continuar él análisis pero:

- APO13 trata en detalle elementos del término formal Sistema de Gestión de Seguridad de la Información SGSI.
- DSS05 trata en detalle temas operacionales como gestionar el acceso físico y lógico, gestionar la seguridad de los puestos de usuarios, proteger contra software malicioso, entre otros.

Por consiguiente no se los descarta y son en adelante son tomados como prioridad principal para continuar el análisis. Por tanto en la Tabla 14 se presentan los procesos TI más significativos a evaluar/implementar en relación a los Objetivos Institucionales de la Universidad de las Fuerzas Armadas, ESPE.

Tabla 14.

Procesos TI más significativos a evaluar/implementar en relación a los Objetivos Institucionales de la Universidad de las Fuerzas Armadas, ESPE.

Procesos de COBIT 5
Evaluar, Orientar, Supervisar
EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno
EDM05 Asegurar la Transparencia hacia las partes interesadas
Alinear, Planificar y Organizar
APO01 Gestionar el Marco de Gestión de TI
APO02 Gestionar la Estrategia
APO07 Gestionar los Recursos Humanos
APO13 Gestionar la Seguridad
Construcción, Adquisición e Implementación
BAI05 Gestionar la introducción de Cambios Organizativos
BAI10 Gestionar la Configuración
Entrega, Dar servicio y Soporte
DSS05 Gestionar los Servicios de Seguridad
Supervisión, Evaluación y Verificación
MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno
MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

3.2.4 Procesos COBIT 5 para Seguridad de la Información.

La presente evaluación tiene como objetivo adaptar a los procesos y procedimientos de seguridad de la información de la Universidad de las Fuerzas Armadas ESPE con las mejores prácticas utilizadas por las empresas de tecnología.

Si bien COBIT 5 abarca a las instituciones tanto a nivel de gobierno como de gestión, el Marco de Referencia COBIT 5 cubre términos generales a nivel empresarial. Es así que la presente evaluación continuará ejecutándose haciendo uso del Marco de Referencia COBIT 5 para Seguridad de la Información. Este marco de trabajo trata completamente la seguridad de la información y su contenido es el más adecuado para obtener mejores resultados en el presente análisis.

De manera adicional, (ISACA, COBIT para Seguridad de la Información, 2012)presenta un anexo del Mapeo el ISO 27000 para definir procedimientos más depurados en caso de ser necesario.

3.2.5. Plan de investigación de campo.

Una vez obtenido el resultado de los procesos más relevantes de la Universidad de las fuerzas armadas ESPE en relación a sus Objetivos Institucionales, el próximo paso es elaborar el Plan de investigación de campo.

Por consiguiente con base en COBIT 5 para seguridad de la información determinamos la matriz de actividades relevantes para que sean consideradas en los procedimientos de la ESPE.

A continuación en la Tabla 15 se detalla una matriz con cada uno de los procesos más relevantes resultantes del análisis con relación al apéndice B de (ISACA, COBIT para Seguridad de la Información, 2012).

Tabla 15.

Matriz detallada con procesos relevantes analizados relacionados a (ISACA, COBIT para Seguridad de la Información, 2012), Apéndice B.

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	01 Alineamiento de TI y estrategia de negocio 03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI 07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	EDM01.01 Evaluar el sistema de gobierno	1. Analizar e identificar los factores del entorno internos y externos (obligaciones legales, regulatorias y contractuales) de la seguridad de la información. 2. Evaluar el grado en el que la seguridad de la información cumple con las necesidades de negocio y regulatorias/cumplimiento. 3. Comprender la cultura empresarial de la toma de decisiones y determinar el modelo óptimo de toma de decisiones para seguridad de la información.
		EDM01.02 Dirigir el sistema de gobierno	1. Obtener el compromiso de la alta dirección con la seguridad de la información y la gestión de riesgos de la información. 2. Asignar una función de seguridad de la información de alcance global dentro de la empresa. 3. Alinear la estrategia de seguridad de la información con la estrategia del negocio. 4. Fomentar un entorno y cultura positivos de seguridad de la información.
		EDM01.03 Monitorear el Sistema de Gobierno	1. Supervisar los mecanismos ordinarios y rutinarios para garantizar que el uso de los sistemas de medida de la seguridad de la información cumplen con la legislación y regulación relacionada con la seguridad de la información.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIIDADES
EDM05 Asegurar la Transparencia hacia las partes interesadas	03 Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI 06 Transparencia de los costes, beneficios y riesgos de las TI 07 Entrega de servicios de TI de acuerdo a los requisitos del negocio	EDM05.01 Evaluar el reporte de requerimientos de las partes interesadas	1. Identificar los requisitos para la elaboración de informes de seguridad de la información a las partes interesadas. 2 Identificar los medios y canales para comunicar los asuntos relativos a la Seguridad de la Información.
		EDM05.02 Dirigir la comunicación de las partes interesadas y realizar reporte	1. Priorizar la notificación de problemas de seguridad de la información a las partes interesadas. 2. Realizar auditorías internas y externas para evaluar la eficacia del programa de gobierno de la seguridad de la información. 3. Elaborar informes de estado de la seguridad de la información de forma regular para las partes interesadas.
		EDM05.03 Monitorear la comunicación con las partes interesadas.	1. Definir la supervisión y elaboración de informes de seguridad de la información.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
APO01 Gestionar el Marco de Gestión de TI	01 Alineamiento de TI y estrategia de negocio 02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas 09 Agilidad de las TI 11 Optimización de activos, recursos y capacidades de las TI 15 Cumplimiento de las políticas internas por parte de las TI 16 Personal del negocio y de las TI competente y motivado 17 Conocimiento, experiencia e iniciativas para la innovación de negocio	APO01.01 Definir la estructura organizacional.	1. Alinear la organización relativa a la seguridad de la información con los modelos organizativos de arquitectura de empresa. 2. Definir la función de seguridad de la información, incluyendo roles internos y externos, capacidades y derechos de decisión requeridos.
		APO01.02 Establecer roles y responsabilidades.	1. Establecer, acordar y comunicar los roles de CISO y de ISM (o equivalentes). 2. Determinar el grado en que otros roles organizativos tienen obligaciones en seguridad de la información y añadirlas a las descripciones de puesto correspondientes.
		APO01.03 Mantener los habilitadores del sistema de gestión.	1. Considerar el entorno interno de la empresa, incluyendo la cultura y la filosofía de la gestión, la tolerancia al riesgo, los valores éticos, el código de conducta, la rendición de cuentas y los requisitos de seguridad de la información. 2. Alinearse con las normas y códigos de buenas prácticas de seguridad de la información aplicable, nacional e internacional, y evaluar las buenas prácticas disponibles de seguridad de la información. 3. Desarrollar políticas de seguridad de la información y afines, teniendo en cuenta los requisitos de negocio, y los legales o regulatorios, y las obligaciones contractuales de seguridad, las políticas organizativas de alto nivel y el entorno interno de la empresa.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
APO01 Gestionar el Marco de Gestión de TI	01 Alineamiento de TI y estrategia de negocio 02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas 09 Agilidad de las TI 11 Optimización de activos, recursos y capacidades de las TI 15 Cumplimiento de las políticas internas por parte de las TI 16 Personal del negocio y de las TI competente y motivado 17 Conocimiento, experiencia e iniciativas para la innovación de negocio	APO01.04 Comunicar los objetivos de gestión y dirección.	1. Definir las expectativas en relación a la seguridad de la información, incluyendo la ética y la cultura específica de la organización. 2. Desarrollar un programa de concienciación en seguridad de la información. 3. Establecer métricas para medir los comportamientos en relación a la seguridad de la información.
		APO01.05 Optimizar la ubicación de la función TI	1. Definir la función de seguridad de la información y todas las actividades y los atributos pertinentes. 2. Definir la ubicación de la función de seguridad de la información en la empresa y obtener el acuerdo de todas las partes implicadas.
		APO01.06 Definir la información (data) y sistemas propietarios.	1. Definir la propiedad de sistemas y datos al nivel de la empresa dentro de los procesos de gestión de seguridad de la información. 2. Asignar custodios de seguridad de la información de datos en los procesos de gestión de seguridad de la información.
		APO01.07 Gestión de mejoramiento continúo de procesos.	1. Considerar formas de mejorar la eficiencia y la eficacia de la función de seguridad de la información. 2. Revisar los informes (tales como los informes de auditoría y las evaluaciones de riesgo) que detallan las debilidades en los controles y procesos de seguridad de la información.
		APO01.08 Mantener el cumplimiento de las políticas y procedimientos.	1. Planificar y realizar evaluaciones periódicas para determinar el cumplimiento de las políticas y procedimientos de seguridad de la información.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
APO02 Gestionar la Estrategia	01 Alineamiento de TI y estrategia de negocio 07 Entrega de servicios de TI de acuerdo a los requisitos del negocio 17 Conocimiento, experiencia e iniciativas para la innovación de negocio	APO02.01 Entendimiento de la dirección de la empresa.	1. Comprender cómo la seguridad de la información debería apoyar los objetivos generales de la empresa y proteger los intereses de las partes implicadas 2. Comprender la vigente arquitectura de empresa e identificar las deficiencias potenciales de seguridad de la información.
		APO02.02 Evaluación del ambiente actual, capacidades y desempeño.	1. Definir unas capacidades básicas de seguridad de la información. 2. Crear criterios de seguridad de la información pertinentes y claros para identificar el riesgo y priorizar las deficiencias a tratar.
		APO02.03 Definir el objetivo de las capacidades TI.	1. Garantizar que los requisitos de seguridad de la información se incluyen en la definición de las capacidades objetivo para TI. 2. Definir el estado objetivo para la seguridad de la información. 3. Definir y consensuar el impacto de los requisitos de seguridad de la información en la arquitectura de la empresa, considerando a las partes interesadas pertinentes.
		APO02.04 Conducir al análisis gap.	1. Realizar un análisis comparativo de la seguridad de la información frente a normas del sector conocida y fiable. 2. Examinar el entorno actual con respecto a las regulaciones y los requisitos de cumplimiento.
		APO02.05 Definir el mapa estratégico y el road map.	1. Definir la estrategia de seguridad de la información y alinearla con las estrategias de TI y de negocio y con los objetivos globales corporativos. 2. Garantizar que la estrategia y la hoja de ruta actuales de TI tienen en consideración los requisitos de seguridad de la información. 3. Crear un plan de acción que incluya una planificación tentativa, interdependencias entre las iniciativas y métricas (el qué) y objetivos (el cuánto) que puedan relacionarse con los beneficios corporativos.
		APO02.06 Comunicar la estrategia TI y la dirección	1. Definir el plan de seguridad de la información, identificando las consecuencias para la empresa de la seguridad de la información. 2. Comunicar la estrategia de seguridad de la información y el plan de seguridad de la información a la empresa y a todas las partes interesadas pertinentes. 3. Dar a conocer la función de seguridad de la información dentro de la empresa, y fuera de ella si es pertinente.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
APO07 Gestionar los Recursos Humanos	01 Alineamiento de TI y estrategia de negocio 11 Optimización de activos, recursos y capacidades de las TI 13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. 16 Personal del negocio y de las TI competente y motivado 17 Conocimiento, experiencia e iniciativas para la innovación de negocio	APO07.01 Mantener la adecuada dotación de personal.	1. Asegurar que los requisitos de seguridad de la información asociados a dotar el proceso de personal, son incorporados en los procesos de contratación de TI para empleados, subcontratistas y proveedores.
		APO07.02 Identificar el personal clave TI.	1. Asegurar la segregación de funciones en los puestos críticos.
		APO07.03 Mantener las habilidades y competencias del personal.	1. Proporcionar formación y programas de desarrollo profesional sobre seguridad de la información. 2. Hacer uso de los programas de certificación personal para asegurar un conjunto de habilidades profesionales, de calidad, en seguridad de la información. 3. Establecer los oportunos programas educativos, de formación y de concienciación, de alcance corporativo, en seguridad de la información.
		APO07.04 Evaluar el desempeño del trabajo del empleado.	1. Incorporar criterios de seguridad de la información a los procesos de evaluación del personal.
		APO07.05 Planear y encaminar el uso de TI y los recursos humanos del negocio.	1. Gestionar la asignación de personal de seguridad de la información de acuerdo a las necesidades de negocio.
		APO07.06 Gestionar los contratos del personal.	1. Obtener la aceptación formal del personal en relación a los requisitos y políticas de seguridad de la información

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
APO13 Gestionar la Seguridad	02 Cumplimiento y soporte de TI al cumplimiento del negocio de las leyes y regulaciones externas 04 Riesgos de negocio relacionados con las TI gestionados 06 Transparencia de los costes, beneficios y riesgo de las TI 10 Seguridad de la información, infraestructura de procesamiento y aplicaciones 14 Disponibilidad de información útil y relevante para la toma de decisiones	AP013.01 Establecer y mantener un SGSI	1. Definir el alcance y los límites del SGSI en términos de las características de la empresa, la organización, su localización, activos y tecnología. 2. Definir un SGSI de acuerdo con la política de empresa y alineada con la empresa, la organización, su localización, activos y tecnología. 3. Alinear el SGSI con el enfoque global de la gestión de la seguridad en la empresa. 4. Obtener autorización de la dirección para implementar y operar o cambiar el SGSI. 5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI. 6. Definir y comunicar los roles y las responsabilidades de la gestión de la seguridad de la información. 7. Comunicar el enfoque de SGSI.
		AP013.02 Definir y gestionar un plan de tratamiento de riesgo de seguridad de información.	1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos y la arquitectura de la empresa. 2. Mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad. 3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información. 4. Recomendar programas de formación y concienciación en seguridad de la información. 5. Integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información.
		AP013.03 Supervisar y revisar el SGSI.	1. Realizar revisiones periódicas del SGSI, incluyendo aspectos de políticas, objetivos y prácticas de seguridad del SGSI. 2. Realizar auditorías internas al SGSI a intervalos planificados. 3. Realizar revisiones periódicas del SGSI por la Dirección para asegurar que el alcance sigue siendo adecuado. 4. Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
BAI05 Gestionar la introducción de Cambios Organizativos	08 Uso adecuado de aplicaciones, información y soluciones tecnológicas 13 Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad. 17 Conocimiento, experiencia e iniciativas para la innovación de negocio	BAI05.01 Establecer el deseo de cambio.	1. Identificar y comunicar los puntos críticos o débiles relativos a seguridad de la información. 2. Proporcionar liderazgo visible a través del compromiso de la alta dirección con la seguridad de la información para facilitar los cambios.
		BAI05.02 Conformar un grupo (personal) de implementación efectivo.	1. Designar profesionales de la seguridad de la información cualificados para servir en los equipos de implementación. 2. Desarrollar una visión común para todo el equipo de seguridad de la información.
		BAI05.03 Comunicar la visión deseada.	1. Comunicar la visión relativa a seguridad de la información como apoyo a la visión corporativa.
		BAI05.04 Empoderar el rol del personal a cargo e identificar las victorias a corto plazo.	1. Alinear las prácticas de seguridad de la para apoyar la visión. 2. Asignar de manera clara la responsabilidad de cada persona del equipo de seguridad de información.
		BAI05.05 Habilitar la operación y el uso.	1. Desarrollar medidas prácticas de seguridad de la información.
		BAI05.06 Insertar nuevos enfoques.	1. Hacer seguimiento continuo de la concienciación en seguridad de la información y adaptar pertinentemente las métricas.
		BAI05.07 Sustentar los cambios.	1. Informar y formar al nuevo personal y proporcionar sesiones de actualización de concienciación en seguridad de la información.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
BAI10 Gestionar la Configuración	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas 11 Optimización de activos, recursos y capacidades de las TI 14 Disponibilidad de información útil y relevante para la toma de decisiones	BAI10.01 Establecer y mantener un modelo de configuración.	0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.
		BAI10.02 Establecer y mantener un repositorio de configuración y una línea base.	1. Incluir una configuración de seguridad de la información para los elementos configurables como servidores/hardware, dispositivos de red y dispositivos finales. 2. Identificar requerimientos de seguridad de la información para los activos actuales y tener en cuenta las dependencias. 3. Supervisar el cumplimiento con las líneas de referencia de configuración de seguridad establecida y aprobada y con sus actualizaciones.
		BAI10.03 Mantener y controlar los intems de configuración.	0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.
		BAI10.04 Realizar reportes de estatus y configuración.	0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.
		BAI10.05 Verificar y revisar la integridad del repositorio de configuración.	0. No existen guías específicas de seguridad de la información relevantes para esta práctica. Las actividades genéricas de COBIT 5 pueden usarse como guía adicional.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
DSS05 Gestionar los Servicios de Seguridad	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas 04 Riesgos de negocio relacionados con las TI gestionados 10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	DSS05.01 Proteger contra malware.	1. Divulgar concienciación sobre el software malicioso y forzar procedimientos y responsabilidades de prevención. 2. Instalar y activar herramientas de protección frente a software malicioso en todas las instalaciones de proceso. 3. Revisar y evaluar regularmente la información sobre nuevas posibles amenazas. 4. Filtrar el tráfico entrante, como correos electrónicos y descargas, para protegerse frente a información no solicitada.
		DSS05.02 Gestionar la red y la seguridad de la conectividad.	1. Basándose en el análisis de riesgos y en los requerimientos del negocio, establecer y mantener una política de seguridad para las conexiones. 2. Permitir sólo a los dispositivos autorizados tener acceso a la información y a la red de la empresa. Configurar estos dispositivos para forzar la solicitud de contraseña. 3. Implementar mecanismos de filtrado de red, como cortafuegos y software de detección de intrusiones, con políticas apropiadas para controlar el tráfico entrante y saliente. 4. Configurar los equipamientos de red de forma segura. 5. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red.
		DSS05.03 Gestionar la seguridad de los endpoints.	1. Configurar los sistemas operativos de forma segura. 2. Implementar mecanismos de bloqueo de los dispositivos. 3. Cifrar la información almacenada de acuerdo a su clasificación. 4. Gestionar el acceso y control remoto. 5. Gestionar la configuración de la red de forma segura. 6. Implementar el filtrado del tráfico de la red en dispositivos de usuario finales. 7. Proteger la integridad del sistema. 8. Proveer de protección física a los dispositivos de usuario finales. 9. Deshacerse de los dispositivos de usuario finales de forma segura.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
DSS05 Gestionar los Servicios de Seguridad	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas 04 Riesgos de negocio relacionados con las TI gestionados 10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	DSS05.04 Gestionar la identidad del usuario y acceso lógico.	1. Mantener los derechos de acceso de los usuarios de acuerdo con los requerimientos de las funciones y procesos de negocio. 2. Autenticar todos los accesos a los activos de información basándose en su clasificación de seguridad. 3. Administrar todos los cambios de derechos de acceso (creación, modificación y eliminación) para que tengan efecto en el momento oportuno. 4. Segregar y gestionar cuentas de usuarios privilegiadas. 5. Realizar regularmente revisiones de la gestión de todas las cuentas y privilegios relacionados. 6. Asegurar que todos los usuarios y su actividad en los sistemas TI son identificables unívocamente. 7. Mantener una pista de auditoría de los accesos a la información clasificada como altamente sensible.
		DSS05.05 Gestionar acceso físico para evaluar TI.	1. Gestionar las peticiones y concesiones de acceso a las instalaciones de procesamiento. 2. Asegurar que los perfiles de acceso están actualizados basado en la función del trabajo y responsabilidades. 3. Registrar y supervisar todos los puntos de entrada a los emplazamientos de TI. 4. Instruir a todo el personal para mantener visible la identificación en todo momento. 5. Escoltar a los visitantes en todo momento mientras estén en las dependencias. 6. Restringir el acceso a ubicaciones de TI sensibles estableciendo restricciones en el perímetro, tales como vallas, muros. 7. Realizar regularmente formación de concienciación de seguridad física.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
DSS05 Gestionar los Servicios de Seguridad	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas 04 Riesgos de negocio relacionados con las TI gestionados 10 Seguridad de la información, infraestructura de procesamiento y aplicaciones	DSS05.06 Gestionar documentos sensibles y dispositivos de salida.	1. Establecer procedimientos para gobernar la recepción, uso, eliminación y destrucción de formularios especiales y dispositivos de salida hacia, dentro y fuera de la empresa. 2. Asignar privilegios de acceso a documentos sensibles y dispositivos de salida. 3. Establecer un inventario de documentos sensibles y dispositivos de salida, y realizar regularmente conciliaciones. 4. Establecer salvaguardas física apropiadas sobre formularios especiales y dispositivos sensibles. 5. Destruir la información sensible y proteger los dispositivos de salida.
		DSS05.07 Monitorear la infraestructura para eventos relacionados con la seguridad.	1. Registrar los eventos relacionados con las seguridades reportadas por las herramientas de monitorización de la seguridad de la infraestructura, identificando el nivel de información que debe guardarse en base a la consideración de riesgo. Retenerla durante un período apropiado para ayudar en futuras investigaciones. 2. Definir y comunicar la naturaleza y características de los incidentes potenciales relacionados con la seguridad de forma que sean fácilmente reconocibles y sus impactos comprendidos para permitir una respuesta acorde. 3. Revisar regularmente los registros de eventos para detectar incidentes potenciales. 4. Mantener un procedimiento para la recopilación de evidencias en línea con las normas de evidencias forenses locales y asegurar que todos los empleados están concienciados de los requerimientos. 5. Asegurar que los tiques de incidentes de seguridad se crean en el momento oportuno cuando la monitorización identifique incidentes de seguridad potenciales.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas 04 Riesgos de negocio relacionados con las TI gestionados 15 Cumplimiento de las políticas internas por parte de las TI	MEA02.01 Monitorear los controles internos.	1. Realizar una revisión periódica de las políticas y procedimientos de seguridad de la información. 2. Determinar el alcance del aseguramiento p.ej. controles de seguridad de la información a evaluar. 3. Establecer un enfoque formal para el aseguramiento de seguridad de la información.
		MEA02.02 Revisar la efectividad de los controles de los procesos de negocio.	1. Medir la eficacia de los controles de seguridad de la información. 2. Realizar revisiones regulares de aplicaciones, sistemas y redes.
		MEA02.03 Realizar controles de autoevaluaciones.	1. Realizar evaluaciones del aseguramiento de seguridad de la información (independientes y auto-evaluaciones) para identificar debilidades de los controles.
		MEA02.04 Identificar y reportar deficiencias de los controles.	1. Revisar los informes de incidentes de seguridad de la información para identificar deficiencias de los controles. Informar y abordar las deficiencias detectadas.
		MEA02.05 Asegurar que los proveedores del aseguramiento son independientes y calificados.	1. Establecer competencias y cualificaciones para el proveedor de aseguramiento.
		MEA02.06 Planificar las iniciativas de aseguramiento.	1. Aceptar los objetivos de la revisión de aseguramiento de seguridad de la información.
		MEA02.07 Realizar un alcance las iniciativas de aseguramiento.	1. Documentar los detalles del compromiso de la organización en completar la revisión.
		MEA02.08 Ejecutar las iniciativas de aseguramiento.	1. Producir y emitir informes firmados sobre el aseguramiento de seguridad de la información.

Continua

PROCESOS	METAS TI	DESCRIPCION	ACTIVIDADES
MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos	02 Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas 04 Riesgos de negocio relacionados con las TI gestionados	MEA03.01 Identificar los requerimientos de cumplimiento externo.	1. Establecer acuerdos para supervisar la conformidad de seguridad de la información con requerimientos externos. 2. Identificar objetivos de cumplimiento de seguridad de la información con requerimientos externos. 3. Determinar los requerimientos externos de cumplimiento que deben satisfacerse (incluyendo legales, regulatorios, de privacidad y contractuales). 4. Identificar y comunicar las fuentes de materiales relativos a seguridad de la información que ayuden a cumplir los requerimientos de cumplimiento externos.
		MEA03.02 Optimizar el resultado de los requerimientos externos.	1. Revisar y comunicar los requerimientos externos a todos los grupos de interés relevantes.
		MEA03.03 Confirmar el cumplimiento externo.	1. Recopilar y analizar los datos de conformidad relacionados con la gestión de la seguridad y de los riesgos de la información
		MEA03.04 Obtener aseguramiento del cumplimiento externo.	1. Obtener evidencias de las terceras partes.

Adicional (ISACA, COBIT para Seguridad de la Información, 2012) presenta en sus anexos un mapeo de sus procesos con ISO/IEC 27001 e ISO/IEC 27002. En la Figura 8 se indica el mapeo de los procesos utilizados en la presente evaluación.

COBIT 5 para Seguridad de la Información	ISO/IEC 27001	¿Relevante? ¿Aplicado?	ISO/IEC 27002	¿Relevante? ¿Aplicado?
EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno	5.1 Compromiso de la Dirección A.5 Política de Seguridad		6.1.1 Compromiso de la dirección con la seguridad de la información	
EDM05 Asegurar la transparencia hacia las partes interesadas	A.10 Gestión de las comunicaciones y operaciones		6.1.1 Compromiso de la dirección con la seguridad de la información 6.1.2 Coordinación de la seguridad de la información 6.1.3 Establecimiento de responsabilidades de la seguridad de la información 6.1.4 Proceso de autorización de instalaciones para el tratamiento de la información 6.1.5 Acuerdos de confidencialidad 6.1.6 Contacto con autoridades 6.1.7 Contacto con grupos de interés especiales 6.1.8 Revisión independiente de la seguridad de la información	
APO01 Gestionar la estrategia	5.1 Compromiso de la dirección A.5 Política de Seguridad A.6 Organización de la seguridad de la información		Organización de seguridad de la información	
APO02 Gestionar la estrategia	4.2.1 Construir el SGSI			

Continua

COBIT 5 para Seguridad de la Información	ISO/IEC 27001	¿Relevante? ¿Aplicado?	ISO/IEC 27002	¿Relevante? ¿Aplicado?
APO07 Gestionar los recursos humanos	5.2.2 Formación, concienciación y competencia A.8 Seguridad ligada a los recursos humanos		Seguridad de la Información de Recursos Humanos	
APO13 Gestionar la seguridad	Tratado a lo largo de esta norma		Tratado a lo largo de esta norma	
BAI05 Gestionar la introducción de cambios organizativos				
BAI10 Gestionar la configuración			7.1.1 Inventario de activos 7.1.2 Propiedad de los activos 7.2.2 Etiquetado y manipulado de la información 10.7.4 Seguridad de la documentación del sistema 11.4.3 Identificación de los equipos en las redes 12.4.1 Control del software en explotación 12.4.2 Protección de los datos de prueba del sistema 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo 12.5.3 Restricciones a los cambios en los paquetes de software 12.6.1 Control de las vulnerabilidades técnicas 15.1.5 Prevención del uso indebido de los recursos de tratamiento de la información	

Continua

COBIT 5 para Seguridad de la Información	ISO/IEC 27001	¿Relevante? ¿Aplicado?	ISO/IEC 27002	¿Relevante? ¿Aplicado?
DSS05 Gestionar los servicios de seguridad	Tratado a lo largo de esta norma		Tratado a lo largo de esta norma	
MEA02 Supervisar, evaluar y valorar el sistema de control interno	4.2.3 Supervisar y revisar el SGSI 6. Auditoría interna del SGSI A.15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico		5.1.1 Documento de política de seguridad de la información 5.1.2 Revisión de la política de seguridad de la información 6.1.8 Revisión independiente de la seguridad de la información 6.2.3 Tratamiento de la seguridad en contratos con terceros 10.2.2 Supervisión y revisión de los servicios prestados por terceros 10.10.2 Supervisión del uso del sistema 10.10.4 Registros de administración y operación 15.2.1 Cumplimiento de políticas y normas de seguridad 15.2.2 Comprobación del cumplimiento técnico 15.3.1 Controles de auditoría de los sistemas de información	
MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos	6. Auditoría interna del SGSI A.15.1 Cumplimiento de los requisitos legales A.15.3 Consideraciones sobre la auditoría de los sistemas de información		6.1.6 Contacto con las autoridades 15.1.1 Identificación de la legislación aplicable 15.1.2 Derechos de propiedad intelectual (IPR) 15.1.4 Protección de datos y privacidad de la información de carácter personal	

Figura 8. Mapeo de procesos COBIT 5 con ISO/IEC 27001 e ISO/IEC 27002. Tomado de (ISACA, COBIT para Seguridad de la Información, 2012)

Asimismo, de acuerdo a (ISO/IEC 27001 Mapping Guide, 2013) y (www.informationshield.com, 2013) cada proceso de ISO/IEC 27001:2005 y ISO/IEC 27002:2005 tiene un mapeo con la nueva versión ISO/IEC 27001:2013 e ISO/IEC 27002:2013, los cuales se presentan en el Anexo 2.

De esta manera se procede a la elaboración del Cuestionario PCDG-01 y PDCG-02 con el fin de correlacionar información de los representantes de UTICS en la ESPE.

Las preguntas fueron elaboradas usando (ISACA, COBIT para Seguridad de la Información, 2012). Temas específicos no cubiertos por COBIT 5 para seguridad de la información fueron tomados en directamente de ISO 27001:2013 e ISO 27002:2013 considerando el mapeo con la versión 2005.

3.2.5.1 Personal de seguridad de información, roles y responsabilidades

Elaborados los cuestionarios, es necesario conocer a los funcionarios responsables de la seguridad de información en la universidad. De acuerdo a la información entregada por la ESPE, no existe documento formal que indique roles y responsabilidades de personal para seguridad de la información. Es así que las preguntas fueron dirigidas directamente al Ing. Rommel Atisimbay, Director de la UTIC; a través de sus respuestas al cuestionario y de la información de la propia de la ESPE entregada por la Ing. Magali Reascos, Especialista TICs de la UTIC, se continuará con el presente proyecto. El Cuestionario y sus respuestas se indican en el Anexo 3.

3.2.5.2. Inventario de Aplicaciones.

La seguridad de información comprende activos sobre los cuales la información es procesada de acuerdo a las necesidades de la universidad; la presente evaluación implica tomar acciones sobre dichos activos así como de los controles vigentes para procesamiento de la información. Como fue

mencionado en el literal 3.2 de este documento, mediante el documento INVENTARIO DE APLICACIONES INFORMATICAS ESPE, la universidad entregó de manera formal el listado de los aplicativos que actualmente operan y brinda el servicio requerido por la ESPE para cumplir con sus objetivos de negocio. Estos son:

- Sistema Académico.
- Sistema Financiero Olympo.
- Sistema Recursos Humanos
- Portal Web
- Sistema Banner.

El documento formal del inventario se indica en el Anexo 1.

CAPITULO IV

INFORME FINAL DE LA EVALUACION TECNICA INFORMATICA DE LOS SISTEMAS DE SEGURIDAD DE INFORMACION DE LA ESPE, SEDE PRINCIPAL

4.1 Análisis de los Cuestionarios PCDG-01 y PCDG-02

De acuerdo a los resultados obtenidos, se procede a realizar el Análisis de Riesgos en base a todas las actividades realizadas, Anexo 4**.**

Las consideraciones que se toma para el desarrollo del análisis en el Anexo 4 son las siguientes:

- Se encuentra los procesos de Tecnología de la Información significativos a evaluar en relación a los objetivos institucionales de la Universidad de las Fuerzas Armadas (véase Tabla 14).
- Se procede a realizar el uso del marco de referencia COBIT 5 para seguridad de la información (véase literal 3.2.4). Se desarrolla el plan investigativo de campo (véase literal 3.2.5).
- Desarrollado los puntos anteriores se realiza la matriz de procesos relevantes con sus actividades (véase Tabla 15).
- Se realiza el mapeo de los procesos de COBIT 5 relevantes encontrados con la ISO/IEC 27002:2013 (véase Figura 11), donde se obtiene las preguntas de los cuestionarios PCDG-01 y PCDG-02, de acuerdo a las actividades encontradas en la Tabla 10.

Para desarrollar el análisis de riesgos se considera lo siguiente:

- La evaluación del riesgo se identifica, cuantifica, prioriza los riesgos frente a los criterios para la aceptación del riesgo y los objetivos pertinentes para la organización. Tomado (NTE INEN ISO/IEC 27002, 2009).

- La evaluación del riesgo incluye un enfoque sistemático para estimar la magnitud del riesgo (análisis del riesgo), por lo que se considera para la valoración del riesgo tres categorías: Alta, Media y Baja (véase Anexo 4).Esta muestra el análisis de riesgo mediante probabilidad x impacto de los cuestionarios PCDG-01 y PCDG-02.

En base a las respuestas negativas de los cuestionarios PCDG-01 y PCDG-02, se encuentra los hallazgos que se evalúan de acuerdo a los puntos anteriores mencionados (véase Anexo 5). Esta presenta recomendaciones sobre las actividades según su prioridad: ALTA, MEDIA, BAJA, siendo el resumen de la Tabla 11.

4.2 Declaración de la finalidad de la auditoria.

La presente evaluación pretende adaptar los procesos y procedimientos actuales de seguridad de la información de la Universidad de las Fuerzas Armadas ESPE, con las mejores prácticas utilizadas por las organizaciones para proteger sus sistemas de información.

Si bien COBIT 5 es gobernar y administrar información independiente de cualquier medio que se utilice, esta cubre términos generales a nivel empresarial. Es así que la presente evaluación continuará ejecutándose haciendo uso del Marco de Referencia COBIT 5 para Seguridad de la Información. Este marco de trabajo para Seguridad de la Información presenta un Anexo del Mapeo al ISO 27000 para definir procedimientos más depurados en caso de ser necesario en el presente análisis (véase Figura 13).

4.3 Procesos de Tecnología de la Información que es objeto de la auditoria

Los procesos que se encuentran en el análisis son aquellas que son más significativas para los sistemas de información de la Universidad de las Fuerzas Armadas ESPE (véase Figura 12).

4.4 Alcance de la auditoria

De acuerdo con la normativa vigente NTE INEN-ISO/IEC 27002:2009 y con apoyo del marco de referencia de procesos de TI para seguridad COBIT for Security además de la normas ISO/EC 27001:2013, ISO 27002:2013 se realiza una auditoría de Seguridad de la información en la Universidad de las Fuerzas Armadas ESPE, durante el periodo del 12 de Enero 2015 al 12 de Mayo 2015. El alcance de nuestra auditoría consistió en una evaluación técnica de la Seguridad de la información.

Se requiere que la auditoría sea planeada y realizada para obtener suficientes, pertinentes y válidas pruebas, que proporcione una base razonable de conclusiones, opiniones y recomendaciones de la misma.

4.5 Objetivos de la auditoria

Determinar si los controles adecuados en sus procesos se encuentran implementados y, determinar el nivel de seguridad actual que garantice la disponibilidad, integridad, accesibilidad de la información sensible de la Universidad de la Fuerzas Armadas ESPE.

Evaluar el nivel de cumplimiento de los procedimientos formales de la Universidad de las Fuerzas Armadas ESPE en comparación con los lineamientos de las normas ISO 27001:2013, ISO 27002:2013 y COBIT 5.

4.6 Metodología de la auditoria

4.6.1 Planificación de la Auditoría

Para determinar el alcance y los objetivos de la auditoría, se realizaron pasos previos, que incluyeron el análisis de la misión de la Universidad de las Fuerzas Armadas ESPE, las operaciones relevantes y tecnología de apoyo. Identificamos las necesidades operacionales, legales, reglamentarias y la infraestructura de TI de la universidad auditada, revisando la documentación pertinente y la realización de entrevistas con el auditado en gestión.

La planificación de la auditoría incluyó revisar:

- Políticas y procedimientos actuales
- Contratos con terceros
- Identificación de factores críticos de éxito de la Universidad y de Tecnología de la Información.
- Identificar los criterios de auditoría, el material evaluado y determinar la idoneidad de los controles establecidos.

Hemos llevado a cabo visitas a las instalaciones de la universidad y de las áreas operativas de TI y se realizó una evaluación de riesgos para determinar los puntos críticos donde la universidad debe mitigar los mismos (véase literal 4.1).

4.7 Resultados de la auditoria

4.7.1 EDM01.- Asegurar el establecimiento y mantenimiento del marco de gobierno.

a) Hallazgo.- No disponen de un documento de políticas de seguridad

Riesgo.- Esto implica no tener directrices de control en la universidad referente a la seguridad de la información.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requieren acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Elaborar, implementar el manual de políticas de seguridad.

b) Hallazgo.- No se definen actividades específicas a los funcionarios correspondientes.

Riesgo.- Esto implica que no se tiene responsabilidades por parte de los funcionarios.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Elaborar, implementar reglamentos de responsabilidades de los funcionarios.

c) Hallazgo.- No cumple con la normativa vigente con respecto a la seguridad de la información.

Riesgo.- Esto implica que en el caso de una auditoria por el ente de control se encuentre un sin número de no conformidades que pueden ocasionar problemas para la universidad.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Se debe implementar metodologías para salvaguardar la información y cumplir con la normativa vigente.

d) Hallazgo.- No se desarrollan programas de concienciación referente a la seguridad de la información

Riesgo.- Esto implica que los funcionarios desconozcan que la universidad este implementando metodologías referentes a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Se debe elaborar cronogramas de capacitación que puedan solventar las necesidades de los funcionarios respecto a la seguridad de la información.

e) Hallazgo.- La dirección no tiene un conocimiento adecuado de los beneficios de la aplicación de metodologías de seguridad de la información

Riesgo.- Esto implica que no se tendrá un apoyo para la implementación en la universidad, referente a la seguridad de la información.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.

f) Hallazgo.- No se tiene un pleno conocimiento de la normativa vigente

Riesgo.- Esto implica que no se tendrá un apoyo para la implementación en la universidad, referente a la seguridad de la información, además no se tendrá directrices para solventar la misma.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Se debería capacitar al personal de las áreas correspondientes de la aplicación de las metodologías, buenas prácticas para salvaguardar la información.

g) Hallazgo.- No se encontró la aplicación de seguridad de la información en obligaciones internas y externas.

Riesgo.- Esto implica que no se tienen responsabilidades de los funcionarios y/o terceros de la universidad, referente a la seguridad de la información.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Implementar procedimientos que ayuden a dar aplicabilidad a los acuerdos de confidencialidad tanto internos como externos.

4.7.2 EDM05 Asegurar la Transparencia hacia las partes interesadas

a) Hallazgo (6.1.1 Roles y responsabilidades de seguridad de la información, ISO/IEC 27002:2013).- No se dispone de responsabilidad formal en la aplicación, seguimiento del cumplimiento de la normativa vigente.

Riesgo.- Esto implica que no se tendrá un apoyo para la implementación en la universidad, referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Socializar, segregar funciones formalmente al personal adecuado de la universidad, para realizar las actividades concernientes a la seguridad de la información.

4.7.3 APO02 Gestionar la Estrategia

a) Hallazgo.- No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información.

Riesgo.- Esto implica que el personal de la universidad no conoce y por consecuencia no es consiente, en temas referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.

b) Hallazgo.- No se tiene informes de intrusión para protección de la red, ni se dispone de procedimientos, ni metodología a ser implementada

Riesgo.- Esto implica que los sistemas puedan ser vulnerables pudiendo generar alteración en la información de la universidad.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Realizar un cronograma de pruebas de intrusión periódicas, aplicando buenas prácticas para solventar los procedimientos de análisis de vulnerabilidades.

c) Hallazgo.- No se dispone registros ni procedimiento para acceso y control remoto a los sistemas.

Riesgo.- Esto implica que los accesos a los sistemas no estén garantizados para su uso pudiendo generar alteración en la información de la universidad.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Realizar procedimientos para acceso remoto y socializar a los responsables de utilizar esto las políticas de seguridad de la universidad en base a la normativa vigente.

d) Hallazgo.- No se ha realizado análisis de riesgos referente a la seguridad de la información.

Riesgo.- Esto implica que se desconoce los puntos críticos donde se debe efectuar una atención inmediata para la implementación en la universidad, referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Se debe realizar un análisis de riesgos de seguridad de la información para verificar el estado de avance del mismo.

4.7.4 APO07 Gestionar los Recursos Humanos

a) Hallazgo (7.1.2 Términos y condiciones de contratación, ISO/IEC 27002:2013).- No se incluye ningún tema adicional respecto a seguridad de la información en la contratación de personal.

Riesgo.- Esto implica que los funcionarios puedan utilizar de manera incorrecta la información y sistemas de la universidad sin tener ninguna incidencia en la responsabilidad que esto implique, referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Se debe incluir temas relacionados con el compromiso del personal para el cumplimiento de la seguridad de la información.

b) Hallazgo (7.2.1 Responsabilidades de gestión, ISO/IEC 27002:2013).- No se definen responsabilidades en las actividades referentes a la seguridad de la información.

Riesgo.- Esto implica que los funcionarios puedan manipular la información, sistemas sensibles de la universidad, sin tener responsabilidades referentes a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Socializar, segregar funciones formalmente al personal adecuado de la universidad, para realizar las actividades concernientes a la seguridad de la información.

c) Hallazgo (7.1 Funciones y responsabilidades, ISO/IEC 27002:2013).- No se dispone de personal que tenga responsabilidad formal en la aplicación, seguimiento del cumplimiento de la normativa vigente.

Riesgo.- Esto implica que no se tendrá una estrategia específica para la implementación en la universidad, referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Socializar, segregar funciones formalmente al personal adecuado de la universidad, para realizar las actividades concernientes a la seguridad de la información. Gestionar la asignación de personal en el caso de no disponer.

d) Hallazgo (7.1.2 Términos y condiciones de contratación, ISO/IEC 27002:2013).- No se tiene de un acuerdo de confidencialidad con respecto al cumplimiento de la seguridad de la información.

Riesgo.- Esto implica que se podría tener un desconocimiento referente a la seguridad de la información.

Bajo: El riesgo puede causar problemas mínimos a la Universidad. Para controlar el riesgo será requerida la atención normal de Personal de Desarrollo Organizacional

Recomendación.- Realizar acuerdos de confidencialidad para el cumplimiento de la seguridad de la información.

4.7.5 APO13 Gestionar la Seguridad

a) Hallazgo (6.1 Organización interna, ISO/IEC 27002:2013).- No se dispone de un plan estratégico de seguridad de la información.

Riesgo.- Esto implica que no se tendrá una estrategia específica para la implementación en la universidad, referente a la seguridad de la información.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Aprobar, implementar el plan estratégico de seguridad de la información.

4.7.6 BAI05 Gestionar la introducción de Cambios Organizativos

a) Hallazgo.- No existen procedimientos para la identificación de puntos críticos que afecten la seguridad de la información.

Riesgo.- Esto implica que de existir una vulnerabilidad el tiempo de respuesta para solventar el mismo será más extenso para la universidad.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Realizar procedimientos que ayuden a la identificación, control vulnerabilidades encontradas en la universidad referentes a la seguridad de la información.

b) Hallazgo.- No se dispone de personal calificado referente actividades de la seguridad de la información.

Riesgo.- Esto implica que no se tendrá una estrategia específica para la implementación en la universidad, referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Realizar capacitaciones que fortalezcan las necesidades en la implementación de equipos referente a la seguridad de la información.

c) Hallazgo.- No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información.

Riesgo.- Esto implica que no se tendrá una estrategia específica para la implementación en la universidad, referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.

4.7.7 BAI10 Gestionar la Configuración

a) Hallazgo (8.2.2 Etiquetado de información y 8.2.3 Manejo de activo, ISO/IEC 27002:2013).- No se dispone de un reglamento de uso de servicios de procesamiento de la información.

Riesgo.- Esto implica que se generen varias metodologías que puedan interrumpir la implementación en la universidad, referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Aprobar, implementar reglamentos que ayuden al procesamiento de la información.

b) Hallazgo (8.1.2 Responsable de los activos y 8.2 Clasificación de la información, ISO/IEC 27002:2013).- No se dispone de metodologías, procedimientos para definir los niveles de acceso a la información, no se dispone de un análisis RISK para identificar la información sensible.

Riesgo.- Esto implica que todos los funcionarios pueden manipular la información sensible de la universidad, referente a la seguridad de la información.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Se debe realizar un análisis RISK, para solventar e identificar la información sensible de la universidad.

Se debe realizar un reglamento, procedimientos del manejo de la información sensible.

c) Hallazgo (14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en la plataforma operativa, ISO/IEC 27002:2013).- No se dispone de procedimientos ni registros de verificación de cambios a los sistemas.

Riesgo.- Esto implica que los sistemas no estén garantizados para su uso pudiendo generar alteración en la información de la universidad.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Se debe realizar procedimientos para la verificación de cambios y validación de los sistemas.

d) Hallazgo (12.6.1 Administración de vulnerabilidades técnicas, ISO/IEC 27002:2013).- No se tiene documentación de respaldo, ni procedimientos en el caso de encontrarse vulnerabilidades en el sistema.

Riesgo.- Esto implica que de existir un problema en los sistemas se perderá la información sensible de la universidad.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Realizar procedimiento que aseguren el cumplimiento de la política vigente referente a seguridad de la información

4.7.8 DSS05 Gestionar los Servicios de Seguridad

a) Hallazgo (6.1 Organización interna y 7.2.2 Educación, formación y concienciación sobre la seguridad de la información, ISO/IEC 27002:2013).- No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información.

Riesgo.- Esto implica que el personal de la universidad no conoce y por consecuencia no es consiente, en temas referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.

b) Hallazgo (8.1.1 Inventario de activos, ISO/IEC 27002:2013).- No se realiza un inventario de dispositivos actualizado.

Riesgo.- Esto implica que de existir una pérdida o robo no se garantiza la información y configuraciones realizadas en los sistemas de información de la universidad.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Se debe realizar un reglamento, procedimientos inventarios de la información y dispositivos sensibles.

c) Hallazgo (13 Seguridad de comunicaciones, ISO/IEC 27002:2013).- No se tiene informes de intrusión para protección de la red, ni se dispone de procedimientos, ni metodología a ser implementada.

Riesgo.- Esto implica que no se tendrá una estrategia en caso de incidentes referente a la seguridad de la información siendo vulnerable la universidad.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Realizar un cronograma de pruebas de intrusión periódicas, aplicando buenas prácticas para solventar los procedimientos de análisis de vulnerabilidades.

d) Hallazgo (13.1.1 Controles de red, ISO/IEC 27002:2013).- No se dispone de registros ni procedimiento para acceso y control remoto a los sistemas

Riesgo.- Esto implica que se tenga un libre acceso sin supervisión incrementando el niel de incidentes referente a la seguridad de la información siendo vulnerable la universidad.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Realizar procedimientos para acceso remoto y socializar a los responsables de utilizar esto las políticas de seguridad de la universidad en base a la normativa vigente.

4.7.9 MEA02 Supervisar, Evaluar y Valorar el Sistema de Control Interno

a) Hallazgo (12.7.1 Controles de auditoría de los sistemas de información, ISO/IEC 27002:2013).- No se encontró registros de eventos que comprometan la seguridad de la información.

Riesgo.- Esto implica que no se tendrá un apoyo para la implementación en la universidad, referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Elaborar, implementar registros que sucedan con respecto a la seguridad de la información, estandarizar formatos para levantamiento de los eventos.

b) Hallazgo (6.1.5 Seguridad de la información en gestión de proyectos y 18.2.2 Cumplimiento de políticas y normas de seguridad, ISO/IEC

27002:2013).- No se encontró seguimiento de parte de la dirección para verificar el alcance de la aplicación de la normativa vigente.

Riesgo.- Esto implica que no se tiene un apoyo, interés para la implementación en la universidad, referente a la seguridad de la información.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.

c) Hallazgo (18.2 Revisión sobre seguridad de la información, ISO/IEC 27002:2013).- No existen procedimientos que aseguren el cumplimiento de la seguridad de la información en las áreas comprometidas con esta.

Riesgo.- Esto implica que las áreas no tengan metodologías para la implementación en la universidad, referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Realizar procedimiento que aseguren el cumplimiento de la política vigente referente a seguridad de la información.

d) Hallazgo (15.3.1 Controles de auditoría de los sistemas de información, ISO/IEC 27002:2013).- No se dispone de registros de evaluaciones a los sistemas de información.

Riesgo.- Esto implica que no se realizan evaluaciones a los sistemas de información siendo puntos vulnerables para la universidad, referente a la seguridad de la información.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Realizar cronogramas de revisión, verificación de los sistemas para el cumplimiento de la normativa vigente referente a la seguridad de la información

4.7.10 MEA03 Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos

a) Hallazgo (6.1.3 Contacto con las autoridades, ISO/IEC 27002:2013).- No se realiza el seguimiento correspondiente a las no-conformidades encontradas.

Riesgo.- Esto implica que no se cumple, con las recomendaciones que realiza la entidad reguladora y en consecuencia genere problemas para la implementación en la universidad, referente a la seguridad de la información.

Alto: El riesgo puede tener un impacto muy adverso en la universidad. Se requiere acciones significativas y de alta prioridad en la atención de las Direcciones involucradas.

Recomendación.- Realizar las actividades que se recomienda por parte de la auditoria para mitigar el riesgo y solventar el SGSI

b) Hallazgo (6.1.3 Contacto con las autoridades, ISO/IEC 27002:2013).- No se tienen procedimientos de respuesta en caso de incidentes en las instalaciones de la universidad.

Riesgo.- Esto implica que no se tendrá una estrategia en caso de incidentes referente a la seguridad de la información siendo vulnerable la universidad.

Medio: El riesgo puede tener un impacto limitado en la universidad. Se requiere acciones específicas y de atención al personal de Dirección de Operaciones y Desarrollo Organizacional, para mitigar el riesgo.

Recomendación.- Realizar procedimientos que ayuden a la eficaz respuesta en temas relacionados a seguridad física de las instalaciones, se debe implementar un plan de contingencias para estos casos.

4.8 Conclusiones

- Del análisis efectuado se encontró que se tiene un estimado del 33% de vulnerabilidades críticas, un 60% de vulnerabilidades de nivel medio y apenas un 7% de vulnerabilidades de nivel bajo, que deben ser solventadas por la Universidad de las Fuerzas Armadas ESPE de forma primordial según su el nivel encontrado, esto para mitigar el riesgo de las mismas.
- La información presentada demuestra que no se dispone de documentos formales, que puedan colaborar a la puesta en marcha de la implementación de un sistema de gestión de seguridades de la información.
- La implementación de controles no solo depende de una buena estructuración de la política, sino también de su correcta socialización y compromiso de las autoridades de la institución, el cumplimiento de la

normativa vigente y de metodologías que ayuden a salvaguardar la información sensible de la Universidad de las Fuerzas Armadas ESPE, debe ser compromiso de todos los entes que conforman la institución.

- Para los accesos a la información se pudo encontrar que no se dispone de procedimientos para clasificar la misma, según la importancia que la institución defina, tampoco de niveles de custodia que puedan exigir la responsabilidad de la integridad de la información.

4.9 Recomendaciones

- Se debe cumplir con la normativa vigente en relación a la seguridad de la información, que rige para instituciones públicas, para así salvaguardar la información, sistemas sensibles que maneja la institución.
- Realizar un plan de trabajo donde contemple buenas prácticas de gobierno de TI, considerando el desarrollo de planes estratégicos de tecnología, planes de contingencia, análisis de riesgos de las vulnerabilidades en los sistemas que dispone la Universidad de las Fuerzas Armadas ESPE.
- Fortalecer la comunicación y compromiso con las autoridades de la institución para que formen parte de los objetivos de la implementación de un sistema de gestión de seguridad de la información.
- Realizar un cronograma de evaluaciones periódicas a los sistemas de información, para solventar las vulnerabilidades que se encuentren en estas y así mitigar el riesgo como podría ser: perdida de información, manipulación de los sistemas, intrusiones no autorizadas, malware, etc.
- Concienciar a los funcionarios de la institución, las ventajas que brinda el cumplimiento de las políticas, reglamentos, procedimientos y controles en el manejo de los sistemas de información, una buena estrategia para

mitigar el riesgo de vulnerabilidades es tener personal capacitado referente a buenas prácticas de seguridad de la información.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- El Marco de Referencia COBIT 5 ha permitido ampliar la evaluación de la Universidad de las fuerzas armadas ESPE a nivel de gobierno y gestión considerando adicionalmente al estándar ISO 27001 e ISO 27002. De esta manera se ha complementado el trabajo realizado considerando las mejores prácticas en seguridad de la información.
- La Universidad de las Fuerzas Armadas ESPE se encuentra en proceso de implementar el Sistema de Gestión de Seguridad de la Información, SGSI a nivel formal lo cual permite adaptarlo al presente trabajo.
- La fase de obtención de información de los procesos en seguridad de información de la Universidad de las Fuerzas Armadas ESPE presentó contratiempos esencialmente porque personal de la UTICS debía atender sus tareas contractuales como prioritarias. En su debido momento se entendió esta situación pero obstaculizó el avance regular del presente trabajo.
- La investigación realizada en este documento muestra la adaptabilidad de metodologías relacionadas con respecto a la seguridad de la información, teniendo así un complemento para satisfacer las necesidades de estudio y verificando el cumplimiento de las normativas vigentes que rigen a las instituciones públicas.
- Los sistemas tecnológicos son parte esencial de la sociedad y por ende del cumplimiento de los objetivos estratégicos de la institución, por lo que las metodologías empleadas en este documento reflejan el compromiso

tanto la parte técnica como de la dirección, para generar un correcto desempeño en las actividades encomendadas, que se verán fortalecidas con la implementación del sistema de gestión de seguridad de la información para salvaguardar uno de los principales activos de la Universidad de las Fuerzas Armadas ESPE como es su información.

- La Universidad de las Fuerzas Armadas ESPE, del análisis efectuado se encontró que se tiene un porcentaje de madurez de apenas el 7% en la implementación de un Sistema de Gestión de Seguridad de la Información, teniendo además un 60% de vulnerabilidades de nivel medio que podrían ser solventadas, para tener un porcentaje de madurez más acorde a los objetivos institucionales de la Universidad.

5.2 Recomendaciones

- La presente evaluación ha manifestado sus recomendaciones en relación a los procesos relevantes y al Plan Estratégico Institucional ESPE 2014-2017. Más allá de acoger las recomendaciones es importante mapear todos los procesos de COBIT 5 que no fueron considerados como prioritarios en el presente trabajo con el fin de mejorar en todos los procesos y procedimientos de la institución.
- Al momento de recopilar información personal de la UTICS hizo todo lo que estuvo a su alcance para facilitar lo solicitado, pero se pudo constatar que su actual carga laboral ocupa gran parte de su tiempo lo cual derivó en la demora en la entrega de documentos. Adicional a las recomendaciones indicado producto de la evaluación de seguridad de información, se pide analizar la actual carga laboral de los funcionarios de la UTICS para mejorar trabajos/apoyo externos a las funciones relacionadas a su cargo.

- Aplicar las metodologías en este documento sugeridas, con el fin de tener un apropiado criterio de las funcionalidades que los sistemas de gestión de seguridad de la información, los mismos que generan confidencialidad, integridad y disponibilidad de la información.
- Fomentar metodologías de estudio en las carreras de sistemas en temas como: pruebas de penetración, análisis de riesgos de vulnerabilidades, ethical hacking, pruebas de estrés en los sistemas que maneje la institución, para así fortalecer el conocimiento en este campo y crear grupos de trabajo que sean capaces de solventar las amenazas en temas de seguridad de la información.
- Realizar análisis de riesgo para mitigar las amenazas en los sistemas que disponga la Universidad de las Fuerzas Armadas ESPE, como una de las estrategias principales para la continuidad de la implementación del sistema de gestión de seguridad de la información. Capacitar al personal responsable en estos temas para fortalecer las áreas donde se comprometa información sensible para la institución así también definir responsabilidades para no afectar su labor dentro de la institución.
- La Universidad de las Fuerzas Armadas ESPE, debe solventar los hallazgos encontrados en el presente documento para tener un Sistema de Gestión de Seguridad de la Información fortalecido que ayude a conseguir los objetivos corporativos cumpliendo con las normativas vigentes, y esta debe ser implementada con el compromiso de todos los que conforman la Institución.

BIBLIOGRAFIA

Aguirre Freire, D., & Palacios Cruz, J. (2014). *Evaluaciíon técnica de seguridades del data Center del Municipio de Quito.* Sangolquí.

EPN. (2015). *Escuela Politenica Nacional*. Fonte: http://www.epn.edu.ec/investigacion/red-ecuatoriana-de-universidades-para-investigacion-y-postgrados

ESPE. (2014). Plan Estrategico Institucional ESPE 2014-2017. *Plan Estrategico Institucional ESPE 2014-2017* .

GOVERNANCE INSTITUTE IT. (2008). *Alineando COBIT 4.1, ITIL e ISO 27002*. Fonte: http://www.youblisher.com/p/147336-COBIT-y-empresas.

ISACA. (2014). *Banco de Medio Oriente mejora la seguridad de la información y Desarrollo de un marco de gobierno para la organización de soporte mundial en GlaxoSmithKline, utilizando COBIT*. Fonte: http://www.isaca.org/Knowledge-Center/cobit/cobit-focus/Documents/COBIT-Focus-Volume-1-2014_nlt_Spa_0314.pdf.

ISACA. (2012). COBIT 5 AN ISACA FRAMEWORK.

ISACA. (2012). COBIT para Seguridad de la Información. In: ISACA, *COBIT para Seguridad de la Información.*

ISO. (2014). Fonte: http://www.iso27000.es/iso27000.html

ISO. (2012). *ISO 27000.ES*. Fonte: ISO Survey: http://www.iso27000.es/certificacion.html

ISO/IEC 27001 Mapping Guide. (2013). Fonte: Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013: http://www.bsigroup.com/Documents/iso-27001/resources/BSI-ISO27001-mapping-guide-UK-EN.pdf

Miranda, K. (Junio de 2014). *Mapeo de controles del Anexo A ISO 27001:2013, Comparación con ISO 27001:2005.*Fonte: http://www.segu-info.com.ar/terceros/?titulo=ISO%2027001

Muñoz, I., & Ulloa, G. (2011). *Gobierno de TI – Estado del arte*. Fonte: http://www.icesi.edu.co/revistas/index.php/sistemas_telematica/article/view/1052/1076.

nacional, E. P. (2015). *Escuela Politecnica nacional*. Fonte: http://www.epn.edu.ec/investigacion/red-ecuatoriana-de-universidades-para-investigacion-y-postgrados/

PPElVerdadero. (5 de Febrero de 2014). *PPElVerdadero*. Fonte: PP El Verdadero: http://www.ppelverdadero.com.ec/pp-al-dia/item/cnt-recibe-certificacion-de-seguridad-de-la-informacion.html

*Proyecto para realizar Evaluación Técnica Informática de la Universidad de las Fuerzas Armadas ESPE*2014Sangolquí

Telconet. (2015). *Telconet*. Fonte: Telconet: http://www.telconet.net/telconet/certificaciones

www.informationshield.com. (2013). Fonte: ISO 27002:2013 Version Change Summary: http://www.informationshield.com/papers/ISO27002-2013%20Version%20Change%20Summary.pdf

ANEXOS

ANEXO 1

INFORMACION ENTREGADA POR LA ESPE

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

Sangolquí, 29 de abril de 2015
Oficio No. 2015-046-ESPE-d-6-1

Señor Ingeniero
Raúl Cajamarca

Señor Ingeniero
Diego Guanotasig
MAESTRANTE
Presente.-

ASUNTO: Remitiendo información

De mi consideración:

En referencia al memorando No. 2015-0014-PET-ESPE-a del 6 de marzo de 2015 y al oficio S/N del 27 de abril del año en curso remito a ustedes, señores Ingenieros, los cuestionarios y la información solicitada para la realización de la Evaluación Técnica de los procesos de la Unidad de Tecnologías de Información bajo los lineamientos de Cobit 5, cabe señalar que dicha información fue entregada en formato digital de la cual se adjunta el respectivo detalle.

Sin otro particular, me suscribo de usted.

Atentamente,

Ing. Rommel Asitimbay Morales
DIRECTOR DE LA UNIDAD DE TECNOLOGÍA DE INFORMACIÓN Y COMUNICACIÓN
e.c ARCH-ESPE-d-6
JOD

Elaborado por. Onofa J.
Supervisado por. Ing. Reascos M.
Ing. Asitimbay R.

ACUERDO DE CONFIDENCIALIDAD Y ENTREGA DE INFORMACIÓN

Comparecen a la suscripción del presente acuerdo, por una parte Ing. Magali Reascos a nombre y en representación de la Universidad de las Fuerzas Armadas ESPE, y por otra parte el Ing. Paúl Cajamarca e Ing. Diego Guanotasig, quienes han acordado celebrar el presente Acuerdo de Confidencialidad que se regirá por las siguientes cláusulas:

PRIMERA Objeto.- El objeto del presente acuerdo es fijar los términos y condiciones bajo los cuales las partes mantendrán la confidencialidad de los datos e información entregados.

SEGUNDA Confidencialidad.- Las partes acuerdan que cualquier información entregada, será mantenida en estricta confidencialidad. La parte receptora correspondiente sólo podrá revelar información confidencial a quienes la necesiten y estén autorizados previamente por la parte de cuya información confidencial se trata.

TERCERA. Excepciones.- No habrá deber alguno de confidencialidad en los siguientes casos: a) Cuando la parte receptora tenga evidencia de que conoce previamente la información recibida; b) Cuando la información recibida sea de dominio público y, c) Cuando la información deje de ser confidencial por ser revelada por el propietario.

CUARTA. Duración.- Este acuerdo regirá durante el tiempo que dure la Evaluación Técnica a los Procesos de la Unidad de Tecnologías de Información y Comunicaciones hasta un término de tres años contados a partir de su fecha.

QUINTA. Derechos de Propiedad.- Toda información entregada es de propiedad exclusiva de la parte de donde proceda. En consecuencia, no se utilizará información de la otra para su propio uso.

SEXTA. Modificación o Terminación.- Este acuerdo solo podrá ser modificado o darse por terminado con el consentimiento expreso por escrito de ambas partes.

SÉPTIMA. Validez.- El presente Acuerdo requiere para su validez la firma de las partes.

Para constancia, y en señal de aceptación, se firma el presente acuerdo en dos ejemplares, por las partes que en él han intervenido, en la ciudad de Sangolquí, a los 29 días del mes de abril de 2015.

ENTREGA CONFORME:

NOMBRE: Ing. Magali Reascos
CÉDULA: 1713702387
CARGO:Especialista de Tic`s

RECIBE CONFORME:

NOMBRE: Paúl Cajamarca
CÉDULA: 1714472724
CARGO: Maestrante

RECIBE CONFORME:

NOMBRE: Ing. Diego Guanotasig
CÉDULA:
CARGO: Maestrante

UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

UNIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

DETALLE DE LA INFORMACIÓN ENTREGADA PARA LA EVALUACIÓN TÉCNICA DE LOS PROCESOS DE UTIC BAJO LINEAMIENTOS DE COBIT 5

Información entregada a :

Ing. Raúl Cajamarca

Ing. Diego Guamotasig

ORD.	DETALLE DE LA INFORMACIÓN ENTREGADA
1	PLAN ESTRATEGICO INSTITUCIONAL ESPE 2014-2017
2	PLAN DE DESARROLLO UTIC 2012-2016
3	PLANIFICACIÓN UTIC 2014
4	PLAN DE CONTINGENCIA UTIC 2014
5	PLANIFICACIÓN UTIC 2014
6	REGISTRO INCIDENTES 032015-052015
7	PLAN DE CAPACITACIÓN 2014
8	SOLUCION ERRORES CONOCIDOS
9	PROCEDIMIENTO DE RESPALDOS
10	CONTRATO ANTIVIRUS
11	PARAMETRIZACIÓN SISTEMA
12	INFORME INCIDENTES ESTADO
13	INVENTARIO DE APLICACIONES
14	PROCESOS DE NEGOCIO ESPE 2014
15	CARACTERISTICAS TECNICAS APLICACIONES
16	MONITOREO PRTG 2014
17	CATÁLOGO DE SERVICIOS DE TIC'S
18	CATALOGO DE PROVEEDORES CONTRATOS 2014
19	INSTRUCTIVO-GESTIÓN-DOCUMENTAL-DAU
20	COMUNICADOS SERVICIOS DE TIC
21	CATÁLOGO DE PROYECTOS DE TIC'S
22	ESTRUCTURA UTIC 2015
23	REGLAMENTO-ORGANICO-GESTION-ORGANIZACIONAL-PROCESOS-CODIFICADO-UNIVERSIDAD-ESPE-
24	PLAN DE ADQUISICIONES EQUIPO INF 2014

Elaborado por: Ing. Magali Rosero

INVENTARIO DE APLICACIONES INFORMÁTICAS - ESPE

ORD.	NOMBRE DE LA APLICACIÓN	DESCRIPCION	FECHA DE OPERACIÓN
1	Sistema Académico	Sistema Académico antiguo contiene histórico de estudiantes	2000
2	Sistema Financiero OLYMPO	Sistema Financiero Contable	2004
3	Sistema Recursos Humanos	Sistema de Recursos Humanos SIFRHE en proceso de migración al Sistema Banner	2004
4	Portal Web	Página Web de la ESPE	2005
5	Sistema de Educación Virtual	Sistema de Educación virtual para modalidad a distancia	2005
6	Sistema BANNER – ESPE Sistema de Gestión Académica	Sistema de matrículas, registro académico, registro y consulta de notas, currículo académico, administración de planta física (aulas), planificación académica (asignaturas, NRC (paralelos), restricciones, asignación de cupos, docentes), inscripciones y admisiones pregrado y postgrado. historial académico.	2010
	Sistema BANNER – ESPE Sistema de Gestión Administrativa Financiera	Sistemas de Recursos humanos, administración de personal.	2010
	Sistema BANNER – ESPE Sistema de Gestión Documental	Sistema de digitalización y administración de documentación impresa.	2010
	Sistema BANNER - ESPE Sistema de Portal (luminis)	Sistema que intrega servicios web, despliegue de información a través de canales, basado en los roles asignados.	2010
	Sistema BANNER – ESPE Sistema de Work Flow	Sistema que automatiza la secuencia de acciones, actividades o tareas, utilizadas para la ejecución de los procesos.	2010

Ing. Patricia Nogales

SISTEMAS DE INFORMACION (E)

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

RECTORADO DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE

ORDEN DE RECTORADO 2014-232-ESPE-a-3

ROQUE APOLINAR MOREIRA CEDEÑO
General de Brigada
Rector de la Universidad de las Fuerzas Armadas-ESPE

CONSIDERANDO:

Que, el Art. 226 de la Constitución de la República del Ecuador señala: *"Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.";*

Que, el Art. 350 de la Constitución de la República del Ecuador señala: *"El Sistema de Educación Superior tiene como finalidad la formación académica y profesional con visión científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo";*

Que el Art.351 de la Constitución de la República del Ecuador indica: *"El sistema de educación superior estará articulado al sistema nacional de educación y al Plan Nacional de Desarrollo; la ley establecerá los mecanismos de coordinación del sistema de educación superior con la Función Ejecutiva. Este sistema se regirá por los principios de autonomía responsable, cogobierno, igualdad de oportunidades, calidad, pertinencia, integralidad, autodeterminación para la producción del pensamiento y conocimiento, en el marco del diálogo de saberes, pensamiento universal y producción científica tecnológica global";*

Que, el Art. 355 de la Carta Suprema, entre otros principios, establece: *"El Estado reconocerá a las universidades y escuelas politécnicas autonomía académica, administrativa, financiera y orgánica, acorde con los objetivos del régimen de desarrollo y los principios establecidos en la Constitución. Se reconoce a las universidades y escuelas politécnicas el derecho a la autonomía, ejercida y comprendida de manera solidaria y responsable. Dicha autonomía garantiza el ejercicio de la libertad académica y el derecho a la búsqueda de la verdad, sin restricciones; el gobierno y gestión de sí mismas, en consonancia con los principios de alternancia, transparencia y los derechos políticos; y la producción de ciencia, tecnología, cultura y arte. La autonomía no exime a las instituciones del sistema de ser fiscalizadas, de la responsabilidad social, rendición de cuentas y participación en la planificación nacional…";*

Que, el Art. 18 de la Ley Orgánica de Educación Superior establece: *"La autonomía responsable que ejercen las universidades y escuelas politécnicas consiste en: […] d) La libertad para nombrar a sus autoridades, profesores o profesoras, investigadores o investigadoras, las y los servidores y las y los trabajadores, atendiendo a la alternancia y equidad de género, de conformidad con la Ley; e) La libertad para gestionar sus procesos internos […] h) La libertad para administrar los recursos acorde con los objetivos del régimen de desarrollo, sin perjuicio de la fiscalización a la institución por un órgano contralor interno o externo, según lo establezca la Ley; […]";*

Que, el Art. 47 de la LOES dispone: *"Las universidades y escuelas politécnicas públicas y particulares obligatoriamente tendrán como autoridad máxima a un órgano colegiado académico superior que estará integrado por autoridades, representantes de los profesores, estudiantes y graduados. [...]";*

Que, el Art. 12 del Estatuto de la Universidad dispone que: *"El Honorable Consejo Universitario es el órgano colegiado de cogobierno académico superior y autoridad máxima de la Universidad de las Fuerzas Armadas-ESPE",*

Que, el Art. 47 del prenombrado Estatuto señala que: *"El Rector, será designado por el Jefe del Comando Conjunto de las Fuerzas Armadas de la terna de Oficiales que remita cada Fuerza a la que le corresponda ejercer el rectorado, que será en orden de precedencia de las Fuerzas; durará en sus funciones cinco años; y, sus deberes y atribuciones son: [...] k. Dictar acuerdos, instructivos, resoluciones y poner en ejecución aquellos dictados por el H. Consejo Universitario, mediante órdenes de rectorado; [...]";*

Que, mediante oficio 13-DIEDMIL-126, del 11 de septiembre de 2013, el Teniente General Leonardo Barreiro Muñoz, Jefe del Comando Conjunto designó al General de Brigada Roque Apolinar Moreira Cedeño como Rector de la Universidad de las Fuerzas Armadas "ESPE";

Que, el Art.14, literal p, del Estatuto de la Universidad establece que es atribución del H. Consejo Universitario: *"Aprobar o modificar el Plan Estratégico Institucional y el Plan Operativo Anual de la Institución..."*;

Que, el H. Consejo Universitario Provisional conoció: El memorando 2014-001-2014-ESPE-CPEI-scp, de fecha 4 de julio de 2014, dirigido por el Coronel de EMC. Francisco Armendáriz S., en su calidad de Presidente del Comité de Planificación y Evaluación Institucional, al señor Rector de la ESPE, en el que remite el Plan Estratégico de Desarrollo Institucional PEDI 2014-2017, Nivel I (NI), que fue aprobado por el Comité de Planificación y Evaluación Institucional, en sesión ordinaria del 13 de junio de 2014.

Que, el H. Consejo Universitario Provisional, en sesión ordinaria ESPE-HCUP-SO-2014-015, del 18 de agosto de 2014, al tratar el tercer punto del orden del día, adoptó la resolución ESPE-HCUP-RES-2014-067;

Que, el Art. 45 del Estatuto de la Universidad de las Fuerzas Armadas-ESPE, establece que: "*El Rector es la primera autoridad ejecutiva de la Universidad de las Fuerzas Armadas "ESPE" y ejercerá la representación legal, judicial y extrajudicial de la misma...*"; y,

En ejercicio de sus atribuciones,

RESUELVE:

Art. 1.- Poner en ejecución la resolución ESPE-HCUP-RES-2014-067, adoptada por el H. Consejo Universitario Provisional, al tratar el tercer punto del orden del día en sesión ordinaria del 18 de agosto de 2014, en el siguiente sentido:

"Aprobar el Plan Estratégico Institucional PEDI 2014-2017, nivel I, con las siguientes observaciones:

a. *Incluir un objetivo dentro de la política general que se relacione con el Comando Conjunto, todo en concordancia con el artículo 1 del Estatuto de la Universidad.*
b. *Agregar el mapa estratégico*
c. *Utilizar la denominación completa de la Universidad de las Fuerzas Armadas-ESPE."*

Esta resolución es de cumplimiento obligatorio y entra en vigencia una vez emitida la orden rectorado".

Art. 2.- El Plan Estratégico Institucional PEDI 2014-2017, nivel I, se anexa a esta orden de rectorado en catorce (14) hojas, como parte constitutiva e inseparable de la misma

Art. 3.- Del cumplimiento de esta orden de rectorado encárguense los señores: Vicerrector Administrativo; Vicerrector Académico General; Vicerrector de Docencia; Vicerrector de Investigación, Innovación y Transferencia de Tecnología; director de la extensión Latacunga; director de las unidades académicas externas; y, directora de la Unidad de Finanzas.

NOTIFÍQUESE Y CÚMPLASE

Expedida en el Rectorado de la Universidad de las Fuerzas Armadas-ESPE, el 3 de septiembre de 2014.

El Rector de la Universidad de las Fuerzas Armadas-ESPE

ROQUE APOLINAR MOREIRA CEDEÑO
General de Brigada

RAMC/ EVGL/OBC/PJLA

ESPE
SECRETARÍA GENERAL
Sangolquí, a 04 SET. 2014
CERTIFICO:
Que es fiel COPIA del original.

Campus universitario Sangolquí: Av. Gral. Rumiñahui s/n Telf: (593-02) 3 989 400
Fax: (593-02) 2334 952 / Código postal: 171103 / Casillero postal: 171 5 231 - B
Página Web: www.espe.edu.ec / Sangolquí - Ecuador

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE

PLAN ESTRATÉGICO DE DESARROLLO INSTITUCIONAL

PEDI 2014 – 2017

ÍNDICE

1. PRESENTACIÓN

La Universidad de las Fuerzas Armadas – ESPE, supera las nueve décadas de existencia como una institución de educación superior al servicio de la sociedad y se proyecta como líder en la formación de grado y postgrado, integrando la docencia, la investigación y la vinculación con la comunidad, bajo un enfoque de sistemas y procesos.

El desarrollo de la ESPE es fruto del trabajo desinteresado de sus autoridades, personal académico y administrativo, quienes con sus ideas, criterios y esfuerzo, han sido y son los gestores de los cambios institucionales y del reconocido prestigio alcanzado en el contexto nacional e internacional.

Se caracteriza por ser una institución innovadora frente a los cambios del entorno y a las tendencias mundiales en educación superior. Posicionada entre las mejores universidades del país, se centra en la construcción y desarrollo del conocimiento científico y tecnológico para ser reconocida como una universidad de investigación. Su organización es corporativa y de tipo matricial, determinada por sus procesos de valor.

La Universidad de las Fuerzas Armadas – ESPE para su desarrollo sigue el ciclo universal PHVA (Planificar – Hacer – Verificar – Actuar). En función de la verificación o evaluación de los resultados del "hacer", se retorna a la planificación o a la ejecución (retroalimentación con fines de ajuste y mejora) y se impulsa de esta manera el desarrollo institucional en la dimensión tiempo. En la fase de planificación se genera o actualiza el Plan Estratégico Institucional y se lo despliega para su operacionalización y ejecución.

El presente Plan Estratégico traza el rumbo para el desarrollo de nuestra universidad; posibilita el alineamiento e integración de esfuerzos para alcanzar los objetivos y metas en él planteados y orienta nuestras acciones hacia el logro de una visión de futuro compartida. El éxito en su ejecución, requiere del compromiso y disciplina de todos quienes conformamos la comunidad universitaria ESPE; por ello, os invito a fortalecer el trabajo participativo y proactivo, para que con los logros que se alcancen, nuestra institución sea cada vez más grande y se consolide como un referente de la educación superior en el país y en la región.

2. MARCO LEGAL

La Universidad de las Fuerzas Armadas – ESPE, es una institución de educación superior, con personería jurídica, autonomía administrativa y patrimonio propio, de derecho público, con domicilio en la ciudad de Quito, y sede matriz en la ciudad de Sangolquí; se rige por la Constitución de la República del Ecuador, la Ley Orgánica de Educación Superior y su Reglamento; otras leyes conexas; su estatuto aprobado por el Consejo de Educación Superior – CES, mediante resolución RPC-SO-24-No. 248 – 2013 emitida el 26 de junio de 2013; los reglamentos internos expedidos de acuerdo con la ley y por normas emitidas por sus órganos de administración y autoridades.

2.1.- CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR:

- Art.280.- "El Plan Nacional de Desarrollo es el instrumento al que se sujetarán las políticas, programas y proyectos públicos; la programación y ejecución del presupuesto del Estado; y la inversión y la asignación de los recursos públicos; y coordinar las competencias exclusivas entre el Estado central y los gobiernos autónomos descentralizados. Su observancia será de carácter obligatorio para el sector público e indicativo para los demás sectores."

- Art. 350.- "El sistema de educación superior tiene como finalidad **la formación académica y profesional con visión científica y humanística; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo."**
- Art. 351.- "El sistema de educación superior estará articulado al sistema nacional de educación y al Plan Nacional de Desarrollo; la ley establecerá los mecanismos de coordinación del sistema de educación superior con la Función Ejecutiva. Este sistema se regirá por los principios de autonomía responsable, cogobierno, igualdad de oportunidades, calidad, pertinencia, integralidad, autodeterminación para la producción del pensamiento y conocimiento, en el marco del diálogo de saberes, pensamiento universal y producción científica tecnológica global."
- Art. 352.- "El sistema de educación superior estará integrado por universidades y escuelas politécnicas; institutos superiores técnicos, tecnológicos y pedagógicos; y conservatorios de música y artes, debidamente acreditados y evaluados.
- Estas instituciones, sean públicas o particulares, no tendrán fines de lucro."
- Art. 355.- "El Estado reconocerá a las universidades y escuelas politécnicas autonomía académica, administrativa financiera y orgánica, acorde a los objetivos del régimen de desarrollo y los principios establecidos en la Constitución.
- Se reconoce a las universidades y escuelas politécnicas el derecho a la autonomía, ejercida y comprendida de manera solidaria y responsable.
- Dicha autonomía garantiza el ejercicio de la libertad académica y el derecho a la búsqueda de la verdad, sin restricciones; el gobierno y gestión de sí mismas, en consonancia con los principios de alternancia, transparencia y los derechos políticos; y la producción de ciencia, tecnología, cultura y arte. .....
- La autonomía no exime a las instituciones del sistema de ser fiscalizadas, de la responsabilidad social, rendición de cuentas y participación en la planificación nacional.
- La Función Ejecutiva no podrá privar de sus rentas o asignaciones presupuestarias, o retardar las transferencias a ninguna institución del sistema, ni clausurarlas o reorganizarlas de forma total o parcial."
- Art. 356.- "La educación superior pública será gratuita hasta el tercer nivel."*(incluye otros párrafos)*
- Art. 357.- "El Estado garantizará el financiamiento de las instituciones públicas de educación superior. Las universidades y escuelas politécnicas públicas podrán crear fuentes complementarias de ingresos para mejorar su capacidad académica, invertir en la investigación y en el otorgamiento de becas y créditos, que no implicarán costo o gravamen alguno para quienes estudian en el tercer nivel. La distribución de estos recursos deberá basarse fundamentalmente en la calidad y otros criterios definidos en la ley.
- La ley regulará los servicios de asesoría técnica, consultoría y aquellos que involucren fuentes alternativas de ingresos para las universidades y escuelas politécnicas, públicas y particulares."

2.2.- LEY ORGÁNICA DE EDUCACIÓN SUPERIOR

- Art. 8.- Fines de la Educación Superior
- Art. 12.- Principios del Sistema de Educación Superior
- Art. 13.- Funciones del Sistema de Educación Superior
- Art. 14; 18; 24; 27; 28; 34 al 39; 80; 93; 95; 98; 107; 117; 118; 125; 127;138;156 al 160

- **Disposición General Quinta.-** "Las universidades y escuelas politécnicas elaborarán planes operativos y planes estratégicos de desarrollo institucional concebidos a mediano y largo plazo, según sus propias orientaciones. Estos planes deberán contemplar las acciones en el campo de la investigación científica y establecer la articulación con el Plan Nacional de Ciencia y Tecnología, Innovación y Saberes Ancestrales, y con el Plan Nacional de Desarrollo. Cada institución deberá realizar la evaluación de estos planes y elaborar el correspondiente informe, que deberá ser presentado al Consejo de Educación Superior, al Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior y para efecto de la inclusión en el Sistema Nacional de Información para la Educación Superior, se remitirá a la Secretaria Nacional de Educación Superior, Ciencia, Tecnología e Innovación."

2.3.- REGLAMENTO GENERAL A LA LEY ORGÁNICA DE EDUCACIÓN SUPERIOR:

- Art. 11.- "Del examen nacional de evaluación de carreras y programas académicos"
- Art. 12.- "Del examen de habilitación para el ejercicio profesional"
- Art.14.- "De la Tipología de instituciones de Educación Superior."
- Art.15.- "De la evaluación según la tipología de las instituciones de educación superior"

2.4.- REGLAMENTO DE RÉGIMEN ACADÉMICO

- Artículo 2.- Objetivos del régimen académico
- Artículo 74.- Investigación institucional
- Artículo 77.- Pertinencia de las carreras y programas académicos
- Artículo 78.- Fortalezas o dominios académicos de las IES
- Artículo 79.- Dominios académicos y planificación territorial
- Artículo 80.- Consultorías y prestación de servicios
- Artículo 82.- Vinculación con la sociedad y educación continua

3. ALINEAMIENTO AL PLAN NACIONAL DEL BUEN VIVIR – PNBV

- **OBJETIVO 4: "Fortalecer las capacidades y potencialidades de la ciudadanía."**

POLÍTICAS:

4.1. Alcanzar la universalización en el acceso a la educación inicial, básica y bachillerato, y democratizar el acceso a la educación superior

4.4. Mejorar la calidad de la educación en todos sus niveles y modalidades, para la generación de conocimiento y la formación integral de personas creativas, solidarias, responsables, críticas, participativas y productivas, bajo los principios de igualdad, equidad social y territorialidad

4.5. Potenciar el rol de docentes y otros profesionales de la educación como actores clave en la construcción del Buen Vivir

4.6. Promover la interacción recíproca entre la educación, el sector productivo y la investigación científica y tecnológica, para la transformación de la matriz productiva y la satisfacción de necesidades

4.7. Promover la gestión adecuada de uso y difusión de los conocimientos generados en el país

4.9. Impulsar la formación en áreas de conocimiento no tradicionales que aportan a la construcción del Buen Vivir

- **OBJETIVO 10: "Impulsar la transformación de la matriz productiva"**

POLÍTICAS:

10.1. Diversificar y generar mayor valor agregado en la producción nacional

10.2. Promover la intensidad tecnológica en la producción primaria de bienes intermedios y finales

10.3. Diversificar y generar mayor valor agregado en los sectores prioritarios que proveen servicios

10.4. Impulsar la producción y la productividad de forma sostenible y sustentable, fomentar la inclusión y redistribuir los factores y recursos de la producción en el sector agropecuario, acuícola y pesquero

10.5. Fortalecer la economía popular y solidaria –EPS–, y las micro, pequeñas y medianas empresas –Mipymes– en la estructura productiva

10.9. Impulsar las condiciones de competitividad y productividad sistémica necesarias para viabilizar la transformación de la matriz productiva y la consolidación de estructuras más equitativas de generación y distribución de la riqueza

- **OBJETIVO 11: "Asegurar la soberanía y eficiencia de los sectores estratégicos para la transformación industrial y tecnológica"**

POLÍTICAS:

11.1. Reestructurar la matriz energética bajo criterios de transformación de la matriz productiva, inclusión, calidad, soberanía energética y sustentabilidad, con incremento de la participación de energía renovable

11.2. Industrializar la actividad minera como eje de la transformación de la matriz productiva, en el marco de la gestión estratégica, sostenible, eficiente, soberana, socialmente justa y ambientalmente sustentable

11.3. Democratizar la prestación de servicios públicos de telecomunicaciones y de tecnologías de información y comunicación (TIC), incluyendo radiodifusión, televisión y espectro radioeléctrico, y profundizar su uso y acceso universal

11.4. Gestionar el recurso hídrico, en el marco constitucional del manejo sustentable y participativo de las cuencas hidrográficas y del espacio marino

11.5. Impulsar la industria química, farmacéutica y alimentaria, a través del uso soberano, estratégico y sustentable de la biodiversidad

4. DIRECCIONAMIENTO ESTRATÉGICO

4.1 PRINCIPIOS FILOSÓFICOS

1. La institución se debe fundamentalmente a la nación ecuatoriana; a ella orienta todo su esfuerzo, contribuyendo a la solución de sus problemas, mediante la formación profesional y técnica, la investigación, y el estudio y planteamiento de soluciones para los problemas del país;

2. La institución es abierta a todas las corrientes del pensamiento universal, sin proselitismo político, ni religioso;

3. La autonomía responsable, cogobierno, igualdad de oportunidades, calidad, pertinencia, integralidad y autodeterminación para la producción del pensamiento y conocimiento en el marco del diálogo de saberes, pensamiento universal y producción científica tecnológica global;

4. La búsqueda permanente de la excelencia a través de la práctica de la cultura de la calidad en todos sus actos;

5. La formación consciente, participativa y crítica con libertad académica y rigor científico, que comprenda y respete los derechos fundamentales del ser humano y de la comunidad;

6. El cultivo de valores morales, éticos y cívicos, respetando los derechos humanos con profunda conciencia ciudadana; coadyuva a la búsqueda de la verdad y forma hombres y mujeres de honor, libres y disciplinados;

7. El mantenimiento de las bases históricas de la identidad nacional, para incrementar el orgullo de lo que somos, y así proyectarnos hacia el futuro;

8. La conservación, defensa y cuidado del medio ambiente y el racional aprovechamiento de los recursos naturales; y,

9. La práctica de los valores tradicionales de orden, disciplina, lealtad, justicia, gratitud y respeto, en el contexto de la responsabilidad, la honestidad a toda prueba, el autocontrol, la creatividad, el espíritu democrático, la solidaridad y la solución de los problemas mediante el diálogo y la razón.

4.2 VALORES INSTITUCIONALES

La conducta de todos y cada uno de los miembros de la comunidad universitaria ESPE, se mantendrá siempre bajo la práctica de los valores institucionales que se describen en su "Código de Ética"

4.3 MISIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS - ESPE

Formar académicos y profesionales de excelencia; generar, aplicar y difundir el conocimiento y, proponer e implementar alternativas de solución a problemas de interés público en sus zonas de influencia.

INDICADORES PARA LA MISIÓN:

- Grado de preferencia social por los graduados y postgraduados de la ESPE
- Resultados en los exámenes nacional de evaluación de carreras y programas académicos de habilitación para el ejercicio profesional
- Número de proyectos ejecutados y con resultados de alto impacto científico, tecnológico y/o social en las zonas de influencia

4.4 VISIÓN

Líder en la gestión del conocimiento y de la tecnología en el Sistema de Educación Superior, con reconocimiento internacional y referente de práctica de valores éticos, cívicos y de servicio a la sociedad.

INDICADORES PARA LA VISION

- Nivel de posicionamiento nacional, regional (Latinoamérica) e internacional de la Universidad de Fuerzas Armadas – ESPE.
- Posicionamiento de la imagen "ESPE" en el contexto académico del país

4.5 POLÍTICA GENERAL

Como institución de educación superior de las Fuerzas Armadas la universidad es dependiente del Comando Conjunto de las Fuerzas Armadas en: política institucional en el ámbito de educación superior, designación de autoridades ejecutivas; y asignación del personal militar necesario para su funcionamiento, orientando el esfuerzo institucional de forma sinérgica y participativa hacia la excelencia académica y organizacional.

4.6 POLÍTICA DE CALIDAD DE LA ESPE

En la Universidad de las Fuerzas Armadas – ESPE, nuestros estudiantes y usuarios son las personas más importantes a las que tenemos que servir y satisfacer, cumpliendo con lo que ofrecemos en los plazos establecidos y mejorando permanentemente todos los procesos académicos y administrativos.

La exigencia académica, el bienestar y la seguridad de todos quienes conformamos la comunidad ESPE y el respeto al medio ambiente son nuestras prioridades, para dentro de un marco de principios y valores, desarrollar una Cultura de Calidad Institucional

5. PLAN ESTRATÉGICO DE DESARROLLO INSTITUCIONAL - PEDI

5.1 PERSPECTIVAS O DIMENSIONES ESTRATÉGICAS

- De Talento Humano, Financiera e Infraestructura
- De Procesos

- De Estudiantes y Usuarios
- De Impacto en la Ciudadanía

5.2 OBJETIVOS ESTRATÉGICOS, INDICADORES Y ESTRATEGIAS

PERSPECTIVA: IMPACTO SOCIAL

OBJETIVO ESTRATÉGICO 1 – OE 1:

Incrementar el reconocimiento de la Universidad de las Fuerzas Armadas – ESPE como una institución referente en educación superior.

INDICADORES:

- Posicionamiento de la universidad en el contexto de las universidades y escuelas politécnicas del país.
- Índice de preferencia social para estudiar en la Universidad de Fuerzas Armadas – ESPE.

ESTRATEGIAS:

1.1 Alcanzar estándares nacionales e internacionales de calidad.

1.2 Implementar nuevas alianzas estratégicas con entidades académicas nacionales e internacionales.

1.3 Desarrollar eventos de difusión de actividades y resultados logrados en los programas de investigación y vinculación.

1.4 Implementar alianzas de cooperación con gobiernos locales y entidades de los sectores productivos para impulsar el desarrollo de las zonas de influencia.

1.5 Mejorar y ampliar la participación en proyectos comunitarios en las zonas de influencia.

PERSPECTIVA: USUARIOS Y CLIENTES

OBJETIVO ESTRATÉGICO 2 – OE 2:

Incrementar la calidad de los profesionales y postgraduados

INDICADORES:

- Grado de preferencia de entidades empleadoras por los graduados y postgraduados de la universidad.
- Índice de satisfacción de los graduados y postgraduados con la formación lograda en la universidad.

ESTRATEGIAS:

2.1 Actualizar periódicamente los estudios de demanda y pertinencia de las carreras y programas de postgrado, para adecuar la oferta académica de la Universidad.

2.2 Crear e implementar nuevas relaciones de cooperación académica de la Universidad con los sectores productivos y sociales.

2.3 Desarrollar y ampliar las actividades de investigación y vinculación social de los estudiantes de tercer y cuarto nivel.

OBJETIVO ESTRATÉGICO 3 – OE 3:

Incrementar la producción científica - tecnológica y su calidad.

INDICADORES:

- Número de documentos publicados en medios indexados y categorizados como de alta calidad.
- Prototipos de interés social, ambiental y económico generados por año.

ESTRATEGIAS:

3.1 Generar programas y proyectos de investigación con alto impacto.

3.2 Crear modelos y prototipos de interés para las zonas de influencia.

3.3 Generar libros y publicaciones de impacto, indexados a nivel internacional.

3.4 Desarrollar programas de especialización y maestrías de investigación intercolaborativos.

3.5 Crear programas de doctorado.

OBJETIVO ESTRATÉGICO 4 – OE 4:

Incrementar el impacto social de los programas de vinculación

INDICADORES:

- Tasa de incremento de los proyectos de vinculación con impacto verificado.
- Número de proyectos ejecutados conjuntamente con empresas y gobiernos locales en apoyo al desarrollo de la zona de influencia.

ESTRATEGIAS:

4.1 Actualizar la oferta de servicios de la universidad hacia la comunidad.

4.2 Implementar modelos y prototipos desarrollados por la universidad en las zonas de influencia.

4.3 Generar programas de apoyo al emprendimiento productivos en las zonas de influencia.

4.4 Implementar programas educativos para grupos vulnerables en las zonas de influencia.

4.5 Incrementar el número de proyectos estudiantiles en las zonas de influencia.

PERSPECTIVA: PROCESOS

OBJETIVO ESTRATÉGICO 5 – OE 5:

Incrementar la eficiencia y eficacia del sistema formativo de grado y postgrado

INDICADORES:

- Promedio de calificaciones obtenidas por los estudiantes de grado en el examen de fin de carrera.
- Tasa de graduación por promoción en los plazos previstos.

ESTRATEGIAS:

5.1 Innovar el modelo formativo, orientado al desarrollo de competencias.

5.2 Mejorar las competencias del personal académico.

5.3 Actualizar la oferta de carreras de grado en áreas específicas del conocimiento.

5.4 Actualizar la oferta de programas de postgrado.

5.5 Implementar programas de cuarto nivel conjuntamente con otras universidades, nacionales e internacionales.

5.6 Mejorar los procesos de formación articulados con las líneas de investigación y sus respectivos grupos, en las áreas de vinculación en las zonas de influencia.

OBJETIVO ESTRATÉGICO 6 – OE 6:

Incrementar la capacidad del sistema de investigación integrándolo con el modelo formativo.

INDICADORES:

- Porcentaje de personal académico ejecutando actividades de investigación
- Porcentaje de equipamiento disponible orientado a la investigación

ESTRATEGIAS:

6.1 Incrementar el número de investigadores titulares (PhD).

6.2 Implementar grupos y redes de investigación multidisciplinarios con investigadores internos y externos.

6.3 Implementar la infraestructura física y tecnológica para el desarrollo de la investigación.

6.4 Generar un ambiente que promueva e impulse la investigación y facilite la movilidad.

6.5 Mejorar los procesos de investigación articulados a la formación y vinculación.

6.6 Enviar a los investigadores a participar en proyectos de investigación conjunta en universidades extranjeras para publicación de los resultados en revistas o libros indexados.

OBJETIVO ESTRATÉGICO 7 – OE 7:

Incrementar la capacidad y calidad del sistema de vinculación integrándolo con el sistema de investigación y con el modelo formativo

INDICADORES:

- Porcentaje de estudiantes participando en proyectos de vinculación.
- Porcentaje de personal académico que participa en actividades de vinculación.

ESTRATEGIAS:

7.1 Incrementar la participación de estudiantes y profesores en actividades de vinculación con la sociedad.

7.2 Mejorar el sistema de vinculación con la sociedad.

7.4 Mejorar los procesos de vinculación articulados a la formación y la investigación, orientados a aplicar alternativas de solución en las zonas de influencia.

OBJETIVO ESTRATÉGICO 8 – OE 8:

Incrementar las capacidades de sustentación institucional. (Talento Humano – Finanzas – Recursos Físicos y Tecnológicos).

INDICADORES:

- Índice de satisfacción con el ambiente o clima laboral.
- Índice de ejecución presupuestaria.
- Tasa de incremento de ingresos por autogestión.

ESTRATEGIAS:

5.1 Mejorar la gestión del talento humano

5.2 Mejorar la eficiencia y eficacia en la gestión presupuestaria.

5.3 Generar mayor cantidad de recursos financieros por autogestión

5.4 Renovar y desarrollar la infraestructura física y tecnológica de apoyo a la gestión académica y administrativa.

AUTENTICADO

Carlos Sarango Erazo
CRNL (S.P.)
DIRECTOR UPDI

REVISADO

Javier F. Armendáriz S.
CRNL. EMC
VICERRECTOR ACADEMICO GENERAL

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
SECRETARÍA GENERAL
Sangolquí, a 04 SET. 2014
CERTIFICO:
Que es fiel COPIA del original.

Consolidación y elaboración: VAG – JAS - UPDI - CFS/GCM/SFP

UNIVERSIDAD DE LAS FUERZAS ARMADAS – ESPE
MAPA ESTRATÉGICO

ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

PERSPECTIVAS O DIMENSIONES ESTRATÉGICAS

IMPACTO SOCIAL

USUARIOS Y CLIENTES

PROCESOS

TALENTO HUMANO

RECURSOS

VISIÓN DE FUTURO

INCREMENTAR EL RECONOCIMIENTO DE LA ESPE COMO UNA UNIVERSIDAD REFERENTE EN EDUCACION SUPERIOR

INCREMENTAR LA CALIDAD DE LOS PROFESIONALES Y POSTGRADUADOS

INCREMENTAR LA PRODUCCIÓN CIENTÍFICA Y TECNOLÓGICA Y SU CALIDAD

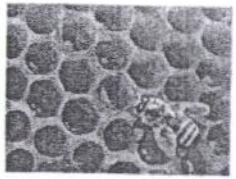
INCREMENTAR EL IMPACTO SOCIAL DE LOS PROGRAMAS DE VINCULACIÓN

INCREMENTAR LA EFICIENCIA Y EFICACIA DEL SISTEMA FORMATIVO DE GRADO Y POSTGRADO

INCREMENTAR LA CAPACIDAD DEL SISTEMA DE INVESTIGACIÓN INTEGRÁNDOLO CON EL MODELO FORMATIVO

INCREMENTAR LA CAPACIDAD Y CALIDAD DEL SISTEMA DE VINCULACIÓN INTEGRÁNDOLO CON EL SISTEMA DE INVESTIGACIÓN Y EL MODELO FORMATIVO

INCREMENTAR LAS CAPACIDADES DE SUSTENTACIÓN INSTITUCIONAL
(TALENTO HUMANO - FINANZAS - RECURSOS F / T)



ANEXO 2

MAPEO ENTRE ISO/IEC 27001:2005 CON ISO/IEC 27001:2013

MAPEO ENTRE ISO/IEC 27002:2005 CON ISO/IEC 27002:2013

ISO/IEC 27001 Mapping guide

Mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013

Introduction

This document presents a mapping between the requirements of ISO/IEC 27001:2005 and ISO/IEC 27001:2013. It has been designed for guidance purposes only.

There are two groups of tables. The first group deals with ISMS requirements:

1. **New ISMS requirements**;
2. **A mapping between ISMS requirements in ISO/IEC 27001:2013 and ISO/IEC 27001:2005** where the requirement is essentially the same;
3. **The reverse mapping** (i.e. ISO/IEC 27001:2005 and ISO/IEC 27001:2013);
4. **Deleted requirements** (i.e. ISO/IEC 27001:2005 requirements that do not feature in ISO/IEC 27001:2013).

The second group deals with Annex A controls:

1. **New Annex A controls**;
2. **A mapping between Annex A controls in ISO/IEC 27001:2013 and ISO/IEC 27001:2005** where the Annex A control is essentially the same;
3. **The reverse mapping** (i.e. ISO/IEC 27001:2005 and ISO/IEC 27001:2013);
4. **Deleted controls** (ISO/IEC 27001:2005 Annex A control that do not feature in ISO/IEC 27001:2013).

Please note that Annex A controls are not ISMS requirements unless they are deemed by an organization to be applicable in its Statement of Applicability.

bsi.

...making excellence a habit.™

Group 1 - ISMS requirements

New ISMS requirements

Clause (in ISO/IEC 27001:2013)	Requirement
4.2(a)	the interested parties that are relevant to the information security management system; and
4.3(c)	interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.
5.1(b)	ensuring the integration of the information security management system requirements into the organization's business processes;
6.1.1(a)	ensure information security management system can achieve its intended outcome(s);
6.1.1(b)	prevent, or reduce, undesired effects; and
6.1.1(c)	achieve continual improvement.
6.1.2(a)	establishes and maintains information security risk criteria that include:
6.2(b)	be measurable (if practicable)
6.2(c)	take into account applicable information security requirements,
6.2(c)	and results from risk assessment and risk treatment;
6.2(f)	what will be done;
6.2(g)	what resources will be required;
6.2(h)	who will be responsible;
6.2(i)	when it will be completed; and
6.2(k)	how the results will be evaluated.
7.3(a)	the information security policy;
7.4(a)	on what to communicate;
7.4(b)	when to communicate;
7.4(c)	with whom to communicate;
7.4(d)	who shall communicate; and
7.4(e)	the processes by which communication shall be effected.
7.5.1(b)	documented information determined by the organization as being necessary for the effectiveness of the information security management system.
8.1	The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1.
9.1(c)	when the monitoring and measuring shall be performed;
9.1(d)	who shall monitor and measure;
9.1(f)	who shall analyse and evaluate these results.
9.3(c)(4)	fulfilment of information security objectives;
10.1(a)	react to the nonconformity, and as applicable:
10.1(a)(1)	take action to control and correct it; and
10.1(a)(2)	deal with the consequences;
10.1(e)	make changes to the information security management system, if necessary.
10.1(f)	the nature of the nonconformities and any subsequent actions taken, and

Mapping of ISO/IEC 27001:2013 to ISO/IEC 27001:2005

Note that when looking at the mapping at an individual requirement level, one finds that some 2013 ISMS requirements actually map on to 2005 Annex A controls.

Clause (in ISO/IEC 27001:2013)	Requirement	ISO/IEC 27001:2005
4.1	The organization shall determine external and inte...	**8.3, 8.3(a), 8.3(e)**
4.2(a)	the interested parties that are relevant to the i...	**This is a new requirement**
4.2(b)	the requirements of these interested parties rele...	**5.2.1(c), 7.3(c)(4), 7.3(c)(5)**
4.3	The organization shall determine the boundaries an...	**4.2.1(a)**
4.3(a)	the external and internal issues referred to in 4...	**4.2.3(f)**
4.3(b)	the requirements referred to in 4.2; and	**4.2.3(f)**
4.3(c)	interfaces and dependencies between activities pe...	**This is a new requirement**
4.3(c)	The scope shall be available as documented informa...	**4.3.1(b)**
4.4	The organization shall establish, implement, maint...	**4.1, 5.2.1(a)**
5.1(a)	ensuring the information security policy and the ...	**4.2.1(b)(3)**
5.1(b)	ensuring the integration of the information secur...	**This is a new requirement**
5.1(c)	ensuring that the resources needed for the inform...	**5.1(e)**
5.1(d)	communicating the importance of effective informa...	**5.1(d)**
5.1(e)	ensuring that the information security management...	**5.1(b), 5.1(g), 5.1(h)**
5.1(f)	directing and supporting persons to contribute to...	**5.1(b), 5.1(g), 5.1(h)**
5.1(g)	promoting continual improvement; and	**5.1(d)**
5.1(h)	supporting other relevant management roles to dem...	**5.1**
5.2	Top management shall establish an information secu...	**4.2.1(b)(5), 5.1(a)**
5.2(a)	is appropriate to the purpose of the organization...	**4.2.1(b)**
5.2(b)	includes information security objectives (see 6.2...	**4.2.1(b)(1)**
5.2(c)	includes a commitment to satisfy applicable requi...	**4.2.1(b)(2), 4.3.3**
5.2(d)	includes a commitment to continual improvement of...	**5.1(d)**
5.2(e)	be available as documented information;	**4.3.1(a)**
5.2(f)	be communicated within the organization;	**5.1(d)**
5.2(g)	be available to interested parties, as appropriat...	**4.3.2(f)**
5.3	Top management shall ensure that the responsibilit...	**5.1(c)**
5.3(a)	ensuring that the information security management...	**4.3.3**
5.3(b)	reporting on the performance of the information s...	**4.3.3**
6.1.1	When planning for the information security managem...	**4.2.1(d), 8.3(a)**
6.1.1(a)	ensure information security management system can...	**This is a new requirement**
6.1.1(b)	prevent, or reduce, undesired effects; and	**This is a new requirement**
6.1.1(c)	achieve continual improvement.	**This is a new requirement**
6.1.1(d)	actions to address these risks and opportunities,...	**4.2.1(e)(4), 8.3(b), 8.3(c)**

Continued >>

Clause (in ISO/IEC 27001:2013)	Requirement	ISO/IEC 27001:2005
6.1.1(e)(1)	integrate and implement the actioninto its info...	**4.3.1(f), 8.3(c)**
6.1.1(e)(2)	evaluate the effectiveness of these actions.	**7.2(f)**
6.1.2	The organization shall define and apply an informa...	**4.2.1(c), 4.2.1(c)(1)**
6.1.2(a)	establishes and maintains information security ri...	**This is a new requirement**
6.1.2(a)(1)	the risk acceptance criteria; and	**4.2.1(b)(4), 4.2.1(c)(2), 5.1(f)**
6.1.2(a)(2)	criteria for performing information security risk...	**4.2.3(d)**
6.1.2(b)	ensures that repeated risk assessments shall prod...	**4.2.1(c)(2)**
6.1.2(c)	Identify the information security risks.	**4.2.1(d)**
6.1.2(c)(1)	apply the information security risk assessment pr...	**4.2.1(d)(1), 4.2.1(d)(2), 4.2.1(d)(3), 4.2.1(d)(4)**
6.1.2(c)(2)	identify the risk owners;	**4.2.1(d)(1)**
6.1.2(d)	analyses the information security risks:	**4.2.1(e)**
6.1.2(d)(1)	assess the potential consequences that would resu...	**4.2.1(e)(1)**
6.1.2(d)(2)	assess the realistic likelihood of the occurrence...	**4.2.1(e)(2)**
6.1.2(d)(3)	determine the levels of risk;	**4.2.1(e)(3)**
6.1.2(e)	evaluates the information security risks:	**4.2.1(e)(4)**
6.1.2(e)(1)	compare the results of risk analysis with the ris...	**4.2.1(e)(4)**
6.1.2(e)(2)	prioritise the analysed risks for risk treatment....	**4.2.1(e)(4)**
6.1.2(e)(2)	The organization shall retain documented informati...	**4.3.1(d), 4.3.1(e)**
6.1.3	The organization shall define and apply an informa...	**4.2.1(c)(1)**
6.1.3(a)	select appropriate information security risk trea...	**4.2.1(f), 4.2.1(f)(1), 4.2.1(f)(2), 4.2.1(f)(3), 4.2.1(f)(4)**
6.1.3(b)	determine all controls that are necessary to impl...	**4.2.1(g)**
6.1.3(c)	compare the controls determined in 6.1.3 b) above...	**4.2.1(j)(1), 4.2.1(j)(3)**
6.1.3(d)	produce a Statement of Applicability that contain...	**4.2.1(j), 4.2.1(j)(1), 4.2.1(j)(2), 4.2.1(j)(3), 4.3.1(i)**
6.1.3(e)	formulate an information security risk treatment ...	**4.2.2(a)**
6.1.3(f)	obtain risk owners' approval of the information s...	**4.2.1(h)**
6.1.3(f)	The organization shall retain documented informati...	**4.3.1(f)**
6.2	The organization shall establish information secur...	**5.1(b)**
6.2(a)	be consistent with the information security polic...	**5.1(d)**
6.2(b)	be measurable (if practicable)	**This is a new requirement**
6.2(c)	take into account applicable information security...	**This is a new requirement**
6.2(c)	and results from risk assessment and risk treatmen...	**This is a new requirement**
6.2(d)	be communicated, and	**5.1(d)**
6.2(e)	be updated as appropriate.	**4.2.3(b)**
6.2(e)	The organization shall retain documented informati...	**4.3.1(a)**
6.2(f)	what will be done;	**This is a new requirement**

Continued >>

Clause (in ISO/IEC 27001:2013)	Requirement	ISO/IEC 27001:2005
6.2(g)	what resources will be required;	**This is a new requirement**
6.2(h)	who will be responsible;	**This is a new requirement**
6.2(i)	when it will be completed; and	**This is a new requirement**
6.2(k)	how the results will be evaluated.	**This is a new requirement**
7.1	The organization shall determine and provide the r...	**4.2.2(g), 5.2.1**
7.2(a)	determine the necessary competence of person(s) d...	**5.2.2, 5.2.2(a)**
7.2(b)	ensure these persons are competent on the basis o...	**5.2.2**
7.2(c)	where applicable, take actions to acquire the nec...	**5.2.2(b), 5.2.2(c)**
7.2(d)	retain appropriate documented information as evid...	**5.2.2(d)**
7.3(a)	the information security policy;	**This is a new requirement**
7.3(b)	their contribution to the effectiveness of the in...	**4.2.2(e), 5.2.2(d)**
7.3(c)	the implications of not conforming with the infor...	**4.2.2(e), 5.2.2(d)**
7.4	The organization shall determine the need for inte...	**4.2.4(c), 5.1(d)**
7.4(a)	on what to communicate;	**This is a new requirement**
7.4(b)	when to communicate;	**This is a new requirement**
7.4(c)	with whom to communicate;	**This is a new requirement**
7.4(d)	who shall communicate; and	**This is a new requirement**
7.4(e)	the processes by which communication shall be eff...	**This is a new requirement**
7.5.1(a)	documented information required by this Internati...	**4.3.1(a), 4.3.1(b), 4.3.1(h), 4.3.1(i)**
7.5.1(b)	documented information determined by the organiza...	**This is a new requirement**
7.5.2(a)	identification and description (e.g. a title, dat...	**4.3.2(j)**
7.5.2(b)	format(e.g. language, software version, graphics)...	4.3.1(i)
7.5.2(c)	review and approval for suitability and adequacy.	**4.3.2(a), 4.3.2(b)**
7.5.3	Documented information required by the information...	4.3.2
7.5.3(a)	it is available and suitable for use, where and w...	**4.3.2(d)**
7.5.3(b)	it is adequately protected (e.g. from loss of con...	**4.3.3**
7.5.3(c)	distribution, access, retrieval and use;	**4.3.2(f), 4.3.2(h), 4.3.2(i)**
7.5.3(d)	storage and preservation, including preservation ...	**4.3.2(e), 4.3.3**
7.5.3(e)	control of changes (e.g. version control);	**4.3.2(c)**
7.5.3(f)	retention and disposition	**4.3.2(f)**
7.5.3(f)	Documented information of external origin determin...	**4.3.2(g)**
8.1	The organization shall plan, implement and control...	**This is a new requirement**
8.1	The organization shall also implement plans to ach...	**4.2.2(f)**
8.1	The organization shall keep documented information...	**4.3.3**
8.1	The organization shall control planned changes and...	**A.10.1.2, A.12.5.1, A.12.5.2, A.12.5.3**
8.1	review the consequences of unintended changes, tak...	**4.2.2(h), 8.3(b), 8.3(c)**

Continued >>

Clause (in ISO/IEC 27001:2013)	Requirement	ISO/IEC 27001:2005
8.1	The organization shall ensure that outsourced proc...	**A.10.2.1, A.10.2.2, A.10.2.3, A.12.5.5**
8.2	The organization shall perform information securit...	**4.2.3(d)**
8.2	The organization shall retain documented informati...	**4.3.1(e)**
8.3	The organization shall implement the information s...	**4.2.2(b), 4.2.2(c)**
8.3	The organization shall retain documented informati...	**4.3.3**
9.1	The organization shall evaluate the information se...	**4.2.3(a)(3), 4.2.3(b), 4.2.3(c), 4.2.3(f), 6(d)**
9.1(a)	what needs to be monitored and measured, including...	**4.2.2(d)**
9.1(b)	the methods for monitoring, measurement, analysis...	**4.2.2(d)**
9.1(c)	when the monitoring and measuring shall be perfor...	**This is a new requirement**
9.1(d)	who shall monitor and measure;	**This is a new requirement**
9.1(e)	when the results from monitoring and measurement ...	**4.2.3(b)**
9.1(f)	who shall analyse and evaluate these results.	**This is a new requirement**
9.1(f)	The organization shall retain appropriate document...	**4.3.1(g)**
9.2	The organization shall conduct internal audits at ...	**4.2.3(e), 6**
9.2(a)(1)	the organization's own requirements for its infor...	**6(b)**
9.2(a)(2)	the requirements of this International Standard.	**6(a)**
9.2(b)	is effectively implemented and maintained.	**6(c)**
9.2(c)	plan, establish, implement and maintain an audit ...	**6(d)**
9.2(d)	define the audit criteria and scope for each audi...	**6(d)**
9.2(e)	select auditors and conduct audits to ensure obje...	**6(d)**
9.2(f)	ensure that the results of the audits are reporte...	**6(d)**
9.2(g)	retain documented information as evidence of the ...	**4.3.1(h), 4.3.3**
9.3	Top management shall review the organization's inf...	**5.2.1(e), 7.1**
9.3(a)	the status of actions from previous management re...	**7.2(g)**
9.3(b)	changes in external and internal issues that are ...	**4.2.3(d)(1), 4.2.3(d)(2), 4.2.3(d)(3), 4.2.3(d)(4), 4.2.3(d)(5), 4.2.3(d)(6), 7.2(c), 7.2(e), 7.2(h)**
9.3(c)	feedback on the information security performance,...	**7.2(f)**
9.3(c)(1)	nonconformities and corrective actions;	**7.2(d)**
9.3(c)(2)	monitoring and measurement evaluation results;	**7.2(f)**
9.3(c)(3)	audit results; and	**7.2(a)**
9.3(c)(4)	fulfilment of information security objectives;	**This is a new requirement**
9.3(d)	feedback from interested parties;	**7.2(b)**
9.3(e)	results of risk assessment and status of risk tre...	7.2(e), 7.2(f)
9.3(f)	opportunities for continual improvement.	**7.2(i)**
9.3(f)	The outputs of the management review shall include...	**4.2.3(f), 7.1, 7.3(a)**

Continued >>

Clause (in ISO/IEC 27001:2013)	Requirement	ISO/IEC 27001:2005
9.3(f)	and any need for changes to the information securi...	**4.2.3(d)(1), 4.2.3(d)(2), 4.2.3(d)(3), 4.2.3(d)(5), 4.2.3(d)(6), 4.2.3(g), 7.1, 7.3(b), 7.3(c), 7.3(c)(1), 7.3(c)(2), 7.3(c)(3), 7.3(c)(4), 7.3(c)(5), 7.3(c) (6), 7.3(d), 7.3(e)**
9.3(f)	The organization shall retain documented informati...	**4.3.1(h), 7.1**
10.1(a)	react to the nonconformity, and as applicable:	**This is a new requirement**
10.1(a)(1)	take action to control and correct it; and	**This is a new requirement**
10.1(a)(2)	deal with the consequences;	**This is a new requirement**
10.1(b)	evaluate the need for action to eliminate the cau...	**8.2(c), 8.3(b)**
10.1(b)(1)	reviewing the nonconformity;	**8.2(a)**
10.1(b)(2)	determining the causes of the nonconformity;	**8.2(b)**
10.1(b)(3)	determining if similar nonconformities exist, or ...	**8.3(a)**
10.1(c)	implement any action needed;	**4.2.4(b), 8.2, 8.2(d)**
10.1(d)	review the effectiveness of any corrective action...	**8.2, 8.2(f)**
10.1(e)	make changes to the information security manageme...	**This is a new requirement**
10.1(e)	Corrective actions shall be appropriate to the eff...	**8.3**
10.1(f)	the nature of the nonconformities and any subsequ...	**This is a new requirement**
10.1(g)	the results of any corrective action.	**8.2(e)**
10.2	The organization shall continually improve the sui...	**4.2.4(a), 4.2.4(b), 4.2.4(d), 5.2.1(f), 8.1**

Mapping of ISO/IEC 27001:2005 to ISO/IEC 27001:2013

Clause (in ISO/IEC 27001:2005)	Requirement	ISO/IEC 27001:2013
4.1	The organization shall establish, implement, opera...	**4.4**
4.2.1(a)	Define the scope and boundaries of the ISMS in te...	**4.3**
4.2.1(b)	Define an ISMS policy in terms of the characteris...	**5.2(a)**
4.2.1(b)(1)	includes a framework for setting objectives and e...	**5.2(b)**
4.2.1(b)(2)	takes into account business and legal or regulato...	**5.2(c)**
4.2.1(b)(3)	aligns with the organization's strategic risk man...	**5.1(a)**
4.2.1(b)(4)	establishes criteria against which risk will be e...	**6.1.2(a)(1)**
4.2.1(b)(5)	has been approved by management.	**5.2**
4.2.1(c)	Define the risk assessment approach of the organi...	**6.1.2**
4.2.1(c)(1)	Identify a risk assessment methodology that is su...	**6.1.2, 6.1.3**
4.2.1(c)(2)	Develop criteria for accepting risks and identify...	**6.1.2(a)(1)**
4.2.1(c)(2)	The risk assessment methodology selected shall ens...	**6.1.2(b)**
4.2.1(d)	Identify the risks.	**6.1.1, 6.1.2(c)**
4.2.1(d)(1)	Identify the assets within the scope of the ISMS,...	**6.1.2(c)(1), 6.1.2(c)(2)**
4.2.1(d)(2)	Identify the threats to those assets.	**6.1.2(c)(1)**
4.2.1(d)(3)	Identify the vulnerabilities that might be exploi...	**6.1.2(c)(1)**
4.2.1(d)(4)	Identify the impacts that losses of confidentiali...	**6.1.2(c)(1)**
4.2.1(e)	Analyse and evaluate the risks.	**6.1.2(d)**
4.2.1(e)(1)	Assess the business impact upon the organization ...	**6.1.2(d)(1)**
4.2.1(e)(2)	Assess the realistic likelihood of such a securit...	**6.1.2(d)(2)**
4.2.1(e)(3)	Estimate the levels of risks.	**6.1.2(d)(3)**
4.2.1(e)(4)	Determine whether the risk is acceptable or requi...	**6.1.1(d), 6.1.2(e), 6.1.2(e)(1), 6.1.2(e)(2)**
4.2.1(f)	Identify and evaluate options for the treatment o...	**6.1.3(a)**
4.2.1(f)(1)	applying appropriate controls;	**6.1.3(a)**
4.2.1(f)(2)	knowingly and objectively accepting risks, provid...	**6.1.3(a)**
4.2.1(f)(3)	avoiding risks; and	**6.1.3(a)**
4.2.1(f)(4)	transferring the associated business risks to oth...	**6.1.3(a)**
4.2.1(g)	Select control objectives and controls for the tr...	**6.1.3(b)**
4.2.1(g)	Controls objectives and controls shall be selected...	**6.1.3(b)**
4.2.1(g)	The control objectives and controls from Annex A s...	**This is a deleted requirement**
4.2.1(h)	Obtain management approval of the proposed residu...	**6.1.3(f)**
4.2.1(i)	Obtain management authorization to implement and ...	**This is a deleted requirement**
4.2.1(j)	A Statement of Applicability shall be prepared tha...	**6.1.3(d)**
4.2.1(j)(1)	the control objectives and controls, selected in ...	**6.1.3(c), 6.1.3(d)**
4.2.1(j)(2)	the control objectives and controls currently imp...	**6.1.3(d)**

Continued >>

Clause (in ISO/IEC 27001:2005)	Requirement	ISO/IEC 27001:2013
4.2.1(j)(3)	the exclusion of any control objectives and contr...	**6.1.3(c), 6.1.3(d)**
4.2.2(a)	Formulate a risk treatment plan that identifies t...	**6.1.3(e)**
4.2.2(b)	Implement the risk treatment plan in order to ach...	**8.3**
4.2.2(c)	Implement controls selected in 4.2.1g) to meet th...	**8.3**
4.2.2(d)	Define how to measure the effectiveness of the se...	**9.1(a), 9.1(b)**
4.2.2(e)	Implement training and awareness programmes (see ...	7.3(b), 7.3(c)
4.2.2(f)	Manage operations of the ISMS.	**8.1**
4.2.2(g)	Manage resources for the ISMS (see 5.2).	**7.1**
4.2.2(h)	Implement procedures and other controls capable o...	**8.1**
4.2.3(a)(1)	promptly detect errors in the results of processi...	**This is a deleted requirement**
4.2.3(a)(2)	promptly identify attempted and successful securi...	**This is a deleted requirement**
4.2.3(a)(3)	enable management to determine whether the securi...	**9.1**
4.2.3(a)(4)	help detect security events and thereby prevent s...	**This is a deleted requirement**
4.2.3(a)(5)	determine whether the actions taken to resolve a ...	**This is a deleted requirement**
4.2.3(b)	Undertake regular reviews of the effectiveness of...	**6.2(e), 9.1, 9.1(e)**
4.2.3(c)	Measure the effectiveness of controls to verify t...	**9.1**
4.2.3(d)	Review risk assessments at planned intervals and ...	**6.1.2(a)(2), 8.2**
4.2.3(d)(1)	the organization;	**9.3(b), 9.3(f)**
4.2.3(d)(2)	technology;	**9.3(b), 9.3(f)**
4.2.3(d)(3)	business objectives and processes;	**9.3(b), 9.3(f)**
4.2.3(d)(4)	identified threats;	**9.3(b)**
4.2.3(d)(5)	effectiveness of the implemented controls; and	**9.3(b), 9.3(f)**
4.2.3(d)(6)	external events, such as changes to the legal or ...	**9.3(b), 9.3(f)**
4.2.3(e)	Conduct internal ISMS audits at planned intervals...	**9.2**
4.2.3(f)	Undertake a management review of the ISMS on a...	**4.3(a), 4.3(b), 9.1**
4.2.3(f)	improvements in the ISMS process are identified (s...	**9.3(f)**
4.2.3(g)	Update security plans to take into account the fi...	**9.3(f)**
4.2.3(h)	Record actions and events that could have an impa...	**This is a deleted requirement**
4.2.4(a)	Implement the identified improvements in the ISMS...	**10.2**
4.2.4(b)	Take appropriate corrective and preventive act...	**10.1(c)**
4.2.4(b)	Apply the lessons learnt from the security experie...	**10.2**
4.2.4(c)	Communicate the actions and improvements to all i...	**7.4**
4.2.4(d)	Ensure that the improvements achieve their intend...	10.2
4.3.1	Documentation shall include records of management ...	**This is a deleted requirement**
4.3.1	It is important to be able to demonstrate the rela...	**This is a deleted requirement**
4.3.1(a)	documented statements of the ISMS policy (see 4.2...	**5.2(e), 6.2(e), 7.5.1(a)**
4.3.1(b)	the scope of the ISMS	**(see 4.2.1a));4.3(c), 7.5.1(a)**

Continued >>

Clause (in ISO/IEC 27001:2005)	Requirement	ISO/IEC 27001:2013
4.3.1(c)	procedures and controls in support of the ISMS;	**This is a deleted requirement**
4.3.1(d)	a description of the risk assessment methodology...	**6.1.2(e)(2)**
4.3.1(e)	the risk assessment report (see 4.2.1c) to 4.2.1g...	**6.1.2(e)(2), 8.2**
4.3.1(f)	the risk treatment plan (see 4.2.2b));	**6.1.1(e)(1), 6.1.3(f)**
4.3.1(g)	documented procedures needed by the organizati...	**9.1(f)**
4.3.1(g)	and describe how to measure the effectiveness of c...	**9.1(f)**
4.3.1(h)	records required by this International Standard (...	**7.5.1(a), 9.2(g), 9.3(f)**
4.3.1(i)	the Statement of Applicability.	**6.1.3(d), 7.5.1(a)**
4.3.1(i)	NOTE 3: Documents and records may be in any form o...	**7.5.2(b)**
4.3.2	Documents required by the ISMS shall be protected ...	**7.5.3**
4.3.2	A documented procedure shall be established to def...	**This is a deleted requirement**
4.3.2(a)	approve documents for adequacy prior to issue;	**7.5.2(c)**
4.3.2(b)	review and update documents as necessary and re-a...	**7.5.2(c)**
4.3.2(c)	ensure that changes and the current revision stat...	**7.5.3(e)**
4.3.2(d)	ensure that relevant versions of applicable docum...	**7.5.3(a)**
4.3.2(e)	ensure that documents remain legible and readily ...	**7.5.3(d)**
4.3.2(f)	ensure that documents are available to those w...	**5.2(g), 7.5.3(c)**
4.3.2(f)	and are transferred, stored and ultimately	**7.5.3(f)**
4.3.2(f)	disposed of in accordance with the procedures appl...	**7.5.3(f)**
4.3.2(g)	ensure that documents of external origin are iden...	**7.5.3(f)**
4.3.2(h)	ensure that the distribution of documents is cont...	**7.5.3(c)**
4.3.2(i)	prevent the unintended use of obsolete documents;...	**7.5.3(c)**
4.3.2(j)	apply suitable identification to them if they are...	**7.5.2(a)**
4.3.3	Records shall be established and maintained to pro...	**9.2(g)**
4.3.3	They shall be protected and controlled.	**7.5.3(b)**
4.3.3	The ISMS shall take account of any relevant legal ...	**5.2(c)**
4.3.3	Records shall remain legible, readily identifiable...	**7.5.3(d)**
4.3.3	The controls needed for the identification, storag...	**This is a deleted requirement**
4.3.3	Records shall be kept of the performance of the pr...	**5.3(a), 5.3(b), 8.1, 8.3**
4.3.3	and of all occurrences of significant security inc...	**This is a deleted requirement**
5.1	Management shall provide evidence of its commitmen...	**5.1(h)**
5.1(a)	establishing an ISMS policy;	**5.2**
5.1(b)	ensuring that ISMS objectives and plans are estab...	**5.1(e), 5.1(f), 6.2**
5.1(c)	establishing roles and responsibilities for infor...	**5.3**
5.1(d)	communicating to the organization the importan...	**5.1(d), 5.2(f), 6.2(a), 6.2(d), 7.4**
5.1(d)	and the need for continual improvement;	**5.1(g), 5.2(d)**
5.1(e)	providing sufficient resources to establish, impl...	**5.1(c)**

Continued >>

Clause (in ISO/IEC 27001:2005)	Requirement	ISO/IEC 27001:2013
5.1(f)	deciding the criteria for accepting risks and for...	**6.1.2(a)(1)**
5.1(g)	ensuring that internal ISMS audits are conducted ...	**5.1(e), 5.1(f)**
5.1(h)	conducting management reviews of the ISMS (see 7)...	**5.1(e), 5.1(f)**
5.2.1	The organization shall determine and provide the r...	**7.1**
5.2.1(a)	establish, implement, operate, monitor, review, m...	**4.4**
5.2.1(b)	ensure that information security procedures suppo...	**This is a deleted requirement**
5.2.1(c)	identify and address legal and regulatory require...	**4.2(b)**
5.2.1(d)	maintain adequate security by correct application...	**This is a deleted requirement**
5.2.1(e)	carry out reviews when necessary, and to react ap...	**9.3**
5.2.1(f)	where required, improve the effectiveness of the ...	**10.2**
5.2.2	The organization shall ensure that all personnel w...	**7.2(a), 7.2(b)**
5.2.2(a)	determining the necessary competencies for person...	**7.2(a)**
5.2.2(b)	providing training or taking other actions (e.g. ...	**7.2(c)**
5.2.2(c)	evaluating the effectiveness of the actions taken...	**7.2(c)**
5.2.2(d)	maintaining records of education, training, skill...	**7.2(d)**
5.2.2(d)	The organization shall also ensure that all releva...	**7.3(b), 7.3(c)**
6	The organization shall conduct internal ISMS audit...	**9.2**
6(a)	conform to the requirements of this International...	**9.2(a)(2)**
6(b)	conform to the identified information security re...	**9.2(a)(1)**
6(c)	are effectively implemented and maintained; and	**9.2(b)**
6(d)	perform as expected.	**9.1**
6(d)	An audit programme shall be planned, taking into c...	**9.2(c)**
6(d)	The audit criteria, scope,	**9.2(d)**
6(d)	frequency and methods shall be defined.	**9.2(c)**
6(d)	Selection of auditors and conduct of audits shall ...	**9.2(e)**
6(d)	Auditors shall not audit their own work.	**9.2(e)**
6(d)	The responsibilities and requirements for planning...	**This is a deleted requirement**
6(d)	The management responsible for the area being audi...	**9.2(f)**
7.1	Management shall review the organization's ISMS at...	**9.3**
7.1	This review shall include assessing opportunities ...	**9.3(f)**
7.1	and the need for changes to the ISMS, including th...	**9.3(f)**
7.1	The results of the reviews shall be clearly docume...	**9.3(f)**
7.2(a)	results of ISMS audits and reviews;	**9.3(c)(3)**
7.2(b)	feedback from interested parties;	**9.3(d)**
7.2(c)	techniques, products or procedures, which could b...	**9.3(b)**
7.2(d)	status of preventive and corrective actions;	**9.3(c)(1)**
7.2(e)	vulnerabilities or threats not adequately address...	**9.3(b), 9.3(e)**

Continued >>

Clause (in ISO/IEC 27001:2005)	Requirement	ISO/IEC 27001:2013
7.2(f)	results from effectiveness measurements;	**6.1.1(e)(2), 9.3(c), 9.3(c)(2), 9.3(e)**
7.2(g)	follow-up actions from previous management review...	**9.3(a)**
7.2(h)	any changes that could affect the ISMS; and	**9.3(b)**
7.2(i)	recommendations for improvement.	**9.3(f)**
7.3(a)	Improvement of the effectiveness of the ISMS.	**9.3(f)**
7.3(b)	Update of the risk assessment and risk treatment ...	**9.3(f)**
7.3(c)	Modification of procedures and controls that effe...	**9.3(f)**
7.3(c)(1)	business requirements;	**9.3(f)**
7.3(c)(2)	security requirements ;	**9.3(f)**
7.3(c)(3)	business processes effecting the existing busines...	**9.3(f)**
7.3(c)(4)	regulatory or legal requirements;	**4.2(b), 9.3(f)**
7.3(c)(5)	contractual obligations; and	**4.2(b), 9.3(f)**
7.3(c)(6)	levels of risk and/or risk acceptance criteria.	**9.3(f)**
7.3(d)	Resource needs.	**9.3(f)**
7.3(e)	Improvement to how the effectiveness of controls ...	**9.3(f)**
8.1	The organization shall continually improve the eff...	**10.2**
8.2	The organization shall take action to eliminate th...	**10.1(c), 10.1(d)**
8.2	The documented procedure for corrective action sha...	**This is a deleted requirement**
8.2(a)	identifying nonconformities;	**10.1(b)(1)**
8.2(b)	determining the causes of nonconformities;	**10.1(b)(2)**
8.2(c)	evaluating the need for actions to ensure that no...	**10.1(b)**
8.2(d)	determining and implementing the corrective actio...	**10.1(c)**
8.2(e)	recording results of action taken (see 4.3.3); an...	**10.1(g)**
8.2(f)	reviewing of corrective action taken.	**10.1(d)**
8.3	The organization shall determine action to elimina...	**4.1**
8.3	Preventive actions taken shall be appropriate to t...	**10.1(e)**
8.3	The documented procedure for preventive action sha...	**This is a deleted requirement**
8.3(a)	identifying potential nonconformities and their c...	**4.1, 6.1.1, 10.1(b)(3)**
8.3(b)	evaluating the need for action to prevent occurre...	**6.1.1(d), 8.1, 10.1(b)**
8.3(c)	determining and implementing preventive action ne...	**6.1.1(d), 6.1.1(e)(1), 8.1**
8.3(d)	recording results of action taken (see 4.3.3); an...	**This is a deleted requirement**
8.3(e)	reviewing of preventive action taken.	**This is a deleted requirement**
8.3(e)	The organization shall identify changed risks and ...	**4.1**
8.3(e)	The priority of preventive actions shall be determ...	**This is a deleted requirement**

Deleted ISMS requirements

Clause (in ISO/IEC 27001:2005)	Deleted requirement
4.2.1(g)	The control objectives and controls from Annex A shall be selected as part of this process as suitable to cover these requirements.
4.2.1(i)	Obtain management authorization to implement and operate the ISMS.
4.2.3(a)(1)	promptly detect errors in the results of processing;
4.2.3(a)(2)	promptly identify attempted and successful security breaches and incidents;
4.2.3(a)(4)	help detect security events and thereby prevent security incidents by the use of indicators; and
4.2.3(a)(5)	determine whether the actions taken to resolve a breach of security were effective.
4.2.3(h)	Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3).
4.3.1	Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and the recorded results are reproducible.
4.3.1	It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessment and risk treatment process, and subsequently back to the ISMS policy and objectives.
4.3.1(c)	procedures and controls in support of the ISMS;
4.3.2	A documented procedure shall be established to define the management actions needed to:
4.3.3	The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.
4.3.3	and of all occurrences of significant security incidents related to the ISMS.
5.2.1(b)	ensure that information security procedures support the business requirements;
5.2.1(d)	maintain adequate security by correct application of all implemented controls;
6(d)	The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.3.3) shall be defined in a documented procedure.
8.2	The documented procedure for corrective action shall define requirements for:
8.3	The documented procedure for preventive action shall define requirements for:
8.3(d)	recording results of action taken (see 4.3.3); and
8.3(e)	reviewing of preventive action taken.
8.3(e)	The priority of preventive actions shall be determined based on the results of the risk assessment.

Group 2 - Annex A controls

New Annex A controls

Annex A control (in ISO/IEC 27001:2013)		
A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of project.
A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be established and implemented.
A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development efforts.
A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure development environment for system development and integration efforts that cover the entire system development lifecycle.
A.14.2.8	System security testing	Testing of security functionality shall be carried out during development.
A.15.1.1	Information security policy for supplier relationships	Information security requirements for mitigating the risks associated with supplier access to organization's assets shall be documented.
A.15.1.3	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.
A.16.1.4	Assessment and decision on information security events	Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.
A.16.1.5	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.
A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.

Mapping of Annex A controls in ISO/IEC 27001:2013 to ISO/IEC 27001:2005

Annex A control (in ISO/IEC 27001:2013)		Annex A control (in ISO/IEC 27001:2005)
A.5.1.1	Policies for information security	**A.5.1.1**
A.5.1.2	Review of the policies for information security	**A.5.1.2**
A.6.1.1	Information security roles and responsibilities	**A.6.1.3, A.8.1.1**
A.6.1.2	Segregation of duties	**A.10.1.3**
A.6.1.3	Contact with authorities	**A.6.1.6**
A.6.1.4	Contact with special interest groups	**A.6.1.7**
A.6.1.5	Information security in project management	**This is a new Annex A control**
A.6.2.1	Mobile device policy	**A.11.7.1**
A.6.2.2	Teleworking	**A.11.7.2**
A.7.1.1	Screening	**A.8.1.2**
A.7.1.2	Terms and conditions of employment	**A.8.1.3**
A.7.2.1	Management responsibilities	**A.8.2.1**
A.7.2.2	Information security awareness, education and training	**A.8.2.2**
A.7.2.3	Disciplinary process	**A.8.2.3**
A.7.3.1	Termination or change of employment responsibilities	**A.8.3.1**
A.8.1.1	Inventory of assets	**A.7.1.1**
A.8.1.2	Ownership of assets	**A.7.1.2**
A.8.1.3	Acceptable use of assets	**A.7.1.3**
A.8.1.4	Return of assets	**A.8.3.2**
A.8.2.1	Classification of information	**A.7.2.1**
A.8.2.2	Labelling of information	**A.7.2.2**
A.8.2.3	Handling of assets	**A.10.7.3**
A.8.3.1	Management of removable media	**A.10.7.1**
A.8.3.2	Disposal of media	**A.10.7.2**
A.8.3.3	Physical media transfer	**A.10.8.3**
A.9.1.1	Access control policy	**A.11.1.1**
A.9.1.2	Access to networks and network services	**A.11.4.1**
A.9.2.1	User registration and de-registration	**A.11.2.1, A.11.5.2**
A.9.2.2	User access provisioning	**A.11.2.1**
A.9.2.3	Privilege management	**A.11.2.2**
A.9.2.4	Management of secret authentication information of users	**A.11.2.3**
A.9.2.5	Review of user access rights	**A.11.2.4**
A.9.2.6	Removal or adjustment of access rights	**A.8.3.3**
A.9.3.1	Use of secret authentication information	**A.11.3.1**

Continued >>

Annex A control (in ISO/IEC 27001:2013)		Annex A control (in ISO/IEC 27001:2005)
A.9.4.1	Information access restriction	**A.11.6.1**
A.9.4.2	Secure log-on procedures	**A.11.5.1, A.11.5.5, A.11.5.6**
A.9.4.3	Password management system	**A.11.5.3**
A.9.4.4	Use of privileged utility programs	**A.11.5.4**
A.9.4.5	Access control to program source code	**A.12.4.3**
A.10.1.1	Policy on the use of cryptographic controls	**A.12.3.1**
A.10.1.2	Key management	**A.12.3.2**
A.11.1.1	Physical security perimeter	**A.9.1.1**
A.11.1.2	Physical entry controls	**A.9.1.2**
A.11.1.3	Securing office, rooms and facilities	**A.9.1.3**
A.11.1.4	Protecting against external end environmental threats	**A.9.1.4**
A.11.1.5	Working in secure areas	**A.9.1.5**
A.11.1.6	Delivery and loading areas	**A.9.1.6**
A.11.2.1	Equipment siting and protection	**A.9.2.1**
A.11.2.2	Supporting utilities	**A.9.2.2**
A.11.2.3	Cabling security	**A.9.2.3**
A.11.2.4	Equipment maintenance	**A.9.2.4**
A.11.2.5	Removal of assets	**A.9.2.7**
A.11.2.6	Security of equipment and assets off-premises	**A.9.2.5**
A.11.2.7	Security disposal or re-use of equipment	**A.9.2.6**
A.11.2.8	Unattended user equipment	**A.11.3.2**
A.11.2.9	Clear desk and clear screen policy	**A.11.3.3**
A.12.1.1	Documented operating procedures	**A.10.1.1**
A.12.1.2	Change management	**A.10.1.2**
A.12.1.3	Capacity management	**A.10.3.1**
A.12.1.4	Separation of development, test and operational environments	**A.10.1.4**
A.12.2.1	Controls against malware	**A.10.4.1, A.10.4.2**
A.12.3.1	Information backup	**A.10.5.1**
A.12.4.1	Event logging	**A.10.10.1, A.10.10.2, A.10.10.5**
A.12.4.2	Protection of log information	**A.10.10.3**
A.12.4.3	Administrator and operator logs	**A.10.10.3, A.10.10.4**
A.12.4.4	Clock synchronisation	**A.10.10.6**
A.12.5.1	Installation of software on operational systems	**A.12.4.1**
A.12.6.1	Management of technical vulnerabilities	**A.12.6.1**
A.12.6.2	Restrictions on software installation	**This is a new Annex A control**
A.12.7.1	Information systems audit controls	**A.15.3.1**
A.13.1.1	Network controls	**A.10.6.1**

Continued >>

Annex A control (in ISO/IEC 27001:2013)		Annex A control (in ISO/IEC 27001:2005)
A.13.1.2	Security of network services	**A.10.6.2**
A.13.1.3	Segregation in networks	**A.11.4.5**
A.13.2.1	Information transfer policies and procedures	**A.10.8.1**
A.13.2.2	Agreements on information transfer	**A.10.8.2**
A.13.2.3	Electronic messaging	**A.10.8.4**
A.13.2.4	Confidentiality or non-disclosure agreements	**A.6.1.5**
A.14.1.1	Security requirements analysis and specification	**A.12.1.1**
A.14.1.2	Securing applications services on public networks	**A.10.9.1, A.10.9.3**
A.14.1.3	Protecting application services transactions	**A.10.9.2**
A.14.2.1	Secure development policy	**This is a new Annex A control**
A.14.2.2	System change control procedures	**A.12.5.1**
A.14.2.3	Technical review of applications after operating platform changes	**A.12.5.2**
A.14.2.4	Restrictions on changes to software packages	**A.12.5.3**
A.14.2.5	Secure system engineering principles	**This is a new Annex A control**
A.14.2.6	Secure development environment	**This is a new Annex A control**
A.14.2.7	Outsourced development	**A.12.5.5**
A.14.2.8	System security testing	**This is a new Annex A control**
A.14.2.9	System acceptance testing	**A.10.3.2**
A.14.3.1	Protection of test data	**A.12.4.2**
A.15.1.1	Information security policy for supplier relationships	**This is a new Annex A control**
A.15.1.2	Addressing security within supplier agreements	**A.6.2.3**
A.15.1.3	Information and communication technology supply chain	**This is a new Annex A control**
A.15.2.1	Monitoring and review of supplier services	**A.10.2.2**
A.15.2.2	Managing changes to supplier services	**A.10.2.3**
A.16.1.1	Responsibilities and procedures	**A.13.2.1**
A.16.1.2	Reporting information security events	**A.13.1.1**
A.16.1.3	Reporting information security weaknesses	**A.13.1.2**
A.16.1.4	Assessment and decision on information security events	**This is a new Annex A control**
A.16.1.5	Response to information security incidents	**This is a new Annex A control**
A.16.1.6	Learning from information security incidents	**A.13.2.2**
A.16.1.7	Collection of evidence	**A.13.2.3**
A.17.1.1	Planning information security continuity	**A.14.1.2**
A.17.1.2	Implementing information security continuity	**A.14.1.1, A.14.1.3, A.14.1.4**
A.17.1.3	Verify, review and evaluate information security continuity	**A.14.1.5**
A.17.2.1	Availability of information processing facilities	**This is a new Annex A control**
A.18.1.1	Identification of applicable legislation and contractual requirements	**A.15.1.1**
A.18.1.2	Intellectual property rights (IPR)	**A.15.1.2**

Continued >>

Annex A control (in ISO/IEC 27001:2013)		Annex A control (in ISO/IEC 27001:2005)
A.18.1.3	Protection of records	**A.15.1.3**
A.18.1.4	Privacy and protection of personally identifiable information	**A.15.1.4**
A.18.1.5	Regulation of cryptographic controls	**A.15.1.6**
A.18.2.1	Independent review of information security	**A.6.1.8**
A.18.2.2	Compliance with security policies and standards	**A.15.2.1**
A.18.2.3	Technical compliance review	**A.15.2.2**

Mapping of Annex A controls in ISO/IEC 27001:2005 to ISO/IEC 27001:2013

ISO/IEC 27001:2005		ISO/IEC 27001:2013
A.5.1.1	Information security policy document	**A.5.1.1**
A.5.1.2	Review of the information security policy	**A.5.1.2**
A.6.1.1	Management commitment to information security	**This is a deleted Annex A control**
A.6.1.2	Information security coordination	**This is a deleted Annex A control**
A.6.1.3	Allocation of information security responsibilities	**A.6.1.1**
A.6.1.4	Authorisation process for information processing facilities	**This is a deleted Annex A control**
A.6.1.5	Confidentiality agreements	**A.13.2.4**
A.6.1.6	Contact with authorities	**A.6.1.3**
A.6.1.7	Contact with special interest groups	**A.6.1.4**
A.6.1.8	Independent review of information security	**A.18.2.1**
A.6.2.1	Identification of risks related to external parties	**This is a deleted Annex A control**
A.6.2.2	Addressing security when dealing with customers	**This is a deleted Annex A control**
A.6.2.3	Addressing security in third party agreements	**A.15.1.2**
A.7.1.1	Inventory of assets	**A.8.1.1**
A.7.1.2	Ownership of assets	**A.8.1.2**
A.7.1.3	Acceptable use of assets	**A.8.1.3**
A.7.2.1	Classification guidelines	**A.8.2.1**
A.7.2.2	Information labeling and handling	**A.8.2.2**
A.8.1.1	Roles and responsibilities	**A.6.1.1**
A.8.1.2	Screening	**A.7.1.1**
A.8.1.3	Terms and conditions of employment	**A.7.1.2**
A.8.2.1	Management responsibilities	**A.7.2.1**

Continued >>

ISO/IEC 27001:2005		ISO/IEC 27001:2013
A.8.2.2	Information security awareness, education and training	**A.7.2.2**
A.8.2.3	Disciplinary process	**A.7.2.3**
A.8.3.1	Termination responsibilities	**A.7.3.1**
A.8.3.2	Return of assets	**A.8.1.4**
A.8.3.3	Removal of access rights	**A.9.2.6**
A.9.1.1	Physical security perimeter	**A.11.1.1**
A.9.1.2	Physical entry controls	**A.11.1.2**
A.9.1.3	Securing offices, rooms and facilities	**A.11.1.3**
A.9.1.4	Protecting against external and environmental threats	**A.11.1.4**
A.9.1.5	Working in secure areas	**A.11.1.5**
A.9.1.6	Public access, delivery and loading areas	**A.11.1.6**
A.9.2.1	Equipment sitting and protection	**A.11.2.1**
A.9.2.2	Supporting utilities	**A.11.2.2**
A.9.2.3	Cabling security	**A.11.2.3**
A.9.2.4	Equipment maintenance	**A.11.2.4**
A.9.2.5	Security of equipment off-premises	**A.11.2.6**
A.9.2.6	Secure disposal or re-use of equipment	**A.11.2.7**
A.9.2.7	Removal of property	**A.11.2.5**
A.10.1.1	Documented operating procedures	**A.12.1.1**
A.10.1.2	Change management	**8.1*, A.12.1.2**
A.10.1.3	Segregation of duties	**A.6.1.2**
A.10.1.4	Separation of development, test and operational facilities	**A.12.1.4**
A.10.2.1	Service delivery	**8.1***
A.10.2.2	Monitoring and review of third party services	**8.1*, A.15.2.1**
A.10.2.3	Managing changes to third party services	**8.1*, A.15.2.2**
A.10.3.1	Capacity management	**A.12.1.3**
A.10.3.2	System Acceptance	**A.14.2.9**
A.10.4.1	Controls against malicious code	**A.12.2.1**
A.10.4.2	Controls against mobile code	**A.12.2.1**
A.10.5.1	Information back-up	**A.12.3.1**
A.10.6.1	Network controls	**A.13.1.1**
A.10.6.2	Security of network services	**A.13.1.2**
A.10.7.1	Management of removable media	**A.8.3.1**
A.10.7.2	Disposal of Media	**A.8.3.2**
A.10.7.3	Information Handling procedures	**A.8.2.3**
A.10.7.4	Security of system documentation	**This is a deleted Annex A control**
A.10.8.1	Information exchange policies and procedures	**A.13.2.1**

Continued >>

ISO/IEC 27001:2005		ISO/IEC 27001:2013
A.10.8.2	Exchange agreements	**A.13.2.2**
A.10.8.3	Physical media in transit	**A.8.3.3**
A.10.8.4	Electronic messaging	**A.13.2.3**
A.10.8.5	Business Information Systems	**This is a deleted Annex A control**
A.10.9.1	Electronic commerce	**A.14.1.2**
A.10.9.2	Online-transactions	**A.14.1.3**
A.10.9.3	Publicly available information	**A.14.1.2**
A.10.10.1	Audit logging	**A.12.4.1**
A.10.10.2	Monitoring system use	**A.12.4.1**
A.10.10.3	Protection of log information	**A.12.4.2, A.12.4.3**
A.10.10.4	Administrator and operator logs	**A.12.4.3**
A.10.10.5	Fault logging	**A.12.4.1**
A.10.10.6	Clock synchronisation	**A.12.4.4**
A.11.1.1	Access control policy	**A.9.1.1**
A.11.2.1	User registration	**A.9.2.1, A.9.2.2**
A.11.2.2	Privilege management	**A.9.2.3**
A.11.2.3	User password management	**A.9.2.4**
A.11.2.4	Review of user access rights	**A.9.2.5**
A.11.3.1	Password use	**A.9.3.1**
A.11.3.2	Unattended user equipment	**A.11.2.8**
A.11.3.3	Clear desk and clear screen policy	**A.11.2.9**
A.11.4.1	Policy on use of network services	**A.9.1.2**
A.11.4.2	User authentication for external connections	**This is a deleted Annex A control**
A.11.4.3	Equipment identification in networks	**This is a deleted Annex A control**
A.11.4.4	Remote Diagnostic and configuration port protection	**This is a deleted Annex A control**
A.11.4.5	Segregation in Networks	**A.13.1.3**
A.11.4.6	Network Connection control	**This is a deleted Annex A control**
A.11.4.7	Network routing control	**This is a deleted Annex A control**
A.11.5.1	Secure log-on procedures	**A.9.4.2**
A.11.5.2	User identification and authentication	**A.9.2.1**
A.11.5.3	Password management system	**A.9.4.3**
A.11.5.4	Use of system utilities	**A.9.4.4**
A.11.5.5	Session time-out	**A.9.4.2**
A.11.5.6	Limitation of connection time	**A.9.4.2**
A.11.6.1	Information access restriction	**A.9.4.1**
A.11.6.2	Sensitive system isolation	**This is a deleted Annex A control**

Continued >>

ISO/IEC 27001:2005		ISO/IEC 27001:2013
A.11.7.1	Mobile computing and communications	**A.6.2.1**
A.11.7.2	Teleworking	**A.6.2.2**
A.12.1.1	Security requirements analysis and specification	**A.14.1.1**
A.12.2.1	Input data validation	**This is a deleted Annex A control**
A.12.2.2	Control of internal processing	**This is a deleted Annex A control**
A.12.2.3	Message integrity	**This is a deleted Annex A control**
A.12.2.4	Output data validation	**This is a deleted Annex A control**
A.12.3.1	Policy on the use of cryptographic controls	**A.10.1.1**
A.12.3.2	Key management	**A.10.1.2**
A.12.4.1	Control of operational software	**A.12.5.1**
A.12.4.2	Protection of system test data	**A.14.3.1**
A.12.4.3	Access control to program source code	**A.9.4.5**
A.12.5.1	Change control procedures	**8.1*, A.14.2.2**
A.12.5.2	Technical review of applications after operating system changes	**8.1*, A.14.2.3**
A.12.5.3	Restrictions on changes to software packages	**8.1*, A.14.2.4**
A.12.5.4	Information leakage	**This is a deleted Annex A control**
A.12.5.5	Outsourced software development	**8.1*, A.14.2.7**
A.12.6.1	Control of technical vulnerabilities	**A.12.6.1**
A.13.1.1	Reporting information security events	**A.16.1.2**
A.13.1.2	Reporting security weakness	**A.16.1.3**
A.13.2.1	Responsibilities and Procedures	**A.16.1.1**
A.13.2.2	Learning from information security incidents	**A.16.1.6**
A.13.2.3	Collection of evidence	**A.16.1.7**
A.14.1.1	Including information security in the business continuity management process	**A.17.1.2**
A.14.1.2	Business continuity and risk assessment	**A.17.1.1**
A.14.1.3	Developing and implementing continuity plans including formation security.	**A.17.1.2**
A.14.1.4	Business continuity planning framework	**A.17.1.2**
A.14.1.5	Testing, maintaining and re-assessing business continuity plans	**A.17.1.3**
A.15.1.1	Identification of applicable legislation	**A.18.1.1**
A.15.1.2	Intellectual property rights (IPR)	**A.18.1.2**
A.15.1.3	Protection of organisational records	**A.18.1.3**
A.15.1.4	Data protection and privacy of personal information	**A.18.1.4**
A.15.1.5	Prevention of misuse of information processing facilities	**This is a deleted Annex A control**
A.15.1.6	Regulation of cryptographic controls	**A.18.1.5**
A.15.2.1	Compliance with security policies and standards	**A.18.2.2**
A.15.2.2	Technical compliance checking	**A.18.2.3**
A.15.3.1	Information system audit controls	**A.12.7.1**
A.15.3.2	Protection of information systems audit tools	**This is a deleted Annex A control**

* These controls map (at least partially) onto ISMS requirements. For example, Clause 8.1 in ISO/IEC 27001:2013 requires organizations to ensure that outsourced processes are controlled.

Deleted Annex A controls

ISO/IEC 27001:2005 requirements that do not feature in ISO/IEC 27001:2013

A.6.1.1	Management commitment to information security
A.6.1.2	Information security coordination
A.6.1.4	Authorisation process for information processing facilities
A.6.2.1	Identification of risks related to external parties
A.6.2.2	Addressing security when dealing with customers
A.10.7.4	Security of system documentation
A.10.8.5	Business Information Systems
A.11.4.2	User authentication for external connections
A.11.4.3	Equipment identification in networks
A.11.4.4	Remote Diagnostic and configuration port protection
A.11.4.6	Network Connection control
A.11.4.7	Network routing control
A.11.6.2	Sensitive system isolation
A.12.2.1	Input data validation
A.12.2.2	Control of internal processing
A.12.2.3	Message integrity
A.12.2.4	Output data validation
A.12.5.4	Information leakage
A.15.1.5	Prevention of misuse of information processing facilities
A.15.3.2	Protection of information systems audit tools

Acknowledgement

These tables are based on work performed by David Brewer and Sabrina Feng and are reproduced by permission of IMS-Smart Limited.

BSI UK
Kitemark Court
Davy Avenue, Knowlhill
Milton Keynes, MK5 8PP
United Kingdom

T: +44 845 080 9000
E: certification.sales@bsigroup.com
bsigroup.com

We know ISO/IEC 27001;
BSI shaped the original standard.

BSI...

- Shaped the original ISO/IEC 27001 standard
- Has the most highly trained and knowledgeable assessors
- Offers the widest range of support solutions in the market place
- Is the number one certification body in the UK, USA and Korea
- Looks after more than 70,000 global clients
- Has an unrivalled International reputation for excellence

bsi.

BSI UK
Kitemark Court
Davy Avenue, Knowlhill
Milton Keynes, MK5 8PP
United Kingdom

T: +44 845 080 9000
E: certification.sales@bsigroup.com
bsigroup.com

Information Shield
www.informationshield.com
888.641.0500
sales@informationshield.com
Information Security Policies
Made Easy

ISO 27002:2013 Version Change Summary

This table highlights the control category changes between ISO 27002:2005 and the 2013 update. Changes are color coded.

Control Category Change Key

Control Removed

Control Moved or Renamed

Control Added (new outline)

Change Map Key

Minimum Changes to Domain

Several key changes to Domain

Major changes to Domain

Change	2005 Control Category	2013 Control Category
LOW	**5 SECURITY POLICY**	**5 IFNORMATION SECURITY POLICIES**
	5.1 INFORMATION SECURITY POLICY	5.1 Management direction for information security
	5.1.1 Information security policy document	5.1.1 Policies for information security
	5.1.2 Review of the information security policy	5.1.2 Review of the policies for information security
MED	**6 ORGANIZATION OF INFORMATION SECURITY**	**6 ORGANIZATION OF INFORMATION SECURITY**
	6.1 INTERNAL ORGANIZATION	6.1 Internal organization
	6.1.1 Management commitment to information security (Removed)	
	6.1.2 Information security co-ordination (removed)	
	6.1.3 Allocation of information security responsibilities.	6.1.1 Information security roles and responsibilities
	10.1.3 Segregation of duties (moved)	6.1.2 Segregation of duties (Moved)
	6.1.6 Contact with authorities	6.1.3 Contact with authorities
	6.1.7 Contact with special interest groups	6.1.4 Contact with special interest groups
	6.1.8 Independent review of information security (moved)	**6.1.5 Information security in project management (New)**

	11.7 MOBILE COMPUTING AND TELEWORKING (Moved)	6.2 Mobile devices and teleworking
	11.7.1 Mobile computing and communications	6.2.1 Mobile device policy
	11.7.2 Teleworking	6.2.2 Teleworking
LOW	**8 Human Resource Security**	**7 Human Resource Security**
	8.1 PRIOR TO EMPLOYMENT	7.1 Prior to employment
	8.1.1 Roles and responsibilities (Removed)	
	8.1.2 Screening	7.1.1 Screening
	8.1.3 Terms and conditions of employment	7.1.2 Terms and conditions of employment
	8.2 DURING EMPLOYMENT	7.2 During employment
	8.2.1 Management responsibilities	7.2.1 - Management responsibilities
	8.2.2 Information security awareness, education, and training	7.2.2 - Information security awareness, education and training
	8.2.3 Disciplinary process	7.2.3 Disciplinary process
	8.3 TERMINATION OR CHANGE OF EMPLOYMENT	7.3 Termination and change of employment
	8.3.1 Termination responsibilities	7.3.1 Termination or change of employment responsibilities
MED	**7 Asset Management**	**8 Asset management**
	7.1 RESPONSIBILITY FOR ASSETS.	8.1 Responsibility for assets
	7.1.1 Inventory of assets	8.1.1 Inventory of assets
	7.1.2 Ownership of assets	8.1.2 Ownership of assets
	7.1.3 Acceptable use of assets	8.1.3 Acceptable use of assets
	8.3.2 Return of assets (moved)	8.1.4 Return of assets
	7.2 INFORMATION CLASSIFICATION	8.2 Information classification
	7.2.1 Classification guidelines	8.2.1 Classification of information
	7.2.2 Information labeling and handling	8.2.2 Labeling of information
		8.2.3 Handling of assets (New)
	10.7 MEDIA HANDLING (Moved)	8.3 Media handling
	10.7.1 Management of removable media	8.3.1 Management of removable media
	10.7.2 Disposal of media	8.3.2 Disposal of media
	10.7.3 Information handling procedures	8.3.3 Physical media transfer
	10.7.4 Security of system documentation (Removed)	

	11 ACCESS CONTROL	**9 ACCESS CONTROL**
	11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL	9.1 Business requirements of access control
	11.1.1 Access control policy	9.1.1 Access control policy
		9.1.2 Access to networks and network services
	11.2 USER ACCESS MANAGEMENT.	9.2 User access management
	11.2.1 User registration	9.2.1 User registration and de-registration
		9.2.2 User access provisioning
	11.2.2 Privilege management	9.2.3 Management of privileged access rights
	11.2.3 User password management (moved)	9.2.4 Management of secret authentication information of users
	11.2.4 Review of user access rights	9.2.5 Review of user access rights
	8.3.3 Removal of access rights (Moved)	9.2.6 Removal or adjustment of access rights
	11.3 USER RESPONSIBILITIES	9.3 User responsibilities
	11.3.1 Password use.	**9.3.1 Use of secret authentication information (New)**
	11.5 OPERATING SYSTEM ACCESS CONTROL	9.4 System and application access control
	11.6.1 Information access restriction	9.4.1 Information access restriction
	11.5.1 Secure log-on procedures	9.4.2 Secure logon procedures
	11.5.2 User identification and authentication	
	11.5.3 Password management system	9.4.3 Password management system
	11.5.4 Use of system utilities	9.4.4 Use of privileged utility programs
	12.4.3 Access control to program source code (moved)	9.4.5 Access control to program source code
	11.5.5 Session time-out (Removed)	
	11.5.6 Limitation of connection time	
	11.6 APPLICATION AND INFORMATION ACCESS CONTROL	
	11.6.2 Sensitive system isolation	
LOW	**12.3 CRYPTOGRAPHIC CONTROLS**	**10 Cryptography (NEW)**
	12.3.1 Policy on the use of cryptographic controls	10.1.1 Policy on the use of cryptographic controls
	12.3.2 Key management	10.1.2 Key management
LOW	**9 PHYSICAL AND ENVIRONMENTAL SECURITY**	**11 PHYSICAL AND ENVIRONMENTAL SECURITY**
	9.1 SECURE AREAS	11.1 Secure areas

	9.1.1 Physical security perimeter	11.1.1 Physical security perimeter
	9.1.2 Physical entry controls	11.1.2 Physical entry controls
	9.1.3 Securing offices, rooms, and facilities	11.1.3 Securing offices, rooms and facilities
	9.1.4 Protecting against external and environmental threats	11.1.4 Protecting against external and environ- mental threats
	9.1.5 Working in secure areas	11.1.5 Working in secure areas
	9.1.6 Public access, delivery, and loading areas	11.1.6 Delivery and loading areas
	9.2 EQUIPMENT SECURITY	11.2 Equipment
	9.2.1 Equipment siting and protection.	11.2.1 Equipment siting and protection
	9.2.2 Supporting utilities	11.2.2 Supporting utilities
	9.2.3 Cabling security	11.2.3 Cabling security
	9.2.4 Equipment maintenance	11.2.4 Equipment maintenance
	9.2.7 Removal of property (Moved)	11.2.5 Removal of assets (moved)
	9.2.5 Security of equipment off-premises	11.2.6 Security of equipment and assets off premises
	9.2.6 Secure disposal or re-use of equipment	11.2.7 Secure disposal or re- use of equipment
	11.3.2 Unattended user equipment (moved)	11.2.8 Unattended user equipment
	11.3.3 Clear desk and clear screen policy (Moved)	11.2.9 Clear desk and clear screen policy
HIGH	**10. Operations Security**	**12 Operations security**
	10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES	12.1 Operational procedures and responsibilities
	10.1.1 Documented operating procedures	12.1.1 Documented operating procedures
	10.1.2 Change management	12.1.2 Change management
	10.3.1 Capacity management	12.1.3 Capacity management
	10.1.4 Separation of development, test, and operational facilities	12.1.4 Separation of development, testing and operational environments
	10.3 SYSTEM PLANNING AND ACCEPTANCE.	
	10.3.2 System acceptance	
	10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE	**12.2 Protection from malware**
	10.4.1 Controls against malicious code.	12.2.1 Controls against mal-Ware
	10.4.2 Controls against mobile code (combined)	
	10.5 BACK-UP	**12.3 Backup**
	10.5.1 Information back-up	12.3.1 Information backup
	10.10 MONITORING	**12.4 Logging and monitoring**
	10.10.1 Audit logging	12.4.1 Event logging

	10.10.2 Monitoring system use (combined)	
	10.10.3 Protection of log information	12.4.2 Protection of log information
	10.10.4 Administrator and operator logs	12.4.3 Administrator and operator logs
	10.10.5 Fault logging (Removed)	
	10.10.6 Clock synchronization	12.4.4 Clock synchronisation
	12.4 SECURITY OF SYSTEM FILES	
	12.4.1 Control of operational software	**12.5 Control of operational software**
		12.5.1 Installation of soft-ware on operational systems
	12.6 TECHNICAL VULNERABILITY MANAGEMENT	**12.6 Technical vulnerability management**
	12.6.1 Control of technical vulnerabilities	12.6.1 Management of technical vulnerabilities
		12.6.2 Restrictions on software installation
	15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS (Moved)	**12.7 Information systems audit considerations**
	15.3.1 Information systems audit controls	12.7.1 Information systems audit controls
	15.3.2 Protection of information systems audit tools	
HIGH	**11.4 NETWORK ACCESS CONTROL.**	**13 Communications security**
	11.4.1 Policy on use of network services	13.1 Network security management
	11.4.2 User authentication for external connections	13.1.1 Network controls
	11.4.3 Equipment identification in networks	13.1.2 Security of network services
	11.4.4 Remote diagnostic and configuration port protection	
	11.4.5 Segregation in networks	13.1.3 Segregation in net works
	11.4.6 Network connection control	
	11.4.7 Network routing control	
	10.8 EXCHANGE OF INFORMATION (Moved)	13.2 Information transfer
	10.8.1 Information exchange policies and procedures	13.2.1 Information transfer policies and procedures
	10.8.2 Exchange agreements	13.2.2 Agreements on information transfer
	10.8.3 Physical media in transit (removed)	
	10.8.4 Electronic messaging	13.2.3 Electronic messaging
	10.8.5 Business information systems (removed)	**13.2.4 Confidentiality or non- disclosure agreements**
HIGH	**12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE**	**14 System acquisition, development and maintenance**
	12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS	14.1 Security requirements of information systems

	12.1.1 Security requirements analysis and specification	14.1.1 Information security requirements analysis and specification
	12.2 CORRECT PROCESSING IN APPLICATIONS (Removed)	**14.1.2 Securing application services on public networks**
	12.2.1 Input data validation	**14.1.3 Protecting application services transactions**
	12.2.2 Control of internal processing	
	12.2.3 Message integrity	
	12.2.4 Output data validation	
	12.4 SECURITY OF SYSTEM FILES (Moved)	
	12.4.1 Control of operational software	
	12.4.3 Access control to program source code	
		14.2 Security in development and support processes
	12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	14.2.1 Secure development policy
	12.5.1 Change control procedures	14.2.2 System change control procedures
	12.5.2 Technical review of applications after operating system changes	14.2.3 Technical review of applications after operating platform changes
	12.5.3 Restrictions on changes to software packages	14.2.4 Restrictions on changes to software packages
	12.5.4 Information leakage (Removed)	14.2.5 Secure system engineering principles
		14.2.6 Secure development environment
	12.5.5 Outsourced software development	14.2.7 Outsourced development
		14.2.8 System security testing
		14.2.9 System acceptance testing
		14.3 Test data (New)
	12.4.2 Protection of system test data	14.3.1 Protection of test data
MED	**6.2 EXTERNAL PARTIES**	**15 Supplier relationships**
	6.2.1 Identification of risks related to external parties	15.1 Information security in supplier relationships
	6.2.2 Addressing security when dealing with customers	15.1.1 Information security policy for supplier relationships
	6.2.3 Addressing security in third party agreements	15.1.2 Addressing security within supplier agreements
		15.1.3 Information and communication technology supply chain (New)
	10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT	
	10.2.1 Service delivery	15.2 Supplier service delivery management
	10.2.2 Monitoring and review of third party services	15.2.1 Monitoring and review of supplier services
	10.2.3 Managing changes to third party services	15.2.2 Managing changes to supplier services
LOW	**13 INFORMATION SECURITY INCIDENT MANAGEMENT**	**13 INFORMATION SECURITY INCIDENT MANAGEMENT**

	13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS	16.1 Management of information security incidents and improvements
	13.2.1 Responsibilities and procedures	16.1.1 Responsibilities and Procedures
	13.1.1 Reporting information security events	16.1.2 Reporting information security events
	13.1.2 Reporting security weaknesses	16.1.3 Reporting information security weaknesses
	13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES.	**16.1.4 Assessment of and decision on information security events (new)**
		16.1.5 Response to information security incidents (new)
	13.2.2 Learning from information security incidents	16.1.6 Learning from information security incidents
	13.2.3 Collection of evidence	16.1.7 Collection of evidence
MED	**14 BUSINESS CONTINUITY MANAGEMENT**	
	14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT	**17 Information security aspects of business continuity management**
	14.1.1 Including information security in the business continuity management process	17.1 Information security continuity
	14.1.2 Business continuity and risk assessment	**17.1.1 Planning information security continuity**
	14.1.3 Developing and implementing continuity plans including information security	**17.1.2 Implementing information security continuity**
	14.1.4 Business continuity planning framework	
	14.1.5 Testing, maintaining and re-assessing business continuity plans	17.1.3 Verify, review and evaluate information security continuity
		17.2 Redundancies (new)
		17.2.1 Availability of information processing facilities
MED	**15 COMPLIANCE**	**15 COMPLIANCE**
	15.1 COMPLIANCE WITH LEGAL REQUIREMENTS	18.1 Compliance with legal and contractual requirements
	15.1.1 Identification of applicable legislation	18.1.1 Identification of applicable legislation and contractual requirements
	15.1.2 Intellectual property rights (IPR)	18.1.2 Intellectual property Rights
	15.1.3 Protection of organizational records	18.1.3 Protection of records
	15.1.4 Data protection and privacy of personal information	18.1.4 Privacy and protection of personally identifiable information
	15.1.5 Prevention of misuse of information processing facilities (Removed)	
	15.1.6 Regulation of cryptographic controls	18.1.5 Regulation of cryptographic controls
		18.2 Information security reviews (New)
	15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE	

	6.1.8 Independent review of information security (moved)	18.2.1 Independent review of information security
	15.2.1 Compliance with security policies and standards.	18.2.2 Compliance with security policies and standards
	15.2.2 Technical compliance checking	18.2.3 Technical compliance review

Color Key

Control Removed

Control Moved or Renamed

Control Added (new outline)

Change Key

Minimum Changes to Domain

Several key changes to Domain

Major changes to Domain

**Information based on ISO 2700:2013 – Security Techniques - Code of practice for information security controls, released in November, 2013 and published by the British Standards Institute (BSI) and ANSI.*

ANEXO 3

RESPUESTAS DE CUESTIONARIO PCDG-01 y PCDG-02

CUESTIONARIO PCDG-01

ELABORACION DE TESIS: EVALUACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DE LA ESPE SEDE PRINCIPAL

RESPONSABLES:

PAUL CAJAMARCA LL.

DIEGO GUANOTASIG

Existe en la institución un documento formal de las políticas de seguridad de la información aprobada por la alta dirección?

Si [ ] No [X] No Aplica [ ]

En la institución se ha definido la función seguridad de la información incluyendo roles, capacidades, derechos de decisión y actividades?

Si [ ] No [X] No Aplica [ ]

La institución está alineada con códigos y buenas prácticas de seguridad de información aplicables, nacionales o internacionales?

Si [ ] No [X] No Aplica [ ]

La institución ha definido expectativas respecto a la seguridad de la información?

Si [X] No [ ] No Aplica [ ]

Se han desarrollado las políticas de seguridad de información y afines teniendo en cuenta los requisitos de la institución, requisitos regulatorios, etc?

Si [X] No [ ] No Aplica [ ] Salvador

Se han desarrollado programas de concienciación de seguridad de información?

Si [ ] No [X] No Aplica [ ]

Se han definido la ubicación dentro de la institución de la función seguridad de la información?

Si [X] No [ ] No Aplica [ ]

La alta dirección tiene un compromiso de apoyo a la función seguridad de la información?

Si [ ] No [X] No Aplica [ ]

La seguridad de la información cumple completamente con las necesidades de la institución?

Si [ ] No [X] No Aplica [ ]

La seguridad de la información cumple con regulaciones y obligaciones contractuales internas y externas?

Si [ ] No [X] No Aplica [ ]

Existe en la institución una visión relativa a la seguridad de información como apoyo a la visión corporativa?

Si [✓] No [ ] No Aplica [ ]

Se revisan las evaluaciones del riesgo a intervalos planeados tomando en cuenta cambios en la organización, tecnología, amenazas identificadas, etc?

Si [✓] No [ ] No Aplica [ ] Plan de Continuidad

Se registran las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño de la seguridad de información?

Si [ ] No [X] No Aplica [ ]

Se realiza una revisión gerencial de la seguridad de información para asegurar que el alcance permanezca adecuado?

Si [ ] No [X] No Aplica [ ]

Existe personal encargado que coordine y sea responsable de los roles y funciones con respecto a la seguridad de la información?

Si [ ] No [✓] No Aplica [ ]

Se dispone de acuerdos de confidencialidad, políticas, reglamentos aprobados para el manejo de la información sensible?

Si [X] No [ ] No Aplica [ ] Torneo de claves USI

Se ha socializado al personal los beneficios del aporte de la seguridad de la información a los objetivos generales de la institución?

Si [ ] No [X] No Aplica [ ]

Se ha realizado revisiones periódicas en el alcance y los límites del Sistema de Gestión de Seguridad de la Información por parte de Dirección para asegurar este proceso?

Si [ ] No [X] No Aplica [ ]

Cuenta con un plan estratégico de seguridad de la información?

Si [ ] No [X] No Aplica [ ]

Existe un reglamento para el uso de los servicios de procesamiento de la información?

Si [ ] No [X] No Aplica [ ]

Se ha realizado campañas de socialización sobre software malicioso y otros que puedan afectar a la seguridad de la información?

Si [ ] No [X] No Aplica [ ]

Se ha socializado al personal tener siempre visible su identificación para el acceso a las ubicaciones de TI?

Si [X] No [ ] No Aplica [ ]

Todos los documentos referentes a políticas, reglamentos, procedimientos se encuentran legalmente aprobados y bajo la normativa vigente de la institución?

Si [X] No [ ] No Aplica [ ]

Se dispone de reglamentos, procedimientos para garantizar la protección de datos y la privacidad de acuerdo a la legislación vigente, con cláusulas en el contrato de trabajo?

Si [X] No [ ] No Aplica [ ]

Se dispone y socializa acuerdos de confidencialidad de seguridad de la información aprobados para requerimientos externos?

Si [ ] No [X] No Aplica [ ]

Una vez encontradas las no-conformidades y causas la gerencia realiza las acciones correspondientes para corregir estas y protege el acceso de las auditorías realizadas?

Si [ ] No [X] No Aplica [ ]

Se dispone de procedimientos específicos para contactarse con las autoridades (policía, bomberos, autoridades de supervisión) para reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley?

Si [ ] No [X] No Aplica [ ]

CUESTIONARIO PCDG-02

ELABORACION DE TESIS: EVALUACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION DE LA ESPE SEDE PRINCIPAL

RESPONSABLES:

PAUL CAJAMARCA LL.

DIEGO GUANOTASIG

Existe en la institución un documento formal de las políticas de seguridad de la información aprobada por la alta dirección?

Si [ ] No [X] No Aplica [ ]

En la institución se ha definido la función seguridad de la información incluyendo roles, capacidades, derechos de decisión y actividades?

Si [ ] No [X] No Aplica [ ]

La institución está alineada con códigos y buenas prácticas de seguridad de información aplicables, nacionales o internacionales?

Si [ ] No [X] No Aplica [ ]

Se han desarrollado las políticas de seguridad de información y afines teniendo en cuenta los requisitos de la institución, requisitos regulatorios, etc?

Si [ ] No [X] No Aplica [ ]

Se han desarrollado programas de concienciación de seguridad de información?

Si [ ] No [X] No Aplica [ ]

Se ha definido la propiedad de sistemas y datos en la institución dentro de los procesos de gestión de la seguridad de la información?

Si [ ] No [X] No Aplica [ ]

Se realizan evaluaciones periódicas de seguridad de información (auditorias) para determinar cumplimiento de políticas y procedimientos de seguridad de información?

Si [ ] No [X] No Aplica [ ]

Se identifican y revisan regularmente los requerimientos de confidencialidad o acuerdos de no divulgación para protección de información?

Si [ ] No [X] No Aplica [ ]

La alta dirección tiene un compromiso de apoyo a la función seguridad de la información?

Si [X] No [ ] No Aplica [ ]

El documento de las políticas de seguridad de información es revisado regularmente a intervalos planeados o si ocurren cambios significativos?

Si [ ] No [X] No Aplica [ ]

La seguridad de la información cumple completamente con las necesidades de la organización?

Si [X] No [ ] No Aplica [ ]

La seguridad de la información cumple con regulaciones y obligaciones contractuales internas y externas?

Si [X] No [ ] No Aplica [ ]

Los requisitos de seguridad de información para contratación de personal están incorporados en los procesos de contratación de TI para empleados/subcontratistas/proveedores?

Si [ ] No [X] No Aplica [ ]

Se han definido y documentado roles y responsabilidades para seguridad de información en concordancia con las políticas de seguridad de información?

Si [ ] No [X] No Aplica [ ]

Se proporciona formación y programas de desarrollo profesional de seguridad de la información en la institución?

Si [X] No [ ] No Aplica [ ]

Se les otorga a los funcionarios el apropiado conocimiento, y capacitación de las políticas y procedimientos de seguridad de información en relación a su función laboral?

Si [ ] No [X] No Aplica [ ]

Se gestiona la asignación de personal de seguridad de información de acuerdo a las necesidades de la organización?.

Si [ ] No [X] No Aplica [ ]

Se obtiene aceptación formal por parte de los personal contratado en relación a requisitos y políticas de seguridad de información?

Si [ ] No [X] No Aplica [ ]

Existe un proceso disciplinario formal para los funcionarios que cometen una violación en seguridad de información?

Si [ ] No [X] No Aplica [ ]

Existe un proceso para identificar y comunicar puntos críticos y débiles relacionados con seguridad de información?

Si [ ] No [X] No Aplica [ ]

Se designan profesionales de seguridad de información cualificados para servir en los equipos de implantación?

Si [ ] No [X] No Aplica [ ]

Existe en la institución una visión relativa a la seguridad de información como apoyo a la visión corporativa?

Si [X] No [ ] No Aplica [ ]

Se otorga formación e información al nuevo personal respecto a la concienciación de la seguridad de la información?

Si [ ] No [X] No Aplica [ ]

Se identifican prontamente los incidentes y violaciones de seguridad fallido y exitosos?

Si [X] No [ ] No Aplica [ ]

Se revisan los informes de incidentes de seguridad de la información para identificar deficiencias de los controles? Informes de Seguridad

Si [X] No [ ] No Aplica [ ]

Se revisan las evaluaciones del riesgo a intervalos planeados tomando en cuenta cambios en la organización, tecnología, amenazas identificadas, etc?

Si [X] No [ ] No Aplica [ ] PC.

Se registran las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño de la seguridad de información?

Si [ ] No [X] No Aplica [ ]

Existe un procedimiento en el cual los gerentes/responsables/ aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad son realizados correctamente en cumplimiento con las políticas y estándares de seguridad?.

Si [ ] No [X] No Aplica [ ]

Los sistemas de información son chequeados regularmente para el cumplimiento de implementación de la seguridad?.

Si[ ] No[X] No Aplica[ ]

Existen procedimientos actualizados, que ayuden a gestionar la seguridad de la información?

Si[X] No[ ] No Aplica[ ] Proyectados

Se realiza evaluaciones internas periódicas con respecto a la gestión de seguridad de la información?

Si[ ] No[X] No Aplica[ ]

Se ha realizado análisis de riesgo para priorizar los puntos más críticos a solventar con respecto a la seguridad de la información?

Si[ ] No[X] No Aplica[ ]

Se ha cumplido con la normativa vigente que rige para la institución con respecto a la seguridad de la información?

Si[ ] No[X] No Aplica[ ]

Se registra las acciones y eventos que podrían tener un impacto en la efectividad o el diseño del Sistema de gestión de Seguridad de la información?

Si[ ] No[X] No Aplica[ ]

Se dispone de un inventario de los componentes más críticos que pueden afectar la disponibilidad de la información?

Si[X] No[ ] No Aplica[ ] PC

Se dispone de programas de formación referente a la seguridad de la información?

Si[ ] No[X] No Aplica[ ]

Se dispone de procedimientos para los controles de seguridad de la información como: identificación de acceso de equipos a la red, instalación de software, en elementos configurables como servidores/hardware?

Si[X] No[ ] No Aplica[ ]

Se encuentran todos los activos claramente identificados y asignados a un responsable de la institución, manteniendo un inventario actualizado?

Si[X] No[ ] No Aplica[ ]

Se dispone de niveles de seguridad en el acceso de la documentación que maneja la institución?

Si [ ] No [X] No Aplica [ ]

Se realizan pruebas cuando se cambia los sistemas operativos, para asegurar que no haya impacto en las aplicaciones críticas para la institución?

Si [ ] No [X] No Aplica [ ]

Se dispone de procedimientos de reacción en el caso de encontrar vulnerabilidades técnicas en el sistema?

Si [ ] No [X] No Aplica [ ]

Se dispone de herramientas para la protección de software malicioso y otros, por ejemplo: antivirus, filtrado de la red?

Si [X] No [ ] No Aplica [ ]

Se administra todos los cambios de derecho de acceso(creación, modificación, eliminación) basándose en la documentación y aprobación correspondiente?

Si [X] No [ ] No Aplica [ ]

Se realizan pruebas de intrusión periódicas para determinar la adecuación de la protección de la red?

Si [ ] No [X] No Aplica [ ]

Se dispone de procedimientos para el acceso y control remoto para los sistemas?

Si [ ] No [X] No Aplica [ ]

Se dispone de procedimientos para cifrar la información almacenada de acuerdo a su clasificación?

Si [ ] No [X] No Aplica [ ]

Se realiza regularmente revisiones de gestión de todas las cuentas y privilegios relacionados a la información clasificada?

Si [X] No [ ] No Aplica [ ]

Se restringe los accesos a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) con dispositivos de seguridad, según su función de trabajo, responsabilidades y registrando su entrada?

Si [X] No [ ] No Aplica [ ]

Se ha establecido un inventario de documentos sensibles y dispositivos de salida?

Si [ ] No [/] No Aplica [ ]

Se tiene un registro, procedimiento de recopilación de eventos de seguridad para detectar incidentes potenciales?

Si [ ] No [X] No Aplica [ ]

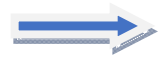
ANEXO 4

ANÁLISIS DE RESPUESTAS DEL CUESTIONARIO PCDG-01 y PCDG-02

Tabla 1 Análisis de respuestas del cuestionario PCDG-01 y PCDG-02

MATRIZ ANÁLISIS CUESTIONARIO									
SEGURIDAD DE LA INFORMACIÓN UNIVERSIDAD DE LAS FUERZAS ARMADAS(ESPE)									
	PREGUNTAS	RESPUESTAS			HALLAZGO	IMPACTO	PROBABILIDAD	RIESGO	RECOMENDACIONES
		Si	No	N/A					
PCDG-01									
1	Existe en la institución un documento formal de las políticas de seguridad de la información aprobada por la alta dirección?		X		No disponen de un documento de políticas de seguridad	ALTA	MEDIA	ALTA	Elaborar, implementar el manual de políticas de seguridad
2	En la institución se ha definido la función seguridad de la información incluyendo roles, capacidades, derechos de decisión y actividades?		X		No se definen actividades específicas a los funcionarios correspondientes	ALTA	ALTA	ALTA	Elaborar, implementar reglamentos de responsabilidades de los funcionarios
3	La institución está alineada con códigos y buenas prácticas de seguridad de información aplicables, nacionales o internacionales?		X		No cumple con la normativa vigente con respecto a la seguridad de la información	MEDIA	ALTA	MEDIA	Se debe implementar metodologías para salvaguardar la información
4	La institución ha definido expectativas respecto a la seguridad de la	X							

Continua



	información?								
5	Se han desarrollado las políticas de seguridad de información y afines teniendo en cuenta los requisitos de la institución, requisitos regulatorios, etc?	X							
6	Se han desarrollado programas de concienciación de seguridad de información?		X		No se desarrollan programas de concienciación referente a la seguridad de la información	BAJA	MEDIA	MEDIA	Se debe elaborar cronogramas de capacitación que puedan solventar las necesidades de los funcionarios respecto a la seguridad de la información
7	Se han definido la ubicación dentro de la institución de la función seguridad de la información?	X							
8	La alta dirección tiene un compromiso de apoyo a la función seguridad de la información?		X		La dirección no tiene un conocimiento adecuado de los beneficios de la aplicación de metodologías de seguridad de la información	ALTA	MEDIA	ALTA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
9	La seguridad de la información cumple completamente con las necesidades de la institución?		X		No se tiene un pleno conocimiento de la normativa vigente	MEDIA	MEDIA	MEDIA	Se debería capacitar al personal de las áreas correspondientes de la aplicación de las metodologías, buenas prácticas para salvaguardar la

Continua

									información
10	La seguridad de la información cumple con regulaciones y obligaciones contractuales internas y externas?		X		No se encontró la aplicación de seguridad de la información en obligaciones internas y externas	MEDIA	ALTA	ALTA	Implementar procedimientos que ayuden a dar aplicabilidad a los acuerdos de confidencialidad tanto internos como externos.
11	Existe en la institución una visión relativa a la seguridad de información como apoyo a la visión corporativa?	X							
12	Se revisan las evaluaciones del riesgo a intervalos planeados tomando en cuenta cambios en la organización, tecnología, amenazas identificadas, etc?	X							
13	Se registran las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño de la seguridad de información?		X		No se encontró registros de eventos que comprometan la seguridad de la información	BAJA	MEDIA	MEDIA	Elaborar, implementar registros que sucedan con respecto a la seguridad de la información, estandarizar formatos para levantamiento de los eventos.
14	Se realiza una revisión gerencial de la seguridad de información para asegurar que el alcance permanezca adecuado?		X		No se encontró seguimiento de parte de la dirección para verificar el alcance de la	ALTA	ALTA	ALTA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa

Continua

					aplicación de la normativa vigente				vigente.
15	Existe personal encargado que coordine y sea responsable de los roles y funciones con respecto a la seguridad de la información?		X		No se dispone de responsabilidad formal en la aplicación, seguimiento del cumplimiento de la normativa vigente.	BAJA	MEDIA	MEDIA	Socializar, segregar funciones formalmente al personal adecuado de la institución, para realizar las actividades concernientes a la seguridad de la información.
16	Se dispone de acuerdos de confidencialidad, políticas, reglamentos aprobados para el manejo de la información sensible?	X							
17	Se ha socializado al personal los beneficios del aporte de la seguridad de la información a los objetivos generales de la institución?		X		No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	MEDIA	MEDIA	MEDIA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
18	Se ha realizado revisiones periódicas en el alcance y los límites del Sistema de Gestión de Seguridad de la Información por parte de Dirección para asegurar este proceso?		X		No se realiza revisiones periódicas de SGSI	ALTA	MEDIA	ALTA	Socializar, segregar funciones formalmente al personal adecuado de la institución, para realizar las actividades concernientes a la seguridad de la información.

Continua

19	Cuenta con un plan estratégico de seguridad de la información?		X		No se dispone de un plan estratégico de seguridad de la información	ALTA	ALTA	ALTA	Aprobar, implementar el plan estratégico de seguridad de la información
20	Existe un reglamento para el uso de los servicios de procesamiento de la información?		X		No se dispone de un reglamento de uso de servicios de procesamiento de la información	BAJA	MEDIA	MEDIA	Aprobar, implementar reglamentos que ayuden al procesamiento de la información
21	Se ha realizado campañas de socialización sobre software malicioso y otros que puedan afectar a la seguridad de la información?		X		No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	ALTA	BAJA	MEDIA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
22	Se ha socializado al personal tener siempre visible su identificación para el acceso a las ubicaciones de TI?	X							
23	Todos los documentos referentes a políticas, reglamentos, procedimientos se encuentran legalmente aprobados y bajo la normativa vigente de la institución?	X							
24	Se dispone de reglamentos, procedimientos para garantizar la protección de datos y la privacidad de acuerdo a la legislación vigente, con cláusulas en el contrato de trabajo?	X							

Continua

25	Se dispone y socializa acuerdos de confidencialidad de seguridad de la información aprobados para requerimientos externos?		X		No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	ALTA	MEDIA	ALTA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
26	Una vez encontradas las no-conformidades y causas la gerencia realiza las acciones correspondientes para corregir estas y protege el acceso de las auditorías realizadas?		X		No se realiza el seguimiento correspondiente a las no-conformidades encontradas	ALTA	ALTA	ALTA	Realizar las actividades que se recomienda por parte de la auditoria para mitigar el riesgo y solventar el SGSI
27	Se dispone de procedimientos específicos para contactarse con las autoridades (policía, bomberos, autoridades de supervisión) para reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley?		X		No se tienen procedimientos de respuesta en caso de incidentes en las instalaciones de la institución	MEDIA	MEDIA	MEDIA	Realizar procedimientos que ayuden a la eficaz respuesta en temas relacionados a seguridad física de las instalaciones, se debe implementar un plan de contingencias para estos casos.
PCDG-02									
28	Los requisitos de seguridad de información para contratación de personal están incorporados en los procesos de contratación de TI para empleados/subcontratistas/proveedores?		X		No se incluye ningún tema adicional respecto a seguridad de la información en la contratación de personal	BAJA	MEDIA	MEDIA	Se debe incluir temas relacionados con el compromiso del personal para el cumplimiento de la seguridad de la información

Continua

29	Se han definido y documentado roles y responsabilidades para seguridad de información en concordancia con las políticas de seguridad de información?		X		No se definen responsabilidades en las actividades referente a la seguridad de la información	MEDIA	MEDIA	MEDIA	Socializar, segregar funciones formalmente al personal adecuado de la institución, para realizar las actividades concernientes a la seguridad de la información.
30	Se proporciona formación y programas de desarrollo profesional de seguridad de la información en la institución?	X							
31	Se les otorga a los funcionarios el apropiado conocimiento, y capacitación de las políticas y procedimientos de seguridad de información en relación a su función laboral?		X		No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	MEDIA	BAJA	MEDIA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
32	Se gestiona la asignación de personal de seguridad de información de acuerdo a las necesidades de la organización?.		X		No se dispone de personal que tenga responsabilidad formal en la aplicación, seguimiento del cumplimiento de la normativa vigente.	MEDIA	MEDIA	MEDIA	Socializar, segregar funciones formalmente al personal adecuado de la institución, para realizar las actividades concernientes a la seguridad de la información. Gestionar la asignación de personal en el caso de no disponer
33	Se obtiene aceptación formal por parte del personal contratado en relación a requisitos y políticas de seguridad de información?		X		No se tiene de un acuerdo de confidencialidad con respecto al cumplimiento de	BAJA	BAJA	BAJA	Realizar acuerdos de confidencialidad para el cumplimiento de la seguridad de la información

Continua

					la seguridad de la información				
34	Existe un proceso disciplinario formal para los funcionarios que cometen una violación en seguridad de información?		X		No se tiene de un acuerdo de confidencialidad con respecto al cumplimiento de la seguridad de la información	MEDIA	BAJA	MEDIA	Realizar acuerdos de confidencialidad para el cumplimiento de la seguridad de la información
35	Existe un proceso para identificar y comunicar puntos críticos y débiles relacionados con seguridad de información?		X		No existen procedimientos para la identificación de puntos críticos que afecten la seguridad de la información	ALTA	MEDIA	ALTA	Realizar procedimientos que ayuden a la identificación, control vulnerabilidades encontradas en la institución referentes a la seguridad de la información
36	Se designan profesionales de seguridad de información calificados para servir en los equipos de implantación?		X		No se dispone de personal calificado referente actividades de la seguridad de la información	MEDIA	BAJA	MEDIA	Realizar capacitaciones que fortalezcan las necesidades en la implementación de equipos referente a la seguridad de la información
37	Existe en la institución una visión relativa a la seguridad de información como apoyo a la visión corporativa?	X							

Continua

38	Se otorga formación e información al nuevo personal respecto a la concienciación de la seguridad de la información?		X		No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	MEDIA	MEDIA	MEDIA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
39	Se identifican prontamente los incidentes y violaciones de seguridad fallidas y exitosas?	X							
40	Se revisan los informes de incidentes de seguridad de la información para identificar deficiencias de los controles?	X							
41	Se revisan las evaluaciones del riesgo a intervalos planeados tomando en cuenta cambios en la organización, tecnología, amenazas identificadas, etc?	X							
42	Se registran las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño de la seguridad de información?		X		No se encontró registros de eventos que comprometan la seguridad de la información	BAJA	BAJA	BAJA	Elaborar, implementar registros que sucedan con respecto a la seguridad de la información, estandarizar formatos para levantamiento de los eventos.
43	Existe un procedimiento en el cual los gerentes/responsables/ aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad son realizados correctamente en cumplimiento con las políticas y estándares de seguridad?.		X		No existen procedimientos que aseguren el cumplimiento de la seguridad de la información en las áreas comprometidas con esta.	MEDIA	MEDIA	MEDIA	Realizar procedimiento que aseguren el cumplimiento de la política vigente referente a seguridad de la información

Continua

44	Los sistemas de información son chequeados regularmente para el cumplimiento de implementación de la seguridad?.		X		No se dispone de registros de evaluaciones a los sistemas de información	MEDIA	BAJA	MEDIA	Realizar cronogramas de revisión, verificación de los sistemas para el cumplimiento de la normativa vigente referente a la seguridad de la información
45	Existen procedimientos actualizados, que ayuden a gestionar la seguridad de la información?	X							
46	Se realiza evaluaciones internas periódicas con respecto a la gestión de seguridad de la información?		X		No se dispone de registros de evaluaciones a los sistemas de información	BAJA	BAJA	BAJA	Realizar cronogramas de revisión, verificación de los sistemas para el cumplimiento de la normativa vigente referente a la seguridad de la información
47	Se ha realizado análisis de riesgo para priorizar los puntos más críticos a solventar con respecto a la seguridad de la información?		X		No se ha realizado análisis de riesgos referente a la seguridad de la información	MEDIA	MEDIA	MEDIA	Se debe realizar un análisis de riesgos de seguridad de la información para verificar el estado de avance del mismo.
48	Se ha cumplido con la normativa vigente que rige para la institución con respecto a la seguridad de la información?		X		No se cumple con la implementación de la normativa vigente	ALTA	MEDIA	ALTA	Crear un grupo que se encargue en la aplicación de la normativa vigente, realizar un cronograma de trabajo donde se comprometa

Continua

									a las autoridades de la institución
49	Se registra las acciones y eventos que podrían tener un impacto en la efectividad o el diseño del Sistema de gestión de Seguridad de la información?		X		No se encontró registros de eventos que comprometan la seguridad de la información	MEDIA	MEDIA	MEDIA	Elaborar, implementar registros que sucedan con respecto a la seguridad de la información, estandarizar formatos para levantamiento de los eventos.
50	Se dispone de un inventario de los componentes más críticos que pueden afectar la disponibilidad de la información?	X							
51	Se dispone de programas de formación referente a la seguridad de la información?		X		No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	MEDIA	MEDIA	MEDIA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
52	Se dispone de procedimientos para los controles de seguridad de la información como: identificación de acceso de equipos a la red, instalación de software, en elementos configurables como servidores/hardware?	X							

Continua

53	Se encuentran todos los activos claramente identificados y asignados a un responsable de la institución, manteniendo un inventario actualizado?	X							
54	Se dispone de niveles de seguridad en el acceso de la documentación que maneja la institución?		X		No se dispone de metodologías, procedimientos para definir los niveles de acceso a la información, no se dispone de un análisis RISK para identificar la información sensible	ALTA	ALTA	ALTA	Se debe realizar un análisis RISK, para solventar e identificar la información sensible de la institución. Se debe realizar un reglamento, procedimientos del manejo de la información sensible
55	Se realizan pruebas cuando se cambia los sistemas operativos, para asegurar que no haya impacto en las aplicaciones críticas para la institución?		X		No se dispone de procedimientos ni registros de verificación de cambios a los sistemas.	BAJA	BAJA	MEDIA	Se debe realizar procedimiento para la verificación de cambios y validación de los sistemas.
56	Se dispone de procedimientos de reacción en el caso de encontrar vulnerabilidades técnicas en el sistema?		X		No se tiene documentación de respaldo, ni procedimientos en el caso de encontrarse vulnerabilidades en el sistema	MEDIA	MEDIA	MEDIA	Realizar procedimiento que aseguren el cumplimiento de la política vigente referente a seguridad de la información
57	Se dispone de herramientas para la protección de software malicioso y otros, por ejemplo: antivirus, filtrado de la red?	X							

Continua

58	Se administra todos los cambios de derecho de acceso(creación, modificación, eliminación) basándose en la documentación y aprobación correspondiente?	X							
59	Se realizan pruebas de intrusión periódicas para determinar la adecuación de la protección de la red?		X		No se tiene informes de intrusión para protección de la red, ni se dispone de procedimientos, ni metodología a ser implementada	ALTA	MEDIA	ALTA	Realizar un cronograma de pruebas de intrusión periódicas, aplicando buenas prácticas para solventar los procedimientos de análisis de vulnerabilidades
60	Se dispone de procedimientos para el acceso y control remoto para los sistemas?		X		No se dispone que se tenga registros ni procedimiento para acceso y control remoto a los sistemas	MEDIA	MEDIA	MEDIA	Realizar procedimientos para acceso remoto y socializar a los responsables de utilizar esto las políticas de seguridad de la institución en base a la normativa vigente
61	Se dispone de procedimientos para cifrar la información almacenada de acuerdo a su clasificación?		X		No se dispone de procedimientos de clasificación de la información (análisis RISK), ni de metodologías para cifrar la información sensible	MEDIA	MEDIA	MEDIA	Se debe realizar un análisis RISK, para solventar e identificar la información sensible de la institución. Se debe realizar un reglamento, procedimientos de encriptación de la

Continua

									información sensible
62	Se realiza regularmente revisiones de gestión de todas las cuentas y privilegios relacionados a la información clasificada?	X							
63	Se restringe los accesos a las ubicaciones de TI (salas de servidores, edificios, áreas o zonas) con dispositivos de seguridad, según su función de trabajo, responsabilidades y registrando su entrada?	X							

Continua

64	Se ha establecido un inventario de documentos sensibles y dispositivos de salida?		X		No se dispone de procedimientos de clasificación de la información (análisis RISK), ni de metodologías para cifrar la información sensible No se realiza un inventario de dispositivos actualizado.	ALTA	MEDIA	ALTA	Se debe realizar un análisis RISK, para solventar e identificar la información sensible de la institución. Se debe realizar un reglamento, procedimientos inventarios de la información y dispositivos sensibles
65	Se tiene un registro, procedimiento de recopilación de eventos de seguridad para detectar incidentes potenciales?		X		No se encontró registros de eventos que comprometan la seguridad de la información	BAJA	MEDIA	MEDIA	Elaborar, implementar registros que sucedan con respecto a la seguridad de la información, estandarizar formatos para levantamiento de los eventos.
		22	43						

ANEXO 5

RESUMEN ANALISIS DE RIESGOS

Tabla 2 Resumen Análisis de Riesgos

RESUMEN MATRIZ ANÁLISIS CUESTIONARIO				
SEGURIDAD DE LA INFORMACIÓN UNIVERSIDAD DE LAS FUERZAS ARMADAS(ESPE)				
	PREGUNTAS	**HALLAZGO**	**RIESGO**	**RECOMENDACIONES**
PCDG-01				
1	Existe en la institución un documento formal de las políticas de seguridad de la información aprobada por la alta dirección?	No disponen de un documento de políticas de seguridad	ALTA	Elaborar, implementar el manual de políticas de seguridad
2	En la institución se ha definido la función seguridad de la información incluyendo roles, capacidades, derechos de decisión y actividades?	No se definen actividades específicas a los funcionarios correspondientes	ALTA	Elaborar, implementar reglamentos de responsabilidades de los funcionarios
3	La institución está alineada con códigos y buenas prácticas de seguridad de información aplicables, nacionales o internacionales?	No cumple con la normativa vigente con respecto a la seguridad de la información	MEDIA	Se debe implementar metodologías para salvaguardar la información
4	Se han desarrollado programas de concienciación de seguridad de información?	No se desarrollan programas de concienciación referente a la seguridad de la información	MEDIA	Se debe elaborar cronogramas de capacitación que puedan solventar las necesidades de los funcionarios respecto a la seguridad de la información
5	La alta dirección tiene un compromiso de apoyo a la función seguridad de la información?	La dirección no tiene un conocimiento adecuado de los beneficios de la aplicación de metodologías de seguridad de la información	ALTA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.

Continua

6	La seguridad de la información cumple completamente con las necesidades de la institución?	No se tiene un pleno conocimiento de la normativa vigente	MEDIA	Se debería capacitar al personal de las áreas correspondientes de la aplicación de las metodologías, buenas prácticas para salvaguardar la información
7	La seguridad de la información cumple con regulaciones y obligaciones contractuales internas y externas?	No se encontró la aplicación de seguridad de la información en obligaciones internas y externas	ALTA	Implementar procedimientos que ayuden a dar aplicabilidad a los acuerdos de confidencialidad tanto internos como externos.
8	Se registran las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño de la seguridad de información?	No se encontró registros de eventos que comprometan la seguridad de la información	MEDIA	Elaborar, implementar registros que sucedan con respecto a la seguridad de la información, estandarizar formatos para levantamiento de los eventos.
9	Se realiza una revisión gerencial de la seguridad de información para asegurar que el alcance permanezca adecuado?	No se encontró seguimiento de parte de la dirección para verificar el alcance de la aplicación de la normativa vigente	ALTA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
10	Existe personal encargado que coordine y sea responsable de los roles y funciones con respecto a la seguridad de la información?	No se dispone de responsabilidad formal en la aplicación, seguimiento del cumplimiento de la normativa vigente.	MEDIA	Socializar, segregar funciones formalmente al personal adecuado de la institución, para realizar las actividades concernientes a la seguridad de la información.
11	Se ha socializado al personal los beneficios del aporte de la seguridad de la información a los objetivos generales de la institución?	No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	MEDIA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.

Continua

12	Se ha realizado revisiones periódicas en el alcance y los límites del Sistema de Gestión de Seguridad de la Información por parte de Dirección para asegurar este proceso?	No se realiza revisiones periódicas de SGSI	ALTA	Socializar, segregar funciones formalmente al personal adecuado de la institución, para realizar las actividades concernientes a la seguridad de la información.
13	Cuenta con un plan estratégico de seguridad de la información?	No se dispone de un plan estratégico de seguridad de la información	ALTA	Aprobar, implementar el plan estratégico de seguridad de la información
14	Existe un reglamento para el uso de los servicios de procesamiento de la información?	No se dispone de un reglamento de uso de servicios de procesamiento de la información	MEDIA	Aprobar, implementar reglamentos que ayuden al procesamiento de la información
15	Se ha realizado campañas de socialización sobre software malicioso y otros que puedan afectar a la seguridad de la información?	No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	MEDIA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
16	Se dispone y socializa acuerdos de confidencialidad de seguridad de la información aprobados para requerimientos externos?	No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	ALTA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
17	Una vez encontradas las no-conformidades y causas la gerencia realiza las acciones correspondientes para corregir estas y protege el acceso de las auditorías realizadas?	No se realiza el seguimiento correspondiente a las no-conformidades encontradas	ALTA	Realizar las actividades que se recomienda por parte de la auditoria para mitigar el riesgo y solventar el SGSI
18	Se dispone de procedimientos específicos para contactarse con las autoridades (policía, bomberos, autoridades de supervisión) para reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley?	No se tienen procedimientos de respuesta en caso de incidentes en las instalaciones de la institución	MEDIA	Realizar procedimientos que ayuden a la eficaz respuesta en temas relacionados a seguridad física de las instalaciones, se debe implementar un plan de contingencias para estos casos.

Continua

PCDG-02				
19	Los requisitos de seguridad de información para contratación de personal están incorporados en los procesos de contratación de TI para empleados/subcontratistas/proveedores?	No se incluye ningún tema adicional respecto a seguridad de la información en la contratación de personal	MEDIA	Se debe incluir temas relacionados con el compromiso del personal para el cumplimiento de la seguridad de la información
20	Se han definido y documentado roles y responsabilidades para seguridad de información en concordancia con las políticas de seguridad de información?	No se definen responsabilidades en las actividades referente a la seguridad de la información	MEDIA	Socializar, segregar funciones formalmente al personal adecuado de la institución, para realizar las actividades concernientes a la seguridad de la información.
21	Se les otorga a los funcionarios el apropiado conocimiento, y capacitación de las políticas y procedimientos de seguridad de información en relación a su función laboral?	No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	MEDIA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
22	Se gestiona la asignación de personal de seguridad de información de acuerdo a las necesidades de la organización?.	No se dispone de personal que tenga responsabilidad formal en la aplicación, seguimiento del cumplimiento de la normativa vigente.	MEDIA	Socializar, segregar funciones formalmente al personal adecuado de la institución, para realizar las actividades concernientes a la seguridad de la información. Gestionar la asignación de personal en el caso de no disponer
23	Se obtiene aceptación formal por parte del personal contratado en relación a requisitos y políticas de seguridad de información?	No se tiene de un acuerdo de confidencialidad con respecto al cumplimiento de la seguridad de la información	BAJA	Realizar acuerdos de confidencialidad para el cumplimiento de la seguridad de la información
24	Existe un proceso disciplinario formal para los funcionarios que cometen una violación en seguridad de información?	No se tiene de un acuerdo de confidencialidad con respecto al cumplimiento de la seguridad de la información	MEDIA	Realizar acuerdos de confidencialidad para el cumplimiento de la seguridad de la información

Continua

25	Existe un proceso para identificar y comunicar puntos críticos y débiles relacionados con seguridad de información?	No existen procedimientos para la identificación de puntos críticos que afecten la seguridad de la información	ALTA	Realizar procedimientos que ayuden a la identificación, control vulnerabilidades encontradas en la institución referentes a la seguridad de la información
26	Se designan profesionales de seguridad de información calificados para servir en los equipos de implantación?	No se dispone de personal calificado referente actividades de la seguridad de la información	MEDIA	Realizar capacitaciones que fortalezcan las necesidades en la implementación de equipos referente a la seguridad de la información
27	Se otorga formación e información al nuevo personal respecto a la concienciación de la seguridad de la información?	No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	MEDIA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.
28	Se registran las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño de la seguridad de información?	No se encontró registros de eventos que comprometan la seguridad de la información	BAJA	Elaborar, implementar registros que sucedan con respecto a la seguridad de la información, estandarizar formatos para levantamiento de los eventos.
29	Existe un procedimiento en el cual los gerentes/responsables/ aseguran que todos los procedimientos de seguridad dentro de su área de responsabilidad son realizados correctamente en cumplimiento con las políticas y estándares de seguridad?.	No existen procedimientos que aseguren el cumplimiento de la seguridad de la información en las áreas comprometidas con esta.	MEDIA	Realizar procedimiento que aseguren el cumplimiento de la política vigente referente a seguridad de la información
30	Los sistemas de información son chequeados regularmente para el cumplimiento de implementación de la seguridad?.	No se dispone de registros de evaluaciones a los sistemas de información	MEDIA	Realizar cronogramas de revisión, verificación de los sistemas para el cumplimiento de la normativa vigente referente a la seguridad de la

Continua

				información
31	Se realiza evaluaciones internas periódicas con respecto a la gestión de seguridad de la información?	No se dispone de registros de evaluaciones a los sistemas de información	BAJA	Realizar cronogramas de revisión, verificación de los sistemas para el cumplimiento de la normativa vigente referente a la seguridad de la información
32	Se ha realizado análisis de riesgo para priorizar los puntos más críticos a solventar con respecto a la seguridad de la información?	No se ha realizado análisis de riesgos referente a la seguridad de la información	MEDIA	Se debe realizar un análisis de riesgos de seguridad de la información para verificar el estado de avance del mismo.
33	Se ha cumplido con la normativa vigente que rige para la institución con respecto a la seguridad de la información?	No se cumple con la implementación de la normativa vigente	ALTA	Crear un grupo que se encargue en la aplicación de la normativa vigente, realizar un cronograma de trabajo donde se comprometa a las autoridades de la institución
34	Se registra las acciones y eventos que podrían tener un impacto en la efectividad o el diseño del Sistema de gestión de Seguridad de la información?	No se encontró registros de eventos que comprometan la seguridad de la información	MEDIA	Elaborar, implementar registros que sucedan con respecto a la seguridad de la información, estandarizar formatos para levantamiento de los eventos.
35	Se dispone de programas de formación referente a la seguridad de la información?	No se cuenta con programas, cronogramas de socialización referente a temas de seguridad de la información	MEDIA	Realizar charlas informativas sobre los beneficios de la seguridad de la información, cumplir con la normativa vigente.

Continua

36	Se dispone de niveles de seguridad en el acceso de la documentación que maneja la institución?	No se dispone de metodologías, procedimientos para definir los niveles de acceso a la información, no se dispone de un análisis RISK para identificar la información sensible	ALTA	Se debe realizar un análisis RISK, para solventar e identificar la información sensible de la institución. Se debe realizar un reglamento, procedimientos del manejo de la información sensible
37	Se realizan pruebas cuando se cambia los sistemas operativos, para asegurar que no haya impacto en las aplicaciones críticas para la institución?	No se dispone de procedimientos ni registros de verificación de cambios a los sistemas.	MEDIA	Se debe realizar procedimientos para la verificación de cambios y validación de los sistemas.
38	Se dispone de procedimientos de reacción en el caso de encontrar vulnerabilidades técnicas en el sistema?	No se tiene documentación de respaldo, ni procedimientos en el caso de encontrarse vulnerabilidades en el sistema	MEDIA	Realizar procedimiento que aseguren el cumplimiento de la política vigente referente a seguridad de la información
39	Se realizan pruebas de intrusión periódicas para determinar la adecuación de la protección de la red?	No se tiene informes de intrusión para protección de la red, ni se dispone de procedimientos, ni metodología a ser implementada	ALTA	Realizar un cronograma de pruebas de intrusión periódicas, aplicando buenas prácticas para solventar los procedimientos de análisis de vulnerabilidades
40	Se dispone de procedimientos para el acceso y control remoto para los sistemas?	No se dispone que se tenga registros ni procedimiento para acceso y control remoto a los sistemas	MEDIA	Realizar procedimientos para acceso remoto y socializar a los responsables de utilizar esto las políticas de seguridad de la institución en base a la normativa vigente

Continua

41	Se dispone de procedimientos para cifrar la información almacenada de acuerdo a su clasificación?	No se dispone de procedimientos de clasificación de la información (análisis RISK), ni de metodologías para cifrar la información sensible	MEDIA	Se debe realizar un análisis RISK, para solventar e identificar la información sensible de la institución. Se debe realizar un reglamento, procedimientos de encriptación de la información sensible
42	Se ha establecido un inventario de documentos sensibles y dispositivos de salida?	No se dispone de procedimientos de clasificación de la información (análisis RISK), ni de metodologías para cifrar la información sensible No se realiza un inventario de dispositivos actualizado.	ALTA	Se debe realizar un análisis RISK, para solventar e identificar la información sensible de la institución. Se debe realizar un reglamento, procedimientos inventarios de la información y dispositivos sensibles
43	Se tiene un registro, procedimiento de recopilación de eventos de seguridad para detectar incidentes potenciales?	No se encontró registros de eventos que comprometan la seguridad de la información	MEDIA	Elaborar, implementar registros que sucedan con respecto a la seguridad de la información, estandarizar formatos para levantamiento de los eventos.
		ALTA	14	
		MEDIA	26	
		BAJA	3