
UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

**VICERRECTORADO DE INVESTIGACIÓN, Y VINCULACIÓN CON LA COLECTIVIDAD**

**MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS**

**VII PROMOCIÓN**

**TESIS DE GRADO MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS**

# TEMA: PLAN DE SEGURIDAD DE LA INFORMACIÓN DE LA ESPE SEDE MATRIZ

**AUTORES: SALGADO CORRALES, RAFAEL LEONIDAS**
**TAPIA YEROVI, SANTIAGO XAVIER**

**DIRECTOR: Eco. CHIRIBOGA B., GABRIEL, MSc.**

**SANGOLQUÍ, MAYO DEL 2015**

**Universidad de las Fuerzas Armadas- ESPE**
**Vicerrectorado de Investigación y Vinculación con la colectividad**
**Unidad de gestión de postgrados**
**Maestría en Evaluación y Auditoría de Sistemas Tecnológicos**
**Promoción VII**

## CERTIFICADO

En mi calidad de Director del proyecto "Plan de Seguridad de la Información de la ESPE sede Matriz", realizado por: Ing. Salgado Corrales, Rafael Leonidas e Ing. Tapia Yerovi, Santiago Xavier, para optar por el título de Magister en Evaluación y Auditoria de Sistemas Tecnológicos, **CERTIFICO,** que dicho proyecto ha sido dirigido y revisado periódicamente y cumple con las normas establecidas por la ESPE, en el reglamento de estudiantes de posgrados y considero que reúne los requisitos y los méritos suficientes para ser sometida a la presentación pública y evaluación por parte del tribulan examinador que se designe

Sangolquí, Mayo del 2015

---

**Eco. CHIRIBOGA BARRERA, GABRIEL EDUARDO MSc.**
**DIRECTOR**

**Universidad de las Fuerzas Armadas- ESPE**
**Vicerrectorado de Investigación y Vinculación con la colectividad**
**Unidad de gestión de postgrados**
**Maestría en Evaluación y Auditoría de Sistemas Tecnológicos**
**Promoción VII**

## DECLARACIÓN

La Tesis de grado titulada: "Plan de Seguridad de la Información de la ESPE sede Matriz"

Ha sido desarrollada en base a una investigación, respetando derechos intelectuales de terceros, cuyas fuentes son citadas e incorporadas en la bibliografía, consecuentemente este trabajo es de nuestra autoría.
En virtud de esta declaración, nos responsabilizamos del contenido, veracidad y alcance científico de esta tesis.

Sangolquí, Mayo del 2015

---------- ----------

Ing. Rafael Salgado Corrales Ing. Santiago Tapia Yerovi

**Universidad de las Fuerzas Armadas- ESPE**
**Vicerrectorado de Investigación y Vinculación con la colectividad**
**Unidad de gestión de postgrados**
**Maestría en Evaluación y Auditoría de Sistemas Tecnológicos**
**Promoción VII**

## AUTORIZACIÓN

Nosotros: Salgado Corrales Rafael Leonidas y Tapia Yerovi Santiago Xavier autorizamos a la Universidad de Fuerzas Armadas - ESPE, la publicación en la biblioteca virtual de la institución del trabajo "Plan de Seguridad de la Información de la ESPE sede Matriz", cuyo contenido y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, Mayo del 2015

---------- ----------

Ing. Rafael Salgado Corrales Ing. Santiago Tapia Yerovi

## DEDICATORIA

“Nadie está a salvo de las derrotas. Pero es mejor perder algunos combates en la lucha de nuestros sueños, que ser derrotado sin saber siquiera por qué está luchando”

**“Paulo Coelho”**

Dedicado a mi querida familia: Rafael, Emilio, Carito, Teresita y Arturito; por todo su amor, compañía, comprensión y enseñanzas.

Rafael Salgado Corrales

## DEDICATORIA

A mí hijo Ignacio José, mi mayor motivo para seguir adelante.

A Maruja Poveda, y su continúa guía y protección.

A Piedad, Efraín, Ana, Hermel, Silvita, Alicia, Beatriz, Inés y Juanita, por quienes he llegado a donde estoy ahora.

A mis amigos y en general a todas las personas con los que día a día sonrío, aprendo y crezco día tras día.

Santiago Xavier Tapia Yerovi

## AGRADECIMIENTO

Agradezco a Dios por encaminar cada uno de mis pasos en la culminación de este gran reto.

A mi familia, a ti Carol Elisa que estas a mi lado incondicionalmente, a nuestros hijos Rafael y Emilio quienes me dan esa energía cada día para hacer las cosas con ganas.

A mis padres Arturito y Teresita, por todo su apoyo, motivación, y enseñanzas.

A todos los profesores personas profesionales que impartieron sus conocimientos y experiencias a los largo de esta carrera universitaria.

Al Economista Gabriel Chiriboga por ser nuestra guía en la culminación de este trabajo.

Rafael Salgado Corrales

## AGRADECIMIENTO

Agradezco a mi esposa e hijo, quienes han estado junto a mi de manera incondicional.

A Piedad, Efraín, Silvita, Hermel, Alicia, Beatriz e Inés.

Al Eco. Gabriel Chiriboga y al Ing. Mario Ron, quienes hicieron posible este trabajo.

A todas las personas que directa o indirectamente han sido mi guía y soporte en éste continúo caminar por la vida.

Santiago Xavier Tapia Yerovi

# ÍNDICE GENERAL

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# LISTADO DE ANEXOS

## RESUMEN

Siendo la Universidad de las Fuerzas Armadas - ESPE, una institución pública de educación superior, la presente tesis, hace uso a un estudio técnico de las buenas prácticas internacionalmente aceptadas, de marcos referenciales actuales para gestión y gobierno de TI y la seguridad de la información (COBIT v5, NTE ISO/IEC 27000, etc.); además se considerara la normativa vigente (Acuerdo Ministerial 166, EGSI), que combinadas fortalecen y apoyan los procesos internos de TI que la Universidad posee para llevar a cabo los logros institucionales de gestión de la información. El objetivo de la presente obra es: "Elaborar el Plan de Seguridad de la información de la ESPE sede Matriz"; donde se considerara la evaluación de la situación actual, el análisis de las capacidades, fortalezas, amenazas y potenciales riesgos de seguridad de la información y la propia elaboración del Plan de Seguridad de la Información, la misma estará en la capacidad de llevar procesos de TI con seguridad, debidamente: documentados, monitoreados y sujetos a mejora continua, en un ambiente regulatorio donde se mitigarán debidamente los potenciales efectos de dichas vulnerabilidades encontradas y permitirá una respuesta competente y oportuna ante eventuales incidentes de seguridad que podrían atentar negativamente con la información de la institución. Las conclusiones y recomendaciones de este proyecto orientan su esfuerzo a evaluar y dar propuestas para corregir las falencias que sean provocadas por la pérdida en la calidad en la administración de la información.

**PALABRAS CLAVE:**

- **COBIT**
- **NTE ISO/IEC 27000**
- **SEGURIDAD**
- **EGSI**
- **ESPE**

## ABSTRACT

As the University of the Armed Forces - ESPE, a public institution of higher education, this thesis makes use of a technical study of internationally accepted good practices, current reference frameworks for management and governance of IT and information security (v5 COBIT, NTE ISO/IEC 27000, so on.); plus the applicable regulations (Ministerial Agreement 166, EGSI), which combined strengthen and support internal IT processes that the University has to carry out the institutional achievements of information management is considered. The aim of this work is: "Security Information Plan for ESPE's headquarters"; where the evaluation of the current situation is considered, the analysis of the capabilities, strengths, threats and potential risks of information security and self-development of the Plan of Information Security, it will be in the ability to bring IT processes safely, properly: documented, monitored and subject to continuous improvement, in a regulatory environment where properly mitigate the potential impacts of such vulnerabilities found and will allow a competent and timely response to any security incidents that may adversely undermine the information institution. The conclusions and recommendations of this project direct their effort to evaluate and proposals to correct deficiencies that are caused by the loss of quality in information management.

**KEYWORDS:**

- **COBIT**
- **NTE ISO/IEC 27000**
- **SECURITY**
- **EGSI**
- **ESPE**

# CAPÍTULO 1

## 1.1 Introducción

La información es un activo que en la actualidad se le ha dado un gran valor en las empresas, por lo que se ha tomado conciencia de la protección que se debe tener con ella. Antiguamente la información se la manejaba manualmente, los documentos más importantes se los mantenían bajo llave y se restringía la manipulación de esta a los empleados.

La tecnología ha obligado a que estos procesos manuales evolucionen transformando los documentos físicos en archivos digitales, con esto también se genera la necesidad de proteger esta información de amenazas externas como internas que pueden afectar a la continuidad en la empresa.

Por esto el objetivo principal de la seguridad de la información es garantizar la continuidad en la empresa reduciendo riesgos, para que de esta manera las operaciones del negocio no puedan verse afectadas.

Los ataques a los sistemas tecnológicos que se han visto expuestas las empresas para manipular su información han generado un sentido de urgencia mayor que antes, con respecto a la necesidad de mantener la seguridad. Las empresas pueden haber reforzado las medidas de seguridad, pero nunca conocerían con precisión cuándo o cómo pueden estar expuestas. Con el objeto de brindar la más completa protección empresarial, se requiere un sistema efectivo y eficiente de seguridad a través de un plan de seguridad.

## 1.2 Justificación e Importancia

Mediante el Plan de Seguridad de la Información a realizarse, la Universidad de las Fuerzas Armadas estará en capacidad de tomar de decisiones, conociendo las deficiencias y vulnerabilidades que tiene su actual gestión en la parte informática, de modo que, al realizar el estudio técnico basado en buenas prácticas internacionalmente aceptadas, se verán reflejadas las deficiencias existentes en la institución, podrán gestionar y mitigar debidamente los potenciales efectos de dichas

vulnerabilidades encontradas y permitirá una respuesta rápida, ágil y oportuna ante eventuales incidentes de seguridad que podrían atentar negativamente en contra de la información de la institución.

Este proyecto de tesis orienta su esfuerzo a evaluar y dar propuestas para corregir las falencias que se evidencien y sean causa de pérdida en la calidad en la entrega de los servicios que ofrece la Universidad de las Fuerzas Armadas; lográndose de esta manera mejor calidad en los procesos de gestión de la información que la misma gestiona.

Las normas en las cuales vamos a basar el plan de seguridad propuesto son: la familia de normas NTE INEN ISO 27000 y COBIT versión 5.

### 1.3 Planteamiento del Problema

La Universidad de las Fuerzas Armadas en su sede principal al ser un ente de educación superior que gestiona, procesa y almacena información susceptible referente a las siguientes áreas:

- Sistema escolástico comprendiendo: calificaciones e historial académico junto a información personal de su alumnado (de pregrado y post grado).
- Información propia de su actividad de investigación científica.
- Información inherente a su acción económica/administrativa.

En base a esto el manejo de la información debería ser gestionada con procesos y políticas que aseguren la continuidad en la institución, pero al no contar con un Plan de seguridad de la información, queda en evidencia algunas vulnerabilidades como:

- No cuenta con políticas y procesos claramente definidos sobre gestión de la seguridad de la información.
- Falencias en el comportamiento y cultura organizacional con respecto al rol que tienen los interesados en la seguridad de la información (Alumnos, personal docente, personal administrativo, personal militar, visitantes).
- Vulnerabilidad en la manipulación de la información.
- Mala gestión de acceso a áreas susceptibles del campus.

Es por lo antes mencionado, que queda clara la relevancia del presente proyecto, pues emerge como una solución palpable a la gestión de la seguridad de la información en la Escuela Politécnica de las Fuerzas Armadas.

## 1.4 Formulación del Problema

Con el desarrollo del presente proyecto de tesis, se busca dar respuesta a las siguientes interrogantes que surgen del análisis de la situación actual de la Universidad de las Fuerzas Armadas.

- ¿Cuál es la situación actual de la institución referente a seguridad de la información?
- ¿Cuáles son las necesidades de protección de la información que posee la institución?
- ¿Cómo se podría mitigar los riesgos asociados al uso de los sistemas informáticos de la Universidad de las Fuerzas Armadas sede principal?

## 1.5 Hipótesis

No Aplica.

## 1.6 Objetivo General

Elaborar el Plan de Seguridad de la Información de la Universidad de las Fuerzas Armadas (sede Principal), alineándolo a los objetivos estratégicos de la institución mediante el uso de marcos referenciales, estándares internacionalmente aceptados y normativa gubernamental vigente.

## 1.7 Objetivos Específicos

- Evaluar la situación actual de la institución en referencia al tratamiento que la misma da a la información.
- Determinar las necesidades de protección de los sistemas informáticos que la institución posee.

- Realizar el Análisis de riesgos e impactos utilizando las normas Técnicas ecuatorianas: ISO IEC 27005 y la ISO/EC 31000.
- Elaborar las políticas de seguridad de la información de la Universidad de las Fuerzas Armadas, aplicadas a un plan de seguridad de la información mediante el uso de la familia de normas técnicas ecuatorianas: NTE ISO/IEC 27000 y el Acuerdo No 166: EGSI.

# CAPÍTULO 2

## 2.1 Marco Teórico

### 2.1.1 Antecedentes del Estado del Arte

El modelo de madurez de COBIT versión 5 al pasar del tiempo se ha basado en las experiencias de sus mentores, los mismos que lo han ido puliendo en base a ajustes y alineándose con otras normas y marcos referenciales como:

- ISO/IEC 31000 para gestión de Riesgos
- ISO/IEC 27000:2013 para Seguridad de la Información,

Es el motivo principal por el cual se ha seleccionado la combinación de dicho marco referencial junto a las normas indicadas para el desarrollo del plan de seguridad de la información de la Universidad de las Fuerzas Armadas.

### 2.1.2 Marco Teórico

La elaboración de un plan de seguridad de la información, supone el uso de buenas prácticas, marcos de referencia y estándares internacionalmente aceptados.

Para el caso puntual de la generación del plan de seguridad de la información para la Universidad de la Fuerzas Armadas se emplearán los siguientes marcos referenciales, estándares y normas que forman parte del entorno regulatorio vigente:

**COBIT Framework versión 5**

Es un marco referencial para gobierno y gestión de TI de las empresas y en términos generales permite -mediante la inclusión de TI-, generar valor a las organizaciones, optimizando el riesgo, haciendo un uso adecuado de recursos y reduciendo costos. COBIT 5 además permite a las TI ser gobernadas y gestionadas de un modo holístico (ver a la empresa como un ente único, sin elementos dispersos), abarcando al negocio de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico, no prescriptivo y se acopla a empresas de cualquier tamaño, indistintamente de su ámbito de acción (ISACA, 2009).

La siguiente imagen resumen los cinco principios que maneja COBIT 5.

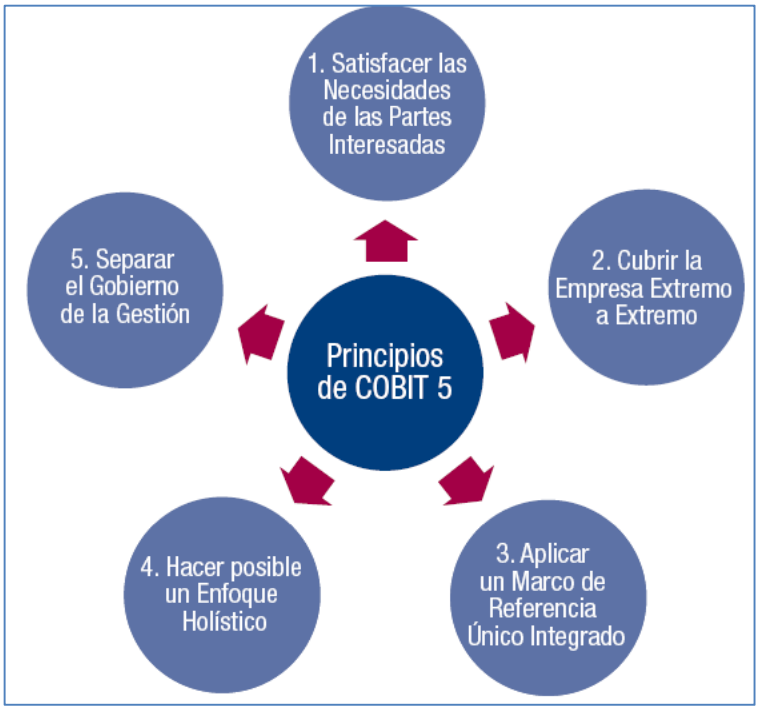


**Figura 1**. Principios de COBIT 5

**Fuente**: (ISACA, 2009)

COBIT 5 está enfocado en trabajar en función a los objetivos estratégicos de la organización, por tanto, su objetivo es alinear a TI con el rumbo de negocio de la empresa, y para tal efecto, hace uso del modelo de cascada de Metas (Fig. 2), la cual partiendo de los objetivos estratégicos de la organización, alinea a las mismas con las metas corporativas COBIT, para luego alinearlas con las metas de TI de COBIT y posteriormente aplicar metas de catalizadores para lograr los objetivos de la empresa mediante un uso adecuado de TI (ISACA, 2009).

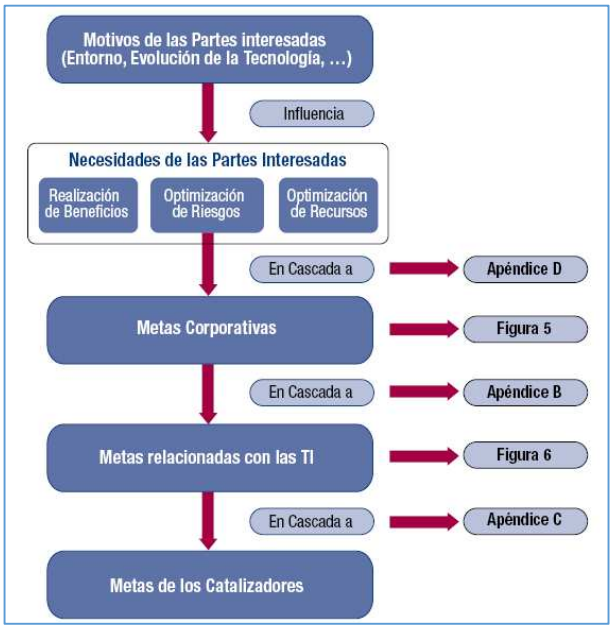


**Figura 2**: Modelo de Cascada de Objetivos COBIT 5.

**Fuente:** (ISACA, 2009)

Los catalizadores son en términos generales acciones que permiten la consecución de las metas de la empresa, y para tal efecto, COBIT ha realizado una clara separación entre gobierno y gestión, para lo cual ha de definido procesos para cada ámbito en su Modelo de Referencia de Procesos (ISACA, 2009).

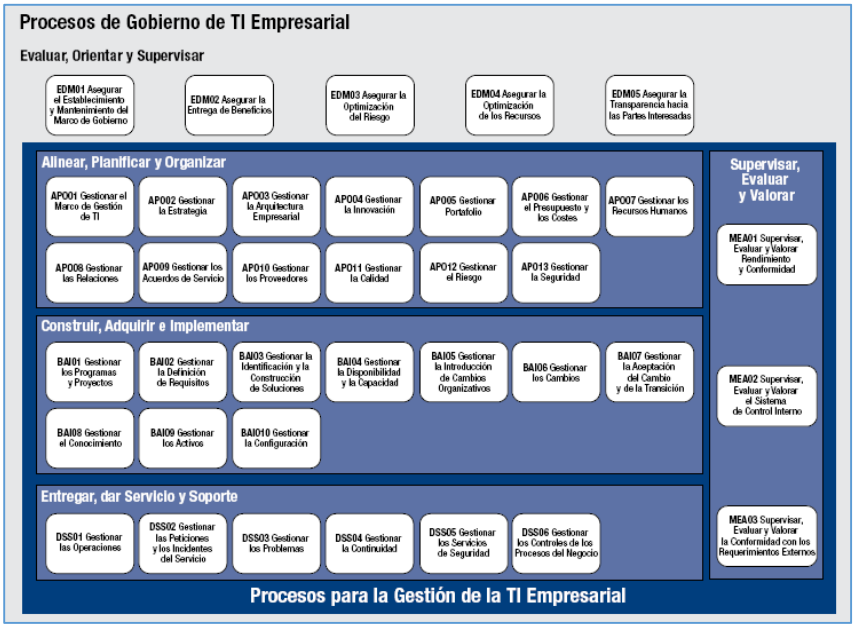


**Figura 3**: Modelo de Referencia de procesos COBIT 5.

**Fuente**: (ISACA, 2009)

**NTE INEN ISO 31000**

Norma Técnica Ecuatoriana gestionada por el INEN enfocada en la gestión de los Riesgos y su objetivo es brindar lineamientos para la gestión del riesgo así como la implementación de dicha gestión a niveles tanto operativos como estratégicos. (INEN, 2014)

**Esquema Gubernamental de la Seguridad de la Información (EGSI)**

Acuerdo Ministerial 166, emitido en Septiembre del año 2013 por la SNAP (Secretaria Nacional de la Administración Pública), en el cual de dictamina la obligatoriedad en entidades públicas –como la Universidad de las Fuerzas Armadas- el uso de la familia de normas Técnicas ecuatorianas NTE INEN ISO/IEC 27000 (Gestión de la Seguridad de la Información) (SNAP, 2009).

**Sistema de Gestión de Seguridad de la Información (NTE INEN ISO/IEC 27000)**

Este Estándar Internacional ha sido preparado para proporcionar un modelo para establecer, Implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. (INEN, 2008)

**Norma ISO/IEC 27001**

Es la principal norma de la serie 27000 y contiene los requisitos para implantar un sistema de seguridad de la información. Esta es la certificación que deben obtener las organizaciones en cuanto se refiere a seguridad de la información.

La norma ISO/IEC 27001 se enfoca en la gestión de riesgos y la mejora de procesos de acuerdo al ciclo de que se basa en planificar, hacer, verificar y actuar. Para implantación la norma en la organización se requiere de un tiempo de 6 a 12 meses.

- Para la certificación, una entidad externa y acreditada audita el sistema para comprobar su validez y emitir el certificado a la organización. Para el éxito

de dicho proceso es recomendable la ayuda de consultores externos expertos en el tema de seguridad de la información.

- ISO/IEC 27001 es la única norma internacional auditable que por sus controles de seguridad ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. Esta se aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad (ISO, 2013).

**Norma ISO/IEC 27002**

Antes llamada ISO/IEC 17799, es una guía de buenas prácticas en la gestión de la seguridad de la información. Esta contiene los dominios, objetivos de control y controles para el proceso de diseño e implantación de sistemas de seguridad de la información. (INEN, 2009)

ISO/IEC 27002:2005 está conformada de 11 dominios, 39 objetivos de control en donde constan los 133 controles recomendados para la seguridad de la información. Los dominios son los siguientes:

- Dominio Política de Seguridad
- Dominio Organización de la Seguridad de Información
- Dominio Gestión de Activos
- Dominio Seguridad de Recursos Humanos
- Dominio Seguridad Física y Ambiental
- Dominio Gestión de Comunicaciones y Operaciones
- Dominio Control de acceso
- Dominio Adquisición, Desarrollo y Mantenimiento de Sistemas de Información
- Dominio Gestión de Incidentes de Seguridad de Información
- Dominio Gestión de la Continuidad Comercial
- Dominio Conformidad

### 2.1.3 Marco Conceptual

Aquí se definen algunos conceptos involucrados de las variables de investigación:

**ISO:** Organización Internacional para la Estandarización, que regula una serie de normas para las industrias.

**INEN:** Instituto Ecuatoriano de Normalización. Entidad Gubernamental ecuatoriana enfocada en regular y estandarizar buenas normas y prácticas internacionalmente aceptadas.

**ISACA:** Siglas de “Information Systems Audit and Control Association”. Es una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.

**Marco de referencia:** Colección de buenas prácticas internacionalmente o localmente aceptadas, debidamente estandarizadas por alguna organización.

**Norma:** Conjunto de lineamientos a seguir en un determinado contexto, por ejemplo acuerno No 166 de la SNAP. EGSI.

**Seguridad de la información:** Conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. ((INEN, 2009))

Se debe proteger los activos, que son los recursos de la Organización que tienen que ver con los sistemas de información de las amenazas que pueden afectar nuestros activos informáticos y para manejar el riesgo de cada amenaza habrá que delimitar:

- Probabilidad de ocurrencia
- Gravedad de la situación generada
- Costo de la medida de prevención

Para actuar en consecuencia y:

- Asumir el riesgo, en el caso que las medidas sean más costosas que las consecuencias de la amenaza o evitarlo.

**Plan de seguridad de la información:** El Plan de Seguridad Informática constituye el documento básico para lograr la confidencialidad, integridad y

disponibilidad de la información y la protección de los medios y los locales donde se utilice la técnica de computación. (ISO, 27001)

En el desarrollo de este plan es necesario formular la política de seguridad, establecer una estructura de gestión de la seguridad informática, elaborar el sistema de medidas de seguridad informática, implantar el programa de seguridad informática y elaborar el plan de contingencia de la entidad. (ISO, 27001)

Previo a la formulación del plan de seguridad informática, se deben considerar diferentes aspectos referentes a la información en la organización. Así, se debe realizar un estudio previo del estado de la seguridad de la información de la organización.(ISO, 27001)

Con este estudio previo se puede ya elaborar el plan de seguridad. Ésta es el conjunto de principios y reglas generales que regulan la forma, propia de cada organización, de proteger las informaciones que maneja en todas las fases de su tratamiento.(ISO, 27001)

Un factor determinante en la elaboración de esta política, y consecuentemente en el éxito del plan de seguridad, es la implicación de los máximos responsables de la institución. A no ser que éstos comprendan y se involucren en los objetivos de la política de seguridad su buen resultado será incierto. El plan de seguridad afecta a todos los servicios y niveles dentro de éstos, así como a los flujos de información entre diferentes servicios, de éstos al exterior y viceversa. Es decir, involucra a todo el sistema de información de la organización. (ISO, 27001)

**Importancia del plan de seguridad:** Es muy importante ser conscientes de que por más que una empresa a nuestro criterio sea la más segura, con el incremento del uso de nueva tecnología para manejar la información nos hemos abierto a un mayor número y tipos de amenazas. Es por eso que en el ambiente competitivo de hoy, es necesario que las entidades aseguren la confidencialidad, integridad y disponibilidad de la información vital corporativa. (ISO, 27001)

Por lo tanto la seguridad informática debe ser dada por una colaboración entre los encargados de la seguridad de la información, que deben disponer de las medidas al alcance de su mano, y los usuarios, que deben ser conscientes de los riesgos que implican determinados usos de los sistemas y de los recursos que consumen cada vez que les pasa algún problema ya que esto les hace que pierdan tiempo de producción y

el consumo de recursos en horas de la recuperación de la actividad normal es en muchos casos irrecuperable. (ISO, 27001)

Sin embargo, gran parte de esa concientización está en manos de los responsables de seguridad de la información apoyados en todo momento por la Gerencia de forma explícita y activa, por ello es importante indicarles no sólo cuales son las principales amenazas en cada momento, sino qué deben hacer para evitarlas, impartiendo así procedimientos de actuación que permitan que las medidas técnicas que se disponen desde informática sean efectivas. (ISO, 27001)

Por consiguiente en este nuevo entorno, es imprescindible que las empresas se preparen no sólo para prevenir el peligro de comprometer sus operaciones de negocio por una falla de seguridad, sino también que se preparen en establecer medidas que permitan reducir los problemas de seguridad que pueden surgir. (ISO, 27001)

**Información:** Se constituye como una colección de datos ya supervisados y ordenados, que sirven para construir un mensaje basado. (ISO, 27005)

**Riesgo:** Efecto causado por la incertidumbre que ha sido ocasionado por factores tanto internos como externos a una organización. (ISO, 27005)

# CAPÍTULO 3

## 3.1 Metodología de Investigación

### 3.1.1 Ubicación geográfica del proyecto de investigación.

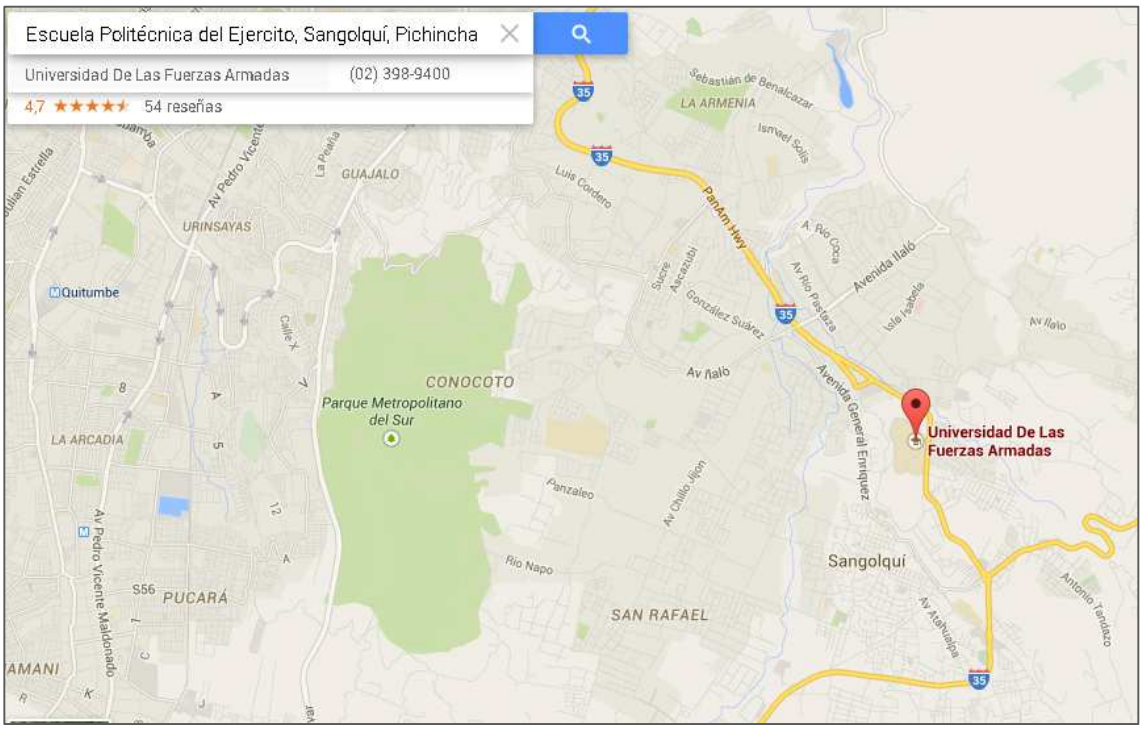


**Figura 4**: Localización Geográfica de la Universidad de las Fuerzas Armadas.

**Fuente**: Mapa generado con la herramienta Google Maps.

**Universidad de las Fuerzas Armadas, ESPE.**

**Ubicación**: Av. Gral. Rumiñahui s/n Sangolquí - Ecuador

Teléfonos: +593(02) 3989400

Fax: +593(2) 2334 952

P.O.BOX 171-5-231B

Provincia: Pichincha

Cantón: Rumiñahi

Parroquia: Sangolquí.

Área de influencia: La comunidad universitaria: docentes, administrativos, estudiantes, etc.

### 3.1.2 Identificación de variables/categorías a utilizar en el proceso investigativo.

El presente proyecto de tesis se basa en análisis cuantitativos, que reflejen porcentualmente el índice de cumplimiento de la Universidad de las Fuerzas Armadas en referencia a temas de Seguridad por tal motivo, las variables a analizar son cada uno de los dominios de cumplimiento de la Familia de Normas Técnicas Ecuatorianas (NTE ISO/IEC 27000).

### 3.1.3 Método de investigación, técnicas e instrumentos de recolección y procesamiento de datos e información

El desarrollo del presente proyecto de tesis emplea una metodología: aplicativa, cualitativa, enfocada en la exploración y bibliográfica; a continuación, una breve descripción de cada uno:

**a) Aplicativa**

Es la aplicación práctica de conocimiento teórico, principalmente extraído de la familia de estándares ISO  NTE INEN-ISO/ IEC 27000 (a nivel de riesgos y controles) y el marco referencial COBIT 5 (a nivel de medición de madurez de procesos); y de ésta manera aplicar los mismo en la generación del Plan de Seguridad de la Información de la ESPE (sede Matriz).

**b) Cualitativa**

Permite obtener respuestas sobre el tema central de esta investigación, usando inferencia estadística, es decir, partiendo de la toma de muestras, se logra resultados generales.

**c) Enfocada en la exploración**

Este método, se caracteriza por la profundización que el investigador debe realizar en un tema específico para obtener respuestas; para este caso puntual, investigar los detalles en torno a la seguridad de la información que den como resultado información de entrada para después de procesarla se pueda emitir conjeturas en cuanto a la situación actual de la institución en su sede Matriz.

**d) Bibliográfica**

Técnica que basa su trabajo en bibliografía o documentación especializada previamente desarrollada sobre el tema central de la investigación, para éste caso, Seguridad de la Información.

**Técnicas:**

**a) Entrevistas**

Técnica que prevé captar información de la fuente misma donde se desarrollan los procesos, para éste caso puntual, el personal de la institución y los procesos que ellos manejan.

**b) Observación**

Técnica que prevé in situ obtener información donde los procesos institucionales se llevan a cabo en manos de los empleados institucionales.

**c) Documental**

El desarrollo del presente proyecto de tesis, supone recabar información bibliográfica con el objetivo de robustecer con sustento teórico la propuesta técnica que se haga en esta evaluación.

### 3.2 Ejecución del Proceso de Investigación

El presente proyecto de tesis, ha sido desarrollado para la Universidad de las Fuerzas Armadas (sede Matriz), ubicada en Sangolquí, -provincia de Pichincha- y tiene como objetivo analizar la situación actual de la misma en referencia al tema de Seguridad de la Información, para lo cual se empleará la familia de normas técnicas ecuatorianas ISO/IEC 27000 junto con el marco de referencia COBIT (versión 5) y el EGSI (SNAP, Acuerdo 166).

Adicionalmente el presente proyecto de tesis, hace uso de la metodología “MPSI ESPE-L” (Metodología Plan de Seguridad de la Información para la ESPE extensión Latacunga, creada por Cristian Aguirre, egresado de la Maestría en Evaluación y Auditoria de Sistemas Tecnológicos); dicha metodología es un compendio de las buenas prácticas definidas en la familia de normas NTE INEN ISO/IEC 27000 en referencia a la Gestión de la Seguridad de la información en la implementación de un SGSI usando como apoyo al marco COBIT versión 5.

La metodología “MPSI ESPE-L” se compone de diez pasos, los mismos que se basan en la norma NTE ISO/IEC 27000 y cuyo resultado final es un **PLAN DE SEGURIDAD DE LA INFORMACIÓN** (en éste caso para la ESPE en su sede Matriz).

Los diez pasos que son parte de la metodología “MPSI ESPE-L” se ilustran en la siguiente tabla:

**Tabla 1**

**Descripción de Metodología**

| Metodología Plan de Seguridad de la Información ESPE (sede Matriz) | |
|---|---|
| **Pasos** | **Descripción** |
| 1 | Proceso de Análisis e identificación de activos en la ESPE (sede Matriz) |
| 2 | Metodología de clasificación de activos en la ESPE (sede Matriz) |
| 3 | Análisis de riesgos (ISO 27005) en la ESPE (sede Matriz) |
| 4 | Metodología de riesgos (ISO 27005) en la ESPE (sede Matriz) |
| 5 | Análisis de controles (ISO 27002) en la ESPE (sede Matriz) |
| 6 | Reporte de análisis de controles (ISO 27002) en la ESPE (sede Matriz) |
| 7 | Análisis requerimientos según ISO 27003 en la ESPE (sede Matriz) |
| 8 | Reporte requerimientos según ISO 27003 en la ESPE (sede Matriz) |
| 9 | Análisis requerimientos ISO 27001 en la ESPE (sede Matriz) |
| 10 | Reporte análisis de requerimientos ISO 27001 en la ESPE (sede Matriz) |

NOTA: El presente proyecto de tesis hará uso de la metodología antes mencionada junto con instrumentos de auditoria que automaticen el procesamiento de la información recolectada; se hará mención a dichos instrumentos a lo largo del documento.

### 3.2.1 Paso 1 Análisis e identificación de activos en la ESPE (sede Matriz)

**Identificación de Activos**

Describe e identifica los principales activos de información de la ESPE (sede Matriz) que se hallan involucrados en el procesamiento de la información que la institución maneja. Considérese a un activo para el plan de Seguridad de la Información a: Hardware, Software, Recurso Humano, datos etc.

Nota: El instrumento de trabajo destinado al tratamiento de activos es el Anexo A (Inventario de Activos).

**Recolección de información referente a Activos de información**

El proceso de recolección de la información se realiza empleando el instrumento para la gestión de "Inventario de Activos" (Anexo A) cuya estructura se detalla a continuación:

**Tabla 2**

**Descripción del Instrumento para Inventarios de activos ESPE (sede Matriz)**

| | |
|---|---|
| **ID** | Codificación del Activo. Se compone de las Siglas propias de activos "AC" y la numeración correspondiente. Ejemplo: AC001. |
| **ACTIVO IDENTIFICADO** | Nombre del Activo identificado. Ejemplo: Sistema Financiero OLYMPO |
| **TIPO DE ACTIVO** | La identificación de los activos está basado en la norma ecuatoriana ISO/IEC 27005:2008 en donde se identifican dos tipos de activos: primarios y los de soporte.<br><br>Los primarios, son procesos e información en extremo sensible para la institución.<br><br>Los activos de soporte, son como su nombre lo indica quienes dan soporte a los primarios. Dentro de éstos dos tipos de activos de definen:<br><br>**Dato:** Información que se crea, envía, recibe y gestionan dentro de la institución.<br><br>**Aplicación:** Software de soporte a los procesos.<br><br>**Personal:** Actores que de una u otra manera se ven involucrados con activos.<br><br>**Servicio:** Servicios que alguna área de la institución suministra a otra área o entidades externas a la misma. |

CONTINÚA

| | |
|---|---|
| | **Tecnología:** Hardware de manejo de información y comunicaciones.<br><br>**Instalación:** Lugar de alojamiento de activos de información. Puede ser interno o externo a la organización.<br><br>**Equipamiento auxiliar:** Activos que no forman parte de ninguno de los anteriores tipos. |
| **DESCRIPCIÓN** | Brinda una ligera descripción del activo. Ejemplo: "Sistema Financiero Contable" |
| **RESPONSABLE** | Detalla el (o los) responsables del activo. Ejemplo: "Ing. Carlos Castro" |

A continuación en la siguiente tabla se muestra la aplicación del instrumento de Inventario de Activos (Anexo A), al gestionar la lista de activos suministrados (bajo requerimiento de los autores del presente proyecto de tesis) por el personal de la UTIC para desarrollo del presente proyecto de tesis.

**Tabla 3**

**Ejemplo aplicación del instrumento para Inventarios de activos ESPE (sede Matriz).**

| ID | ACTIVO IDENTIFICADO | DESCRIPCIÓN | TIPO DE ACTIVO | RESPONSABLE |
|---|---|---|---|---|
| AC001 | Sistema Académico | Sistema Académico -anterior-;contiene datos histórico de estudiantes. | Aplicación | No se define por parte de la UTIC |
| AC002 | Sistema Financiero OLYMI | Sistema Financiero Contable | Aplicación | No se define por parte de la UTIC |
| AC003 | Sistema Recursos Humanc | Sistema de Recursos Humanos SIFRHE; se encuentra en proceso de | Aplicación | No se define por parte de la UTIC |
| AC004 | Portal Web | Portal institucional. | Aplicación | No se define por parte de la UTIC |
| AC005 | Sistema de Educación Virt | Sistema de Educación virtual para modalidad de educación a distancia. | Aplicación | No se define por parte de la UTIC |
| AC006 | Sistema BANNER - ESPE Si | Sistema de matriculas, registro académico, registro y consulta de notas, curriculo académico, administración de planta física (aulas), planificación académica (asignaturas, NRC (paralelos), | Aplicación | No se define por parte de la UTIC |
| AC007 | Sistema BANNER ESPE Sis | Sistemas de Recursos humanos, | Aplicación | No se define por parte de la UTIC |
| AC008 | Sistema BANNER -ESPE Sis | Sistema de digitalización y administración de documentación | Aplicación | No se define por parte de la UTIC |
| AC009 | Sistema BANNER ESPE Sis | Sistema que intraga servicios web, despliegue de información a través de canales, basado en los roles | Aplicación | No se define por parte de la UTIC |
| AC010 | Sistema BANNER ESPE Sis | Sistema que automatiza la secuencia de acciones, actividades | Aplicación | No se define por parte de la UTIC |

### 3.2.2 Paso 2 Metodología de clasificación de activos en la ESPE (sede Matriz)

Como resultado de la fase de Análisis e Identificación de Activos, tenemos la metodología de clasificación de activos, la misma que será expuesta en la implementación de la propuesta.

### 3.2.3 Paso 3 Análisis de riesgos basado en la norma ISO 27005 en la ESPE (sede Matriz)

Un SGSI inicia con la valoración del riesgo ya que las medidas de seguridad que se apliquen, deben apuntarse hacia los riesgos más relevantes para la organización. Para valorar el riesgo, se emplea el estándar ISO 27005 ya que la misma propone varios ejemplos de escenarios donde se pueda realizar la mencionada valorización del riesgo; dicho estándar en su Anexo B del mencionado estándar y propone

adicionalmente ejemplos de amenazas comunes a las organizaciones y que sirven de guía a la tipificación del presente proyecto.

Para el análisis del riesgo, el presente trabajo utiliza el instrumento de Análisis de Riesgo (Anexo B), la cual es una herramienta que permite valorar los riesgos más significativos para una organización. La herramienta está diseñada siguiendo la siguiente fórmula de valoración de riesgo:

- **Riesgo** = Probabilidad de Amenaza (ocurrencia) x Magnitud de Daño (impacto)

La tabla 5 recoge los rangos de valoración en base a los cuales se ha desarrollado la herramienta de valoración de riesgo empleada (Anexo B).

**Tabla 4**

**Valores y condiciones para matriz de riesgo. ESPE (sede Matriz)**

| Valor | Riesgo |
|---|---|
| 1 | Insignificante (incluido Ninguna) |
| 2 | Baja |
| 3 | Mediana |
| 4 | Alta |

En la tabla 5 se detalla el mapa de calor empleada en la herramienta de valorización del riesgo (Anexo B).

**Tabla 5**

**Mapa de calor. ESPE (sede Matriz)**

| Valor | Probabilidad de Amenaza |
|---|---|
| 1-6 | Riesgo Bajo |
| 8-9 | Riesgo Medio |
| 12-16 | Riesgo Alto |

La figura siguiente indica la implementación del mapa de calor, tras la valorización de las condicionales: Probabilidad vs Impacto.

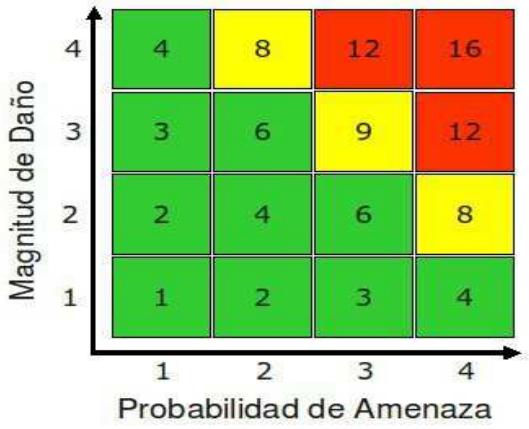


**Figura 5** Probabilidad vs Impacto

**Fuente**: (INEN, ISO 27005)

### 3.2.4 Paso 4 Metodología de riesgos (ISO 27005) en la ESPE (sede Matriz)

Como resultado del paso anterior (3 Análisis de riesgos basado en la norma ISO 27005 en la ESPE en su sede Matriz) tenemos la metodología de riesgos la misma que será expuesta al final del presente capítulo en la implementación de la propuesta.

### 3.2.5 Paso 5 Análisis de controles (ISO 27002) en la ESPE (sede Matriz)

Basándonos en la norma ISO 27001, en sus 11 dominios, 39 objetivos de control y 133 controles (anexo A de la norma) se elaboró un marco general para realizar un análisis de la situación real de la seguridad de la información en la ESPE (sede Matriz); se consideró adicionalmente las recomendaciones de implementación relacionadas en la norma ISO 27002 para estimar el estado y porcentaje de implementación de cada control en la **ESPE (sede Matriz)** ya que los mismos tienen relación directa con los lineamientos descritos en el Esquema Gubernamental para la Seguridad de la Información (EGSI) emitido por la Secretaria Nacional de la Administración Pública (SNAP) en su decreto 166.

La metodología utilizada para realizar este análisis se describe a continuación en la tabla 7 y tiene su correspondiente instrumento de trabajo en el Anexo C.

**Tabla 6**

**Matriz para análisis de controles y brecha para la ESPE (sede Matriz)**

| **Requerimiento, Control u Objetivo de Control ISO 27001** | | | | **IMPLEMENTACIÓN** | | |
|---|---|---|---|---|---|---|
| Requisito | # Sección | Nombre | Descripción/Objetivo | Estado | % | Observación |
| | | | | | | |

**Tabla 7**

**Descripción de matriz para análisis de controles y brecha para la ESPE (sede Matriz)**

| **Nombre** | **Descripción** |
|---|---|
| **Requisito** | Requisito general de la norma. Diferencia si es un control o un objetivo de control. |
| **# de Sección** | Números de sección de la norma ISO 27001:2005. Ejemplo: A.12.5.3 |
| **Nombre** | Nombre del requisito, dominio, objetivo de control o control evaluado. |
| **Descripción/Objetivo** | Una breve descripción extraída de la norma ISO 27002. |
| **Estado** | Corresponde a "Implementado", "Parcialmente implementado" o "No implementado" según corresponda. El estado se encuentra directamente relacionado con el porcentaje (%) de implementación mediante una |

| | |
|---|---|
| | estimación matemática, de manera que si tenemos un control en el 0% equivale a un control "No implementado", si se encuentra por encima del 60% se puede considerar "Implementado" y en los demás casos será "Parcialmente implementado". |
| **%** | Porcentaje estimado de implementación del control o requisito basado en la realidad actual de la **ESPE (sede Matriz)** evaluada respecto a la norma ISO 27001 teniendo en cuenta los lineamientos dados por la norma ISO 27002. |
| **Observaciones** | Se incluyen a manera explicativa sobre la forma o condición específica en la que se encuentra implementado cada control |

### 3.2.6 Paso 6 Reporte de controles (ISO 27002) en la ESPE (sede Matriz)

Como resultado del paso anterior tenemos es el reporte de los controles el mismo que será expuesto al final del presente capítulo en la implementación de la propuesta.

### 3.2.7 Paso 7 Análisis requerimientos ISO 27003 en la ESPE (sede Matriz)

Generar un EGSI, está en directa proporción con el nivel de cumplimiento que una organización tiene versus los requerimientos que la ISO 27003 define.

La metodología utilizada para realizar este análisis se muestra en la tabla 9 y toma los valores modelo de evaluación de procesos (Process Assessment Model, PAM) de COBIT 5, que se basa en la norma ISO 15504 y que se describe a continuación:

**Tabla 8**

**Modelo de evaluación de procesos**

| Nivel 1 | Nivel 2 | Nivel 3 | Nivel 4 | Nivel 5 |
|---|---|---|---|---|
| Inicial | En desarrollo | Definido | Gestionado | Optimizado |

Para esta valoración se elaboró un instrumento (Anexo D) que nos describe las salidas documentadas exigidas por la norma ISO 27003 y tomado de dicha norma para la **ESPE (sede Matriz)** para la implementación de un SGSI la misma que se describe a continuación en la tabla 10:

**Tabla 9**

**Matriz de salidas exigidas en la norma ISO 27003**

| **Nombre** | **Descripción** |
|---|---|
| **Fase de Implementación NTE INEN ISO/IEC 27003** | Identifica la fase en la que la organización se encuentra en el proceso de implementación del SGSI |
| **# de Número de paso** | Números de sección de la norma ISO 27001:2005 |
| **Actividad, referencia NTE INEN ISO/IEC 27003** | Actividad a realizar. |
| **Paso Pre-Requisito** | Paso previo antes de ejecutar el mismo. |
| **Salida Documentada** | Salida del requisito documentada que se tiene como resultado. |
| **Referencia a la NTE INEN ISO/IEC 27001** | Dominio de la norma. |
| **Nivel** | Nivel de madurez del proceso |

### 3.2.8 Paso 8 Reporte requerimientos ISO 27003 en la ESPE (sede Matriz)

El resultado del paso anterior es el reporte del análisis de la norma ISO27003, el mismo que será expuesta al final del presente capítulo en la implementación de la propuesta.

### 3.2.9 Paso 9 Análisis requerimientos ISO 27001 en la ESPE (sede Matriz)

Para este paso vamos utilizar la matriz de evaluación del nivel de madurez en seguridad de la información tomando como base el Modelo de Madurez de la Capacidad (CMM), de COBIT 5 dando una estimación del nivel de madurez de cada uno de los controles implantados en la **ESPE (sede Matriz)**, para con ello obtener una estimación de la madurez de los objetivos de control y dominios planteados en la norma ISO 27002.

De acuerdo al modelo planteado, existen cinco (5) posibles niveles de madurez y un nivel adicional para los controles que se consideran inexistentes (nivel cero). A medida que se avanza en los niveles se considera que el control es más efectivo para la **ESPE (sede Matriz)**, por ello se mide adicionalmente el porcentaje de efectividad para cada control.

Mírese Anexo E.

Expresado de la siguiente forma en la tabla número 11:

**Tabla 10**
**Nivel de madurez ISO 27001**

| | Nivel 1 | Nivel 2 | Nivel 3 | Nivel 4 | Nivel 5 |
|---|---|---|---|---|---|
| | Inicial | En desarrollo | Definido | Gestionado | Optimizado |
| Política | Ausencia de política | Política limitada | Política integral definida y publicada | Política publicada e implementada de manera uniforme | Revisión y mejora continuas de la política |
| Roles y responsabilidades | Roles y responsabilidades no definidos | Roles parcialmente definidos | Roles y responsabilidades bien determinados y definidos | Roles y responsabilidades definidos y ejecutados | Roles y responsabilidades revisados de manera continua |
| Automatización | Manual | Semi automatizada | Automatizada | Automatizada y completamente operativa | Actualización permanente de la automatización |

CONTINÚA

| | | | | | |
|---|---|---|---|---|---|
| Alcance | No implementado | Cobertura limitada | Activos críticos | Completo | Revisión periódica del alcance para garantizar la cobertura total |
| Eficacia | N/A | Baja | Media | Alta | Muy alta |
| Gestión de incidentes | Sin seguimiento | Visibilidad limitada | Seguimiento de incidentes críticos | Seguimiento y cierre de todos los incidentes | RCA aplicado a todos los incidentes y solucionados |
| Medición | Sin medición | Medición limitada | Mediciones integrales definidas | Medido y revisado de forma periódica | Criterios de medición revisados periódicamente |
| Informes | Sin informes | Informes limitados | Informes definidos | Informes enviados a la alta dirección y revisados | Requerimientos de informes periódicamente revisados y actualizados |

Adicionalmente se utilizará la metodología utilizada para medir la escala de madurez de seguridad respecto a la norma ISO 27002 proporcionada por "***Jácome, Andrés, Universitat Oberta de Catalunya, En su proyecto Elaboración del plan de implementación de la norma ISO/IEC 27001:2005 en una empresa del sector retail"*** y que es expresada en la figura12 (Anexo F):

| Efectividad (%) | Nivel de Madurez (CMM) | | Descripción |
|---|---|---|---|
| 0% | L0 | Inexistente | -Carencia completa de cualquier proceso.<br>-La empresa no ha reconocido que existe un problema a resolver. |
| Entre 0% y 10% | L1 | Inicial / Ad-hoc | -El éxito de las actividades de los procesos se basa la mayoría de las veces en esfuerzos individuales.<br>-No existen plantillas definidas a nivel corporativo. |
| Entre 10% y 50% | L2 | Reproducible, pero intuitivo | -Los procesos similares se ejecutan en forma similar por diferentes personas con la misma tarea.<br>-Se normalizan las buenas prácticas en base a la experiencia y al método.<br>-No hay comunicación o entrenamiento formal<br>-Las responsabilidades quedan a cargo de cada individuo.<br>-Se depende del grado de conocimiento de cada individuo. |
| Entre 50% y 90% | L3 | Proceso definido | -La organización entera participa en el proceso.<br>-Los procesos están implantados, documentados y comunicados formalmente. |
| Entre 90% y 95% | L4 | Gestionado y medible | -Se cuenta con indicadores y métricas que permiten cuantificar la evolución de los procesos. |
| Mayor a 95% | L5 | Optimizado | -Los procesos están bajo constante mejora.<br>-En base a los indicadores y métricas se determinan las desviaciones más comunes y se optimizan los procesos. |

**Figura 6** Escala de madurez ISO 27002 para la ESPE (sede Matriz)

**Fuente:** Jácome, Andrés , Universitat Oberta de Catalunya.

### 3.3 Evaluación de resultados y discusión

Tras el análisis realizado durante la ejecución del proyecto en la **ESPE (sede Matriz)** de la Metodología Plan de Seguridad Informática podemos identificar los siguientes resultados:

Paso 1 Análisis e identificación de activos en la ESPE (sede Matriz)

Los activos conocidos proporcionados por la UTIC para el desarrollo del presente proyecto se pueden ver en la Tabla 12.

**Tabla 11**

**Inventario de activos ESPE (sede Matriz)**

| ID | ACTIVO IDENTIFICADO | DESCRIPCIÓN | TIPO DE ACTIVO | RESPONSABLE |
|---|---|---|---|---|
| AC001 | Sistema Académico | Sistema Académico -anterior-;contiene datos histórico de estudiantes. | Aplicación | No se define por parte de la UTIC |
| AC002 | Sistema Financiero OLYMI | Sistema Financiero Contable | Aplicación | No se define por parte de la UTIC |
| AC003 | Sistema Recursos Humanc | Sistema de Recursos Humanos SIFRHE; se encuentra en proceso de | Aplicación | No se define por parte de la UTIC |
| AC004 | Portal Web | Portal institucional. | Aplicación | No se define por parte de la UTIC |
| AC005 | Sistema de Educación Virt | Sistema de Educación virtual para modalidad de educación a distancia. | Aplicación | No se define por parte de la UTIC |
| AC006 | Sistema BANNER - ESPE Si | Sistema de matriculas, registro académico, registro y consulta de notas, curriculo académico, administración de planta física (aulas), planificación académica (asignaturas, NRC (paralelos), | Aplicación | No se define por parte de la UTIC |
| AC007 | Sistema BANNER ESPE Sis | Sistemas de Recursos humanos, | Aplicación | No se define por parte de la UTIC |
| AC008 | Sistema BANNER -ESPE Sis | Sistema de digitalización y administración de documentación | Aplicación | No se define por parte de la UTIC |
| AC009 | Sistema BANNER ESPE Sis | Sistema que intraga servicios web, despliegue de información a través de canales, basado en los roles | Aplicación | No se define por parte de la UTIC |
| AC010 | Sistema BANNER ESPE Sis | Sistema que automatiza la secuencia de acciones, actividades | Aplicación | No se define por parte de la UTIC |

Las amenazas identificadas más comunes y que podrían atentar negativamente en contra de la organización se expresa en la Tabla 13.

**Tabla12**

**Inventario de Amenazas ESPE (sede Matriz)**

| ID | AMENAZA | TIPO |
|---|---|---|
| AMZ001 | Manipulación de la configuración (externa) | INTENCIONADOS |
| AMZ002 | Suplantación de la identidad del usuario | |
| AMZ003 | Acceso no autorizado | |
| AMZ004 | Sabotaje (ataque físico y electrónico) | |
| AMZ005 | Abuso de Privilegio de acceso (interno) | |
| AMZ006 | Robo / Hurto (físico) | |
| AMZ007 | Robo / Hurto de información electrónica | |
| AMZ008 | Introducción de falsa información | |
| AMZ009 | Destrucción de información | |
| AMZ010 | Divulgación de información | |
| AMZ011 | Virus / Ejecución no autorizado de programas | |
| AMZ012 | Indisponibilidad del personal | |
| AMZ013 | Violación a derechos de autor | |
| AMZ014 | Incendio | FISICOS |
| AMZ015 | condiciones inadecuadas de temperatura y/o humedad | |
| AMZ016 | Fallos de servicio de comunicación | |
| AMZ017 | Sobrecarga eléctrica | |
| AMZ018 | Falla de corriente (apagones) | |
| AMZ019 | Averías de origen físico o lógico | |
| AMZ020 | Deficiencias en la organización (falta de inducción al personal) | Sucesos derivados de la inexperiencia, negligencia de usuarios/as y decisiones institucionales |
| AMZ021 | Errores de configuración | |
| AMZ022 | Errores de usuario | |
| AMZ023 | Error de administrador | |
| AMZ024 | Error de monitorización (log) | |
| AMZ025 | Divulgación de información | |
| AMZ026 | Manejo inadecuado de datos críticos (codificar, borrar, etc.) | |
| AMZ027 | Errores de mantenimiento actualización del | |

CONTINÚA

| | | |
|---|---|---|
| | programa | |
| AMZ028 | Errores de mantenimiento actualización de los equipos | |
| AMZ029 | Caída del sistema por agotamiento de recursos | |
| AMZ030 | Transmisión de contraseñas por teléfono | |
| AMZ031 | Falta de definición de perfil, privilegios y restricciones del personal (implantación) | |
| AMZ032 | Falta de mantenimiento físico (proceso, repuestos e insumos) | |
| AMZ033 | Falta de actualización de software (proceso y recursos) | |
| AMZ034 | Introducción de información errónea | |
| AMZ035 | Repudio (Interno) | |

Habiéndose definido los activos de información de la institución, el paso siguiente es el análisis de riesgos en base a las amenazas detectadas. La figura siguiente define el resultado del Análisis de riesgo con el mapa de calor.

**Análisis de Riesgo ESPE (Matriz)promedio**

| | | Probabilidad de Amenaza | | |
|---|---|---|---|---|
| | | **Ataques Intencionados** | **Sucesos de origen físico** | **Negligencia y Decisiones Institucionale** |
| **Impacto** | **Datos e Información** | 9,8 | 8,0 | 7,3 |
| | **Sistemas e Infraestructura** | 5,9 | 7,5 | 6,4 |
| | **Personal (acceso a la informacion)** | 6,7 | 5,0 | 7,8 |

**Figura 7** Análisis riesgo impacto amenaza para la ESPE (sede Matriz)

**Fuente**: Los autores del documento

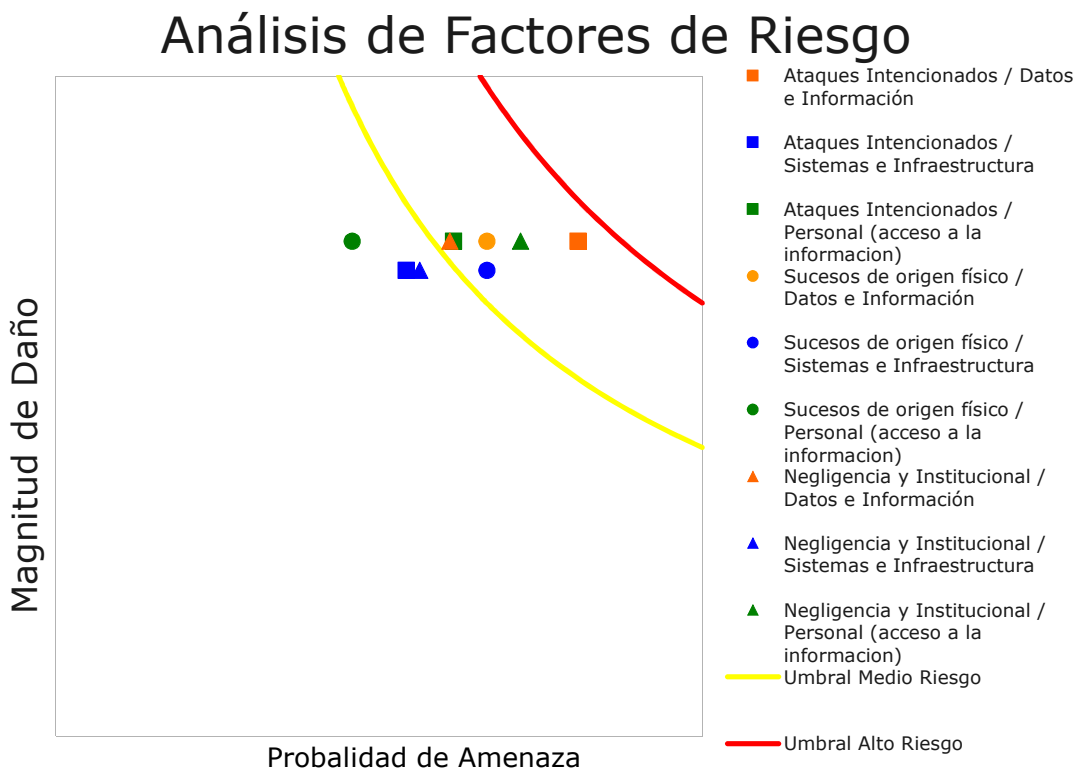


**Figura 8** Análisis de factores de riesgo para la ESPE (sede Matriz)

**Fuente**: Los autores del documento

## Análisis

En el análisis de los resultados de la aplicación de la matriz amenazas vs impacto podemos evidenciar que existen un riesgo de nivel medio en toda la categoría datos e información; riesgo medio en cuanto a la seguridad de la infraestructura suscitado de origen físico e igualmente riesgo medio referente a Personal en referencia a Negligencia y Decisiones Institucionales.

En referencia a las amenazas detectadas como más importantes para la institución tenemos: los ataques intencionados en los datos e información, negligencia institucional y los sucesos de origen físico tanto sobre los datos como sobre la infraestructura.

**Reporte de análisis de controles (ISO 27002) en la ESPE (sede Matriz)**

En cuanto a lo concerniente al análisis de controles definidos en el estándar ISO 27002, tenemos el siguiente análisis porcentual de cumplimiento por cada dominio:

**Tabla 13**
**Estado general de implementación ISO 27001 por dominios de su anexo E**

| # Sección | Nombre | % implementación |
|---|---|---|
| A.5 | Política de Seguridad | 0% |
| A.6 | Aspectos Organizativos de la Seguridad de la Información | 35% |
| A.7 | Gestión de Activos | 42% |
| A.8 | Seguridad Ligada a los Recursos Humanos | 73% |
| A.9 | Seguridad Física y del Entorno | 68% |
| A.10 | Gestión de Comunicaciones y Operaciones | 59% |
| A.11 | Control de Acceso | 59% |
| A.12 | Adquisición,Desarrollo y Mantenimiento de Sistemas de Información | 48% |
| A.13 | Gestión de Incidentes de Seguridad de la Información | 24% |
| A.14 | Gestión de la Continuidad del Negocio | 44% |
| A.15 | Cumplimiento | 63% |
| **TOTAL SGSI** | | **47%** |

De donde se puede concluir que los dominios con meno atención son A5 (Política de Seguridad), A6 (Aspectos Organizativos de la Seguridad de la Información) y A13 (Gestión de Incidentes de la Seguridad de la Información).

La siguientes figuras (15 y 16) indican porcentualmente el nivel de cumplimiento de los controles (agrupados por dominios).

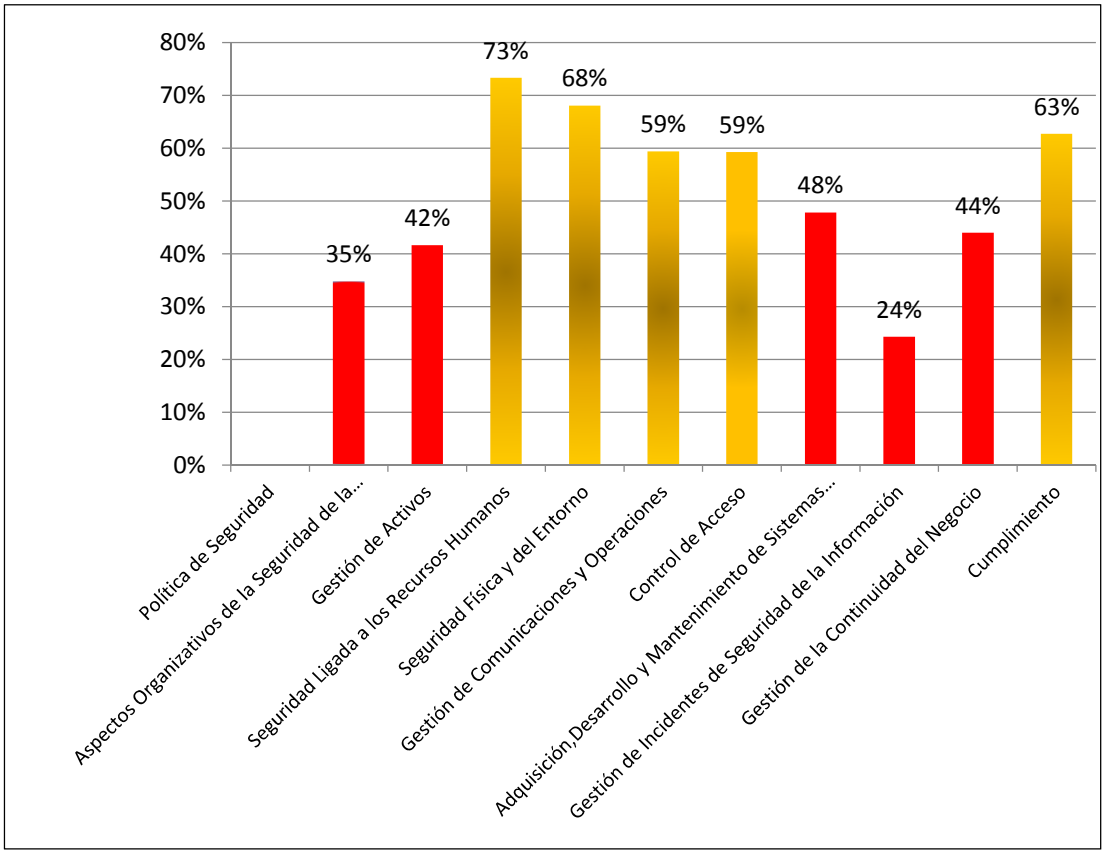


**Figura** 9 Implementación de controles de ISO 27002
**Fuente**: Los autores del documento

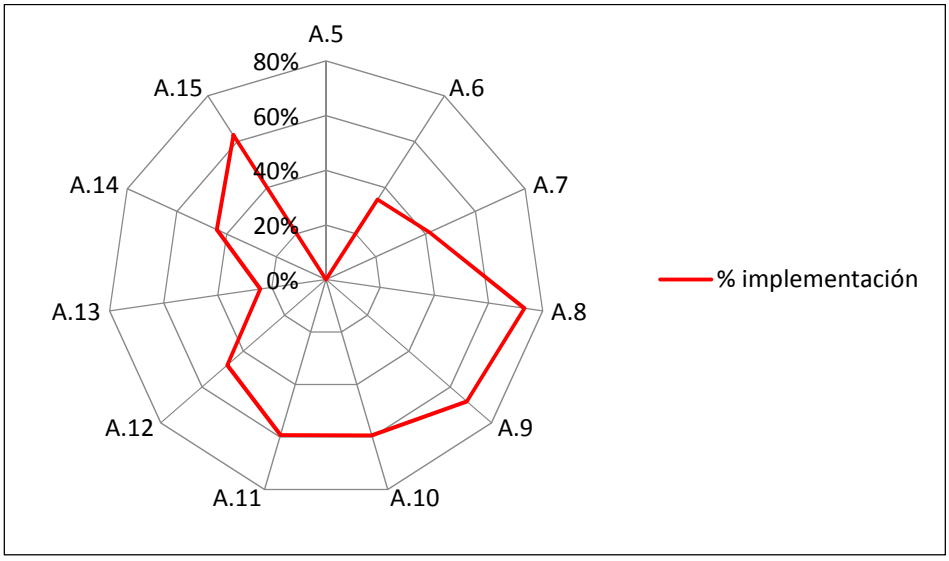


**Figura 10.** Implementación de controles de ISO 27002
**Fuente**: Los autores del documento

**Reporte requerimientos según el estándar ISO 27003 en la ESPE (sede Matriz)**

El estado general de implementación de la Institución de los requerimientos del estándar ISO 27003 referente a seguridad (Anexo E), se pueden hallar en la siguiente tabla.

**Tabla 14**

**Estado general de implementación ISO 27003**

| Norma 27003 | | Evaluación | Calificación /(5) |
|---|---|---|---|
| **A05** | **Obtener Aprobación de la Dirección para la** | 2,0 | 5 |
| **A-06** | **Definición del alcance y política del SGSI** | 3,7 | 5 |
| **A–07** | **Realizar el Análisis de la Organización** | 1,7 | 5 |
| **A-08** | **Realizar la Evaluación del Riesgo y Selección de las Opciones de Tratamiento del Riesgo** | 0,5 | 5 |
| **A-09** | **Modelo de información organizacional** | 3,0 | 5 |

La tabla anterior refleja que los índices de implementación de los requerimientos indicados en el estándar 27003 para implementación de un SGSI.

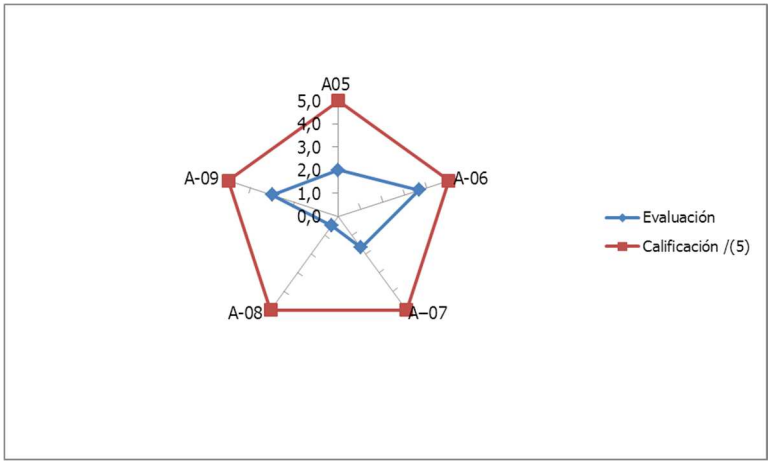


**Figura 11.** Diagrama de Radar de la implementación de controles de ISO 27003

**Fuente**: Los autores del documento

**Reporte de requerimientos según el estándar ISO 27001 en la ESPE (sede Matriz)**

La siguiente tabla muestra el valor porcentual de cumplimiento que la institución tiene en referencia a los dominios y requerimientos indicados en el estándar ISO 27001.

**Tabla 15**

**Estado porcentual de implementación ISO 27001**

| | |
|---|---|
| Implementación de Requisitos Generales ISO 27001 | 13% |

**Nivel de Madurez de la ESPE (sede Matriz) versus requerimientos del ESGSI**

La siguiente tabla muestra el nivel de madurez que la institución tiene en relación a los requerimientos del EGSI, y porcentualmente se refleja en un 47% de cumplimiento.

**Tabla 16**

**Madurez de Seguridad Dominios ISO 27002**

| # Sección | Nombre | Efectividad (%) | Nivel de Madurez | Nivel de Madurez (CMM) |
|---|---|---|---|---|
| A.5 | Política de Seguridad | 0% | 0 | Inexistente |
| A.6 | Aspectos Organizativos de la Seguridad de la Información | 35% | 2 | Inexistente |
| A.7 | Gestión de Activos | 42% | 2 | Inexistente |
| A.8 | Seguridad Ligada a los Recursos Humanos | 73% | 3 | Reproducible, pero intuitivo |
| A.9 | Seguridad Física y del Entorno | 68% | 3 | Reproducible, pero intuitivo |
| A.10 | Gestión de Comunicaciones y Operaciones | 59% | 3 | Reproducible, pero intuitivo |
| A.11 | Control de Acceso | 59% | 2 | Reproducible, pero intuitivo |
| A.12 | Adquisición, Desarrollo y Mantenimiento de Sistemas de Información | 48% | 2 | Proceso definido |
| A.13 | Gestión de Incidentes de Seguridad de la Información | 24% | 2 | Proceso definido |
| A.14 | Gestión de la Continuidad del Negocio | 44% | 1 | Reproducible, pero intuitivo |
| A.15 | Cumplimiento | 63% | 3 | Reproducible, pero intuitivo |
| TOTAL SGSI | | 47% | 2 | Proceso definido |

En las siguientes figuras (18 y 19) se observa el nivel de madurez que tiene la institución referente a los requerimientos del estándar ISO27002, los cuales están en directa relación con el EGSI.

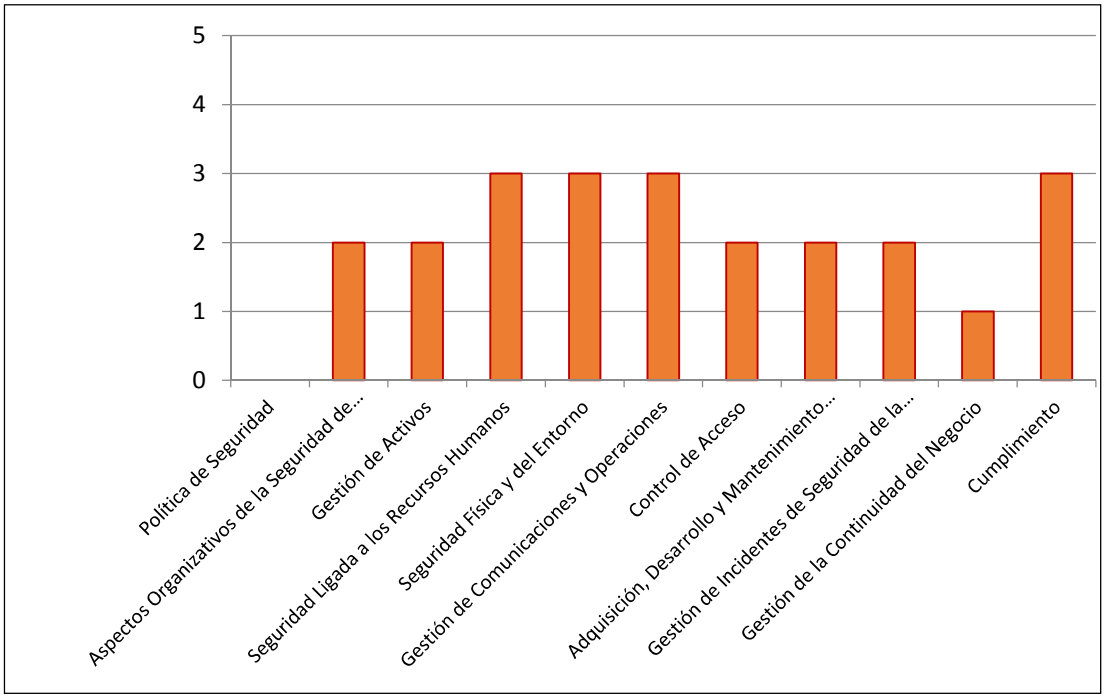


**Figura 12.** Madurez de la Seguridad Dominios ISO 27002 (EGSI)

**Fuente**: Los autores del documento

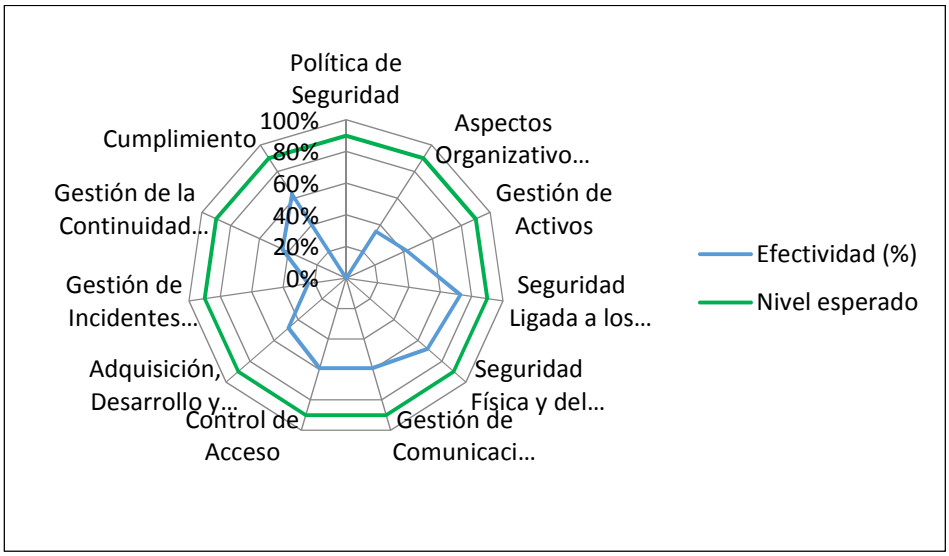


**Figura 13.** Madurez de Seguridad Dominios ISO 27002 (EGSI)

**Fuente**: Los autores del documento

**Metodología para ejecutar la propuesta**

El presente proyecto de tesis basado en el análisis de la situación actual de la institución, y con el sustento teórico de la familia de estándares NTE ISO IEC 27000 y la normativa legal vigente (EGSI), como resultado final, propone el Plan de Seguridad de la Información para la Universidad de las Fuerzas Armadas (sede Matriz) (Anexo H)

# CAPÍTULO 4

## 4.1 Conclusiones

La situación actual de la ESPE en su sede Matriz, referente a Seguridad de la información evidencia que existen procesos que no han sido debidamente formalizados, lo cual revela la urgencia con que el tema de seguridad debería ser implementando en rangos aceptables en la institución.

La investigación del presente trabajo evidencia que aspectos tácitos a la Seguridad de la información tales como: Gestión de Riesgos, gestión de Activos, Políticas de seguridad, etc., no están desarrollados en niveles aceptables, lo cual deja en claro la necesidad urgente de la implementación de lineamientos que brinden niveles de seguridad aceptables sobre la información que maneja la universidad.

Un aspecto básico de seguridad de las instituciones públicas es el cumplimiento de la normativa legal vigente (para este caso, el EGSI, Acuerdo 166), y la investigación ha evidenciado que faltan puntos por cubrir de los lineamientos de dicha norma, por tanto es necesario que la institución genere un plan de implementación de dicho acuerdo.

## 4.2 Recomendaciones

Seguir los lineamientos establecidos en el Plan de Seguridad de la Información expresado como Anexo I del presente documento; dicho documento propone metodología tanto para la gestión, análisis y clasificación de activos, así como para la gestión de Riesgos.

Se recomienda la implementación y alineamiento de los procesos institucionales a buenas prácticas internacionalmente aceptadas de seguridad, específicamente hablamos de la familia de ISOS 27000; así mismo, se recomiendo cumplimiento a la normativa legal vigente en relación a temas de seguridad, específicamente se hace referencia al Esquema Gubernamental de Seguridad de la Información, EGSI.

Se recomienda crear un comité de seguridad en la institución que formalice las políticas de seguridad trasversalmente a toda la institución y que revise, verifique, valide, mejore y socialice las políticas de seguridad de la institución.

**BIBLIOGRAFÍA**

ALIAGA FLORES, Luis Carlos 2013 Diseño de un sistema de gestión de seguridad de información para un instituto educativo Tesis para optar por el título de Ingeniero Informático. Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería.
http://tesis.pucp.edu.pe/repositorio/handle/123456789/933

AMPUERO CHANG, Carlos Enrique
2011 Diseño de un sistema de gestión de seguridad de información para una compañía de seguros. Tesis para optar por el título de Ingeniero Informático. Lima: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería. Consulta: 15 de abril del 2014. http://tesis.pucp.edu.pe/repositorio/handle/123456789/933

ALEXANDER SERVAT, Alberto
2007 Diseño de un sistema de gestión de seguridad de información. Óptica ISO 27001:2005. Primera edición. México: Alfaomega Grupo Editor.

CANO, Jeimy
2011 “El Debido Cuidado en Seguridad de Información. Un Ejercicio de Virtudes para el Responsable de la Seguridad de Información.”. ISACA Journal. 2011, Volumen 2, pp. 1-8.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
2002 ISO/IEC Guide 73:2002 Risk management -- Vocabulary -- Guidelines for use in standards. EEUU.
2004a ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management. EEUU.

2004b ISO/IEC TR 18044:2004 Information technology -- Security techniques -- Information security incident management.EEUU.

2005a ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements.EEUU.

2005b ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management.EEUU.

2010 ISO/IEC 27003:2010 Information technology - Security techniques - Information security management systems implementation guidance.EEUU.86

2008 ISO/IEC 27005:2008 Information technology - Security techniques - Information security risk management.EEUU.

IT GOVERNANCE INSTITUTE

2012 *COBIT 5.* Illinois, USA.

2012 *COBIT 5. Information Securty* Illinois, USA.

JÁCOME LOBO, Andrés Augusto

2014 Elaboración del plan de implementación de la norma ISO/IEC 27001:2005 en una empresa del sector reail. Bogota: Tesis para optar por el título de Máster Universitat Oberta de Catalunya Consulta: 25 de Agosto del 2014. http://openaccess.uoc.edu/webapps/o2/handle/10609/35821


ESPE
UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**VICERRECTORADO DE INVESTIGACIÓN, Y VINCULACIÓN CON LA COLECTIVIDAD**

**MAESTRIA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS**

**VII PROMOCIÓN**

**TESIS DE GRADO MAESTRÍA EN EVALUACIÓN Y AUDITORÍA DE SISTEMAS TECNOLÓGICOS**

# ANEXO:
# PLAN DE SEGURIDAD DE LA INFORMACIÓN DE LA ESPE (SEDE MATRIZ)

**AUTORES: SALGADO CORRALES, RAFAEL LEONIDAS**
**TAPIA YEROVI, SANTIAGO XAVIER**

**DIRECTOR: ECO.CHIRIBOGA, GABRIEL MSc.**

**SANGOLQUÍ, MAYO DEL 2015**

# PLAN DE SEGURIDAD INFORMACIÓN PARA LA ESPE - MATRIZ

## 1. Antecedentes

El presente documento es el resultado del análisis de la situación actual en el tema de seguridad a la Universidad de las Fuerzas Armadas (sede Matriz), en base a lo cual se establece el presente Plan de Seguridad de la Información.

## 2. Objetivo

Generar el Plan de Seguridad de la Información para La Universidad de las Fuerzas Armadas (sede Matriz) basado buenas prácticas respaldadas en estándares de seguridad internacionalmente aceptados y que a su vez cumplan los requerimientos definidos en la normativa legal gubernamental vigente EGSI (2009, SNAP); y de ésta manera poder fomentar una cultura de seguridad robusta en la institución, asegurando de esta manera los atributos mínimos que la información custodiada por la institución debería tener: integridad, disponibilidad y confidencialidad.

## 3. Alcance

El presente Plan de Seguridad de la Información se enfoca en la protección de la información custodiada y/o generada por la Universidad de las Fuerzas Armadas (sede Matriz) basado en los requerimientos definidos en el Acuerdo 166 de la SNAP (EGSI), es decir los controles establecidos en la norma NTE ISO/IEC 27002:2005 (INEN, 2005) y se aplica a todos los miembros de la comunidad universitaria: personal administrativo y docente, alumnado en modalidad pre y post grado y terceros en general que brinden servicios o interactúen de alguna manera con la institución.

Se aclara que el presente documento, es un documento de recomendación, obtenido tras análisis de la situación actual de la institución en base a documentación suministrada y debe estar sujeto al análisis tanto del Director de TI de la institución, como demás personal directivo que tenga injerencia sobre el tema de seguridad en la institución; y será perfectible de acuerdo a la realidad y requerimientos institucionales.

## 4. Política de Seguridad

A continuación se muestra el desarrollo del documento del Plan de Seguridad de las Información para la Universidad de las Fuerzas Armadas (sede Matriz), el cual se ha basado en el análisis de la situación actual de la institución en base a la información

suministrada por el personal encargado y su relación con la normativa legal vigente de cumplimiento obligatorio. (ISO, NTE IEC ISO27002:2005, 2005)

## 4.1. Política de Seguridad de la Información

### *4.1.1. Documento de política de seguridad de la información.*

El tema de Seguridad de la Información requiere el apoyo de la alta dirección de la institución para su implementación en la institución, por tal motivo, el documento de políticas de seguridad de la información deberá en primera instancia ser aprobado por la máxima autoridad de la Universidad de las Fuerzas Armadas (sede Matriz), formalizando el compromiso de apoyo de dicha autoridad con el tema de aseguramiento de la seguridad de la información en la institución y poder de ésta manera lograr difusión del mismo.

El documento de las políticas de la Seguridad deberá contener la siguiente información:

- Topar como tal el tema de seguridad de información y la relevancia del mismo para la institución.
- Explicación a detalle de las políticas, principios, normas y requisitos de cumplimiento en materia de seguridad.
- Los roles, responsabilidades y alcance asignados a cada área para poder gestionar la seguridad de la información de la institución.
- Referencias a documentos técnicos especializados, normativa legal, estándares, etc., que puedan respaldar la política propuesta.

Adicionalmente la mencionada política deberá ser difundida formalmente entre el personal de la institución, para esto, deberá contactarse mediante oficios o documentación similar a los líderes de cada área, quienes deberán difundir la política entre sus subalternos. (ISO, NTE IEC ISO27002:2005, 2005)

### *4.1.2. Revisión de la política de seguridad de la información.*

La política de seguridad es un documento que debe ir modificándose, de acuerdo a la influencia de diversos cambios externos: normativa gubernamental

de cumplimiento, hallazgos y/o avances en temas de Seguridad de la información, cambios en requerimientos internos sobre seguridad en la institución, cambios en la tecnología, etc., por este motivo, se sugiere que la política de seguridad debe revisarse en periodos comprendidos de 4 a 6 meses por un comité de seguridad para la revisión de la política. En ducha revisión se deberán considerar, la eficacia de dicha política, revisando la efectividad de los controles en función de los riesgos en seguridad a los que hace frente la institución. (ISO, NTE IEC ISO27002:2005, 2005)

## 4.2. Aspectos Organizativos para la seguridad de la información

### *4.2.1. Organización Interna*

#### *4.2.1.1. Compromiso de la Dirección con la Seguridad de la Información*

Como se ha mencionado previamente, para lograr efectividad en el proceso de implementación de Seguridad de la Información en la institución es necesario que la Alta Dirección de la Universidad de las Fuerzas Armadas (sede Matriz), formalice el apoyo a la gestión del plan de seguridad, comprometiendo los recursos que fueran necesarios para lograr difundir e implementar la cultura en seguridad de la información en la institución, por tal motivo es necesario involucrar a la alta dirección en la gestión de la seguridad de la información, mostrándole los beneficios, así como los riesgos a los que la organización estaría expuesta al no contar con un plan robusto de Seguridad de la Información. (ISO, NTE IEC ISO27002:2005, 2005)

#### *4.2.1.2. Coordinación de la Seguridad de la Información*

Ejecutar el plan de seguridad requiere acciones coordinadas entre los diversos actores inmersos en el proceso de Seguridad de la institución, por tal motivo es necesario que se definan claramente roles y responsabilidades en el proceso de la seguridad, así como el ámbito de acción que tendrán los implicados junto a un plan de acción que defina claramente las acciones a seguir en caso de la aparición de incidentes de Seguridad. (ISO, NTE IEC ISO27002:2005, 2005)

*4.2.1.3. Asignación de responsabilidades relativas a la seguridad de la información*

El plan de seguridad debe definir con claridad los roles y responsabilidades de cada actor tiene dentro el ámbito de la seguridad de la institución, por tal motivo es necesario que se definan los actores junto con sus acciones que los mismos realizarán, el alcance de dichas acciones así como los límites de la misma y el personal a cargo que ésta persona dispondrá para cumplir sus tareas de seguridad.

Los actores principales son el Director de Tecnologías de la Información y un responsable directo de la seguridad que es un oficial de Seguridad, quienes serán los encargados de conformar el grupo de acción, definiendo competencias a sus subalternos gestores en conjunto de salvaguardar la información de la institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.2.1.4. Proceso de autorización de recursos para el procesado de la información*

Procesar la información implica riesgos directos sobre los atributos de la información que maneja la institución (en su sede Matriz): integridad, disponibilidad y confidencialidad; por tal motivo es necesario que se analice si una actividad atentara significativamente sobre los atributos de la información previamente mencionados; es por tanto necesario que se realice trabajo conjunto del Director de Tecnología (junto a sus subalternos), Director de Seguridad de la Información y Directores de las Áreas en las cuales dicho procesamiento de información podría causar impacto y, analizar cuidadosamente, el impacto que dicho proceso causaría sobre la información, así como responsabilidades directas los autores de dicho procesamiento, y solamente si este proceso de análisis no implica consecuencias directas sobre la información, dar el visto bueno a este procesamiento; en otras palabras, la comisión a formarse, definirá si se realiza o no una acción que pueda desencadenar en eventos de seguridad sobre la información que la institución maneja. (ISO, NTE IEC ISO27002:2005, 2005)

*4.2.1.5. Acuerdos de confidencialidad*

Hay que considerar que la información que maneja la institución, puede categorizarse en niveles de sensibilidad, pudiendo ser: de libre acceso a terceros

en general, de acceso solamente a personeros de la institución (y potencialmente a terceros, por ejemplo, personal tercerizado) y acceso restringido únicamente a la alta dirección y dicho acceso debe ser controlado mediante acuerdos de confidencialidad que permitan:

Delimitar el tipo de acceso, tiempo por el cual se brindará acceso y a qué tipo de información una persona (propia o ajena a la organización) podría tener acceso, por tanto se deberán definir acciones y procesos de cierre de acceso a información. Se deberán incluir cláusulas de confidencialidad y/o de uso de la información, así como las acciones legales que se llevaran en caso del incumplimiento de estos lineamientos. (ISO, NTE IEC ISO27002:2005, 2005)

*4.2.1.6. Contacto con las autoridades*

Podrían existir casos en los que incidentes de seguridad, -por la gravedad de los mismos- los resultados finales en contra de la información de la institución, podría trascender los límites de acción institucional y es donde se ve necesario la intervención de autoridades externas que permitan solventar dichos eventos; usualmente este tipo de incidentes son producto de intervenciones externas que han logrado superar fuertemente los controles establecidos, por ejemplo: atentados por parte de grupos armados especializados, desastres naturales de gran magnitud, condiciones adversas políticas que atenten contra la seguridad nacional, etc., donde como se ha mencionado, la solución a dichos incidentes sobrepasa el ámbito de acción de las autoridades de la institución, y es en este escenario donde la Universidad de las Fuerzas Armadas debería solicitar apoyo a entidades externas para lograr solventar los problemas ocurridos, por ejemplo: Policía Nacional, Grupos élite apara eventos nefastos (GAO, GOE, GEMA, etc.), Cruz Roja, etc.; por tal motivo es responsabilidad del Comité de seguridad, crear protocolos claros a seguirse en caso de ocurrir estos eventos de gravedad alta y definir exactamente el alcance y el tipo de autoridad a la que se contactará en caso de emergencia de Seguridad en la Universidad de las Fuerzas Armadas. (ISO, NTE IEC ISO27002:2005, 2005)

*4.2.1.7. Contacto con grupos de interés*

Un aspecto fundamental que se debe manejar en la gestión de la seguridad es el contacto que la institución debe mantener con entes externos que permitan ampliar la base de conocimientos del personal en temas de seguridad, por tanto es necesario que la Universidad de las Fuerzas Armadas aparte de contar con un experto en seguridad que lidere el tema de Seguridad de la Información en la institución, se mantenga contacto con grupos especializados en el tema de seguridad que permitan evidenciar las falencias que los controles implementados tienen, esto podría conseguirse con acuerdos con entes externos que realicen pruebas controlados de: Hacking Ético, pruebas de penetración, pruebas de stress sobre los sistemas/infraestructura tecnológica de la institución; adicionalmente es necesario que la capacitación en el tema de seguridad sea continua al personal que confronta el día a día temas de seguridad en la institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.2.1.8. Revisión independiente de la Seguridad de la Información*

Como se mencionó en el punto anterior, es necesario que entes externos validen los procesos de seguridad que se llevan en la Universidad de las Fuerzas Armadas, esto con el fin de detectar la validez de los controles implementados y la efectividad en el proceso en sí de gestión de la Seguridad; dicha entidad emitirá un informe, el cual debe ser analizado por: la alta dirección, el comité de seguridad, el Director de TI y líderes de diversas áreas de la institución (pues la seguridad debe ser transversal a la organización). Dicha evaluación realizada por entes externos deberá realizarse una vez por año y dependiendo de los resultados obtenidos el comité de Seguridad tomará las acciones necesarias de remediación. (ISO, NTE IEC ISO27002:2005, 2005)

*4.2.2. Terceros*

*4.2.2.1. Identificación de los riesgos derivados del acceso a terceros*

Considerando que la Universidad de las Fuerzas Armadas (sede Matriz), posee dos tipos de usuarios identificados: Usuarios internos (personal docente, administrativo, alumnos de pre y post grado) y Usuarios Externos (personas en

general que sin tener credenciales de acceso a los sistemas, pueden hacerlo libremente a la red de internet institucional como a la infraestructura física de la misma), y es en este escenario, donde el personal de Seguridad de la Información debería medir los riesgos inherentes relacionados con el segundo grupo de usuarios indicado y con ello poder implementar los controles y procedimientos de seguridad que reduzcan posibles afectaciones a la infraestructura de la institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.2.2.2. Tratamiento de la seguridad con relación a los clientes*

Un cliente se define como un individuo que requiere que la institución le suministre información con el fin de realizar alguna acción; un caso ejemplo es un individuo que requiere información para matricularse en la universidad por primera vez y es donde el personal que tiene contacto con el cliente, estrictamente deberá suministrar información sin sobrepasar la brecha de seguridad que este contacto implica; por tanto el comité de seguridad y demás partes interesadas deberán delimitar este umbral de entrega de información que un cliente no puede sobrepasar afectando de esta manera la seguridad de la información institucional. (ISO, NTE IEC ISO27002:2005, 2005)

*4.2.2.3. Tratamiento de la seguridad en contratos con terceros*

Siempre que la institución firme contratos con terceros deberá incluir: acuerdos sobre confidencialidad y uso adecuado de la información; niveles de disponibilidad aceptables en el contexto de la realidad institucional; apartado legal donde se indiquen los requerimientos legales así las sanciones en caso de incumplimiento por parte del proveedor por la institución y que desemboque en afectación a la seguridad de la información. (ISO, NTE IEC ISO27002:2005, 2005)

## 4.3. Gestión de activos

*4.3.1. Responsabilidad sobre los activos.*

*4.3.1.1. Inventario de activos.*

Un proceso coherente de inventario de activos sigue los siguientes pasos sugeridos:

**Identificación de Activos**

Describe e identifica los principales activos de información que posee la ESPE (sede Matriz) que se hallan involucrados en el procesamiento de la información que la institución maneja. Considérese a un activo de información para el plan de Seguridad de la Información a: Hardware, Software, Recurso Humano, datos, etc. (ISO, NTE IEC ISO27002:2005, 2005)

**Recolección de información**

El proceso de recolección de la información de activos puede realizarse con un instrumento que cubra la siguiente estructura sugerida:

**ID:** Etiquetado del Activo. Ejemplo: ACT_01.

**ACTIVO IDENTIFICADO:** Nombre del Activo identificado. Ejemplo: Sistema Financiero OLYMPO.

**TIPO DE ACTIVO:** La identificación de los activos está basado en la norma ecuatoriana NTE ISO/IEC 27005:2008, donde se identifican dos tipos de activos: primarios y de soporte.

Los primarios, según este estándar, son los procesos e información más sensibles para la organización.

Los activos de soporte, son los activos que dan el debido soporte a estos activos primarios. Dentro de estas dos agrupaciones, se definieron siete distintos tipos específicos de activos:

- **Dato:** Es toda aquella información que se genera, envía, recibe y gestionan dentro de la organización. Dentro de este tipo, podemos encontrar distintos documentos que la institución educativa gestiona dentro de sus procesos.

- **Aplicación:** Todo aquel software que se utilice como soporte en los procesos.
- **Personal:** Son todos los actores que se ven involucrados en el acceso y el manejo de una u otra manera a los activos de información de la organización.
- **Servicio:** Son los servicios que alguna área de la organización suministra a otra área o entidades externas a la misma.
- **Tecnología:** Es todo el hardware donde se maneje la información y las comunicaciones.
- **Instalación:** Es cualquier lugar donde se alojan los activos de información. Este lugar o ambiente puede estar ubicado dentro de la organización tanto como fuera de la misma.

  **Equipamiento auxiliar:** Son los activos que no se hallan definidos en ninguno de los anteriores tipos.

**DESCRIPCIÓN:** Brinda una ligera descripción del activo. Ejemplo: Sistema Financiero Contable.
**RESPONSABLE:** Detalla el (o los) responsables del activo. Ejemplo: Ing. Carlos Córdova. (ISO, Norma Técnica Ecuatoriana para gestión de la Seguridad. Riesgos, 2008)

**Políticas de clasificación de Activos**

Al definir políticas de clasificación de activos estamos en capacidad de identificar a un activo de acuerdo a condiciones propias de prioridad institucional, apuntando al aseguramiento de los criterios de la información: confidencialidad, integridad y disponibilidad como se muestra a continuación:

## Tabla 1

### Clasificación de Activos

| Nivel | Confidencialidad | Integridad | Disponibilidad |
|---|---|---|---|
| 1 | No existen restricciones de confidencialidad, ésta información puede ser usado sin autorización expresa de la institución por cualquier individuo. | Si se borrara y/o modificara la información puede ser fácilmente recuperada. | Si se perdiera el acceso a dicha información, esto no afecta la operación del negocio. |
| 2 | Información conocida por los servidores y funcionarios de la organización. | Si se borrara y/o modificara la información puede ser recuperada, pero ocasionaría perdidas leves tanto en la institución o terceros. | Si se perdiera el acceso a dicha información por un periodo de tiempo mayor o igual a un mes, esto podría ocasionar pérdidas significativas para la institución o para terceros. |
| 3 | Información conocida solamente por un grupo de servidores o funcionarios de la organización. | Si se borrara y/o modificara la información puede ser de difícil recuperación , pero ocasionaría pérdidas significativas en la institución o terceros. | Si se perdiera permanentemente el acceso a dicha información por un periodo de tiempo igual a una semana, esto podría ocasionar pérdidas significativas para la institución o para terceros. |

CONTINÚA

| | | | |
|---|---|---|---|
| 4 | Información conocida solamente por un grupo reducido de servidores o funcionarios de la organización (usualmente de la alta dirección). | Si se borrara y/o modificara la información, no se podría recuperar, pero ocasionaría perdidas graves en la institución o terceros. | Si se perdiera permanentemente el acceso a dicha información por un periodo de tiempo igual a un día, esto podría ocasionar pérdidas significativas para la institución o para terceros. |

**Identificación y Clasificación de activos**

Cuando se han definido claramente los objetivos junto a las tareas parte de la gestión de los activos de información, se debe identificar y clasificar los mismos siguiendo los siguientes pasos:

- Identificación: Halla los procesos críticos dentro de la organización, en base a la cadena de la valor organizacional (supervisado por la alta Dirección). Inicia con el inventario tecnológico de la organización.
- Pre clasificación: Realiza un proceso de pre clasificación de activos basado en los atributos de la información: Confidencialidad, Disponibilidad e Integridad. Define los propietarios de la información y el resultado de esta etapa es un inventario de activos pre clasificados:

**Tabla 2**

**Identificación de Activos**

| Entregable/ Insumo | Tipo | Frecuencia Generación | Confidencialidad | Integridad | Disponibilidad |
|---|---|---|---|---|---|
| Plan de supervisión | Entregable | Trimestral | 3 | 3 | 3 |

Posteriormente, la información debe ser caracterizada, considerando los siguientes aspectos: tipo de información, medio de propagación o soporte, y el tipo de almacenamiento:

**Tabla 3**

**Caracterización de Activos por tipo de información**

| Tipo de Información | | |
|---|---|---|
| Impreso | Digital / Aplicativo | Digital PC |
| 0 | 1 | 1 |

**Tabla4**

**Caracterización de Activos por medio de propagación**

| Medio de propagación o soporte | | | | |
|---|---|---|---|---|
| Red de Datos | Correo | Correo electrónico | Impreso | Unidades extraíbles |
| 1 | 0 | 1 | 0 | 1 |

**Tabla 5**

**Caracterización de Activos por tipo de almacenamiento**

| Tipo de Almacenamiento | | |
|---|---|---|
| Servidores | Archivos | PC |
| 0 | 1 | 1 |

Una vez que se ha realizado el proceso de caracterización, se cuenta la con siguiente información: tipo de información, medio de propagación de la misma, detalles de su almacenamiento; si es de tipo físico o electrónica -o ambas-, y los riesgos a los que la misma se enfrenta.

- Análisis de riesgos: Realiza una identificación y evaluación del riesgo; se hacen ponderaciones del valor del riesgo y la clasificación de activos se realiza basado en el riesgo del activo de información.
- Estrategias de protección: Parte de una Matriz de Clasificación de activos; se debe definir un plan de acción para mitigación de los riesgos hallados que atentan sobre los activos.

*4.3.1.2. Responsable de los activos.*

Al ser los activos de información recursos de alto valor para la organización, los mismos deben tener un propietario, es decir un custodio que tiene la responsabilidad sobre el adecuado tratamiento del activo, y en caso de

que surgieran problemas de seguridad con un activo, es precisamente el propietario de dicho activo quien tendrá la responsabilidad directa. (ISO, NTE IEC ISO27002:2005, 2005)

*4.3.1.3. Acuerdos sobre el uso aceptable de los activos.*

Tras identificar un activo, medir su susceptibilidad, categorizarlo, y ponerlo bajo responsabilidad de un custodio, el Director de TI junto al Director de Seguridad, deberán definir los lineamientos obligatorios sobre el buen uso de un activo de información, los cuales deberán estar alineados asegurar: confidencialidad, integridad y disponibilidad de la información. (ISO, NTE IEC ISO27002:2005, 2005)

*4.4.2. Clasificación de la información*

*4.4.2.1. Directrices de clasificación.*

Para poder clasificar la información, debe primero ser categorizada de acuerdo a la importancia de la misma; para esto de usará un criterio basado en las siguientes preguntas: ¿qué tan susceptible es la información? y ¿la información puede ser divulgada?; al responder la primera pregunta sabremos la relevancia de la información desde la perspectiva institucional y de ésta manera podremos responder a la segunda pregunta teniendo claro el riesgo que podría correr la institución si la información susceptible se difunde; claro, existen niveles de susceptibilidad y divulgación que deberán ser definidos por cada líder de área que maneje información en la institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.4.2.2. Etiquetado y manipulado de la información.*

La información puede ser de dos tipos: digital y física y cada una tiene diferente tratamiento:

**Información en formato digital**

Este tipo de información necesariamente estará contenida en algún medio de tipo magnético: CD, DVD, Discos duros (entiéndase: archivos, correo

electrónico, bases de datos, etc.), memorias extraíbles, etc. por lo cual la principal medida que el custodio de dicha información deberá realizar es una prolija gestión de contraseñas tanto en equipos personales de cómputo como en archivos que contengan información susceptible; y, de ser el caso que la información este contenida en medios magnéticos extraíbles, restrínjase el acceso a dichos medios extraíbles a personal ajeno a las dependencias, almacenando los mismos en gavetas o cajones con la debida protección física. El etiquetado de la información deberá seguir un protocolo que defina en el nombre del archivo o medio magnético, siglas, iniciales o acrónimos que indiquen la prioridad, relevancia, susceptibilidad y características de divulgación de la misma.

**Información en formato físico**

Este tipo de información deberá seguir un proceso de etiquetado similar al usado en los medios magnéticos: siglas, iniciales o acrónimos que indiquen la prioridad, relevancia, susceptibilidad y características de divulgación de la misma; adicionalmente se pueden emplear carpetas o folders que por los colores usados pueda diferenciar la información, por áreas, prioridad, importancia, etc. Finalmente el almacenado de la información física debe realizarse usando los protocolos de almacenaje con los que cuenta la universidad en la actualidad, es decir, usando la infraestructura propia de archivo, y las ventajas que la misma brinda por ejemplo, buenas condiciones climáticas de almacenaje de la documentación, seguridad de acceso, etc.

## 4.4. Seguridad ligada a los recursos humanos

### *4.4.1. Antes del Empleo*

#### *4.4.1.1. Funciones y responsabilidades.*

La seguridad es un tema que debe estar considerado y/o gestionado por el Director de Talento Humano de la Universidad de las Fuerzas Armadas (sede Matriz), por tanto junto a los líderes de cada área y el Director de Seguridad, debe definir claramente tanto las funciones como las responsabilidades de cada

puesto de trabajo y en base a ese perfil definir los riesgos inherentes y el alcance en la acción de cada puesto y con ello poder definir controles que minimicen las amenazas propias de cada puesto. (ISO, NTE IEC ISO27002:2005, 2005)

*4.4.1.2. Investigación de antecedentes.*

Es labor del Director de Talento Humano de la Universidad de las Fuerzas Armadas, previo al proceso de contratación de un nuevo empleado investigar los antecedentes tanto laborales como penales de dicha persona. (ISO, NTE IEC ISO27002:2005, 2005)

*4.4.1.3 Términos y condiciones de contratación.*

Es necesario que el proceso de contratación especifique cláusulas propias de Seguridad de la Información tanto para usuarios internos como para procesos externalizados de servicios, por tal motivo, es necesario que se incluya: condiciones y restricciones del uso de la información, cláusulas de confidencialidad, el alcance, responsabilidad y atribuciones de un cargo, acciones punitivas en caso de infringir los lineamientos de seguridad, condiciones de término de contrato, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.4.2. Durante el empleo.*

*4.4.2.1. Supervisión de las obligaciones.*

Para gestionar el proceso de supervisión de obligaciones tanto de usuarios internos como de entes externos que provean servicios a la institución, en primera instancia se deberá socializar los lineamientos referentes a seguridad de la información de la institución, es decir, se debe asegurar que cada rol tanto interno como externo a la institución tengan pleno conocimiento de las acciones en pro de gestionar seguridad que la institución plantea; posteriormente, se deberá realizar control estricto de las obligaciones, condiciones y restricciones (considerando el ámbito de acción de cada rol) mediante procesos bien definidos de auditoria, que evidencien el cumplimiento de las normas de seguridad de la información para cada ente que de una u otra manera tenga control sobre la información generada en la institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.4.2.2 Formación y capacitación en seguridad de la información.*

La seguridad de la Información es un proceso que debe llevarse continuamente en la institución, evaluando periódicamente la efectividad de los procesos que aseguren el cumplimiento de los objetivos de Seguridad en la institución y una estrategia para lograrlo es la formación continua en temas de seguridad de la información, con campañas masivas y recurrentes que tengan como objetivo el socializar, fomentar y concienciar sobre aspectos de seguridad de la información; adicionalmente, la capacitación continua tanto a los usuarios que están directamente ligados al tema tecnológico como a los usuarios que hacen uso de dicha tecnología, debe establecerse como un objetivo institucional y lograr con ello lograr una robusta cultura organizacional referente a temas de seguridad. (ISO, NTE IEC ISO27002:2005, 2005)

*4.4.2.3 Procedimiento disciplinario.*

Para implementar una efectiva cultura organizacional en el tema de seguridad en la institución (sede Matriz), es importante definir las acciones punitivas que se han de aplicar a quien infrinja los lineamientos en temas de seguridad, es por esto que la política de seguridad de la institución, debe contemplar las sanciones que se llevarán a cabo en contra de quienes incurran en acciones que atenten las normas de seguridad de la información; es importante por tanto, definir el procedimiento disciplinario a emplearse considerándose los diversos tipos de actores, por un lado los usuarios internos (personal administrativo, docente, alumnado) y usuarios externos (entes que brinden servicios a la institución o personas en general que tengan acceso a la infraestructura física y lógica de la organizacional). (ISO, NTE IEC ISO27002:2005, 2005)

*4.4.3. Cese del empleo o cambio del puesto de trabajo.*

*4.4.3.1. Cese de responsabilidades.*

El proceso de cese de responsabilidades debe manejarse entre: la Dirección de Talento Humano, Direcciones administrativas y el Departamento

de TI y de manera conjunta establecer un protocolo para el cese de actividad y/o responsabilidades de un actor en el entorno institucional (tanto usuarios internos como terceros que proporcionen algún tipo de servicio o interactúen con la información propiedad de la institución). Este proceso debe ser coordinado entre las diversas unidades que generan el requerimiento de cese o cambio de responsabilidades junto con el Director de TI, para que este último gestione las acciones respectivas, por ejemplo: gestión de cuentas de usuario y contraseñas, roles y alcance de un puesto, permisos de acceso físico a diversos estamentos en la institución, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.4.3.2. Devolución de activos.*

Un proceso adecuado de cese de actividades o cambio de puesto, debe contemplar la gestión de devolución de activos, misma que permita llevar un rastro exacto de la responsabilidad de un actor sobre activos y que al momento del cese de funciones o cambio de puesto, los activos a cargo sean devueltos a la institución, y se pongan en resguardo de otra persona encargada; este proceso debe controlar el estado del activo tanto al momento de recepción del mismo como al momento de entrega, y estar en la capacidad de sancionar si el activo adecuado al momento de la entrega evidencia que no ha sido mantenido con responsabilidad y se evidencie que el estado del mismo deliberadamente ha sido dañado o se ha limitado la funcionalidad del mismo debido a mala gestión del encargado. (ISO, NTE IEC ISO27002:2005, 2005)

*4.4.3.3. Cancelación de permisos de acceso.*

Al momento de realizar el proceso de cese del empleo o cambio del puesto de trabajo, se deben generar políticas de desvinculación o cese, con lo cual se asegure el retiro total o parcial –de ser el caso- de: atribuciones, permisos de acceso lógico, tarjetas de identificación y permiso de acceso físico a instalaciones de la institución. (ISO, NTE IEC ISO27002:2005, 2005)

## 4.5. Seguridad física y del entorno

### *4.5.1. Áreas seguras.*

#### *4.5.1.1. Perímetro de seguridad física.*

De manera conjunta entre los encargados de: Seguridad, Riesgos, Tecnología y Unidades Administrativas de la Universidad de las Fuerzas Armadas (sede Matriz), se deberán definir las áreas que potencialmente pueden estar sujetas a amenazas, ésta definición se realizará en función a los procesos que se realicen en dichas áreas, los activos que estén contenidos en dichas áreas, el procesamiento de información que se realice en las mismas, etc.; adicionalmente, debe considerarse la sensibilidad de dichas áreas ante atentados físicos. (ISO, NTE IEC ISO27002:2005, 2005)

#### *4.5.1.2. Controles físicos de entrada.*

Una vez que se han definido las áreas susceptibles en la infraestructura física de la Universidad de las Fuerzas Armadas (sede Matriz), se deben implementar los controles físicos necesarios de acceso a las mismas: Controles electrónicos de acceso en ingresos mediante: tarjetas electrónicas, sistemas biométricos, guardias armados, sistemas de vigilancia continua, etc. Deberá considerarse adicionalmente que deberá haber control estricto sobre la lista de personal con permiso único de acceso, para lo cual se llevara bitácoras de acceso y por ninguna razón se permitirá el acceso a dichas a reas a personal ajeno que no cuente con el permiso de acceso necesario; claro, podrán existir circunstancias excepcionales donde sea necesario el ingreso de personal ajeno a dichas instalaciones seguras, por ejemplo: Acceso de personal externo para revisiones, mantenimiento, reparación, etc., del data center institucional, para lo cual se deberá generar protocolos específicos de acceso que salvaguarden la integridad física y lógica de los activos que se encuentren en dichas áreas; por ejemplo: se deberá gestionar el permiso de ingreso de actores externos indicando claramente las acciones que se va a realizar, y limitar el acceso de los mismos a procesos o activos que no formen parte del motivo por el cual dicha persona se la he concedido permiso de acceso; adicionalmente, al personal externo que se le

ha concedido acceso a áreas restringidas, por ninguna circunstancia podrá ingresar sin un responsable directo que controle y audite las acciones por el realizadas. Dicho protocolo adicionalmente, deberá generar un informe detallado de: las acciones realizadas, horas de ingreso y salida, personal que ingresa, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.5.1.3. Seguridad de oficinas, despachos e instalaciones.*

Tanto para: oficina, despachos e instalaciones donde se procese información, se desarrollen procesos propios del negocio de la institución o estén contenidos activos de información relevantes para la institución se deberán incluir controles de acceso, que dependiendo de la susceptibilidad medida proporcionalmente se usará: chapas, candados, cerraduras electrónicas con clave, cerraduras electrónicas biométricas, etc., adicionalmente según análisis de riesgo la inclusión de monitoreo continuo en circuito cerrado de video, guardias armadas, alarmas etc. y de ser el caso se recomienda el traslado a una infraestructura física dentro del mismo campus que brinde mayores garantías de seguridad. (ISO, NTE IEC ISO27002:2005, 2005)

*4.5.1.4. Protección contra amenazas externas y de origen ambiental.*

Debe considerarse que una amenaza externa en contra de la seguridad de la información puede provenir de diferentes fuentes, por ejemplo: ataques físicos en contra de la infraestructura de la institución, condiciones adversas políticas que atenten en contra la seguridad nacional, accidentes como incendios o explosiones en los laboratorios del campus, los cuales deben estar considerados en el plan de seguridad, donde se considere: las medidas de acción a tomarse, los roles y responsabilidades de los implicados, en caso de que el control de la amenaza sobrepase las capacidades de acción de la institución, se deberán considerar planes de contingencia y evacuación, así como estar en contacto con la autoridades respectivas que puedan ayudar a reducir el impacto de dichos incidentes.

Las amenazas de origen ambiental, deben estar consideras en los planes de Políticas de Seguridad y Plan de Contingencia en donde se consideren aspectos como evacuación del personal, gestión de seguridad de activos

abandonados; y por la ubicación geográfica de la ESPE (sede Matriz), potencialmente propensa a sufrir daños por la explosiones volcánicas, se sugiere fuertemente se considere el traslado del data center a una ubicación que suponga menos riesgos ante el mencionado riesgo de explosión volcánica; se sugiere que dicho data center se ubique en un lugar equivalente a un tercer piso. (ISO, NTE IEC ISO27002:2005, 2005)

*4.5.1.5. El trabajo en áreas seguras.*

Tener áreas seguras, implica la implementación de controles de supervisión, cuyo objetivo es brindar áreas que no suponga riesgos de seguridad, para tal efecto, debe incluirse en el documento de políticas de seguridad, procedimientos que aseguren controles de supervisión, por ejemplo: control estricto de personal ajeno a la institución y las acciones que los mismos realizan en la infraestructura de la institución; supervisión de actividades que impliquen riesgos sobre las áreas de trabajo, por ejemplo: trabajo con químicos, gases, fuego, etc.

Adicionalmente, se deberá añadir señalética que advierta a las personas sobre potenciales riesgos que un área podría ofrecer. (ISO, NTE IEC ISO27002:2005, 2005)

*4.5.1.6. Áreas de acceso público y de carga y descarga.*

Considerando la condición de la Universidad de las Fuerzas Armadas, de lugar público al que acuden diversos actores, es labor del Director de Riesgos institucionales definir las áreas a las que se puede brindar libre acceso a personal ajena a la institución, dichos lugares no suponen riesgos de seguridad para la institución; así mismo, deben estar claramente definidos los lugares de carga y descarga en la institución, mismos que no deben suponer riesgos a la seguridad institucional; para ambos casos es necesario asignar recursos de control que monitoreen que las acciones realizadas en estas áreas no perjudican a la seguridad de sede Matriz y de ser el caso, se podría incluir cámaras de monitoreo, guardia armada, etc. (ISO, NTE IEC ISO27002:2005, 2005)

### *4.5.2. Seguridad de los equipos.*

#### *4.5.2.1. Emplazamiento y protección de equipos.*

Para la protección de los equipos que posee la institución, es necesario que se haga un análisis de riesgos junto con la medición de la criticidad ligada a la información gestionada, procesada o almacenada en dichos equipos, y con esto analizar los controles de protección requeridos, por ejemplo: Controles electrónicos de acceso en ingresos mediante: tarjetas electrónicas, sistemas biométricos, guardias armados, sistemas de vigilancia continua, etc. Adicionalmente se debe considerar que las condiciones de emplazamiento de equipos, por ejemplo: para el data center, se debería contar con: políticas de suministro continúo de energía o fuentes alternas de suministro eléctrico, sistemas de enfriamiento, control de temperatura o calefacción, control estricto de uso de estándares en la construcción del data center, considerando: medidas, piso, cableado, humedad, etc.

NOTA: Un aspecto de suma importancia a considerar es el hecho de la ubicación física de los equipos, ya que están en directa proporción: la criticidad con los niveles de protección que debería brindar una ubicación, por tanto, tras análisis de la situación de la seguridad de la Universidad de las Fuerzas Armadas (sede Matriz), se sugiere –como ya se indicó- que se evalúe el cambio de ubicación física del actual data center, pues la actual supone riesgos altos de ataques externos y de origen natural. (ISO, NTE IEC ISO27002:2005, 2005)

#### *4.5.2.2. Instalaciones de suministro.*

En referencia a los servicios de suministro se debe considerar lo siguiente: Para evitar eventos de disrupción del servicio, se debe asegurar el suministro continuo de energía eléctrica para la infraestructura de la Universidad y en caso de falla de la fuente primara de suministro, asegurar que una fuente secundaria entraría en acción en caso de la misma; sistemas UPS podrían ser una solución temporal que ayude a evitar que la entrega del servicio se limite, sin embargo actualmente la Universidad cuenta con una planta eléctrica que sirve como fuente secundaria de suministro eléctrico, por tanto de deben tomar todas las medidas adecuadas para asegurar la disponibilidad de funcionamiento de la

misma ante cualquier evento de corte eléctrico que pudiera suscitarse, para esto, se requerirá un plan de mantenimiento preventivo correctivo de dicha planta para asegurar de esta manera el correcto funcionamiento de la misma. (ISO, NTE IEC ISO27002:2005, 2005)

*4.5.2.3. Seguridad del cableado.*

Existe directa responsabilidad en el mantenimiento de la seguridad del cableado con el Departamento de TI de la Universidad de las Fuerzas Armadas, por tal motivo, deben considerarse las siguientes recomendaciones: para el caso de las líneas de energía y telecomunicaciones deberían ser subterráneas, caso contrario emplear alternativas que aseguren la seguridad física de las mismas; el cableado de red debe usar ductería[1] que evite la intercepción de la información que los atraviesa y no debe atravesar espacios públicos de libre acceso a personal propio o ajeno a la institución; se debe evitar interferencias separando los cables de energía de los de transmisión de datos; se debe usar estándares de clasificación y etiquetado de cables de red y evitar de esta manera errores involuntarios en la manipulación de los mismos. (ISO, NTE IEC ISO27002:2005, 2005)

*4.5.2.4. Mantenimiento de equipos.*

Para un correcto proceso de mantenimiento de equipos, se deberá considerar los siguientes aspectos: las fechas en las que se realicen los mantenimientos no deben cruzarse con el horario habitual de trabajo de la institución, por tanto se sugiere se realice en días no laborables y con esto no interrumpir la entrega del servicio de la institución; deben haber políticas de acceso a áreas restringidas en caso de susceptibilidad de áreas, equipos o procesos; el personal que realice el mantenimiento debe ser supervisado por un responsable interno que valide que el procedimiento no atentara en contra de la infraestructura física o lógica de la institución; deberán realizarse procesos de backup[2] de configuraciones o instalaciones previos al desarrollo de mantenimiento y el mantenimiento deberá ser continuo y preventivo, para lo

[1] Ductos por los cuales atravesarán las líneas de transmisión.
[2] Respaldo de información

cual se debe generar procesos de comunicación con proveedores expertos locales y definir tiempos entre mantenimientos. (ISO, NTE IEC ISO27002:2005, 2005)

*4.5.2.5. Seguridad de equipos fuera de las instalaciones de la sede Matriz.*

Todo proceso de traslado de equipos fuera de las instalaciones de la institución -en su sede Matriz- debe contar con una autorización del Director del Área de TI y el empleado que haga el traslado debe considerar los siguientes puntos de seguridad: deberá llenarse un documento de responsabilidad, donde se incluya: fecha de salida, fecha de regreso, datos personales del responsable y firma de responsabilidad; Si el equipo contiene información susceptible para la institución, debe respaldarse y resguardarse en caso de pérdida del equipo; los equipos trasladados fuera de la institución no pueden ser manipulados por entes externos a la misma; los equipos deben contar con nombres de usuario y contraseñas que evite el acceso al equipo de terceros; adicionalmente se sugiere se considere el implementar alternativas de encriptación de información en caso de que un equipo trasladado fuera de la organización tenga información cuya perdida podría desequilibrar o podría detener la entrega del servicio de la institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.5.2.6. Seguridad en la reutilización o eliminación de equipos.*

El Departamento de TI debería gestionar este proceso, incluyendo los siguientes sugerencias: Todo equipo que se reutilice, debe pasar por un proceso de formateo (físico y lógico) de disco inmediatamente ocurrida su entrega, y evitar de esta manera que información de usuarios anteriores se filtre posteriormente; todo equipo que se vaya a eliminar, debe pasar por un proceso de destrucción de sus unidades de almacenamiento lógico. (ISO, NTE IEC ISO27002:2005, 2005)

## 4.6. Gestión de comunicaciones y operaciones

*4.6.1. Responsabilidades y procedimientos de operación.*

*4.6.1.1. Documentación de procedimientos operativos.*

Los procedimientos operativos involucrados en la operación del negocio deben estar documentados detalladamente y deberán incluir: el conjunto de pasos exactos que lleven al resultado final de un proceso específico de la institución, junto con él/los responsables directos, así como insumos (físicos, lógicos, personal, etc.) requeridos para la ejecución del proceso y salidas de dicho proceso. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.1.2. Gestión de cambios.*

Para realizar tareas de gestión de cambios, debe realizarse coordinadamente entre: el Director de TI, las áreas Administrativas involucradas que han solicitado el cambio –de ser el caso- y los involucrados dentro del Área de TI que gestionan el cambio (por ejemplo: Líder de desarrollo de software, Líder de infraestructura, Líder de Base de Datos, administradores de aplicaciones, desarrolladores, etc.); y el proceso debe estar documentado, iniciando por el requerimiento de cambio, el cual contendrá lo siguiente: persona responsable o unidad requirente del cambio, motivo del requerimiento, impacto en la organización, análisis del valor corporativo a obtenerse con el cambio, fecha de solicitud y firma de responsabilidad; este documento deberá desarrollarse conjuntamente entre la Dirección de TI y las Unidades que peticionan el cambio y deberá ser aprobado por el Director de TI validando y aceptando el requerimiento. Una vez que se implante el cambio debe considerarse lo siguiente: debe documentarse el documento de cambio, con el conjunto de pasos a seguir para la subida a ambiente de producción, el mismo que deberá tener la aceptación del responsable de QA (Aseguramiento de la Calidad) confirmando que los cambios requeridos se han cumplido a cabalidad, se requieren adicionalmente las firmas de aceptación de las personas responsables dentro de TI (por ejemplo: Líder de desarrollo de software, Líder de infraestructura, Líder de Base de Datos, administradores de aplicaciones, desarrolladores, etc.) indicando que han validado el proceso de cambio y que el proceso de actualización se hará de manera controlada buscando la menor afectación en el sistema; este procedimiento debería primero realizarse en un ambiente de pruebas (similar al de producción) y debe realizarse en una fecha y

hora que dicha implementación no limite la entrega de servicios de la institución. Debe considerarse adicionalmente el realizar backups: de configuraciones, bases de datos y códigos fuente en el estado actual (sin el cambio) en caso de que se requiera regresar a una versión anterior. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.1.3. Segregación de tareas.*

La segregación de tareas se constituye como un pilar fundamental en el correcto funcionamiento organizacional, por tanto, es responsabilidad, por una parte del Área administrativa el tener bien definidos: sus procesos, actores, roles y responsabilidades y de esta manera poder asignar recursos coherentemente según la necesidad; por otra parte, la dirección de TI, en concordancia a lo expresado anteriormente debe también el tener bien definidos: sus procesos, actores, roles y responsabilidades, así como recursos necesarios, adicionalmente debe realizar un análisis de perfiles y analizar, aptitudes, destrezas, preparación académica y experiencia y de esta manera poder realizar un correcto proceso de segregación de tareas y competencias. Una vez que la parte administrativa y la parte de TI han delimitado sus ámbitos de acción se debe definir claramente las competencias por cada área y evitar de esta manera el que un departamento cubra tareas que no le competen o que el departamento de TI realice actividades administrativas que no son de su alcance y de esta manera optimizar el trabajo de TI en función de la organización. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.1.4. Separación de los recursos para desarrollo, pruebas y producción.*

Para un óptimo rendimiento de los procesos institucionales, la Dirección de TI, deberá realizar una clara separación entre los diversos ambientes que las buenas normas recomiendan que un área de TI posea: Pruebas, Pre producción y Producción. El ambiente de pruebas se destinará a desarrollar pruebas internas de sistemas de software, dicho ambiente deberá ser similar (a nivel de información) al ambiente de producción; el ambiente de Pre producción deberá tener completa similitud con el ambiente de producción y se emplea para realizar pruebas de los sistemas desarrollados (o externalizados) por la organización o de

ser el caso poner a disposición de entidades externas que realicen interoperabilidad con la institución sin tener acceso al propio ambiente de producción y, el ambiente de Producción es el ambiente en el cual los sistemas y plataformas de software trabajan en el día a día en cumplimiento con las necesidades del negocio.

Al tener esta clara separación de ambientes la gestión de TI, minimiza los riesgos tácitos a la operación y está en la capacidad de proporcionar recursos de manera coherente a la operación del negocio. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.2. Gestión de los servicios contratados a terceros.*

*4.6.2.1. Prestación de servicios.*

Es necesario que la Dirección de TI en los procesos de contratación considere los siguientes aspectos: Se deberán incluir acuerdos de confidencialidad y de buen uso de la información a la que el contratado pudiera tener acceso; se deberán generar documentos detallados con la especificación exacta con los requerimientos que la Universidad de las Fuerzas Armadas requiera del contratado; se deberán definir acuerdos de nivel de servicio en referencia a lo que la institución espera del servicio proporcionado por el contratado (aquí deben indicarse los tiempo de operación aceptable para la operación de la institución); se deben definir las sanciones en caso de que el contratado incumpliera los requerimientos definidos en el contrato; se deben añadir cláusulas que involucren aspectos de seguridad y uso de buenas prácticas y normas internacionalmente aceptadas en el tema de seguridad de la información, en el desarrollo o prestación del servicio. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.2.2. Monitorización y revisión de los servicios contratados.*

Las cláusulas de cumplimiento deben aclarar que la institución estará en la capacidad en cualquier momento durante la duración de la ejecución del contrato, de: monitorizar y revisar el avance del proyecto y de ésta manera verificar que el desarrollo del mismo cumple con los requerimientos reales

definidos por la institución y que se está empleando en el desarrollo del mismo, buenas prácticas, normas, estándares que aseguren: confidencialidad, integridad y disponibilidad en la información de la institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.2.3. Gestión de los cambios en los servicios contratados.*

Para generar el proceso de gestión de cambios con terceros contratados se deben considerar lo expuesto en el numeral 4.6.1.2. (Gestión de cambios.), pero con la consideración adicional que se deben reforzar políticas de cierre de proyectos con terceros, es decir, deberá haber un control riguroso de control de cuentas de usuario, contraseñas y accesos que se ha brindado a en ente contratado; y al finalizar un contrato se debe formar un comité con los miembros involucrados de TI (Infraestructura, Redes, Software, etc.) donde se analice los huecos de seguridad que pudieran quedar producto de la intervención de terceros en la infraestructura y se analice la efectividad de los controles implementados, y de ser el caso mejorarlos, desecharlos o crear controles nuevos que mitiguen los riesgos inherentes a la intervención de terceros en la infraestructura institucional. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.3. Planificación y aceptación del sistema.*

*4.6.3.1. Planificación de capacidades.*

Es competencia del Director de TI (junto a los líderes de las áreas más relevantes: Redes, Infraestructura, Bases de Datos, Software, etc.), realizar un trabajo conjunto que basado en la realidad tecnológica de la institución, indique las capacidades reales de expansión que posee la institución, dimensionando las capacidades físicas, lógicas y de recursos en general que permitan a la institución proyección de crecimiento futuro basado en las fortalezas tecnológicas con que cuenta la Institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.3.2. Aceptación del sistema.*

Es competencia del Director de TI, generar procesos que permitan conocer la realidad tecnológica que posee la institución y con ello estar aptos

para saber las capacidades reales de expansión -tecnológicamente hablando- que tiene la institución y que puedan ayudar a cumplir las metas estratégicas planteadas por la organización, y en base a esto, saber con certeza si es viable: actualizar sistemas, ampliar sistemas, dar de baja sistemas etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.4. Protección contra software malicioso y descargable.*

*4.6.4.1. Controles contra código malicioso.*

Para lograr controlar código malicioso en la institución la primera estrategia que deberá realizarse es generar campañas de difusión de información respecto al tema y concientización sobre los riesgos a los que la institución y los trabajadores se exponen al caer presas de códigos maliciosos; adicionalmente se deben implementar políticas de control que permitan minimizar los riesgos, considerando lo siguiente: políticas de uso de software licenciado; implementar políticas de restricción de descargas y acceso a contenido web malicioso, políticas de uso de antivirus, de ser posible gestionar la adquisición de antivirus corporativo y con ello estar en la capacidad de usar firewalls web, generar tareas programadas para escaneos y actualizaciones del software; restricciones de acceso a la red corporativa desde redes externas, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.4.2. Controles contra código descargado en el cliente.*

Una vez que un código ha sido descargado en un cliente, existe el riesgo de la multiplicación del mismo a través de la red corporativa de la institución, por tanto, para minimizar esta amenaza, se debe trabajar en conjunto con las recomendaciones dictadas en el punto 4.6.4.1. (Controles contra código malicioso.) y adicionalmente se debe socializar políticas de acción inmediata ante códigos maliciosos detectados, en donde se emplearan medidas y procedimientos que eviten el que códigos maliciosos se riegue por la red institucional, por ejemplo el empezar procesos de cuarentena de equipos infectados; adicionalmente es necesario que el grupo humano especializado de TI que enfrente estos incidentes reciba capacitación continua sobre nuevas

amenazas que puedan aparecer, así como las medidas de acción que se debe seguir para erradicar, eliminar y prevenir estos códigos. (ISO, NTE IEC ISO27002:2005, 2005)

*4.5.5. Copias de Seguridad.*

*4.5.5.1. Copias de seguridad de la información.*

Es necesario que se continúe con el proceso de copias de seguridad que la Universidad ha venido llevando, para lo cual se recomienda que este proceso de backup mínimo se realice una vez por mes y se respalde: información propia de la actividad administrativa/financiera de la institución; información escolástica (historiales académicos de pre y post grados, mallas curriculares, etc.); códigos fuente de sistemas, configuraciones, licencias, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.6. Gestión de la seguridad en redes.*

*4.6.6.1. Controles de red.*

Es necesario que el Administrador de Red en la institución, aplique una política que considere aspectos tanto físicos como lógicos que permitan una comunicación óptima entre las diversas áreas de la institución; por ejemplo: gestionar óptimamente la distribución de la red física y que no esté al alcance de terceros que puedan interceptar información de la misma, mantener grafos y diagramas de red actualizados con ubicaciones de componentes de la misma; por ejemplo: switchs, routers, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.6.2. Seguridad en los servicios de red.*

El Administrador de la Red institucional en la Universidad de las Fuerzas Armadas deberá monitorear continuamente los servicios contratados con terceros y validar el fiel cumplimiento de: rangos, tiempos y calidad de servicio acordados en documentos de acuerdo de servicios. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.7. Manipulación de los soportes.*

*4.6.7.1. Gestión de soportes extraíbles.*

El Director de TI deberá definir procedimientos para la gestión de medios de soporte extraíbles, en los cuales se deberá considerar como mínimo lo siguiente: deshabilitar el uso de memorias flash en computadores cuyo uso implique riesgos en la seguridad de la información; proporcionar procedimientos adecuados de almacenaje de medios magnéticos como: cintas, discos, dvd's con información susceptible para la institución por ejemplo: respaldos de información institucional, respaldos de información escolástica de alumnos de pre y post grado, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.7.2. Eliminación de soportes.*

Una vez que un soporte ya no sea necesario para los intereses institucionales, el mismo debe pasar por un proceso de eliminación segura de su contenido y de ser el caso podría incluso ser destruido totalmente; pero considérese que en dicho proceso antes de realizar la eliminación o la destrucción del soporte, se debe realizar un análisis concienzudo de la información, propietario y circunstancias en las que se manejó el soporte, pues potencialmente dicho soporte podría poseer pistas de auditoria cruciales para posteriores procesos de investigación. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.7.3. Procedimientos de manipulación de la información.*

Existen circunstancias en los que los procedimientos normales de manipulación de la información, arrojan problemas de seguridad o simplemente el proceso habitual posee problemas de operación, es en ese escenario, donde se deben definir procesos de manipulación de información adicionales a los comunes, para esto debe considerarse lo siguiente: debe asegurarse la integridad de la información, por tal motivo, se verán estrategias de almacenaje que no permitan que factores externos corrompan la información; se deberá llevar un control minucioso del etiquetado de la información y evitar de esta manera, corrupción de la información, la información deberá resguardarse en un medio

propicio, que no la contamine y que esté libre de intervenciones de terceros o eventos que atenten contra la misma, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.7.4. Seguridad de la documentación de sistemas.*

Deben considerarse los siguientes controles para el ámbito de seguridad de documentación de sistemas: deberán existir medios de almacenaje seguro, deberán haber políticas de restricción de acceso a la información por roles y propietarios; en caso de que la información sea almacenada o transite a través de una red pública, deberán haber los controles necesarios que aseguren la confidencialidad, integridad y disponibilidad de la misma. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.8. Intercambio de información.*

*4.6.8.1 Políticas y procedimientos de intercambio de información*

El Director de TI deberá establecer políticas, procedimientos y controles para el intercambio de información, considerándose lo siguiente: se deberá proteger la información evitando que se dé: intercepción, copiado, modificación, re direccionamiento y destrucción de la misma; detección y protección en contra de códigos maliciosos; protección de información electrónica en forma de información adjunta; políticas de uso aceptable de medios de comunicación electrónica; políticas de uso medios de comunicación inalámbrica; asignar responsabilidades al usuario que genere el intercambio de información; uso de codificación de información; políticas de control de manipulación y uso de información confidencial en medios impresos; controles y restricciones referentes al reenvío de información. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.8.2. Acuerdos para intercambio de información.*

Se deberán establecer políticas para intercambio de información considerando lo siguiente: responsabilidades a nivel de altos directivos en caso de que el intercambio se dé entre instituciones; procedimientos de control de envío analizando las fuentes: emisor y receptor; seguir estándares técnicos que

aseguren una transmisión segura a nivel de paquetes de información; responsabilidades y obligaciones si se presentara perdida de datos e información; rotulación adecuada de la criticidad de la información; definición de propiedad de la información y aseguramiento de políticas de propiedad intelectual; añadir criptografía en la transmisión de información. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.8.3. Soportes físicos en tránsito.*

Si existen medios informáticos que son transportados por mensajeros, debería considerarse: los medios de transporte o mensajería deben brindar niveles aceptables de confiabilidad y de ser necesario se asignara custodia armada en caso de que se incluya información susceptible y evitar de esta manera divulgación o modificación no autorizada; deberán añadirse procesos de embalaje que aseguren su contenido de amenazas como: daños físico debida a la mala manipulación durante el envío. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.8.4. Mensajería electrónica.*

A nivel de seguridad para los mensajes electrónicos, se deberá considerar lo siguiente: se deberá controlar: acceso no autorizado, modificación de información o denegación del servicio; aseguramiento del direccionamiento y transporte seguro; confidencialidad, integridad y disponibilidad de la información; aspectos legales como firmado electrónico, controles mayores de autenticación para el control de acceso en redes de acceso público. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.8.5. Sistemas de información empresariales.*

Los aspectos de seguridad a considerar en torno a los sistemas de información empresariales son: Vulnerabilidades generales conocidas de un sistema, especialmente en aquellos módulos que permiten interactuar a diversas áreas, por ejemplo: procesos administrativo-contables; comunicación comercial; Políticas y controles para manejo de intercambio de información; niveles aceptables de acceso a documentación sensible; restricción de acceso a

información; se deberá categorizar a los usuarios tanto internos como externo y definir sus niveles de acceso; gestión de usuarios, respaldo de información. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.9. Servicios de comercio electrónico.*

*4.6.9.1. Seguridad en comercio electrónico.*

Si existieran requerimientos de comercio electrónico en la institución, deberá considerarse: asegurar niveles de confianza entre las partes involucradas en transacciones; asegurar y cumplir requerimientos de confidencialidad, integridad y confidencialidad de la información; aspectos ligados al no repudio de data; asegurar que aliados estratégicos o terceros que brinden servicios estén alineados con estándares internacionales de seguridad, manejo de información y gestión de transacciones on line; gestionar procesos que eviten la perdida, corrupción o modificación de información (escenario típico de transacciones interrumpidas que no permiten completar las acciones); definir responsabilidades asociadas a transacciones fraudulentas. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.9.2. Seguridad en transacciones en línea.*

Los aspectos de seguridad a considerarse para el caso de transacciones en línea son: asegurar la verdadera identidad de las partes involucradas mediante mecanismos como firma electrónica; las credenciales de usuario deberán ser válidas; se debe asegurar la confidencialidad y la privacidad de los involucrados mientras dure la transacción; el medio de comunicación para a transacción deberá estar protegido para que no pueda ser interceptado; se deberán utilizar protocolos seguros de comunicación; se deberán gestionar procedimientos de log y con esto tener información para auditoria en cualquier momento que se requiera; los detalles de la transacción se deberán almacenar en una base de datos no pública y de acceso restringido; se deberá involucrar autoridades de certificación que aseguren la valides de firmas o certificados. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.9.3. Seguridad en información pública.*

La información que se categorice como pública, deberá estar mantenida en un ambiente de hardware y software seguro que cumpla lo siguiente: deberán generarse procesos de aprobación de la información a publicarse, definiendo claramente la criticidad de la misma y si la misma puede ser accedida públicamente; deberá asegurarse la disponibilidad de la información; deberán generarse políticas de revisión continua de la seguridad de la infraestructura en la que se aloja la información y eliminar amenazas y potenciales vulnerabilidades; deberán asegurarse procesos que aseguren la integridad de la información publicada y evitar que la misma sea modificada, extraída o eliminada; se deberá considerar aspectos legales considerados en la legislación ecuatoriana de protección de datos (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.10. Supervisión*

*4.6.10.1. Registro de auditoria.*

La información de auditoría están bajo la responsabilidad del Administrador de Sistemas de Información y deberán incluir al menos lo siguiente: identificadores de registros en la base de datos; incluir fechas, hora y caracterización de transacciones o actividades; identidad y ubicación de las involucrados (y de ser posible direcciones IP de los equipos donde se generan las transacciones), historial de actividad o logs[3] (incluyendo intentos fallidos de acceso, peticiones y acceso a recursos, modificaciones en configuraciones del sistema, activación, desactivación de controles de seguridad, información resultante de los sistemas de detección de intrusos); privilegios; direcciones y protocolos de red; alarmas en el control de acceso y utilización. (ISO, NTE IEC ISO27002:2005, 2005)

[3] Compendio de información relacionada con la trazabilidad de acciones de: usuarios, procesos, hardware, software, etc.

*4.6.10.2. Supervisión del uso de los sistemas.*

El monitoreo de los sistemas de información con los que cuenta la institución deberán considerar: información del historial de accesos autorizados donde se registre todos los rastros de auditoria indicados en el numeral 4.6.10.1. (Registro de auditoria); información sobre las operaciones privilegiadas como: uso de cuentas privilegiadas, inicio y apagado del sistema, uso dispositivos de entrada y salida; intentos de acceso no autorizado así como el uso de recursos; violaciones a la política de acceso y notificaciones a nivel de 'gateways' y ' firewalls' en la red; alertas de fallas del sistema; intentos de modificación a controles de seguridad de sistemas. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.10.3. Protección de la información de registros*

Con el objetivo de proteger contra cambios no autorizados y problemas operacionales, y el medio de registro se debe considerar: alteraciones en los mensajes; registros editados o borrados; sobre escritura de información de registros. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.10.4. Registros de administración y operación.*

Los registros de diarios de la operación institucional contendrán: hora en que ocurren eventos; información de evento o fallas ocurridas; usuario y el operador/ejecutor -o administrador involucrados-; procesos involucrados. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.10.5. Registro de fallos.*

Para el proceso de registro y/o notificación de fallos ocurridos en la plataforma institucional tecnológica debería considerar: información de la persona que reporta el fallo; descripción completa del fallo (entorno, características, circunstancias en las que ocurrió el fallo, etc.); hora y fecha del fallo; responsable de la solución del problema; solución del problema; hora y fecha de solución del problema; se deberá implementar procesos de revisión de resolución satisfactoria de fallos; revisión de controles y que los mismos no hayan sido corrompidos o inhabilitados en la solución del problema. (ISO, NTE IEC ISO27002:2005, 2005)

*4.6.10.6. Sincronización de reloj.*

Es necesario llevar un control estricto de las horas manejadas en la institución pues el registro de la misma se reflejara en información posterior ligada a aspectos como: auditoria, transacciones comerciales en los sistemas, etc., por lo cual se debe manejar procesos de sincronización de las horas en sistemas de información y dispositivos biométricos que registran el movimiento del personal. (ISO, NTE IEC ISO27002:2005, 2005)

## 4.7. Control de acceso

*4.7.1. Requisitos de negocio para el control de accesos.*

*4.7.1.1. Política de control de accesos.*

Para poder definir las políticas de control de acceso se deberá considerar lo siguiente: Se debe definir claramente las políticas de cumplimiento obligatorio y las que pueden modificar su flexibilidad de cumplimiento, esto considerando: el entorno en el que se desarrollan las actividades de la institución en su sede matriz, los factores sociopolíticos y el factor humano que interactúa con la universidad; Se deben definir procedimientos que identifiquen las zonas de riesgo de la institución en la que un acceso de terceros podría ser perjudicial para la institución, por ejemplo: centros de procesamiento de información, data center, oficinas, etc., y una vez definidas estas áreas se definirá la sensibilidad de las mismas y su directa proporción con los mecanismos de control acceso que se debe implementar; se debe controlar estrictamente los mecanismos que diferencien al personal autorizado del no autorizado, por ejemplo, emisión de carnets institucionales y a la par se deberá capacitar y concientizar al personal sobre el tema. (ISO, NTE IEC ISO27002:2005, 2005)

### *4.7.2. Gestión de acceso de usuario.*

#### *4.7.2.1. Registro de usuario.*

El Administrador de Sistemas de Información deberá considerar los siguientes puntos dentro del proceso de registro y dada de alta de un usuario: uso de identificadores únicos por usuario; definición de roles de usuario, sus atribución y definición de propiedad sobre la información; corroborar niveles de acceso versus ámbito de acción del trabajador versus políticas de seguridad definidas para usuarios; el usuario deberá contar con un detalle por escrito de sus derechos y obligaciones de acceso, mismas que deberán ser aceptadas por el usuario; se requiere políticas para asignación y dada de baja de usuarios; se deberá llevar un registro del usuario o grupo de usuario y las atribuciones de él/ ellos para uso de servicios; definir los protocolos de cancelación de derechos de acceso para usuarios desvinculados de la institución; garantizar la unicidad de un registro de usuario, evitando de esta manera duplicidad e inconsistencias en la información de acceso entre usuarios. (ISO, NTE IEC ISO27002:2005, 2005)

#### *4.7.2.2. Gestión de privilegios.*

Las políticas de gestión de privilegios de usuarios, deberá considerar lo siguiente: se deben identificar los privilegios asociados a activos de información como: sistemas operativos, bases de datos, aplicaciones; los privilegios se deben asignar a usuarios en base a la estricta necesidad del cargo que el mismo desempeña, por tanto deberá haber estricto análisis de dichos requerimientos para que no se otorguen permisos “extra”; previo al proceso de otorgamiento de privilegios a un usuario, deberá estrictamente realizarse una petición de autorización al Director de TI por parte de área requirente solicitando acceso de un usuario y únicamente con esta aprobación se podrá continuar con el proceso de otorgamiento de accesos; los sistemas de software de la institución deberán manejar directamente la asignación de permisos de usuarios, añadiendo siempre un rastro de las los permisos brindados a un usuario y quien lo hizo. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.2.3. Gestión de contraseñas de usuario.*

El Administrador de Sistemas de Información de la institución deberá considerar lo siguiente al momento de definir políticas de gestión de contraseñas de usuario: un usuario al que se la ha asignado usuario y perfiles en los sistemas e la institución deberá firmar acuerdos donde se compromete a hacer uso de las contraseñas a él asignadas, indicando que es de su estricta responsabilidad el uso que haga de las mismas; se deberá emplear mecanismos mediante software que obliguen a los usuarios a actualizar sus contraseñas periódicamente (por ejemplo cada 3 meses); se debe socializar las buenas prácticas de gestión de contraseñas entre los usuarios, y se mencionarán aspectos como: riesgos de un mal uso de contraseña, gestión de contraseñas y puestos limpios, estructura de contraseñas seguras, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.2.4. Revisión de los derechos de acceso de los usuarios.*

Un proceso de revisión de derechos de acceso de usuarios debería contemplar lo siguiente: debe ser un proceso continuo y reiterado en el que se consideren los privilegios (en sus diversos niveles de criticidad) de acceso de los diversos usuarios de la institución; se sugiere que dicho proceso de revisión de derechos se realice cada tres meses y de ser necesario mensualmente los privilegios que suponen mayor criticidad. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.3. Responsabilidades del usuario.*

*4.7.3.1. Uso de contraseñas.*

Para concientizar a los empleados sobre el buen uso que deben hacer de sus contraseñas se debe considerar lo siguiente: no se deben divulgar las contraseñas por ningún concepto; propiciar el mantener escritorios limpios sin contraseñas transcritas en papel; si existen indicios que una contraseña ha sido sustraída, proceder a actualizarla inmediatamente y notificar al personal encargado; contraseñas robustas (longitud mínima de 6 caracteres, deben tener características que permitan el fácil recuerdo de la misma, no deben estar formadas por información fácilmente deducibles por terceros, formarse de grupos alfanuméricos); concientización sobre la actualización periódica de

contraseñas, tiempo sugerido: 3 meses; los sistemas de software deben tener controles que no permitan reutilizar contraseñas y que validen el ingreso de las mismas; no hacer uso de procesos como “Recordar contraseña”. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.3.2. Equipo de usuario desatendido.*

Todo activo de información debe tener asignado un responsable, que se responsabilice por el equipo a su carga y las acciones que se pudieran realizar sobre el mismo; sin embargo para una política de gestión de equipos desatendido debe considerarse lo siguiente: bloqueo del equipo; cerrar sesiones activas; no dejar tareas abiertas que pudieran ser manipuladas por terceros, incluir en los sistemas de software procesos de terminación de la sesión al no detectarse actividad en una máquina; si se ha realizado procesos de acceso remoto a equipos, realizar la desconexión de los mismos al terminar las tareas necesarias. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.3.3. Políticas para puesto de trabajo despejado y pantalla limpia.*

El Director de TI deberá implantar políticas de escritorio despejado y pantalla limpia considerando lo siguiente: bajo ningún motivo se dejará en los puestos de trabajo información crítica, o cuyo contenido pudiera perjudicar a la institución o restrinja su funcionamiento; si un usuario va a abandonar su puesto de trabajo debe bloquear su computadora y dejar debidamente protegidos cajones, armarios, canceles etc. donde se almacene información de acceso restringido, adicionalmente revisará que dispositivos de almacenamiento externo como: memorias flash, discos duros externos, discos, dvd´s no se encuentren conectados al equipo durante el tiempo que el equipo estar desatendido; no se dejarán desatendidas por ningún concepto puertas de entrada, buzones físicos de correo o maquinas como: copiadoras, faxes, escáneres o similares tecnologías de reproducción de información etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.4. Control de acceso a la red.*

*4.7.4.1. Política de uso de los servicios en red.*

Los aspectos a considerarse en las políticas de uso de servicios en red son: Documento donde se detallen las redes, los servicios inherentes a ellas y la lista de aprobación/restricción de acceso (los usuarios que pueden y los que no pueden acceder a dicha red y sus servicios); se debe contar con procedimientos de acceso que permitan determinar las redes y sus servicios versus los usuarios que tienen acceso; controles de gestión y seguridad en el acceso a conexiones y servicios en red. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.4.2. Autenticación de usuario para conexiones externas.*

Es necesario contar con procedimientos que aseguren la gestión de accesos remotos hacia la infraestructura en red de la institución, un ejemplo común es el acceso vía VPN, el cual debe considerar procedimientos y políticas robustas de seguridad, y reducir el alto riesgo que dichas conexiones suponen. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.4.3. Identificación de los equipos en las redes.*

El Administrador de Red institucional deberá poseer procedimientos que permitan tener identificados en todo momento los equipos que forman parte de la red institucional, para lo cual deberá contar con sistemas de monitoreo que le permitan saber en línea los equipos que están conectados en una red; adicionalmente deberá contar con diagramas de topologías de red en conjunto con los usuarios internos definidos. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.4.4. Protección a puertos de: diagnóstico y configuración remotos.*

La gestión de puertos en general debe estar debidamente gestionada en procedimientos y políticas que deberían asegurar que el uso que se haga de los mismos tanto internamente como externamente al ámbito de la red institucional en su sede Matriz será controlado, es decir, deberá censarse los puertos en los

servidores de la infraestructura y por ningún motivo se permitirán se dejarán puertos abiertos que supongan riesgos de seguridad; para el caso de puertos usados en diagnóstico y configuración remotamente, el Administrador de Redes deberá realizar todos los procedimientos que aseguren que dichos puertos serán usados únicamente por el personal con derechos sobre los mismos y de manera segura. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.4.5. Segregación en las redes.*

El Administrador de Red deberá incluir controles que permitan asegurar aspectos de seguridad a nivel de redes, específicamente para segregación de redes deberá considerar lo siguiente: dividir redes en dominios lógicos separados, así como dominios de red tanto internos como externos al del ámbito de su sede Matriz; para protegerlos, existirá un perímetro de seguridad definido mediante un Gateway seguro entre las dos redes; dicho gateway deberá configurarse para que se filtre el tráfico entre dominios y bloquear accesos no autorizados de acuerdo a la política institucional de control de acceso. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.4.6. Control de conexión a la red.*

El control de acceso a la red institucional deberá realizarse en base a las restricciones indicadas en la política institucional de control de acceso, considerando las siguientes aplicaciones: correo electrónico, aplicaciones de transferencia de archivos (unidireccional y bidireccional), acceso interactivo y acceso a red vinculado a fecha u hora. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.4.7. Control de enrutamiento de red.*

Se deberán definir controles de ruteo basándose en la verificación positiva de direcciones tanto de origen como destino, haciendo énfasis en redes compartidas desplegadas fuera de los límites de la red institucional; dichos controles pueden tener una implementación tanto en hardware como en software. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.5. Control de acceso al sistema operativo.*

*4.7.5.1. Procedimientos seguros de inicio de sesión.*

El procedimiento seguro de inicio de sesión es una estrategia que minimiza el riesgo de accesos no autorizado; dicho procedimiento deberá contemplar los siguientes puntos: ocultamiento de información hasta que se realice satisfactoriamente el inicio de sesión, no se mostrarán mensajes de ayuda que proporcionen información adicional en caso de que un atacante accediera a las mismas; se mostrarán advertencias de acceso permitido solo a usuarios debidamente autorizados; se deberá indicar los errores en la información proporcionada en el proceso de inicio de sesión, por ejemplo: “Usuario no válido”; se limitará el número de intentos de inicio de sesión, y en caso de superarse el máximo establecido el sistema automáticamente podría realizar alguna de las siguientes acciones correctivas : bloqueara el acceso, bloquear al usuario, definir tiempos de espera para el próximo intento de inicio de sesión; sea cual fuere la estrategia que se defina, los sistemas deberán lanzar notificaciones de intentos fallidos de inicio de sesión, tanto a la cuenta del usuario como al personal de soporte a cargo del tema; se deberá llevar un log que indique claramente: intentos realizados, ubicación desde la que se realizan los intentos, dirección IP –de ser posible-, fecha y hora. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.5.2. Identificación y autenticación de usuario.*

El Administrador de Sistemas de Información de la institución en su sede Matriz proveerá a todos los usuarios definidos, credenciales únicas de acceso, las mismas que permitirán diferenciar unívocamente a los usuarios, junto con sus roles y ámbito de acción. Es importante almacenar la información relacionada a dicho registro único de usuario para poder hacer un rastro hacia pistas de auditoria que potencialmente fueran requeridas. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.5.3. Sistema de gestión de contraseñas.*

El Administrador de Sistemas de Información deberá tomar en consideración los siguientes puntos referentes a la gestión de contraseñas: como se mencionó en el punto 4.7.5.2. (Identificación y autenticación de usuario), se deberá proporcionar credenciales de acceso y contraseñas únicos a los usuarios definidos, proporcionar la opción de actualización de claves a los usuarios y con ello descentralizar el proceso de reseteo de contraseñas sobre el área de TI; implementar controles que obliguen al usuario a usar contraseñas robustas; usar contraseñas temporales en el primer registro del usuario que obligatoriamente deberán ser cambiadas por el usuario; implementar mecanismos de control que eviten la reutilización de contraseñas; implementar controles que eviten el mostrar contraseñas en pantalla; las contraseñas serán almacenadas y viajaran a través de la red bajo algún mecanismo de encriptación (se sugiere emplear mecanismos que empleen algoritmos actualizados de encriptación). (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.5.4. Uso de recursos del sistema.*

El Administrador de Sistemas de Información de la sede Matriz de la Universidad de las Fuerzas Armadas, deberá tomar en consideración los siguientes puntos referentes al uso de los recursos del sistema: se requieren procedimientos de identificación, autenticación y autorización para el uso de recursos del sistema; segregar recursos a nivel de software; limitar el uso de recursos del sistema a usuarios que han sido autorizados y que se ha verificado su confiabilidad; se deberá realizar un proceso controlado de limitación de la disponibilidad de los recursos del sistema; log de uso de los recursos del sistema; se deberá definir y llevar documentación de los niveles de autorización de acceso a los recursos del sistema; generar políticas y acciones para eliminar recursos de software no utilizados o sub utilizados; generar políticas de segregación de acceso a recursos de software. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.5.5. Desconexión automática de sesión.*

Se deberán generar políticas que aseguren la desconexión de terminales que se encuentren en estado de abandono, debe considerarse: definición tiempos de sesión, y si las aplicaciones detectan inactividad, la sesión automáticamente será eliminada; adicionalmente dicha recomendación podría ampliarse a políticas de apagado de equipo automática y evitar de esa manera riesgos de seguridad con equipos encendidos. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.5.6. Limitación del tiempo de conexión.*

Considérese lo expuesto en el punto 4.7.5.5. (Desconexión automática de sesión) donde adicionalmente se definan horarios en los cuales los usuarios podrán tener acceso a sus equipos, y de requerirse tiempo adicional en horas extras ordinarias o extraordinarias, se lo hará solicitando permisos especiales en la restricción del tiempo de conexión. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.6. Control de acceso a las aplicaciones y la información.*

*4.7.6.1. Restricción de acceso a la información.*

Para lograr generar el proceso de restricción a la información, considérese lo siguientes: es básico tener segregados a los usuarios por perfiles y el ámbito de acción de los mismos, dicha información se registrará en los medios de almacenamiento de la institución y en base a esto, se reflejara el alcance de cada usuario, tanto en los sistemas de información como en los recursos del sistema, por ejemplo: dependiendo de los roles asignados a un usuario, los menús desplegables y acciones serán visibles únicamente si el rol asignado al usuario tiene acceso a los mismos y por ende a la información inherente a las acciones en los sistemas de información. (ISO, NTE IEC ISO27002:2005, 2005)

*4.7.6.2. Aislamiento de sistemas sensibles.*

Para poder gestionar un adecuado proceso de aislamiento de sistemas sensibles, tomar en cuenta lo siguiente: cada propietario de aplicaciones deberá detectar la sensibilidad de un sistema de información en relación a la información o procesos inherentes al mismo versus su impacto en la

organización; se deberán generar entornos propios de ejecución donde se asegure el aislamiento e independencia de sistemas críticos en la organización y con ello evitar que personal sin autorización acceda al mismo; se deben asignar recursos propios para la ejecución de dichos sistemas evitando de esta manera la intervención de personal o eventos externos en la ejecución normal del mismo. (ISO, NTE IEC ISO27002:2005, 2005)

### *4.7.7. Computadores portátiles y tele trabajo.*

#### *4.7.7.1. Computadores portátiles y comunicaciones móviles.*

Para definir una política que considere los riesgos de utilizar medios de computación y comunicación móvil tales como: computadores portátiles, palms, teléfonos móviles, etc., dentro de la infraestructura de la Universidad de las Fuerzas Armadas en su sede Matriz, considérese lo siguiente: añadir a la política aspectos de protección física, controles de acceso, criptografía, respaldos y protección en contra de virus informáticos; dichos aspectos se mencionan a lo largo del presente documento. (ISO, NTE IEC ISO27002:2005, 2005)

#### *4.7.7.2. Teletrabajo.*

Para que una actividad se realice en modalidad teletrabajo, debería asegurarse los siguientes lineamientos: contar con un proceso de aprobación expresa y conjunta por parte de: el Director de TI, Director de Talento Humano y el resto de direcciones que soliciten la aprobación para alguno de sus empleados. La responsabilidad sobre suministrar un punto de conexión seguro y libre de amenazas de seguridad debe ser expresamente asumida por el empleado que solicita permiso para teletrabajo; por otra parte es responsabilidad del encargado de redes de la Universidad de las Fuerzas Armadas –sede Matriz- suministrar un canal seguro (típicamente VPN[4]) que permita que se realice la conexión para el teletrabajo, dicho canal debe cumplir con todos los requisitos de seguridad que impidan que se haga un uso inadecuado de dicho canal de comunicación en contra de la infraestructura de la institución.

[4] Acrónimo de Virtual Private Network ( Redes privada Virtual)

NOTA. Existen en la actualidad alternativas a las VPN para realizar teletrabajo, que usan como medio de propagación la nube, lo cual debe analizarse por: Director de Ti, encargado de Redes, Director de Seguridad y analizar las ventajas así como las desventajas y amenazas a la seguridad de la institución que podría suponer usar esta alternativa. (ISO, NTE IEC ISO27002:2005, 2005)

## 4.8. Adquisición, desarrollo y mantenimiento de sistemas de información

### *4.8.1. Requisitos de seguridad de los sistemas de información.*

#### *4.8.1.1. Requisitos de seguridad de los sistemas de información.*

Para definir los requisitos de seguridad en los sistemas de información de la Universidad de las Fuerzas Armadas (sede Matriz), se deberá: medir la criticidad y analizar los riesgos de los mismos en base a los procesos que los ellos implementan, la información institucional ellos que procesan y el impacto global de los mismos en relación al ámbito institucional; una vez desarrollado el proceso de análisis de criticidad se deberá analizar los controles necesarios que se deberá incluir: controles a nivel de ingreso de información, controles a nivel de roles y asignación de permisos que tienen los usuarios para manipular los sistemas, controles a nivel de gestión de almacenamiento en base a la interacción de los mismos con fuentes de datos como bases de datos; controles a nivel de acceso a las aplicaciones en red; controles a nivel del manejo de información y encriptación de la misma; análisis de los recursos del sistema que dichos sistemas hacen uso y controles a nivel de infraestructura, en servidores de aplicaciones, puertos y la seguridad que los mismos brindan al albergar dichos sistemas. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.2. Tratamiento correcto de las aplicaciones.*

*4.8.2.1. Validación de los datos de entrada.*

El proceso de validación de datos de entrada en sistemas de aplicación debe considerar las siguientes recomendaciones: controles que eviten el encontrar los siguientes errores de entrada de información: valores fuera de rangos establecidos como aceptables, caracteres inválidos, datos faltantes o incompletos, datos no íntegros que excedan los tamaños definidos; procesos de asignación de responsabilidad sobre los usuarios que ingresen información en el sistema; procesos que permitan a los usuarios la notificación de errores encontrados; procesos de implantación de soluciones a errores de validación de entrada; deberá controlarse excepciones en el código fuente para evitar interrupciones en la ejecución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.2.2. Control del proceso interno.*

Para que el diseño de las aplicaciones, permita un trabajo fiable a nivel de procesamiento interno, se deberá considerar los siguientes aspectos: se deberá asegurar que un programa y sus subrutinas se ejecuten siguiente un orden lógico y cronológico en el procesamiento de información; deberá controlarse excepciones en el código fuente para evitar interrupciones en la ejecución; deberán haber procedimiento de depuración del código fuente que detecten bugs o código redundante que haga perder fiabilidad y rendimiento a la aplicación; los sistemas deberán manejar mensajes de advertencia que sirvan de guía en caso de que ocurran errores internos de procesamiento de información; como buena práctica está el hacer un diseño inicial de la aplicación y emplear pruebas unitarias y de integración que ayuden a validar el óptimo funcionamiento de las aplicaciones. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.2.3. Integridad de los mensajes*

La integridad en los mensajes es un aspecto extremadamente importante que va de la mano con la integridad resultante de la información que será almacenada en los sistemas de almacenamiento con que cuenta la institución, y para que la misma no sea almacenada corrompida, es necesario considerar lo

siguiente: se debe contar con mecanismos que aseguren que el proceso de serialización/descerialización[5] de objetos a enviarse a través de la red sea el adecuado y no se tengo como resultado final información corrupta; si se utilizan recursos que viajan a través de una red se puede utilizar algún mecanismo de "hashing[6]" que permita verificar la integridad de información, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.2.4. Validación de los datos de salida.*

Los datos de salida de una aplicación, deben entregar información: fiable, confiable e integra, y para asegurar esto, considérese lo siguiente: controles de conciliación, que permitan validar la información que se tiene versus la que se debería tener; validación mediante inferencia estadística de información, es decir tomar muestras aleatorias de datos y verificar la exactitud de las mismas; deberá haber pruebas de validación de información de salida; procesos de definición de responsabilidades sobre usuarios que manipulan dicha información de salida; deberán usarse controles de log en las aplicaciones que indiquen las acciones, fecha, hora y usuario responsable. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.3. Controles criptográficos.*

*4.8.3.1. Política de uso de los controles criptográficos.*

El uso de controles criptográficos en la Universidad de las Fuerzas Armadas, deberá considerarse en los siguientes escenarios: protección de claves de acceso a sistemas, datos, información y servicios; transmisión de información restringida (o susceptible para la institución, cuya pérdida, robo, o alteración sería catastrófica), fuera del ámbito institucional; resguardo de información definida en el análisis de riesgos. (ISO, NTE IEC ISO27002:2005, 2005)

[5] Descomposición y composición de un objeto al viajar a través de una red
[6] Proceso que asigna un código único referente al contenido de algún archivo.

*4.8.3.2. Gestión de claves.*

Un adecuado proceso de gestión de claves en la Universidad de las Fuerzas Armadas, deberá considerar los siguientes aspectos: hágase referencia al punto 4.7.5.3 (Sistema de gestión de contraseñas); adicionalmente, debe incluirse procedimientos de procesamiento que incluyan controles criptográficos en: el almacenado de claves, así como la transaccionalidad[7] de las mismas al ser transmitidas por la red; deberán adicionalmente, gestionarse procesos de revisión de la validez de los algoritmos de encriptación usados y verificar que dicho algoritmo no ha perdido robustez o que puede ser violado fácilmente. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.4. Seguridad de los archivos del sistema.*

*4.8.4.1. Control del software en explotación.*

Las medidas a considerarse ante los riesgos de seguridad que podrían atentar a nivel de las aplicaciones de software de la Universidad de las Fuerzas Armadas, son los siguientes: el proceso de actualización de librerías debe realizarse únicamente por el personal con la autorización del encargado de proyectos de software; como buena norma, las aplicaciones publicadas en producción deberían contener únicamente el código ejecutable de las mismas y el código fuente debería almacenarse en otra localidad diferente; no se deberá publicar aplicaciones en ambiente producción sin que las mismas hayan pasado por la etapa de verificación de aseguramiento de la calidad; se deberá llevar un registro de auditoria sobre las actualizaciones realizadas, junto con las librerías actualizadas; se deberá llevar un control de versiones de las aplicaciones como medida de contingencia ante desastres; el software suministrado por terceros deberá cumplir las consideraciones antes expuestas, con la restricción adicional que asegure que el control de dicho software está bajo el área de proyectos de software de la institución y que bajo ninguna circunstancia, dicho software podrá ser manipulado fuera del ámbito institucional. (ISO, NTE IEC ISO27002:2005, 2005)

[7] Referente a transacciones

*4.8.4.2. Protección de los datos de prueba del sistema.*

La información contenida en la base de datos de pruebas, debería ser en estructura y contenido –dependiendo del caso-, similar a la base de datos de producción, para asegurar de ésta forma la veracidad de: el procesamiento y resultados de las aplicaciones que interactúen con ella; sin embargo se deben considerar los siguientes aspectos en la protección de la información manejada en la base de datos de pruebas: la información supone criticidad por tanto según análisis del personal de Base de Datos y según las circunstancias se deberá alimentar la base de datos de pruebas únicamente con una porción aceptable de datos que refleje el universo de información; el acceso a la base de datos de pruebas deberá considerar los mismos aspectos de seguridad y acceso que se contemplen en la base de datos de producción, es decir, el acceso a la misma será únicamente proporcionado a personal con la autorización adecuada; se deben mantener mecanismos de encriptación y cifrado similares a los empleados en la base de datos de producción. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.4.3. Control de acceso al código fuente de las aplicaciones.*

El objetivo de controlar el acceso al código fuente de las aplicaciones propiedad de la Universidad de las Fuerzas Armadas, es evitar que el mismo sea accedido y modificado y con ello modificarse los procesos originales como fueron concebidos ocasionando perjuicio a la institución, por tanto debe considerarse las siguientes recomendaciones al resguardar el acceso al código fuente de las aplicaciones: se deberá utilizar una herramienta especializada que gestione versionamiento[8] de código fuente; se deben incluir políticas que normen la obligatoriedad entre el grupo de programadores del uso de dicha herramienta de versionamiento de código, incluyéndola en el ambiente de desarrollo de cada programador; se deberán respaldar las versiones del código fuente en localidades de almacenamiento con diferente ubicación física a la que contiene el código fuente compilado y bajo ninguna circunstancia se almacenarán únicamente en los computadores de los programadores. (ISO, NTE IEC ISO27002:2005, 2005)

[8] Referente a las versiones de productos en software.

*4.8.5. Seguridad en los procesos de desarrollo y soporte.*

*4.8.5.1. Procedimientos de control de cambios.*

El procedimiento de control de cambios en las aplicaciones de la Universidad de las Fuerzas Armadas debe ser planificado y controlado, considerando las siguiente recomendaciones: debe generarse un procedimiento que mantenga un protocolo a seguir para cada cambio en los sistemas de información, el cual defina responsables así como detalle de las actividades a realizar, por ejemplo: ejecución de scripts de base de datos, actualización de librerías, actualización de hojas de estilos, etc.; se debe mantener un registro y deben almacenarse cronológicamente las versiones de las aplicaciones para fines de contingencia; se debe usar mecanismos de control de versiones, tanto a nivel procedimental como administrativos; los cambios en las aplicaciones deben realizarse de manera planificada y siguiendo cronogramas en fechas en los cuales su implantación no suponga riesgo organizacional de interrupción del servicio, por tanto se sugiere que los mismos se realicen posteriormente a la jornada laboral o fines de semana. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.5.2. Revisión técnica de las aplicaciones tras cambios en el sistema operativo.*

Cuando se ha realizado el proceso de cambio, se deben implementar políticas que verifiquen que los cambios realizados se han cumplido a cabalidad de acuerdo a los requerimientos de la institución y que no ocurrirán incidentes de fallo tanto en seguridad como en interrupción del servicio tras dicho cambio, por tal motivo, se recomienda se consideren las siguientes recomendaciones a llevarse en dicho proceso de revisión: se deberá contar con copias de respaldo de versiones anteriores de la aplicación para que en caso de fallo de la versión actual, se pueda regresar a la versión anterior estable; se deberá llevar un registro detallado de: librerías, configuraciones, y requerimientos generales para el correcto funcionamiento de una aplicación a la cual se apliquen cambios; se deberá asegurar que el proceso de aseguramiento de la calidad a la aplicación en pruebas cumple a cabalidad los requerimientos solicitados y asignar responsables de dicha revisión pues sin la aprobación expresa del encargado de

pruebas de calidad no se puede proceder a cambios en producción. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.5.3. Restricciones en los cambios a los paquetes de software.*

Al momento de aplicar cambios en las aplicaciones de software de la institución, se deberá considerar los siguientes aspectos: los cambios deben aplicarse únicamente a código fuente que está bajo el control del área de desarrollo de software, es decir, si existen bibliotecas de terceros, debe analizarse el riesgo que implica modificar este tipo de código, así como el impacto en la seguridad que esta acción podría acarrear; adicionalmente los cambios que se hagan si requieren actualización de bibliotecas de terceros, debe considerarse los riesgos de migración de versiones, pues ello podría acarrear impacto sobre el correcto funcionamiento de las aplicaciones; finalmente, cuando se realicen cambios, los mismos deben realizarse coherentemente analizando los flujos y condiciones iniciales del requerimiento y con ellos evitar que cambios o actualizaciones sobre-escriban lógica de negocio funcional de la aplicación. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.5.4. Fugas de Información.*

Un correcto control de fugas de información en la Universidad de las Fuerzas Armadas deberá considerar las siguientes recomendaciones: en caso de adquisición de aplicaciones de software o contratación de servicios, se deberá realizar dicho procesos únicamente con proveedores acreditados; en los procesos de compra de software se debe incluir cláusulas en la que de ser posible la institución obtenga el código fuente de las aplicaciones y con ellos poder auditar dicho código y poder detectar potenciales fallas en la seguridad que provee el mismo; previo al proceso de implementación de una aplicación, el código fuente debería ser revisado en favor de evitar errores de seguridad que pudieran ser inducidos en la plataforma tecnológica de la institución; generar acuerdos en los cuales los empleados tanto internos como externos se comprometan y responsabilicen con el buen uso de la información que a ellos se les suministre; se deberán firmar acuerdos de confidencialidad con los empleados de la

institución, haciendo énfasis en aquellos que manejan información susceptible para la institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.5.5. Externalización del desarrollo de software.*

Al externalizar el proceso de desarrollo de software a terceros, la institución deberá considerar las recomendaciones siguientes: se deben generar políticas robustas de acuerdos de nivel de servicios; se deben generar políticas de acuerdo de licenciamiento y derechos de propiedad intelectual sobre el código fuente; certificación por parte de la empresa contratada sobre la calidad del software y el uso de buenas prácticas internacionalmente aceptadas de ingeniería de software en el desarrollo de la solución; acuerdos de garantías: técnicas, operativas y económicas; sanciones legales en caso de que la parte contratada incumpla el contrato; etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.8.6. Gestión de vulnerabilidades técnicas.*

*4.8.6.1. Control de las vulnerabilidades técnicas.*

Una vez que se ha detectado una vulnerabilidad técnica en una aplicación se software de la institución, se deberán seguir las siguientes recomendaciones: es necesario generar una política que siga un protocolo de las acciones a seguir, iniciando por la notificación de la vulnerabilidad; posteriormente a dicha notificación se deberá analizar: la validez de la misma, junto a los riesgos asociados; y, en dependencia de la criticidad de dicha vulnerabilidad, se iniciará el proceso de corrección de la misma; de ser posible, se evitará interrumpir la entrega de servicio de la plataforma de la institución, pero si por la criticidad de la vulnerabilidad es necesario interrumpir el servicio, deberá notificarse oportunamente a todas las áreas que hagan uso de la funcionalidad que va a interrumpirse; como se ha mencionado en el documento de ser posible la corrección de la vulnerabilidad debería realizarse en un horario y fecha que no afecte a la normal entrega de servicio de la institución; finalmente, se deberá llevar un inventario de vulnerabilidades de las aplicaciones, con rasgos como: fechas de detección, acción tomada para su solución, impacto causada por la misma, usuario que la notificó etc. (ISO, NTE IEC ISO27002:2005, 2005)

## 4.9. Gestión de incidentes de seguridad en la seguridad de la información

### *4.9.1. Notificación de eventos y puntos débiles de seguridad de la información*

#### *4.9.1.1. Comunicación de eventos en seguridad.*

Considérense las recomendaciones indicadas en el punto: 4.8.6.1 (Control y notificación de las vulnerabilidades técnicas)

#### *4.9.1.2. Comunicación de debilidades en seguridad.*

Considérense las recomendaciones indicadas en el punto: 4.8.6.1 (Control y notificación de las vulnerabilidades técnicas)

### *4.9.2. Gestión de incidentes y mejoras en la seguridad de la información.*

#### *4.9.2.1. Responsabilidades y procedimientos.*

A nivel de incidentes y seguridad, se sugiere el uso de: estrategias de monitoreo y alerta que permitan detectar los incidentes que atenten contra la seguridad de la información institucional; adicionalmente, considérese lo siguiente: establecimiento de procedimientos de manejo de incidentes de seguridad: fallos en sistemas de información e discontinuidad en la entrega de servicio, virus y ccódigo fuente malicioso, ataques de denegación de servicio; errores arrojados por no control de excepciones ante información no precisa e incompleta, manipulación de aspectos como confidencialidad e integridad de la información institucional, uso no adecuado de los sistemas de información institucionales.

Debe contarse con un plan de contingencia que cubra: causas de incidentes, acciones correctivas, procedimientos de notificación/comunicación con las partes a cargo de la recuperación del servicio y reporte a autoridades.

Se deberá contar con procesos que proporcionen información de auditoria, y estar en la capacidad de analizar el problema y tomar las acciones necesarias tanto de denuncia a las respectivas autoridades como inicio de acciones legales civiles o penales. (ISO, NTE IEC ISO27002:2005, 2005)

*4.9.2.2. Aprendizaje de los incidentes de seguridad de la información.*

Tras incidentes de seguridad experimentados en la plataforma de la Universidad de las Fuerzas Armadas (sede Matriz), se debe gestionar procedimientos que permitan recolectar toda la información relacionada al evento: incidente, clasificación del mismo, impacto, activos afectados, responsables, medidas de acción para la solución del mismo, estado del evento; adicionalmente, se deberá usar mecanismos que permitan generar una base de conocimientos sólida conformada por la información recolectada en referencia a los incidentes de seguridad. (ISO, NTE IEC ISO27002:2005, 2005)

*4.9.2.3. Recopilación de evidencias.*

El proceso de recolección de evidencias es un proceso de debe estar generalizado en todos los procesos institucionales que empleen infraestructura tecnológica para el desarrollo de los mimos, por tal motivo, se debe contar con políticas que aseguren que los sistemas en software o de procesamiento de información con los que cuenta la institución, cuenten con mecanismos de almacenamiento de evidencias de auditoria, las mismas que deben conformarse como mínimo de: Usuarios que generan acciones, la acción como tal realizada, fecha y hora, equipo desde el que se realizó la acción; se debe considerar adicionalmente que dicha información por ningún motivo pues ser: modificada, eliminada o sobre escrita, por lo que se deberán adoptar las medidas necesarias para que esto no ocurra; se deberá adicionalmente contar con mecanismos que permitan obtener información de auditoria en: discos duros, discos de almacenamiento extraíble así como los rastros de auditoria que se pueda recabar tanto en: red, infraestructura y base de datos. (ISO, NTE IEC ISO27002:2005, 2005)

## 4.10. Gestión de la continuidad del negocio

*4.10.1. Aspectos de la gestión de continuidad del negocio.*

Tras análisis de la información proporcionada por la Unidad de Tecnologías de la Información de la Universidad de las Fuerzas Armadas (sede Matriz), se evidencia que la institución cuenta con un plan de Gestión de Continuidad de Negocio minuciosamente elaborado que cubre los aspectos necesarios a tratarse en el tema de Continuidad del Negocio; sin embargo, se recomienda que dicho documento se añada al presente Plan de Seguridad de la Información de la institución, validándose que se cumplan los temas siguientes sugeridos: incluir el tema de seguridad de la información en la gestión de continuidad del negocio; evaluación de riesgos; marco de referencia para la planificación del proceso de continuidad del negocio y pruebas, mantenimiento y evaluación del plan de continuidad con el que cuenta la institución. (ISO, NTE IEC ISO27002:2005, 2005)

## 4.11. Cumplimiento

### *4.11.1. Conformidad con los requisitos legales.*

#### *4.11.1.1. Identificación de la legislación aplicable.*

En trabajo conjunto, el Director de TI de la Universidad de las Fuerzas Armadas con el Área Legal de la institución, se deberán definir con exactitud los requerimientos: legales, contractuales y normativos dentro de los cuales se pueda desenvolver la gestión tecnológica y seguridad de la información de la institución. (ISO, NTE IEC ISO27002:2005, 2005)

#### *4.11.1.2. Derechos de propiedad intelectual (IPR).*

En trabajo conjunto, el Director de TI de la Universidad de las Fuerzas Armadas con el Área Legal de la institución, se deberán definir procesos que salvaguarden los intereses institucionales en relación a propiedad intelectual, para lo cual se debe considerar: en procesos de compra o contratación de desarrollo de software se deberá tomar en cuenta la propiedad intelectual del código fuente, para que ningún proceso institucional interno viole este derecho de terceros; sin embargo en caso de que formalmente éstos derechos hayan sido cedidos total o parcialmente a la institución, se deberá realizar todas las acciones

para que la institución tenga derechos de: manipulación y modificación de acuerdo a las necesidades institucionales y de ésta manera evitar monopolios de terceros; y, en caso de que una empresa que haya brindado servicios a la institución no ceda los derechos de : manipulación y modificación, se realizará un análisis de costo/ beneficio para la institución y evaluar si la tercerización de dicho servicio en conjunto con los servicios de soporte serán beneficiosos para la institución. Se deberá considerar adicionalmente, aspecto de licenciamiento de aplicaciones, así como los plazos de contrato de los mismos, evitando que los procesos desemboquen en multas o acciones legales en contra de la institución.

La institución, como alternativa al uso de software propietario, podría acudir al software libre, sin embargo, se deberá hacer un análisis concienzudo que verifique si la implantación del mismo supondrá riesgos a la institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.11.1.3. Protección de los documentos de la Organización.*

La protección de los documentos de la Universidad de las Fuerzas Armadas (sede Matriz), deberá contar con procesos y políticas bien definidas que aseguren que no se de: pérdida, hurto y manipulación no permitida. Debe considerarse protección tanto para documentos físicos como lógicos y dependiendo de las características de los mismos se aplicarán controles de protección apropiados para cada tipo. El acceso a documentación deberá restringirse a los roles y permisos adecuados de usuario, los mismos que deben ser analizados en base a la criticidad de la información a manejarse por el usuario. Deberán asegurarse los respectivos controles físicos y lógicos que aseguren: confidencialidad de la información institucional. (ISO, NTE IEC ISO27002:2005, 2005)

*4.11.1.4. Protección de datos y privacidad de la información de carácter personal.*

El Director de TI de la Universidad de las Fuerzas Armadas, deberá sustentarse en procesos y políticas que aseguren la protección de datos e información personal, para lo cual se deberán establecer políticas de control que aseguren los requisitos mínimos y obligatorios de los datos y la información de

carácter personal: confidencialidad, integridad y disponibilidad. (ISO, NTE IEC ISO27002:2005, 2005)

*4.11.1.5. Prevención del uso indebido de recursos de tratamiento de la información.*

La información siendo un recurso en extremo valiosos para los fines institucionales que persigue la Universidad de las Fuerzas Armadas, debe someterse a procesos que aseguren el buen uso que los usuarios hagan de la misma, para lo cual debe considerarse: políticas bien definidas sobre segregación de usuarios y las atribuciones y alcance que cada uno tenga sobre la información y los recursos de tratamiento de la misma; políticas claras que definan responsabilidades de usuarios propietarios sobre los activos de tratamiento de información, así como definición clara de normativa, sanciones y acciones legales sobre los usuarios que hagan mal uso de los activos de tratamiento de información. (ISO, NTE IEC ISO27002:2005, 2005)

*4.11.1.6. Regulación de controles de criptográficos.*

Para la regulación de controles criptográficos se deberá considerar: la normativa legal vigente relacionada a comercio electrónico y uso de información cifrada, así como el uso de firmas electrónicas; se deberá definir la sensibilidad de la información que maneja la institución, en base a lo cual se definirán políticas sobre el uso de controles criptográficos en la información. (ISO, NTE IEC ISO27002:2005, 2005)

*4.11.2. Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.*

*4.11.2.1. Cumplimiento de las políticas y normas de seguridad*

Esta medida deberá tomarse a nivel de los Directores departamentales de la Universidad de la Fuerzas Armadas (sede Matriz), quienes rigurosamente deberán revisar el cumplimiento de las políticas y normas de seguridad de los trabajadores a su cargo; dicha revisión de cumplimiento deberá: verificar el cumplimiento, analizar causas de incumplimiento y reportar las mismas para que sean sujeto de análisis inter institución y acreditar la validez de las mismas así como reporte de los fallos de las mismas y analizar su potencial re

estructuración, modificación, ampliación o de ser el caso proceder con su eliminación. (ISO, NTE IEC ISO27002:2005, 2005)

*4.11.2.2. Comprobación del cumplimiento técnico.*

La comprobación del cumplimiento técnico deberá realizarse por un delegado del área de Tecnologías de la Información de la institución (sede Matriz), quien desde una perspectiva sistemática y haciendo uso de herramientas tecnológicas que permitan medir el cumplimiento y la efectividad de las políticas y normas de seguridad implantadas en la organización, genere reportes numéricos porcentuales que reflejen la realidad del cumplimiento organizacional y que dichos resultados sirvan de insumo a un proceso de comprobación que permita: analizar potenciales re estructuraciones, modificación, ampliación o de ser el caso proceder con la eliminación de políticas o normas usadas en la institución. (ISO, NTE IEC ISO27002:2005, 2005)

*4.11.3. Consideraciones sobre la auditoria de los sistemas de información.*

*4.11.3.1. Controles de auditoria de los sistemas de información.*

Es necesario que existan controles de auditoria de los sistemas de información que maneja la Universidad de las Fuerza Armadas, pues los mismos asegurarán que exista trazabilidad hacia incidentes o acciones voluntarias o involuntarias que atenten contra la seguridad de la información y los atributos mínimos y obligatorios que la información institucional debe tener: confidencialidad, integridad y disponibilidad. Es necesario que los registros de auditoria como se ha mencionado previamente muestren información completa de las actividades en la plataforma tecnológica de la institución, por tal motiva los controles de auditoria sobre los sistemas de información de la institución deberán contener: fechas y hora de actividad, usuarios que realizan la actividad, terminal o dirección IP desde la cual se genera la acción; información que ha sido sujeto de manipulación, etc. (ISO, NTE IEC ISO27002:2005, 2005)

*4.11.3.2. Protección de las herramientas de auditoría de los sistemas de información.*

La herramientas de auditoria de los sistemas de información empleados en la Universidad de las Fuerzas Armadas (en su sede Matriz), deberán poseer controles rigurosos que aseguren la protección de las mismas, pues el nivel de importancia de estos registros de auditoria está en directa proporción a la propia información que la información resguarda. (ISO, NTE IEC ISO27002:2005, 2005)