UNIVERSIDAD DE CUENCA

FACULTAD DE INGENIERIA

MAESTRIA EN GESTIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

PROYECTO DE TITULACIÓN

DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (DTIC) DE LA UNIVERSIDAD DE CUENCA

PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN GESTIÓN ESTRATÉGICA DE TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN.

AUTOR: Ing. Juan Diego Muñoz Ñauta.
CI: 0103403317

DIRECTOR: Ing. Diego Arturo Ponce Vásquez, PhD.
CI: 0101822609

CUENCA- CUADOR
2016

Resumen

El presente trabajo de tesis consiste en el diseño de políticas de seguridad informática para las tres Unidades que conforman la Dirección de Tecnologías de Información y Comunicación (DTIC): Servicios Informáticos, Sistemas de Información, Redes y Comunicaciones. Para desarrollar de manera eficiente el trabajo de investigación se utilizarán las recomendaciones que sugieren la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009. Manual de Políticas de Seguridad Informática-Mejores Prácticas Internacionales y otros documentos referentes a la seguridad informática.

En el capítulo 1 se revisarán aspectos generales como la problemática, antecedentes, justificación, objetivos. En el capítulo 2 se citarán algunos términos y definiciones, se revisará la estructura de la norma NTE INEN-ISO/IEC 27002:2009, se levantará información de los activos. En el capítulo 3, se analizará el cumplimiento de los controles se seguridad informática que tiene la DTIC, se determinará los dominios de seguridad informática en base al resultado de la información obtenida por medio de visitas de campo, entrevistas al personal. En el capítulo 4 se diseñará las políticas principales y complementarias más relevantes para la DTIC que permitan mejorar los porcentajes de cumplimiento. Finalmente en el capítulo 5 se citarán algunas conclusiones y recomendaciones, adicional se elaborará un documento de políticas para entregar a la DTIC.

Palabras Claves: Políticas de seguridad informática, Tecnologías de Información y Comunicación, norma NTE INEN ISO/IEC 27002.

Abstract

This thesis consists in the design of security policies for the three units that make up the DTIC: Computer Services, Information Systems, and Networks and Communications. To get an efficient development of the research the recommendations suggested by the Ecuadorian Technical Standard NTE INEN ISO / IEC 27002:2009, will be used. They are: The Information Technology and Communication Security Policy Manual - International Best Practices and other documents related to the information technology security.

In Chapter 1, general aspects as: problems, background, justification, objectives. In chapter 2 some terms and definitions will be cited. The structure of the norm NTE INEN ISO / IEC 27002: 2009 will be reviewed. The information about assets will be collected. In chapter 3, the execution of the information technology and communication security controls from DTIC department will be analyzed. The security domains will be determined based on the results of information obtained through field visits and staff interviews. In chapter 4 the most relevant, principal and complementary politics, to DTIC will be designed to improve execution rates. Finally, in Chapter 5 some conclusions and recommendations will be written. Additionally, a policy document will be prepared to deliver to DTIC.

Keywords: Computer Security Policy, Information Technology and Communication, NTE INEN standard ISO / IEC 27002.

Índice General

Índice de Gráficos

Índice de tablas

Yo Juan Diego Muñoz Ñauta, autor del proyecto de tesis "DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (DTIC) DE LA UNIVERSIDAD DE CUENCA", reconozco y acepto el derecho que tiene la Universidad de Cuenca, en base al Art. 5 literal c) de su Reglamento de Propiedad Intelectual, de publicar este trabajo por cualquier medio conocido o por conocer, al ser este requisito para la obtención de mi título de Magister en Gestión Estratégica de Tecnologías de Información y Comunicación. El uso que la Universidad de Cuenca hiciere del presente trabajo, no implicará afección alguna de mis derechos morales o patrimoniales como autor.

Cuenca, 10 de octubre del 2016

Juan Diego Muñoz

CI: 0103403317

Yo Juan Diego Muñoz Ñauta, autor de la tesis "DISEÑO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (DTIC) DE LA UNIVERSIDAD DE CUENCA", certifico que todas las opiniones, ideas y contenidos expuestos en la presente trabajo de investigación son de exclusiva responsabilidad de su autor.

Cuenca, 10 de octubre del 2016

Juan Diego Muñoz

CI: 0103403317

AGRADECIMIENTOS

Un agradecimiento especial a la Universidad de Cuenca por la oportunidad brindada para culminar mis estudios de Maestría, en especial a los miembros que conforman la Dirección de Postgrados, docentes y a todo el personal de apoyo.

A la Dirección de Tecnologías de la Información y Comunicación (DTIC) de la Universidad de Cuenca, y especialmente al Ing. Patricio Guerrero Villavicencio su Director, por la apertura brindada para el desarrollo del presente proyecto de investigación y a todo el personal por todo el apoyo brindado.

Un sincero agradecimiento al Ing. Diego Ponce PhD, por el valioso aporte brindado durante todo el desarrollo del presente estudio.

Juan Diego Muñoz.

DEDICATORIA

Una especial dedicatoria a mi familia, en especial a mi esposa Angélica por el apoyo incondicional, a mis hijas Amy Nicole y Carol Lizeth, por ser mi inspiración para culminar los estudios y compartir mis logros.

Juan Diego Muñoz.

CAPÍTULO 1

1.1. Introducción

Los sistemas informáticos, los equipos de computación, la información generada por las organizaciones, empresas, establecimientos educativos, etc., tienen gran importancia y deben estar debidamente controladas y protegidas. Una alternativa es la implementación de políticas de seguridad informática para garantizar la continuidad del negocio.

Con el incremento de la infraestructura tecnológica de la Universidad de Cuenca, se incrementa la cantidad de usuarios, divisiones departamentales, equipos de comunicación; lo que genera la necesidad de implementar nuevos mecanismos de seguridad que permitan mantener la integridad, disponibilidad y confidencialidad de la información. El adecuado funcionamiento del equipamiento informático, sistemas informáticos, equipos de comunicación deben ir ligados con una correcta selección de controles que permitan alcanzar los intereses institucionales.

1.2. Antecedentes

El presente trabajo se realizará en la Dirección de Tecnologías de Información y Comunicación (DTIC) de la Universidad de Cuenca, la cual está conformada por las siguientes unidades:

Sistemas de información: Aquí se administran los sistemas informáticos, también se desarrollan los nuevos sistemas institucionales.

Redes y Comunicaciones: Aquí se administran los servidores, las redes informáticas, la telemática.

Servicios Informáticos: Aquí se administra el servidor de antivirus, servidor Microsoft

En un estudio inicial se determinó que la Universidad de Cuenca está invirtiendo en sistemas de seguridad físicos como firewalls, dotación de nuevos servidores para mantener la información en la nube, implementación de routers inalámbricos de largo alcance, lo que contribuye a alcanzar las metas propuestas por las autoridades para lograr que la Universidad de Cuenca sea un establecimiento pionero en investigación, cuidado del medio ambiente, incorporando profesionales de alto nivel a la sociedad.

Estas metas demandan un incremento en la infraestructura tecnológica, incrementando el equipamiento informático, creando, mejorando e innovando los sistemas informáticos institucionales. Lo que conlleva a la creación, modificación y actualización de algunos mecanismos de seguridad como por ejemplo: políticas de seguridad informática, para estar preparados ante nuevas amenazas como por ejemplo: virus, spam, ataques, pérdida de la información sea voluntaria o involuntaria.

1.3. Justificación

Los sistemas informáticos, equipos de computación y en especial la información digital son de vital importancia para cualquier organización, establecimiento o entidad sea público o privada. Para la Universidad de Cuenca disponer de la información administrativa, contable, académica en cualquier momento manteniendo la disponibilidad, integridad y confidencialidad de los datos es crucial. Ninguna entidad está exenta de riesgos, amenazas y nadie tiene el 100% de seguridad.

Con el diseño de políticas de seguridad informática que más se ajusten a las necesidades actuales de la Universidad, se pretende reducir el impacto al mínimo posible ante un riesgo de seguridad. Otras de las razones importantes para el desarrollo

de este proyecto es el creciente avance tecnológico que experimenta nuestro país, así como también el avance en nuevas formas, procedimientos, amenazas informáticas que pudieran poner en riesgo a la Universidad.

1.4. Problemática

Una de las principales preocupaciones que tiene la DTIC es mantener bajo control cualquier tipo de riesgos de seguridad informática, por ejemplo las amenazas intencionales y no intencionales.

"Amenazas intencionales: en caso de que deliberadamente se intente producir un daño (por ejemplo el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).

Amenazas no intencionales: en donde se producen acciones u omisiones que si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales)", **(Luján, 2015).**

En un pre análisis se determinó que existen pocas políticas de seguridad informática las mismas que no están debidamente definidas y son desconocidas por la mayoría del personal que allí labora, al no disponer de una adecuada lista de políticas de seguridad y de otros mecanismos complementarios se estaría en un estado de vulnerabilidad en el momento que se presente algún tipo de amenaza informática.

Con la elaboración del presente trabajo se pretende hacer un análisis de la situación actual y diseñar políticas de seguridad informática que más se ajusten a las necesidades actuales que tiene la DTIC.

1.5. Objetivos:

1.5.1. Objetivo General

- Analizar, diseñar políticas de seguridad Informática para la DTIC, en base a la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27002:2009, manual de Políticas de Seguridad Informática-Mejores Prácticas Internacionales.

1.5.2. Objetivos Específicos

- Obtener información del personal que administra los diferentes sistemas informáticos, equipos de comunicación y computación, mediante visitas de campo, entrevistas.
- Analizar el estado actual de la seguridad informática de las tres Unidades que conforman la DTIC.
- Diseñar las políticas de seguridad informática que más se ajusten a las necesidades de cada una de las tres unidades de la DTIC.
- Entregar a la DTIC un documento de políticas de seguridad informática en base de mejores prácticas.

1.6. Alcance

El presente trabajo se basará en un análisis de la situación actual de toda la DTIC, se analizará y cuantificará el cumplimiento actual de la seguridad informática con el apoyo de los controles de la Norma Ecuatoriana NTE INEN-ISO/IEC 27002:2009, se tomará lo más relevante de la norma para identificar los puntos más débiles y seleccionar los controles adecuados.

Con el apoyo del manual de Políticas de Seguridad Informática-Mejores Prácticas Internacionales se diseñará las políticas de seguridad informática y se elaborará el documento que se entregará a la dirección de la DTIC.

CAPÍTULO 2

2.1. Normativa de seguridad informática en Ecuador

"*mediante Acuerdos Ministeriales Nos. 804 y 837 de 29 de julio y 19 de agosto de 2011, respectivamente, la Secretaría Nacional de la Administración Pública creó la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación conformada por delegados del Ministerio de Telecomunicaciones y de la Sociedad de la Información, la Secretaría Nacional de Inteligencia y la Secretaría Nacional de la Administración Pública y dentro de sus atribuciones tiene la de establecer lineamientos de seguridad informática, protección de infraestructura computacional y todo lo relacionado con ésta, incluyendo la información contenida para las entidades de la Administración Pública Central e Institucional*", **(EGSI, 2013).**

Desde el año 2011, la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación del Ecuador desarrolló un Esquema Gubernamental de Seguridad de la Información (EGSI), el cual está elaborado en base a la norma NTE INEN-ISO/IEC 27002:2009 (Adopción idéntica de la norma internacional ISO/IEC 27002:2005), debido a que las Tecnologías de la Información y Comunicación son herramientas imprescindibles para el cumplimiento de la gestión institucional de cualquier entidad pública, por lo que deben cumplir con estándares de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información.

Las entidades gubernamentales ecuatorianas que dependan directamente de la Función Ejecutiva tienen la obligación de implementar un EGSI en sus establecimientos. El tiempo, alcance, selección de controles dependerá directamente de cada institución de acuerdo a su ámbito de acción, estructura orgánica, nivel de madurez de la institución, etc.

En el gráfico 1 se puede apreciar las 10 primeras entidades públicas en un ranking de cumplimiento en la implementación del EGSI en Ecuador, **(Implementación EGSI, 2014)**.

RANKING	ENTIDAD	SIGLAS	EGSI: # DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % DE HITOS CUMPLIDOS DEL TOTAL (126)	EGSI: % CALIDAD DE VERIFICABLES DE LOS HITOS EN EL GPR
1	Dirección Nacional de Registro de Datos Públicos	DINARDAP	122	96,83%	76,20%
2	Instituto Nacional de Economía Popular y Solidaria	IEPS	112	88,89%	99,60%
3	Ministerio de Turismo	MINTUR	107	84,92%	100,00%
4	Banco Central del Ecuador	BCE	107	84,92%	95,60%
5	Secretaría Nacional de Inteligencia	SENAIN	101	80,16%	50,19%
6	Consejo Nacional de Control de Sustancias Estupefacientes y Psicotrópicas	CONSEP	100	79,37%	95,80%
7	Ministerio de Educación	MINEDUC	100	79,37%	100,00%
8	Servicio de Rentas Internas	SRI	98	77,78%	56,12%
9	Secretaría Técnica de Discapacidades	SETEDIS	94	74,60%	93,00%
10	Secretaría Nacional de Planificación y Desarrollo	SENPLADES	82	65,08%	90,44%

Gráfico 1: Entidades Públicas en implementar EGSI

El ranking fue realizado en el año 2014, las 10 primeras entidades públicas son las que tienen el mayor porcentaje de hitos cumplidos al implementar el EGSI de un total de 64 entidades evaluadas, en el listado no se encontró ninguna institución de educación pública.

2.2. Marco Referencial

A continuación se cita algunos conceptos que se van a utilizar para el desarrollo del presente trabajo, muchos de los cuales son utilizados por la norma NTE INEN-ISO/IEC 27002:2009.

2.2.1. Términos y definiciones:

- "***Control:*** *Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de*

naturaleza legal. También se utiliza como sinónimo de salvaguarda o contramedida.

- ***Lineamiento:*** *Una descripción que aclara qué se debiera hacer y cómo, para lograr los objetivos establecidos en las políticas.*
- ***Seguridad de la información:*** *Preservación de confidencialidad, integración y disponibilidad de la información; además, también puede involucrar otras propiedades como autenticidad, responsabilidad, no repudiación y confiabilidad.*
- ***Análisis del riesgo:*** *Proceso general del análisis del riesgo y la evaluación del riesgo.*
- ***Evaluación del riesgo:*** *Proceso de comparar el riesgo estimado con un criterio de riesgo dado para determinar la importancia del riesgo.*
- ***Política:*** *Intención y dirección general expresada formalmente por la gerencia.*
- ***Tratamiento del riesgo****: Proceso de selección e implementación de medidas para modificar el riesgo.*
- ***Amenaza:*** *Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema u organización.*
- ***Vulnerabilidad:*** *La debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas."* , **(INEN 27002, 2009)**
- ***Seguridad informática:*** *"conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información* **(Mifsud, 2012)**

2.2.2. Estructura de la norma NTE INEN-ISO/IEC 27002:2009

La norma está conformada por 11 dominios principales, 39 objetivos de control y 133 controles, a continuación se va a detallar la estructura de la norma respetando la numeración original de la norma internacional ISO/IEC 27002:2005, como se indica a continuación:

"*Dominios (11), Objetivos de control (39), Controles (133)*

5. POLÍTICA DE SEGURIDAD.
- ***5.1 Política de seguridad de la información.***
  - *5.1.1 Documento de política de seguridad de la información.*
  - *5.1.2 Revisión de la política de seguridad de la información.*

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.
- ***6.1 Organización interna.***
  - *6.1.1 Compromiso de la Dirección con la seguridad de la información.*
  - *6.1.2 Coordinación de la seguridad de la información.*
  - *6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.*
  - *6.1.4 Proceso de autorización de recursos para el tratamiento de la información.*
  - *6.1.5 Acuerdos de confidencialidad.*
  - *6.1.6 Contacto con las autoridades.*
  - *6.1.7 Contacto con grupos de especial interés.*
  - *6.1.8 Revisión independiente de la seguridad de la información.*
- ***6.2 Terceros.***
  - *6.2.1 Identificación de los riesgos derivados del acceso de terceros.*
  - *6.2.2 Tratamiento de la seguridad en la relación con los clientes.*
  - *6.2.3 Tratamiento de la seguridad en contratos con terceros.*

7. GESTIÓN DE ACTIVOS.
- ***7.1 Responsabilidad sobre los activos.***
  - *7.1.1 Inventario de activos.*
  - *7.1.2 Propiedad de los activos.*
  - *7.1.3 Uso aceptable de los activos.*
- ***7.2 Clasificación de la información.***
  - *7.2.1 Directrices de clasificación.*
  - *7.2.2 Etiquetado y manipulado de la información.*

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- ***8.1 Antes del empleo.***
  - *8.1.1 Funciones y responsabilidades.*
  - *8.1.2 Investigación de antecedentes.*
  - *8.1.3 Términos y condiciones de contratación.*
- ***8.2 Durante el empleo.***
  - *8.2.1 Responsabilidades de la Dirección.*
  - *8.2.2 Concienciación, formación y capacitación en seguridad de la información*
  - *8.2.3 Proceso disciplinario.*
- ***8.3 Cese del empleo o cambio de puesto de trabajo.***
  - *8.3.1 Responsabilidad del cese o cambio.*
  - *8.3.2 Devolución de activos.*
  - *8.3.3 Retirada de los derechos de acceso.*

9. SEGURIDAD FÍSICA Y DEL ENTORNO.
- ***9.1 Áreas seguras.***
  - *9.1.1 Perímetro de seguridad física.*
  - *9.1.2 Controles físicos de entrada.*
  - *9.1.3 Seguridad de oficinas, despachos e instalaciones.*
  - *9.1.4 Protección contra las amenazas externas y de origen ambiental.*
  - *9.1.5 Trabajo en áreas seguras.*

13.2.3 Recopilación de evidencias.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.

14.1.2 Continuidad del negocio y evaluación de riesgos.

14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.

14.1.4 Marco de referencia para la planificación de la continuidad del negocio.

14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.

15. CUMPLIMIENTO.

15.1 Cumplimiento de los requisitos legales.

15.1.1 Identificación de la legislación aplicable.

15.1.2 Derechos de propiedad intelectual (DPI).

15.1.3 Protección de los documentos de la organización.

15.1.4 Protección de datos y privacidad de la información de carácter personal.

15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.

15.1.6 Regulación de los controles criptográficos.

15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.

15.2.1 Cumplimiento de las políticas y normas de seguridad.

15.2.2 Comprobación del cumplimiento técnico.

15.3 Consideraciones sobre las auditorías de los sistemas de información.

15.3.1 Controles de auditoría de los sistemas de información.

15.3.2 Protección de las herramientas de auditoría de los sistemas de información." **(ISO/IEC 27002, 2005)**

Los controles más utilizados según la norma ecuatoriana NTE INEN-ISO/IEC 27002:2009 catalogados como esenciales para la mayoría de entidades públicas incluyen lo siguiente:

"a) Protección de datos y privacidad de la información personal;

b) Protección de los registros organizacionales;

c) Derechos de propiedad intelectual", **(INEN 27002, 2009).**

La selección de controles dependerá de cada entidad, su estructuración, metas, nivel de madurez, tipo de empresa, se deberá definir cuantos controles serán realmente necesarios.

2.3. Dirección de Tecnologías de la Información y Comunicación (DTIC)

"La Dirección de Tecnologías de Información y Comunicación (DTIC) de la Universidad de Cuenca, fue creada con la aprobación del Estatuto de la Institución mediante resolución del Consejo de Educación Superior del 18 de diciembre del 2013.

La DTIC es el órgano encargado de la gestión, coordinación y ejecución de proyectos en el ámbito de las tecnologías de información y comunicación, orientado al mejoramiento de la calidad académica y administrativa de la Universidad; adicionalmente es de su responsabilidad la operación y mantenimiento de los sistemas de información y de la infraestructura de tecnológica, la seguridad de la información y las instalaciones, y el soporte a usuarios. La DTIC tiene tres coordinaciones: Sistemas de Información, Redes y Comunicaciones, y Servicios Informáticos", **(ucuenca, 2014).**

Antes la DTIC era conocida como el Departamento de desarrollo Informático (DDI) que básicamente tenía la misma estructura, con la creación y aprobación del Consejo Universitario, la DTIC tiene nuevas funciones y su estructura se fortalece con la incorporación de coordinadores para sus tres Unidades internas, cada Unidad tiene establecidas sus funciones y los perfiles para el personal que allí laboran.

2.3.1. Misión:

"La Dirección de Tecnologías de Información y Comunicación, es el órgano encargado de la gestión, coordinación y ejecución de proyectos en el ámbito de las tecnologías de información y comunicación, orientados al mejoramiento de la calidad académica y administrativa de la Universidad." **(Dirección TI, 2013)**

2.3.2. Estructura organizativa

La estructura organizativa de la DTIC aprobada por el Consejo de Educación Superior en el año 2013 está establecida de la siguiente manera:

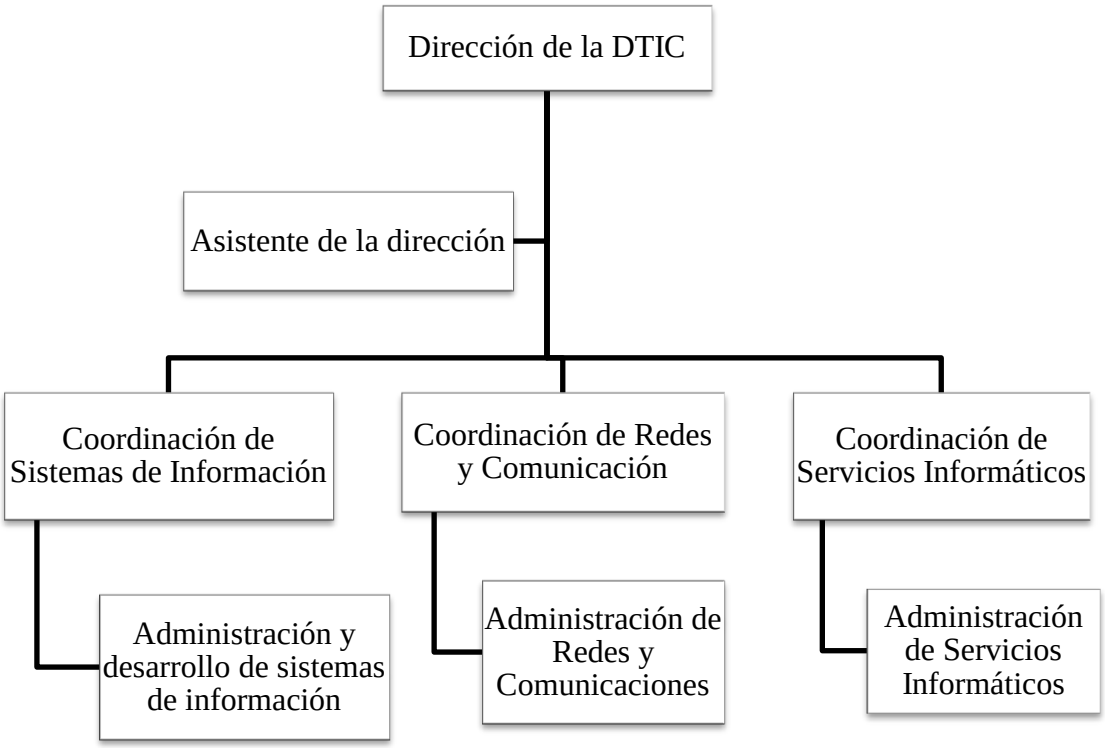

Gráfico 2: Estructura de la DTIC

La DTIC está organizada de la siguiente forma:

Dirección de la DTIC: Dirige, administra, coordina y supervisa las actividades de las tres unidades de la DTIC, está en contacto directo con las autoridades universitarias.

Asistente del director: Es la secretaria y cumple funciones administrativas de la dirección.

Coordinación de Sistemas de Información: Coordina, organiza y supervisa el desarrollo, mantenimiento y actualizaciones de los sistemas informáticos institucionales.

Administración y desarrollo de sistemas de información: Desarrollo, administración, actualización los sistemas informáticos institucionales como por ejemplo: SIUC, ESIUC, sistema financiero. El personal que aquí labora son

considerados como especialistas de soporte de segunda línea de la Unidad de Sistemas de Información.

Coordinación de Redes y Comunicaciones: Organiza, supervisa la administración del Data Center, equipos de comunicación (routers, switchs, telefonía IP), servidores de: correo, sistemas institucionales SIUC, ESIUC, Quipux.

Administración de Redes y Comunicaciones: Administra los servidores institucionales, administran el Data Center, equipos de comunicación, el personal que aquí labora son considerados como especialistas de soporte de segunda línea de la Unidad de Redes y Comunicaciones.

Coordinación de Servicios Informáticos: Organiza, coordina y supervisa las actividades de soporte a usuarios finales, administración del sistema de voto electrónico, sistema de antivirus, administración del sistema de Help Desk.

Administración de Servicios Informáticos: Administra, instala, actualiza, ejecuta el mantenimiento a los computadores, instala paquetes de ofimática, el personal que aquí labora son considerados como soporte de primera línea de la Unidad de Servicios Informáticos.

Se tiene conocimiento que el nuevo director de TIC va a proponer a las autoridades Universitarias la creación de la coordinación de Gestión de Proyectos, para agilitar el desarrollo e implementación de los proyectos que tiene la DTIC a corto y largo plazo.

2.3.3. Levantamiento de activos informáticos

A continuación se va a detallar el hardware, software de los computadores, impresoras, equipos de comunicación, servidores, bases de datos que se utilizan en la DTIC.

2.3.3.1. Estaciones de trabajo e impresoras

A continuación se va a detallar los equipos informáticos que se encuentran en la DTIC:

Cantidad	Tipo	Detalle	Ubicación
1	Portátil	Windows 7 pro	Dirección de TI
1	CPU	Windows 7 pro	Dirección de TI
1	Impresora	Laser Monocromática	Dirección de TI
1	CPU	Windows 7 XP	Asistente del Director de TI
1	Impresora	Laser Monocromática	Asistente del Director de TI
1	Portátil	Windows 7 pro	Sistemas de Información
7	CPU	Windows 7 pro	Sistemas de Información
1	Impresora	Laser Monocromática	Sistemas de Información
5	CPU	Windows 7 pro	Centro de desarrollo de Software
1	Impresora	Laser Monocromática	Centro de desarrollo de Software
1	Portátil	Windows 7 pro	Redes y Comunicaciones
3	CPU	Windows 7 pro	Redes y Comunicaciones
3	CPU	Linux	Redes y Comunicaciones
1	Impresora	Laser Monocromática	Redes y Comunicaciones
1	Portátil	Windows 7 pro	Servicios Informáticos
6	CPU	Windows 7 pro	Servicios Informáticos
1	Impresora	Laser Monocromática	Servicios Informáticos

Tabla 1: Detalle de equipos informáticos de la DTIC

Los computadores con sistemas operativos Windows utilizan paquetes de ofimática Office 2010 y 2013, cabe indicar que la Universidad tiene licenciamiento Microsoft lo

cual permite mantener a los computadores con las últimas actualizaciones y parches de seguridad.

La DTIC cuenta con la protección del antivirus Kaspersky End Point instalado en un servidor central con una consola de administración, se cuenta con servidores esclavos alojados en las diferentes facultades de la Universidad.

2.3.3.2. Servidores

En la siguiente tabla se puede apreciar el detalle de los servidores que se encuentran en el Data Center de la DTIC.

Cantidad	Aplicación	S.O.	Ubicación	Detalle
1	DNS	CentosOS 7	Data Center	Servidor Virtual
4	OwnCloud	Debian 6	Data Center	Servidor Virtual
1	Web Conference	Ubuntu 14	Data Center	Servidor Virtual
2	Aplicaciones	WS 2003 R3	Data Center	Servidor Virtual
1	Desarrollo	WS 2003 R3	Data Center	Servidor Virtual
2	Domino AD	WS 2008 R2	Data Center	Servidor Virtual
2	Open ERP	Ubuntu 14	Data Center	Servidor Virtual
1	E Virtual	CentOS5	Data Center	Servidor Virtual
1	Portal Web	CentosOS 7	Data Center	Servidor Virtual
1	SRA	WS 2008 R2	Data Center	Servidor Virtual
4	Base de Datos	CentosOS 6	Data Center	Servidor Virtual
1	Antivirus	WS 2003 R3	Data Center	Servidor Virtual
2	Correo electrónico	CentosOS 6	Data Center	Servidor Virtual
1	LDAP	CentosOS 6	Data Center	Servidor Virtual

Tabla 2: Detalle de los servidores de la DTIC

Los servidores virtuales se encuentran alojados en dos servidores físicos IBM tipo blade ubicados en el Data Center de la DTIC, El Data Center cuenta con sistemas de protección contra incendios, controles de acceso, sistemas de suministro de energía eléctrica. El Data Center de la DTIC cuenta con sistemas de respaldos en cinta para almacenar la información generada por los sistemas informáticos y mantenerlos en lugares seguros, por medio de un convenio se está alojando respaldos de información de la Universidad de Cuenca en los servidores de la Escuela Politécnica del Litoral (ESPOL).

2.3.3.3. Equipos de comunicación

A continuación se detallan los equipos de comunicación:

Cantidad	Ubicación	Marca	Modelo
12	Facultades	Cisco	3560
138	Facultades	Cisco	2960
220	Facultades	Ruckus	T300
1	Administración Central	Cisco	3560
30	Administración Central	Cisco	2960
1	Administración Central	Cisco	6500
1	Administración Central	Cisco	4500

Tabla 3: Detalle de los equipos de comunicación de la DTIC

Los equipos de comunicación Cisco son administrados por la unidad de Redes y Comunicaciones, la red LAN se encuentra segmentada por VLANs para proteger la información universitaria, administrar y controlar el acceso de los usuarios. Se tiene conocimiento que la Universidad ha invertido en soluciones de seguridad como

Firewall, sistema de detección de intrusos, mecanismos de control de SPAM para el correo electrónico.

2.3.3.4. Bases de datos

A continuación se detallan las bases de datos que son utilizadas por los diferentes sistemas informáticos:

Aplicación	Servidor	S.O.	Base de Datos	Versión
Sistemas académicos SIUC, eSIUC	Virtual	CentOS 5	Oracle	11.2
Sistema de autenticación	Virtual	CentOS 6	Oracle	11.2
Sistema de asistencia	Virtual	CentOS 6	Oracle	11.2
Sistema EVirtual	Virtual	CentOS 5	Oracle	11.2
Portal Web	Virtual	CentOS 7	MySQL	5.5.3
Sistemas Financiero y Talento Humano	Físico	OS / 400	AS400	V5R3M0

Tabla 4: Detalle de las bases de datos

El personal de desarrollo tiene permiso total a las bases de datos “Oracle”, el personal que administra los sistemas informáticos tiene permiso solo para hacer consultas, el administrador del Portal Web tiene permiso total a la base de datos “MySQL”, el administrador del sistema Financiero y Talento Humano tiene permiso total a la base de datos “AS400”. Los usuarios que utilizan los diferentes sistemas informáticos tienen permiso para ingresar y hacer consultas de información. De lo que se tiene conocimiento existe un proceso para hacer respaldos automáticos de la información de las diferentes bases de datos, el cual es ejecutado todos los días en las noches.

Nota: La información de la DTIC fue obtenida con fecha de corte en febrero de 2016

CAPÍTULO 3

3.1. Análisis de las políticas de seguridad informática actuales de la DTIC.

Para realizar el análisis y determinar el grado de madurez que tienen las actuales políticas de seguridad informática de la DTIC, se va a apoyar en la traducción al español de la norma internacional ISO/IEC 27002:2005 que está disponible en internet bajo el nombre de "iso 27002 wiki zoho", **(ISO27002 , 2015),** como lo utilizaron Daniel Romo y Joffre Valarezo en su tesis de pregrado, **(Romo & Valarezo, 2012)**. Debido a que la norma ecuatoriana NTE INEN-ISO/IEC 27002:2009 es la adopción idéntica de la norma internacional ISO/IEC 27002:2005, con algunos cambios en ciertas palabras en la traducción al español ajustándolo a nuestra región.

Se va a realizar una evaluación de los 133 controles de la norma ISO 27002 estableciendo un porcentaje estimado de cumplimiento para cada control, para poder obtener una cuantificación del porcentaje total de cumplimiento actual que tiene la DTIC.

3.1.1. Revisión del cumplimiento de la seguridad informática de la DTIC, basado en los controles de la norma ISO 27002.

Para la revisión del cumplimiento de la seguridad informática en la DTIC, se va a respetar la numeración original de los controles de la norma internacional ISO 27002, los porcentajes de cumplimiento fueron definidos con el personal de la DTIC, se va a utilizar un rango que va desde el 10% al 100% de cumplimiento para cada uno de los 133 controles.

El porcentaje de cumplimiento para cada control es el resultado del promedio de todos los porcentajes proporcionados por los entrevistados para un determinado control, por ejemplo:

Para obtener el porcentaje de cumplimiento "30%" para el control: "*La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes*", del dominio "5.Políticas de seguridad de la información", se procedió de la siguiente manera:

Si tres funcionarios de la DTIC establecieron los porcentajes de cumplimiento: 20, 40 y 30 respectivamente para éste control, el porcentaje final es el promedio de los tres valores: (20+40+30) /3 = 30%.

El análisis y la obtención de los porcentajes de cumplimiento para cada uno de los 133 controles se encuentran detallados en el Anexo A.

Nota: La información obtenida del personal que labora en la DTIC para realizar una cuantificación del porcentaje de cumplimiento actual, se realizó con fecha de corte en marzo de 2016

3.1.2. Análisis de la situación actual de la DTIC.

De acuerdo a la estructura de la Norma ISO 27002, los 133 Controles de seguridad se agrupan en 39 Objetivos de Control y estos a su vez se organizan en 11 Dominios. Con el apoyo de los 133 controles de seguridad, se avaluó la información que fue proporcionada por el personal que labora en cada una de las tres Unidades que conforman la DTIC. Se utilizó un cálculo de indicadores similares a los que se utiliza en la medición de gestión, como lo utilizó el Ing. Darwin Lanche en su tesis de maestría, **(Lanche, 2015)**.

Para cuantificar el porcentaje de cumplimiento total que tiene la DTIC con respecto a la seguridad informática, se definió un "peso" máximo de 100 para

cada uno de los 11 dominios, de la misma forma se estableció un rango de "pesos" que van desde 10 hasta 100 para cada Objetivo de control, cada peso que se estableció para los 39 Objetivos de control fueron considerados en base a la actividades que realizan a diario el personal que labora en la DTIC, de tal manera que la suma de varios Objetivos de control no sobrepasen al "peso" total de su respectivo dominio (100), como se puede apreciar a continuación:

Dominios, Objetivos de Control	Peso Dominio	Peso Objetivo de Control
5. POLÍTICA DE SEGURIDAD.	**100**	
5.1 Política de seguridad de la información.		**100**
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN.	**100**	
6.1 Organización interna.		**50**
6.2 Terceros.		**50**
7. GESTIÓN DE ACTIVOS.	**100**	
7.1 Responsabilidad sobre los activos.		**60**
7.2 Clasificación de la información.		**40**
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**100**	
8.1 Antes del empleo.		**30**
8.2 Durante el empleo.		**30**
8.3 Cese del empleo o cambio de puesto de trabajo.		**40**
9. SEGURIDAD FÍSICA Y DEL ENTORNO.	**100**	
9.1 Áreas seguras.		**50**
9.2 Seguridad de los equipos.		**50**
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES.	**100**	
10.1 Responsabilidades y procedimientos de operación.		**10**
10.2 Gestión de la provisión de servicios por terceros.		**10**
10.3 Planificación y aceptación del sistema.		**10**
10.4 Protección contra el código malicioso y descargable.		**10**
10.5 Copias de seguridad.		**10**
10.6 Gestión de la seguridad de las redes.		**10**
10.7 Manipulación de los soportes.		**10**
10.8 Intercambio de información.		**10**
10.9 Servicios de comercio electrónico.		**10**
10.10 Supervisión.		**10**
11. CONTROL DE ACCESO.	**100**	
11.1 Requisitos de negocio para el control de acceso.		**10**
11.2 Gestión de acceso de usuario.		**20**
11.3 Responsabilidades de usuario.		**20**
11.4 Control de acceso a la red.		**10**
11.5 Control de acceso al sistema operativo.		**10**
11.6 Control de acceso a las aplicaciones y a la información.		**20**
11.7 Ordenadores portátiles y teletrabajo.		**10**
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.	**100**	
12.1 Requisitos de seguridad de los sistemas de información.		**20**
12.2 Tratamiento correcto de las aplicaciones.		**10**
12.3 Controles criptográficos.		**10**
12.4 Seguridad de los archivos de sistema.		**20**

12.5 Seguridad en los procesos de desarrollo y soporte.		**20**
12.6 Gestión de la vulnerabilidad técnica.		**20**
13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	**100**	
13.1 Notificación de eventos y puntos débiles de seguridad de la información.		**50**
13.2 Gestión de incidentes y mejoras de seguridad de la información.		**50**
14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	**100**	
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.		**100**
15. CUMPLIMIENTO.	**100**	
15.1 Cumplimiento de los requisitos legales.		**30**
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.		**30**
15.3 Consideraciones sobre las auditorías de los sistemas de información.		**40**

Tabla 5: Pesos para Dominios y Objetivos de Control

Una vez definido los pesos para los Dominios y Objetivos de Control se contabilizó los porcentajes de cumplimiento de los 133 Controles, en base a los pesos establecidos para cada uno de los Objetivos de Control, de la misma forma se cuantificó los porcentajes de cumplimiento de los Objetivos de Control, para obtener el cumplimiento total en base a los Dominios de la norma ISO 27002.

Se utilizó una hoja de cálculo para obtener los porcentajes de cumplimiento de los 11 Dominios, en el siguiente ejemplo se detalla cómo se calculó el porcentaje de cumplimiento para el dominio "5. POLÍTICA DE SEGURIDAD".

Datos:

Peso del dominio	100
Cantidad de Objetivos de control:	1
Peso del Objetivo de control	100
Cantidad de Controles:	2
Porcentaje de cumplimiento para el control 1:	30%
Porcentaje de cumplimiento para el control 2:	30%

Cálculo:

Para determinar el valor de cada control se divide el peso del Objetivo de control para la cantidad de controles: (100) / 2 = 50, luego se multiplica el porcentaje de cumplimiento de cada control por su respectivo valor: (30% x 50) = 15, luego se suma todos los valores de los controles pertenecientes a cada Objetivo de control:

(15+15) = 30, en el caso de existir más de un Objetivo de control se realiza una suma total de todos sus valores, el resultado obtenido se convierte en porcentaje por medio de una regla de tres (100 = 100%, 30 = ?), en este caso tenemos: (30 x 100%) / 100 = 30%, en el siguiente gráfico se aprecia un ejemplo de cálculo para obtener del porcentaje de cumplimiento para el mismo dominio en una hoja de cálculo:

Gráfico 3: Cálculo de porcentajes de cumplimiento

El mismo procedimiento se realiza para cuantificar todos los porcentajes de cumplimiento de los 11 Dominios de control, el detalle se puede apreciar en la siguiente tabla:

Dominios	**Porcentaje de Cumplimiento**
5. POLÍTICA DE SEGURIDAD	30
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	48
7. GESTIÓN DE ACTIVOS	60
8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	55
9. SEGURIDAD FÍSICA Y DEL ENTORNO	60
10. GESTIÓN DE COMUNICACIONES Y OPERACIONES	60
11. CONTROL DEL ACCESO	67
12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	56
13. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	55

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	54
15. CUMPLIMIENTO	30

Tabla 6: Cumplimiento actual de la DTIC

En la siguiente figura se puede apreciar los porcentajes de cumplimiento actual que tiene la DTIC de manera gráfica:

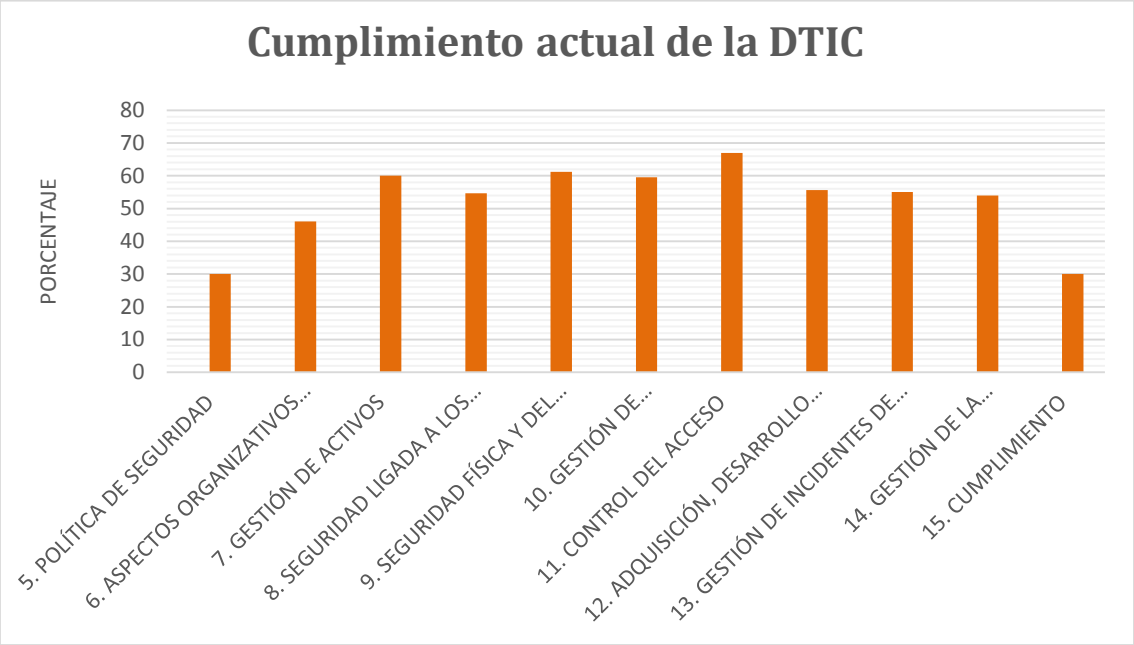

Gráfico 4: Porcentaje de cumplimiento actual de la DTIC

De manera general se puede observar que los dominios de alto cumplimiento son los relacionados con “7. Gestión de Activos”, “10. Gestión de comunicaciones y Operaciones”, “11. Controles de Acceso”, “14. Gestión de la continuidad del Negocio”, debido a los procedimientos establecidos dentro de la DTIC.

Los dominios de cumplimiento bajo son los relacionados con: “5. Políticas se Seguridad”, “15. Cumplimiento”, debido a la falta de políticas de seguridad y la falta de un seguimiento adecuado para el cumplimiento.

Para obtener el porcentaje de cumplimiento total actual, se realizó un cálculo del promedio de todos los porcentajes de los 11 dominios:

(30+48+60+55+60+60+67+56+55+54+30) / 11 = 52

El porcentaje de cumplimiento total actual de la DTIC es del **52%.**

3.1.3. Selección de los dominios indispensables para de la DTIC.

Cabe indicar que no todos los Dominios y Objetivos de Control tienen la misma importancia para las empresas y organizaciones, depende mucho de los objetivos de la empresa, modelo de negocio, tipo de empresa, etc.

En el caso de la Universidad de Cuenca al ser un establecimiento de educación superior pública sin fines de lucro, se determinó los dominios considerados como principales de acuerdo a su importancia, en base a la cualificación de la información obtenida del personal que labora en la DTIC, para lo cual se definió un rango de "pesos" que van desde 1 (baja), 2 (media), 3 (alta).

A continuación se detalla el procedimiento para determinar el nivel de importancia para el dominio "6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN", cuyo valor fue de 2 (media).

Si tres entrevistados establecieron los siguientes valores de importancia para éste dominio:

Entrevistado 1: Valor de importancia del dominio = 1
Entrevistado 2: Valor de importancia del dominio = 2
Entrevistado 3: Valor de importancia del dominio = 2

Para establecer la importancia final del dominio, se consideró la mayor cantidad de valores repetidos, en este caso (2).

Cuando se obtiene cantidades de valores iguales por ejemplo: (1, 1, 2, 2, 3) para un determinado dominio, se toma como referencia la cantidad de valores repetidos más alta, en este caso (2).

El mismo procedimiento se aplicó para determinar la importancia de los 11 dominios de control, en el siguiente gráfico se puede apreciar los dominios más importantes para la DTIC.

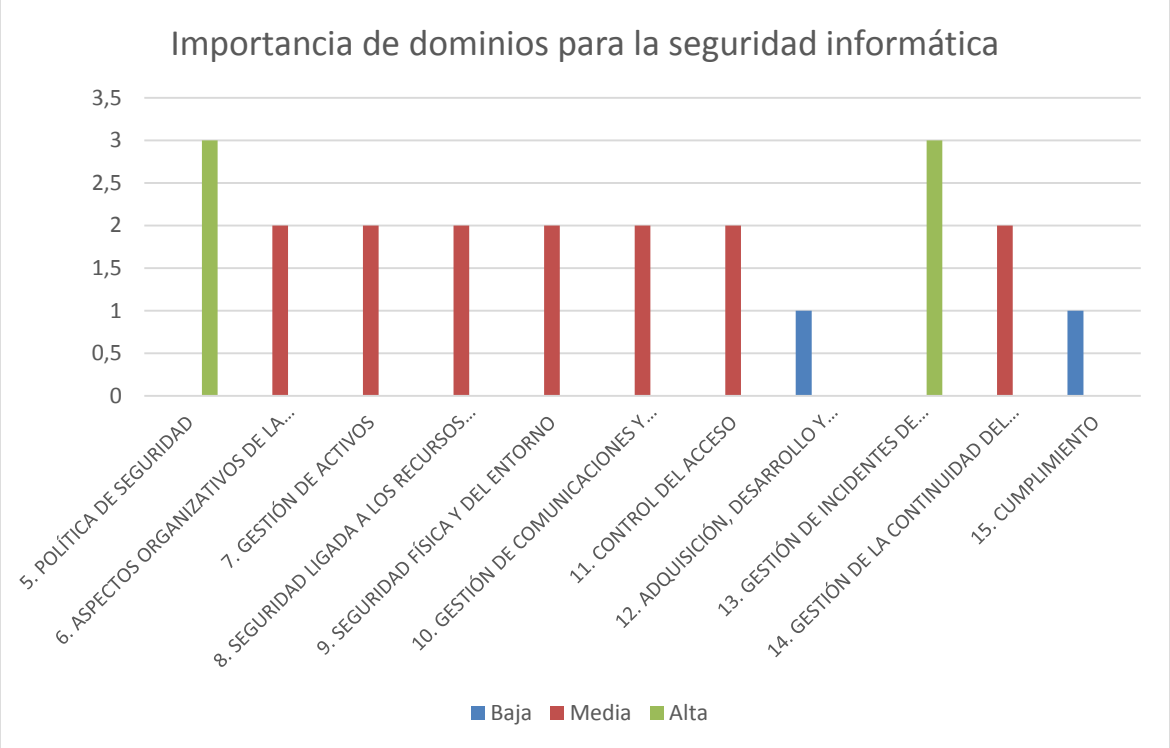

Gráfico 5: Importancia de los Dominios en la DTIC

Como se puede observar en el gráfico los dominios considerados de mayor importancia son: “5. Políticas de Seguridad” y “13. Gestión de incidentes de seguridad de la Información”, los controles considerados de menor importancia son: “12. Adquisición, Desarrollo y mantenimiento de los Sistemas de Información” y “15. Cumplimiento”. Comparando el cumplimiento actual que tiene la DTIC con respecto a la importancia de los dominios, se puede apreciar

que el dominio de “5. Políticas de Seguridad” tiene una importancia “alta” y el porcentaje de cumplimiento bajo del 30%, debido a la ausencia de políticas de seguridad informática en la DTIC. El dominio “13. Gestión de incidentes de seguridad de la Información” tiene una importancia “alta” y el porcentaje de cumplimiento mediano del 55%, debido al tratamiento que se les da a los incidentes en las tres Unidades que conforman la DTIC.

CAPÍTULO 4

4.1. Diseño de políticas de seguridad informática para la DTIC.

Para diseñar las políticas de seguridad informática se utilizó como referencia el manual de "Políticas de seguridad Informática-Mejores Prácticas Internacionales" **(WOOD, 2002)**, como lo utilizaron María Díaz y José Navarro en su tesis de pregrado, **(Díaz & Navarro, 2011)**.

Se modificó la redacción del texto original de algunas políticas de seguridad informática del manual "Políticas de seguridad Informática-Mejores Prácticas Internacionales" cuyo autor es Charles Cresson Wood, para adaptarlas a las necesidades de la DTIC, por ejemplo: se cambió la palabra "Empresa X" de la política original por el nombre "Universidad de Cuenca", como lo recomienda el mismo autor, **(WOOD, 2002, pág. 40)**.

Una vez obtenido el porcentaje de cumplimiento actual y la selección de los dominios indispensables para la DTIC detallados en el capítulo 3, se establecieron políticas de seguridad informática consideradas como principales y algunas políticas consideradas como complementarias, para mejorar los porcentajes de cumplimiento bajo en algunos controles, a continuación se detalla las políticas que necesita la DTIC.

4.1.1. Políticas de seguridad informática principales

La selección de éstas políticas fueron establecidas en base a los dominios con importancia (alta) y los controles con porcentajes de cumplimiento bajo. Las políticas fueron clasificadas de acuerdo a las actividades de cada una de las tres Unidades de la DTIC y se definieron algunas políticas para la Dirección.

4.1.1.1. Unidad de Sistemas de Información

Las políticas para esta unidad son las siguientes:

I. Acceso a la Información de las Aplicaciones de Producción:

Política: El personal que desarrolla un determinado sistema informático para la Universidad de Cuenca no debe tener acceso a la información de otro sistema para el cual no está autorizado.

Comentario: Esta política limita el acceso a un desarrollador hacia la información de otros sistemas informáticos institucionales para los cuales no tiene autorización, por ejemplo, si están trabajando en el desarrollo de un sistema nuevo para Matrículas y Admisión, no necesita acceso a la información del sistema de Activos Fijos, salvo el caso que expresamente necesita alguna información de otro sistema, debe existir el registro de actividades y el respectivo permiso de acceso.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

II. Registros en Sistemas y Aplicaciones Sensibles

Política: Todos los sistemas informáticos institucionales que manejen información sensible de la Universidad de Cuenca, deben generar registros donde consten toda adición, cambio y eliminación de cualquier información.

Comentario: Esta política obliga a generar registros por los cambios efectuados a la información sensible, planes estratégicos y especificaciones de diseños, por ejemplo, la base de datos de nómina debe tener un registro

asociado que indica quién actualizó ciertos parámetros y cuándo, todo cambio en los sistemas sensibles debe ser documentado, probado y reportado al coordinador de la Unidad respectiva. Antes de hacer los cambios en el sistema de producción se debe realizar todas las evaluaciones respectivas en un sistema de pruebas, cuando se realizan los cambios en el sistema de producción se debe dar el seguimiento adecuado para verificar el correcto funcionamiento. Este tipo de información es de mucha ayuda cuando se trate de investigar y corregir problemas como errores y desfalcos.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

III. Registros de Auditoría en los Sistemas

Política: Los registros que tengan información importante sobre la seguridad en los sistemas informáticos deben proporcionar datos suficientes para apoyar a las auditorías de eficacia y cumplimiento.

Comentario: Esta política garantiza que la información almacenada en los registros de los sistemas informáticos y los servidores proporcionarán todos los detalles para permitir que una auditoría interna y externa procedan sin pérdidas de tiempo. Los registros efectivos también pueden ayudar en la resolución de problemas operacionales, como la determinación de la caída del sistema, los registros de auditoria deben estar debidamente actualizados, documentados y almacenados en lugares seguros.

Política Dirigida a: Personal Técnico y Director de TI

Ambientes de Seguridad: Todos

IV. Controles de Acceso a las Operaciones de Producción

Política: Todos los controles de acceso para usuarios finales y administrativos requeridos por las políticas de seguridad informática de la DTIC, se deben definir y habilitar antes de poner en operación los sistemas informáticos institucionales.

Comentario: Esta política ayuda a evitar que el personal técnico publique algún sistema informático sin tener los controles de acceso definidos dentro de un nivel de seguridad razonable. En algunas ocasiones los sistemas pueden ser puestos en operación pero los controles de acceso no han sido activados, o si son activados no están definidos en un nivel seguro. Se debe realizar pruebas de los controles de acceso y el Coordinador de la Unidad debe dar el visto bueno para poner el sistema en producción. Por ejemplo, en muchos casos, los controles de acceso de contraseñas fijas están definidos para un usuario o grupo de usuarios en particular. La política asume que las políticas de control de acceso se hayan establecido previa o simultáneamente con la implementación del sistema informático.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

V. Prueba e Información del Software

Política: Antes de poder en producción cualquier software o información en formato digital a terceras personas, el coordinador de la Unidad de Sistemas de Información debe impedir que se les concedan derechos para modificar la información de los sistemas informáticos a los administradores de otros

sistemas informáticos, como tampoco el acceso a la copia maestra de la información de producción excepto para resolver problemas.

Comentario: Esta política establece la separación de tareas entre el personal que trabaja en el CDS (Centro de Desarrollo de Software), personal de soporte y administradores de los sistemas informáticos institucionales. La intención de esta política es prevenir que la gente que trabaja en una de estas Unidades abuse de sus derechos, y cause daños involuntarios a los programas o a la información. Esta política no se puede implementar a menos que se haya instalado un control de acceso en los sistemas informáticos de producción de la DTIC que adopten esta política.

Política Dirigida a: Personal Técnico y Dirección de TI

Ambientes de Seguridad: Todos

VI. Controles de Datos de Salida

Política: Se debe establecer controles y procedimientos para validar toda la información sensible generada por los sistemas informáticos de la DTIC.

Comentario: Esta política garantiza que la información de salida generada por los sistemas informáticos de la DTIC, sean validados por un proceso efectivo. Por lo general los sistemas son validados, verificados y probados, no existe seguridad de que la información procesada en ellos sea la correcta. También debe haber procedimientos establecidos que definan las responsabilidades de aquellos que están involucrados en los procesos de validación de los datos de salidas. Deben documentarse las políticas para cada uno de estos procesos, para asegurar que se les dé el adecuado nivel de atención y

que sean revisados en forma rutinaria por el coordinar de la Unidad de Servicios Informáticos.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

VII. Funcionalidad de los Sistemas

Política: Con la excepción de los arreglos de emergencia en los sistemas informáticos, sólo aquellas funciones descritas en la documentación autorizada del diseño de los sistemas informáticos deben ser incluidas en los sistemas de producción.

Comentario: Las funciones no documentadas pueden representar riesgos graves de seguridad. Por ejemplo, un mecanismo no documentado que permita al programador original evadir los controles de acceso puede ser utilizado por un usuario no autorizado con malas intenciones. Esta política garantiza que toda la funcionalidad está documentada y aprobada, esta política también puede ser utilizada para disciplinar o despedir a un programador que haya construido una funcionalidad no documentada dentro de un sistema informático institucional.

Política Dirigida a: Personal Técnico y Dirección de TI

Ambientes de Seguridad: Todos

VIII. Mantenimiento de Software

Política: Todos los cambios definitivos realizados en los sistemas informáticos de producción deben ser efectuados utilizando el código fuente y realizar una adecuada documentación.

Comentario: El mantenimiento del código fuente resulta más fácil que el mantenimiento del código objeto. Los cambios en el código objeto conllevan la introducción de nuevos problemas. Es mejor que programador verifique la validez del nuevo código antes de su ejecución. Esto no puede ser efectuado si los cambios son hechos directamente en el código objeto. Esta política requiere que los cambios en el software de producción se hagan en la fuente y no en el objeto. Esta política es importante porque implícitamente requiere que se prepare la documentación para el código fuente.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

IX. Documentación de Cambios en Sistemas de Producción

Política: Toda la documentación que refleje la autorización y desarrollo de todos los cambios significativos realizados en algún sistema informático, debe ser preparada en el lapso de una semana después de efectuado el cambio.

Comentario: Esta política ayuda a que los desarrolladores cumplan con las fechas de preparación de la documentación establecida, algunos desarrolladores se mantendrán posponiendo la preparación de la

documentación por períodos de tiempo extensos. Si llegara a pasar esto existe una gran probabilidad de que por algún motivo haya rotación de personal y la documentación del cambio se quede en el olvido. Al no tener la documentación actualizada es también un impedimento para la solución de los problemas diarios, el adiestramiento de nuevo personal, y los esfuerzos de planificación de contingencias y esfuerzos de recuperación ante desastres.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

X. Documentación de Adiestramiento y Operaciones

Política: Los sistemas informáticos institucionales que se encuentren en fase de desarrollo o que estén sufriendo modificaciones importantes no deben ser movidos a un ambiente de producción sin tener el adecuado adiestramiento y la documentación de operaciones.

Comentario: Sistemas informáticos sin documentación, manejados por personal no adiestrado son muy difíciles de controlar. Cuando existe un problema serio en algún sistema si no se cuenta con la documentación actualiza muy difícilmente se podrá poner operativo a la aplicación lo antes posible, lo mismo sucede con personal inexperto ya que puede ocasionar una pérdida de tiempo y dinero para la Universidad de Cuenca, ya que el personal nuevo puede cometer errores involuntarios. Con esta política se intenta fomentar el adiestramiento adecuado y que la documentación de

operaciones se prepare y autorice antes de que el sistema sea formalmente trasladado a producción.

Política Dirigida a: Personal Técnico y Dirección de TI

Ambientes de Seguridad: Todos

XI. Intentos de Introducir Contraseña

Política: Después de tres intentos erróneos por introducir una contraseña, la identidad del usuario debe quedar suspendida hasta que el administrador del sistema informático lo reinicie, se debe desactivar momentáneamente el acceso al sistema por lo menos durante 15 minutos.

Comentario: Los ataques más exitosos para ingresar a los sistemas informáticos es la deducción de contraseñas, los atacantes podrían utilizar programas para descubrir contraseñas que revisan todas las palabras del diccionario. Esta política ayudará a garantizar que el ataque será infructuoso, bien sea un ataque manual determinado o un ataque mediante la deducción automatizada de la contraseña en especial a los sistemas de acceso Web, los administradores deberán revisar frecuentemente los intentos erróneos de logueo en los servidores de los sistemas informáticos institucionales para determinar si existió intentos infructuosos de acceso y tomar las medidas de seguridad adecuadas.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

4.1.1.2. Unidad de Redes y Comunicaciones

Las políticas para esta unidad son las siguientes:

I. Acceso de Sistemas a la Red

Política: Los sistemas informáticos institucionales y los sistemas operativos que no poseen los parches de seguridad deben ser desconectados de la red LAN de la Universidad de Cuenca.

Comentario: Esta política advierte el hecho de que un sistema informático que no cuente con las medidas de seguridad adecuadas, pone en riesgo a los otros sistemas de la misma red. Así mismo la intención de esta política es también informar a los usuarios finales que estarán temporalmente desconectados de la red en el caso que el computador este con virus. La política puede ser puesta en práctica a través de un software para identificación de vulnerabilidades que permite evaluar el software instalado en computadores remotos, y un software detector de virus, instalado en un servidor de correo o en un cortafuego, estos mecanismos de evaluación de software pueden ser ejecutados nuevamente para determinar si se solucionó el problema en el computador para volverlo a integrar a la red LAN.

Política Dirigida a: Usuarios Finales

Ambientes de Seguridad: Todos

II. Registro de Intentos de Acceso

Política: Se debe registrar todos los intentos de acceso para iniciar una sesión y utilizar algún sistema informático, equipo de comunicació, sin importar si fueron exitosos o no.

Comentario: Esta política apoya la generación de un amplio conjunto de registros de sistemas de operación a lo largo de todos los sistemas informáticos institucionales, correo electrónico, sistemas operativos, equipos de comunicación, frecuentemente los administradores de infraestructura deben revisar los registros en los servidores y almacenar en lugares seguros las evidencias. Los registros también son una entrada muy importante para los sistemas de detección de intrusos en computadores, porque pueden automáticamente alertar al personal técnico sobre un ataque en desarrollo. Una cadena de intentos incorrectos de inicio de sesión sería evidencia de un ataque para adivinar la contraseña o de un usuario que necesita adiestramiento adicional. Estos registros de sistemas captarán el identificador de usuario, hora y fecha, el puerto que utilizó y si el intento de inicio de sesión fue exitoso.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

III. Algoritmos de cifrado evaluados públicamente

Política: Todo algoritmo de cifrado utilizado para proteger la información de producción de la DTIC y los sistemas informáticos, debe ser divulgado públicamente y debe ser evaluado por expertos criptográficos.

Comentario: Esta política evita que la Universidad tenga algún tipo de problemas al crear sistemas de cifrado inseguro o se adquiera de un proveedor un algoritmo débil. La criptografía es muy compleja y es difícil hacerla correctamente. Esta política garantiza que expertos estarán

involucrados en el trabajo de diseño criptográfico, esto garantiza que la Universidad disponga de sistemas informáticos con controles criptográficos validados y seguros. Algunas personas podrán argumentar en contra de esta política indicando que la confidencialidad de la información hará más difícil el descifrado del sistema. Pero nada evita que una organización use algoritmos abiertos mientras que no divulgue cuáles algoritmos emplea.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

4.1.1.3. Unidad de Servicios Informáticos

Las políticas para esta unidad son las siguientes:

I. Protección de la Información

Política: La información debe ser protegida de acuerdo con su confidencialidad, valor y criticidad.

Comentario: Esta política se aplica sin importar el medio o ubicación donde se encuentre almacenada la información relacionada con el puesto de trabajo, los sistemas tecnológicos utilizados para procesarla o los funcionarios que la manejen. Esta política promueve la revisión de las formas en que la información fluye a través de los equipos informáticos dentro de la DTIC. La política conlleva a realizar una auditoría interna y emplear técnicas integradas tales como el análisis de flujo de datos.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

II. Manejo, Acceso y Uso de la Información

Política: La información es un activo vital y todos los accesos, usos y manejos de los datos que se usan en la DTIC, debe tener concordancia con las políticas y normas.

Comentario: Esta política establece un contexto para otras políticas de seguridad informática, es necesario que el personal que labora en la DTIC comprenda cómo la información se ha convertido en un factor crucial para la Comunidad Universitaria. Esta política determina la necesidad de establecer medidas de seguridad informática para el acceso, permisos, manipulación de la información.

Se debe restringir el acceso a la información almacenada en los computadores por medio de claves y protección a las carpetas que contienen información sensible, la información relacionada con la DTIC debe estar segura y contar con copias de respaldo, esta información debe ser usada solo pero el propietario o por algún funcionario con permisos para hacerlo.

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

III. Revocación de Privilegios de Acceso

Política: La DTIC tiene el derecho de revocar los privilegios de acceso hacia cualquier aplicación informática de un determinado usuario en cualquier momento.

Comentario: Esta política comunica a todos los usuarios que ponen en peligro su designación como usuarios autorizados si se involucran en actividades que interfieren con la operación normal de los sistemas informáticos o equipos informáticos de la DTIC, que afecten negativamente la habilidad de otros para utilizar dichos sistemas informáticos o que causen daños físicos a los computadores. Por ejemplo, colapsar un sistema podría ser dañino para otros usuarios y el usuario causante del colapso estaría sujeto a acciones disciplinarias en su contra, incluyendo la revocación de privilegios.

Política Dirigida a: Usuarios Finales

Ambientes de Seguridad: Todos

IV. Computadores Portátiles con Información Sensible

Política: Todos los computadores portátiles, laptops, Tablets y otros dispositivos transportables que contengan información sensible de la DTIC, deben emplear el cifrado de los discos duros para proteger todos los archivos y proteger el arranque del computador mediante clave.

Comentario: Esta política protege la información sensible almacenada en los computadores portátiles. Estas máquinas son frecuentemente robadas, extraviadas o simplemente desaparecen. Desafortunadamente cuando esto pasa, la información almacenada en las unidades de discos duros de esas máquinas se pierde. A pesar de que el costo de los paquetes de hardware y software es significativo, es mucho mayor el costo de la información. El único método confiable para proteger esta información si las máquinas están

desatendidas es el de cifrar la información en la unidad del disco duro. Esta política requiere que todos los archivos almacenados en el disco duro se cifren.

Política Dirigida a: Todos

Ambientes de Seguridad: Medianos y Altos

V. Propiedad de la Información

Política: El coordinador de la Unidad de Servicios Informáticos debe claramente especificar por escrito, la asignación de las responsabilidades de la propiedad de la información para cada funcionario de su Unidad, debe designar a las personas con los privilegios para acceder a la información crítica y confidencial.

Comentario: Esta política establece la delegación clara y documentada de la autoridad para ejercer el control del acceso a la información. Cada funcionario de la Unidad debe estar consciente del tipo de información que maneja, y las complicaciones que ocasionaría a la DTIC si la manipulación de la información es incorrecta o no se tiene protección con la información sensible.

Política Dirigida a: Personal Técnico y Dirección de TI

Ambientes de Seguridad: Todos

VI. Acceso de Lectura a Información Sensible

Política: Los funcionarios de la DTIC que han sido autorizados para ver la información clasificada con un cierto nivel de sensibilidad, pueden acceder sólo a la información de ese nivel o a la de menor nivel de sensibilidad.

Comentario: Esta política establece instrucciones a los funcionarios de la Unidad de Servicios Informáticos en tener una mejor administración de estaciones de trabajo, en el sentido de evitar que los usuarios no autorizados obtengan acceso a cierta información. Por ejemplo, una persona que ha sido autorizada para ver información secreta también puede ver la información Pública y la Confidencial, ya que éstas son menos sensibles que la información secreta. Esta persona, sin embargo, no puede ver la información altamente secreta, a menos que se le haya otorgado una autorización específica. Esta política se aplica a todos los niveles de datos y recomienda usar claves en las carpetas de las estaciones de trabajo y políticas de usuario en el Microsoft Active Directory.

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

VII. Clasificación de la Criticidad de las Aplicaciones Multiusuario

Política: El coordinador de la Unidad de Servicios Informáticos conjuntamente con los propietarios de la información, deben preparar y realizar periódicamente una evaluación del nivel de criticidad de todas las aplicaciones instaladas en los computadores.

Comentario: El proceso mediante el cual los niveles de criticidad son asignados a las aplicaciones instaladas en los computadores, por ejemplo de puede clasificar la criticidad de las aplicaciones en rangos de: bajo, medio, alto, este proceso constituye un paso previo necesario para diseñar un plan de contingencia efectivo. Esta política requiere que se prepare o revise una lista de aplicaciones críticas, a medida que cambien los sistemas y aplicaciones usadas por los funcionarios de la DTIC. Como resultado de estos procesos los planes de contingencia deberían ser periódicamente actualizados.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

VIII. Copias no Autorizadas de Software y Datos

Política: Todos los funcionarios deben abstenerse de hacer copias no autorizadas de software o de cualquier información relacionada con la DTIC, en caso de no disponer del permiso respectivo.

Comentario: Esta política tiene como propósito el designar con claridad la responsabilidad y la culpabilidad legal por el copiado de software y datos no autorizados, dado que no es factible que la Dirección de la DTIC supervise los actos de cada uno de los funcionarios que allí laboran, esta información pone sobre aviso al trabajador con respecto a los riegos que corre por hacer copias no autorizadas. Esta política es importante en cuanto va más allá de la simple prohibición de hacer copias de software y datos no autorizadas.

Política Dirigida a: Usuarios Finales

Ambientes de Seguridad: Todos

4.1.1.4. Dirección de la DTIC.

Las políticas para esta unidad son las siguientes:

I. Comité de Gestión de Seguridad Informática

Política: Un comité de seguridad informática, conformado por el Director y/o los coordinadores de las tres Unidades que conforman la DTIC, deben reunirse trimestralmente para revisar el nivel actual de seguridad informática, revisar los procesos de monitoreo de los incidentes de seguridad reportados, aprobar, crear, modificar los proyectos y políticas de seguridad de la DTIC.

Comentario: Los objetivos de esta política proporciona una misión en temas de seguridad informática a un comité establecido en la DTIC, los comités temporales existen para brindar suficiente apoyo a un proyecto de seguridad informática. El comité debe tener la capacidad de revisar, analizar, evaluar y tomar las acciones necesarias para prevenir y solventar posibles problemas, vulnerabilidades en los sistemas informáticos, equipos de comunicación, estaciones de trabajo. Todas las resoluciones, observaciones, conclusiones de las reuniones que mantenga el comité deben ser redactadas en un documento con firmas de responsabilidad.

Política Dirigida a: Dirección de TI

Ambientes de Seguridad: Todos

II. Acuerdos de Confidencialidad — Organización

Política: Toda divulgación de información secreta, confidencial o privada de la DTIC a terceros se hará a través de la firma de un acuerdo de confidencialidad que incluya restricciones y manejo de la información.

Comentario: Esta política evita el uso no autorizado de la información que maneja la DTIC como por ejemplo: claves de acceso, instrucciones, métodos, datos sensibles, etc. Se debe prohibir la distribución adicional sin el consentimiento del propietario o administrador. Esta política puede expandirse para delinear los requerimientos específicos que deben ser declarados como parte de un acuerdo de confidencialidad, los cuales pueden incluir la devolución de la información, cómo será utilizada, para qué va a ser utilizada y quién recibirá acceso a la misma.

Política Dirigida a: Usuarios Finales

Ambientes de Seguridad: Todos

III. Preparación y Mantenimiento de Planes de Contingencia

Política: La Dirección de TI debe preparar, actualizar y probar una política de recuperación ante desastres, debe especificar el uso de instalaciones alternativas para que los funcionarios de la DTIC puedan continuar las operaciones en caso de interrupción del servicio.

Comentario: Un plan de contingencia para la recuperación ante desastres tiene que ver con asuntos relativos a las instalaciones físicas y otros aspectos, muy aparte de los sistemas informáticos y equipos de comunicación. Los Coordinadores de cada Unidad de la DTIC deben estar a

cargo de crear, supervisar sus planes de contingencia. Por ejemplo, los funcionarios de la Unidad de Redes y Comunicaciones pueden idear los planes de contingencia de los equipos de comunicación y administración de los servidores, los funcionarios de la Unidad de Sistemas de Información crearían los planes de contingencia de los sistemas informáticos institucionales, y los funcionarios de la Unidad de Servicios Informáticos establecerán planes que tengan que ver con las estaciones de trabajo.

Política Dirigida a: Personal Técnico y Dirección de TI

Ambientes de Seguridad: Todos

IV. Accesibilidad del Plan de Contingencia

Política: Los planes de contingencia de los sistemas informáticos institucionales deben estar protegidos y deben ser accesibles de manera continua en Internet por lo menos en dos sitios diferentes, apoyados por proveedores diferentes de servicios en Internet.

Comentario: Esta política asegura disponer de la versión más reciente de los planes de contingencia seguirá estando disponible en el internet, a pesar de lo que pudiera ocurrir en las oficinas, computadores, redes, y otras instalaciones de la Universidad. Por ejemplo, Si el edificio de la Administración Central de la Universidad de Cuenca fuese destruido, la política de contingencia más reciente estaría disponible de inmediato para cualquier persona autorizada que tuviere un computador con conexión a Internet. El software de respaldo en la nube (Dropbox, Google Drive, Owncloud, etc.) también se puede usar para asegurar que los computadores

del personal autorizado tenga la última versión de los planes de contingencia almacenados en los discos duros y en el internet.

Política Dirigida a: Personal Técnico y Dirección de TI

Ambientes de Seguridad: Todos

V. Acuerdos de Confidencialidad de Terceros

Política: Los coordinadores y funcionarios de la DTIC no deben firmar acuerdos de confidencialidad suministrados por terceras personas sin la previa autorización de un asesor legal de la Universidad de Cuenca.

Comentario: Si los funcionarios de la DTIC firmaran acuerdos de confidencialidad con terceras con el fin de acelerar las conversaciones con proveedores, clientes, y socios estratégicos en potencia. Con dicho procedimiento pueden obligar a las autoridades a pagar regalías, multas, demandas, etc. Por temas de acuerdos de confidencialidad, generando un perjuicio económico y legal a la Universidad de Cuenca, el procedimiento correcto sería que se revise la documentación por asesor legal de la Universidad y el personal de Auditoría Interna y si todo está en regla se procede a firmar dicha documentación, además es aconsejable tener una copia de la documentación firmada para respaldo.

Política Dirigida a: Personal Técnico y Usuarios Finales

Ambientes de Seguridad: Todos

VI. Prueba del Plan de Contingencia

Política: Los planes de contingencia para los sistemas informáticos institucionales, equipos de computación y de comunicación deben ser probados, se debe elaborar un informe para la dirección de la DTIC con los detalles de los resultados.

Comentario: Esta política propone realizar prueba periódica de los planes de contingencia, se recomienda por lo menos realizarla cada 3 meses. La confianza en poderse recuperar después de un desastre o de una emergencia se logra mediante la regularidad de pruebas, las cuales son necesarias con el fin de garantizar que las estrategias y procedimientos previamente desarrollados para la recuperación serán pertinentes. Si aún la Universidad no goza de un plan de contingencia, entonces la política no es aplicable.

Política Dirigida a: Personal Técnico y Dirección de TI

Ambientes de Seguridad: Todos

4.1.2. Políticas de seguridad informática complementarias

Las siguientes políticas complementarias ayudarán a las políticas consideradas como principales a mejorar los porcentajes de cumplimiento, las mismas que fueron seleccionadas en términos generales y pueden ser utilizadas en cualquier Unidad de la DTIC.

I. Pruebas de Honestidad y Estabilidad Emocional

Política: Todos los aspirantes a ocupar una vacante en la DTIC deben pasar las pruebas de honestidad y estabilidad emocional autorizadas por el departamento de Talento Humano de la Universidad de Cuenca.

Comentario: Esta política garantiza que la DTIC aplicará pruebas para asegurar que los nuevos funcionarios que ocuparán alguna vacante cumplan con los requisitos de honestidad y estabilidad emocional. Estas pruebas pueden ser escritas, entrevistas de preguntas y repuestas, estudios de casos u otros tipos de prueba. Estas pruebas permiten al Director de TI seleccionar al personal idóneo y evitar trabajadores que son propensos a cometer negligencias, robo de información, ignorar las políticas de seguridad o de vengarse destruyendo información relacionada con la Universidad.

Política Dirigida a: Dirección de TI

Ambientes de Seguridad: Todos

II. Revisión de Antecedentes

Política: Todos los funcionarios en consideración que van ser reubicados en posiciones de confianza en alguna Unidad de la DTIC y los nuevos aspirantes a ocupar alguna vacante, deben pasar la revisión de antecedentes, la cual incluye la verificación de antecedentes policiales, demandas, y empleos anteriores.

Comentario: Esta política informa a la Dirección de la DTIC que se deben conocer bien a quienes están contratando o asignando cargos de confianza, por ejemplo, si una investigación de antecedentes revela que un individuo tiene un historial de problemas laborares anteriores, negligencia profesional, problemas con la justicia. La Dirección puede reconsiderar la decisión de no contratarlo o de no reubicarlo en cargos de confianza.

Política Dirigida a: Dirección de TI

Ambientes de Seguridad: Todos

III. Destrucción de Información

Política: Toda la información relacionada con la DTIC debe ser eliminada o descartada cuando ya no se la necesite.

Comentario: Esta política promueve disponer la información innecesaria de la DTIC a un mínimo posible, se recomienda realizar un cronograma de revisión cada tres meses, para que los funcionarios de la DTIC dediquen un tiempo a revisar la información que manejan, clasificar y reportar a su Coordinar, a su vez el Coordinador debe informar la información que se pretende eliminar al Director de la DTIC, quien tiene la potestad de autorizar al Coordinar de cada Unidad la supervisión de la correcta eliminación de la información que ya no se necesite, conjuntamente con el responsable de la misma. La eliminación se lo podría realizar unos días posteriores a la autorización de la eliminación por parte del Director de la DTIC, este proceso también ayuda a optimizar los espacios de almacenamiento en los computadores. Un diccionario de datos podría ser un importante apéndice a esta política, porque puede ser utilizado para definir qué tipos de datos existen dentro de la organización, su ubicación, su antigüedad y cuáles controles se aplican a los datos.

Política Dirigida a: Personal Técnico y Dirección de TI

Ambientes de Seguridad: Todos

IV. Destrucción de Registros

Política: Los funcionarios de la DTIC no deben eliminar los registros o la información que sea potencialmente importante, sin la previa autorización específica de la Dirección de TI.

Comentario: Esta política informa a los funcionarios que laboran en la DTIC que no deben eliminar la información potencialmente importante, sin la previa autorización de la Dirección de TI. Esta política debe ser acompañada con otras pautas que enumeren los plazos para la retención de los diferentes tipos de información. A esto se conoce como el programa de retención de datos. La política asigna a la Dirección de la DTIC la responsabilidad para la destrucción de registros e información.

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

V. Avisos de Derechos de Autor en Software

Política: Todos los sistemas informáticos y la documentación de la programación que sean propiedad de la Universidad de Cuenca, deben ser incluidos en los avisos de derechos de autor correspondientes.

Comentario: Se puede hacer mención ésta política en los lugares donde han de aparecer los derechos de autor. Por ejemplo, los avisos pudieran aparecer como visualizaciones en pantalla, listas de fuentes de códigos, en manuales del usuario, con esta política lo que se busca es proteger la propiedad de derechos de autor de la Universidad de Cuenca.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

VI. Revisión de los Convenios de Licencia del Software

Política: Los convenios de licenciamiento de los programas instalados en los computadores de la DTIC y de la Universidad de Cuenca, deben ser revisados periódicamente.

Comentario: Esta política informa que la DTIC se preocupa por el cumplimiento de los convenios de licencia de software. La verificación del cumplimiento de los convenios de licencia se automatiza cada día más, por ejemplo, con la herramienta de Help Desk Proactiva Net, se puede tener un inventario de hardware y software de los equipos de la DTIC y de la Administración Central de la Universidad actualizado. La existencia de una política semejante, puede también disuadir al usuario tentado a hacer copias no autorizadas de los programas o licencias.

Política Dirigida a: Personal Técnico y Dirección de TI

Ambientes de Seguridad: Todos

VII. Conciencia del Usuario Sobre Registros de Violaciones de Seguridad

Política: Los usuarios finales deben estar debidamente informados sobre las acciones que constituyen infracciones de seguridad informática y que tales infracciones serán registradas.

Comentario: Esta política pone de manifiesto que todos los usuarios deben estar debidamente informados sobre las acciones que constituyen infracciones de seguridad informática. Como por ejemplo: “No se deberá

entregar las claves personales de los sistemas Operativos o de los Sistemas Informáticos Institucionales a terceros, el uso de las claves son de entera responsabilidad del propietario", se debe informar a los usuarios que sus actividades serán registradas. Si la política va a ser distribuida a los usuarios, puede incluir palabras indicando que "debido a las infracciones, los usuarios están sujetos a acciones disciplinarias que incluyen la terminación de la relación laboral y juicios penales".

Política Dirigida a: Personal Técnico y Usuarios Finales

Ambientes de Seguridad: Todos

VIII. Protección Aplicable del Derecho de Autor

Política: Los funcionarios de la DTIC deben investigar la propiedad intelectual de todo el material que visualicen en Internet, antes de usarlo para cualquier propósito.

Comentario: Esta política evita que los funcionarios de la DTIC violen los derechos de propiedad intelectual de terceros. Se debe mantener informado a todos los funcionarios mediante recordatorios sobre derechos de autor y deslindando responsabilidad a la DTIC y a la Universidad, con esta política la DTIC puede protegerse contra demandas por daños y perjuicios asociados con los actos ilegales de sus trabajadores. Esta política no se limita a los datos y puede demostrar que la DTIC de ninguna manera incita o apoya el copiado de software no autorizado.

Política Dirigida a: Personal Técnico

Ambientes de Seguridad: Todos

IX. Estructura de las Contraseñas

Política: Los funcionarios de la DTIC no deben utilizar contraseñas que sean fácilmente predecibles o deducibles con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical.

Comentario: El mayor problema que se encuentra con mayor frecuencia es el error humano y la elección de contraseñas fijas que se pueden deducir con facilidad. Es recomendable que en los sistemas Informáticos y los Sistemas Operativos se implementen mecanismos de requisitos mínimos de complejidad al momento de escoger la contraseña. Esta política informa a los usuarios que deben seleccionar contraseñas que sean difíciles de deducir por personas no autorizadas.

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

X. Informes de Incidentes

Política: Todas las sospechas de incidentes de seguridad informática deben ser reportadas tan pronto sea posible, a través de los canales internos autorizados de la DTIC.

Comentario: Con esta promueve que todos los problemas e infracciones sean prontamente informados por medio de los canales autorizados como son: sistema de Help Desk, correo electrónico, línea telefónica de la Unidad de Servicios Informáticos. Si las infracciones y los problemas no son

reportados a tiempo pueden acarrear pérdidas económicas y de tiempo para la Universidad. Un buen ejemplo de esto son los virus de computadores que si no son reportados a tiempo, continuarían propagándose por la red LAN e infectando a más equipos. La notificación de algún incidente debe ser reportado en un plazo máximo de 24 horas.

Política Dirigida a: Usuarios Finales

Ambientes de Seguridad: Todos

XI. Acceso Físico para Terceros

Política: El acceso de terceras personas a las oficinas de la DTIC, en donde se maneje información confidencial, debe ser controlado por guardias, recepcionistas u otro personal.

Comentario: El acceso sin control a las oficinas de la DTIC puede provocar sustracción de información, robo de equipos informáticos portátiles y otros problemas. Esta política define una manera de llevar a cabo una estrategia conocida como “control del perímetro”. Para hacer cumplir esta política las entradas a las oficinas de cada una de las Unidades de la DTIC pueden contar con torniquetes u otros mecanismos para garantizar que sólo pueda acceder el personal autorizado utilizando un dispositivo u otro mecanismo de control de acceso, ya que las puertas de las oficinas permanecen abiertas en las jornadas de trabajo.

Política Dirigida a: Todos

Ambientes de Seguridad: Todos

4.2. Proyección del mejoramiento de la seguridad informática en la DTIC

La planificación y el tiempo que se destine para la implementación de las políticas de seguridad informática en la DTIC van a depender de la Dirección y de los Coordinadores de las respectivas Unidades, en base a los proyectos que se encuentren en ejecución y al Plan Operativo Anual (POA) de la DTIC.

Para obtener un estimado del mejoramiento que tuviera la DTIC en aspectos de Seguridad Informática, se realizó una proyección en base a implementaciones de las políticas de seguridad a corto, mediano y largo plazo. Estos plazos fueron establecidos considerando que la DTIC disponga de un equipo de profesionales contratados cuyas actividades serán exclusivamente la elaboración, desarrollo e implementación de las políticas de seguridad antes descritas, ya que el personal que actualmente labora en la DTIC tiene ya definido y organizado las actividades que realizan a diario de acuerdo al POA.

A partir de la fecha de conformación del equipo de profesionales contratados, iniciaría los períodos para el corto, mediano y largo plazo, cumpliendo de esta manera con los tiempos establecidos.

4.2.1. Proyección de mejoramiento a corto plazo

Para proyectar el mejoramiento a corto plazo se considerará un período de 2 meses para implementar las políticas relacionadas con: la elaboración, revisión y entrega de la documentación técnica de adiestramiento, de cambios en los diferentes sistemas informáticos institucionales, políticas para los registros y eventos almacenados en los servidores para determinar intentos de acceso exitosos y fallidos hacia los sistemas informáticos, equipos de comunicación, servidores de aplicaciones y estaciones de trabajo. Adicional se deberá implementar políticas

para proteger la información almacenada en los equipos de computación móviles, definir los permisos para acceder a la información sensible y controlar las copias no autorizadas del software y los datos que son de propiedad de la DTIC.

Para estimar el incremento del porcentaje de cumplimiento en determinados dominios a corto plazo se procedió de la siguiente forma:

Por ejemplo: para estimar el incremento del 30% al 60% del dominio "5. POLÍTICA DE SEGURIDAD" se consideró que en dos meses el director de la DTIC revise y apruebe la documentación de las políticas de seguridad definidas para éste período de tiempo, a su vez el equipo de profesionales contratado difunda la vigencia de las políticas aprobadas al personal técnico. Los administradores de los diferentes sistemas informáticos deben coordinar con los profesionales contratados para la elaboración de la documentación técnica y de adiestramiento, también se debe coordinar la implementación de mecanismos para proteger la información almacenada en los computadores de la DTIC.

Este mismo procedimiento se utilizó para estimar el incremento de los porcentajes de cumplimiento en algunos controles para los siguientes períodos a mediano y largo plazo.

Para obtener el porcentaje de cumplimiento total a corto plazo, se realizó un cálculo del promedio de todos los porcentajes de los 11 dominios:

(60+54+72+55+61+60+70+56+55+54+30)/11= 57

El porcentaje de cumplimiento a corto plazo sería del **57%.**

En el siguiente gráfico se puede apreciar el mejoramiento de los porcentajes de cumplimiento a corto plazo.

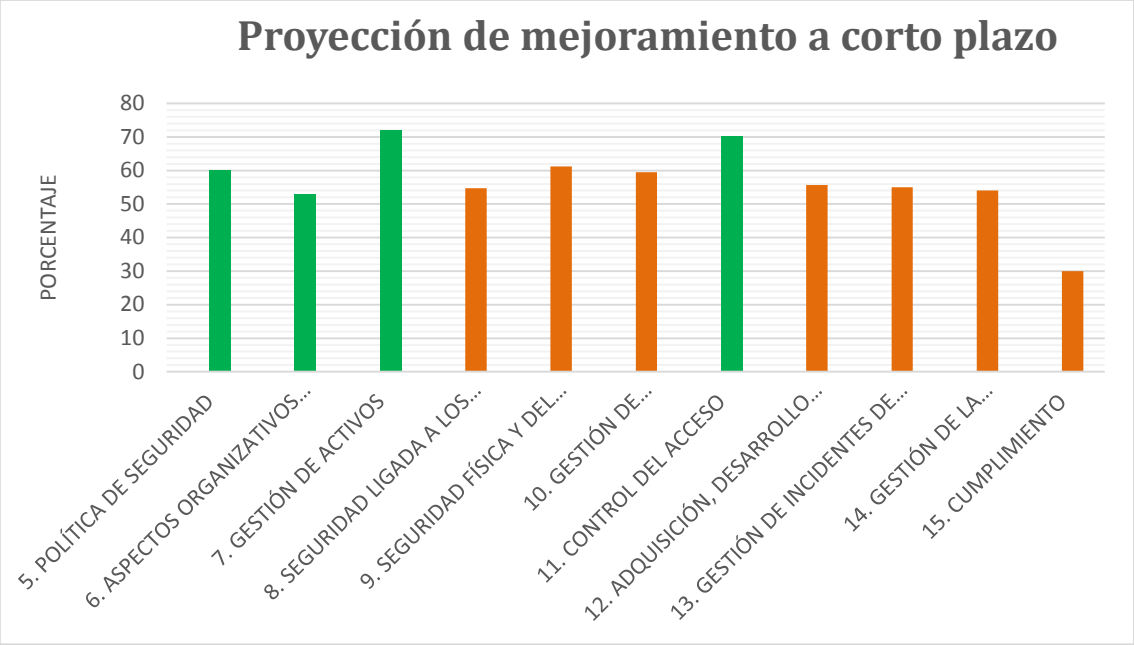

Gráfico 6: Proyección estimada del mejoramiento a corto plazo

Los dominios de seguridad que incrementarían el porcentaje de cumplimiento a corto plazo son lo que se encuentran de color verde.

4.2.2. Proyección de mejoramiento a mediano plazo

Para proyectar el mejoramiento a mediano plazo se considerará un período de 6 meses para implementar las políticas relacionadas con: controles de acceso, registro de auditorías, documentación de cambios, control de datos de salida, para los sistemas informáticos institucionales. Adicional se deberá incluir políticas para: intentos de introducir una contraseña, acceso, manejo, propiedad de la información, revocación de privilegios de acceso a los datos y a la información que se encuentran en los servidores y las estaciones de trabajo que se usan en la DTIC. Para obtener el porcentaje de cumplimiento total a mediano plazo, se realizó un cálculo del promedio de todos los porcentajes de los 11 dominios:

(80+63+72+55+61+60+70+68+76+54+30)/11= 63

El porcentaje de cumplimiento a mediano plazo sería del **63%.**

En el siguiente gráfico se puede apreciar el mejoramiento de los porcentajes de cumplimiento estimado a mediano plazo.

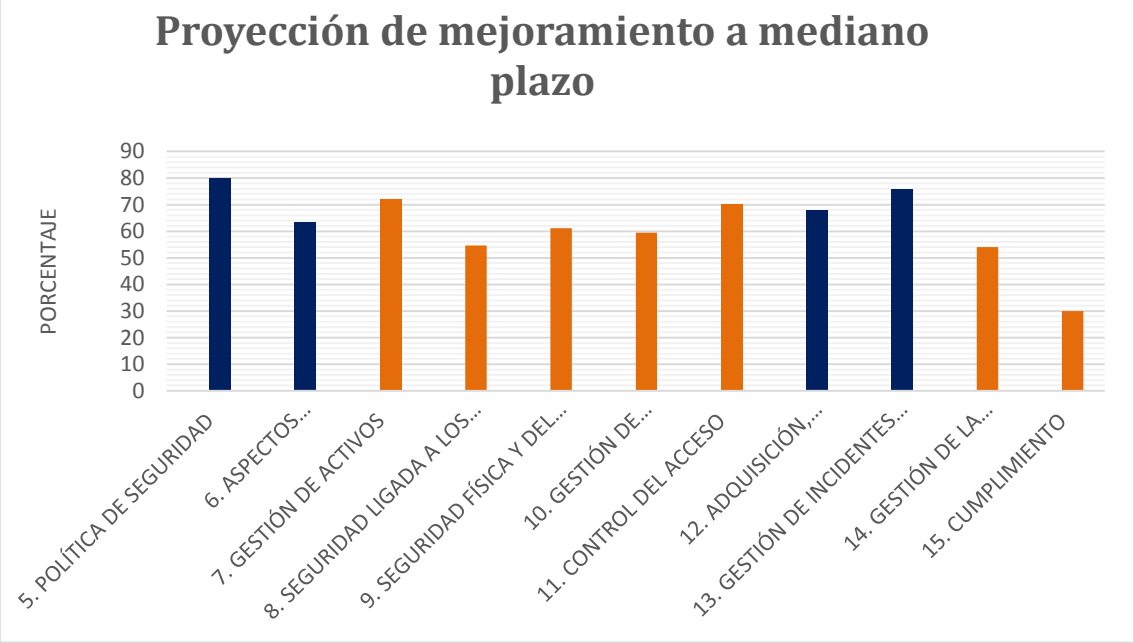

Gráfico 7: Proyección estimada del mejoramiento a mediano plazo

Los dominios de seguridad que incrementarían el porcentaje de cumplimiento a mediano plazo son lo que se encuentran de color azul.

4.2.3. Proyección de mejoramiento a largo plazo

Para proyectar el mejoramiento a largo plazo se considerará un período de 12 meses para implementar las políticas relacionadas con: funcionalidad, mantenimiento de los sistemas informáticos, protección y clasificación de la información, conformación de un Comité de Gestión de Seguridad Informática, conformación, revisión y pruebas de planes de contingencia. Adicional se aplicarían las políticas complementarias relacionadas con: pruebas de honestidad, revisión de antecedentes para los aspirantes a integrarse a la DTIC y a

funcionarios en labores, revisión y destrucción de información y registros almacenados en los servidores, revisión de convenios de licenciamiento de software, protecciones de derechos de autor.

Para obtener el porcentaje de cumplimiento total a largo plazo, se realizó un cálculo del promedio de todos los porcentajes de los 11 dominios:

(95+63+72+65+65+60+70+68+81+80+87)/11= 73

El porcentaje de cumplimiento a largo plazo sería del **73%.**

En el siguiente gráfico se puede apreciar el mejoramiento de los porcentajes de cumplimiento estimado a largo plazo.

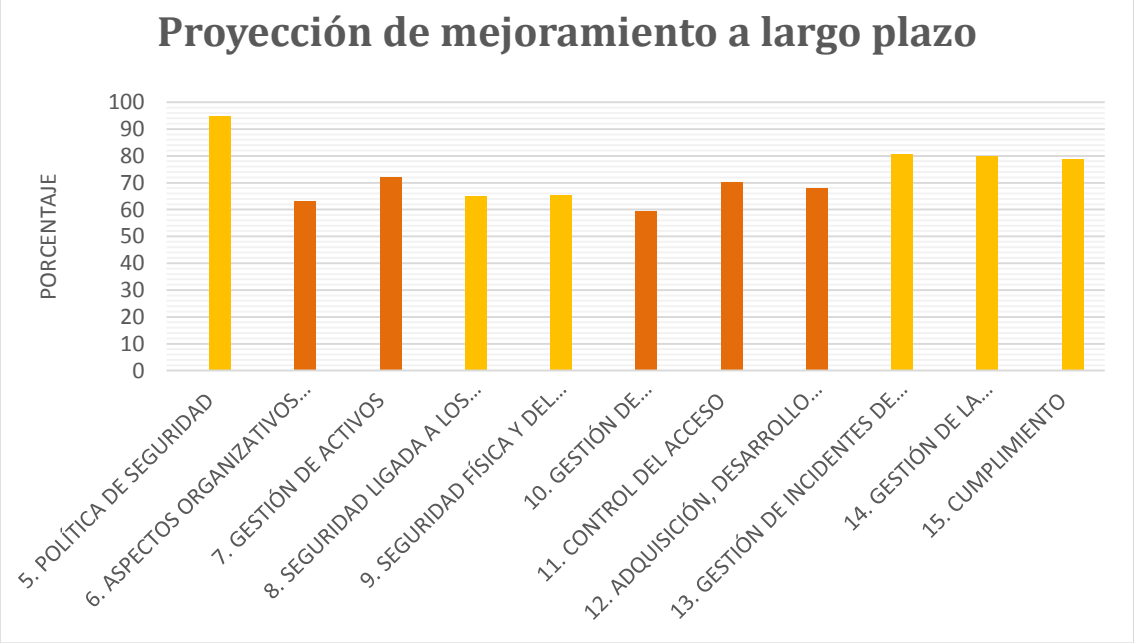

Gráfico 8: Proyección estimada del mejoramiento a largo plazo

Los dominios de seguridad que incrementarían el porcentaje de cumplimiento a largo plazo son lo que se encuentran de color amarillo.

Como se puede apreciar en el Gráfico 7, el porcentaje de cumplimiento estimado sería del 73% y no llegaría al 100%, debido a que no todos los dominios de seguridad incrementaron su porcentaje de cumplimiento, esto se da por la naturaleza de la Universidad de Cuenca al ser un establecimiento de Educación Superior Público, en donde existieron algunos controles de seguridad que su porcentaje de cumplimiento es 0% y no aplican en la Universidad.

CAPÍTULO 5

5.1. Conclusiones

Al finalizar el presente trabajo de tesis se citan algunas conclusiones:

- Luego de haber obtenido, revisado y analizado la información relacionada con temas de seguridad informática que fue proporcionada por el personal que labora en las tres Unidades que conforman la DTIC, se pudo estimar que el porcentaje de cumplimiento inicial es del 52 % de acuerdo a los 11 dominios de seguridad de la norma ISO 27002, cabe indicar que existieron controles que su porcentaje de cumplimiento fueron del 0%, debido a la naturaleza de la Universidad; recordando que la norma ISO 27002 está diseñada para cualquier tipo de entidad sea pública o privada, pequeña, mediana o grande.

  En los resultados de la cuantificación del cumplimiento actual de la DTIC se pudo constatar que los puntos más débiles son la falta de políticas de seguridad informática, lo que conlleva a una falta de revisión y verificación del cumplimiento, adicionalmente existe algunos inconvenientes con la seguridad física y del entorno, como por ejemplo: falta de seguridades en las puertas de acceso en las oficinas de la DTIC en el horario de trabajo, además la falta de documentación técnica y de adiestramiento dificulta la resolución de problemas diarios y la elaboración de planes de contingencia adecuados para garantizar la recuperación de los servicios que brinda la DTIC a toda la comunidad Universitaria ante desastres e interrupciones del servicio.

- Con la identificación de la importancia que tienen los dominios de seguridad informática de la norma ISO 27002, por medio del análisis de la información

proporcionada por los funcionarios que laboran en las tres Unidades que conforman la DTIC, se pudo cualificar que controles se consideran como los más urgentes para mejorar los porcentajes de cumplimiento actual, también se pudo evidenciar que existe una gran preocupación por la ausencia de algunas políticas de seguridad informática en todas las Unidades de la DTIC.

Según expertos en seguridad informática consideran que por más seguridades físicas que cuente una institución, siempre va a existir el riesgo en el factor humano, ya que se puede cometer errores voluntarios e involuntarios y poner en riesgo a la información institucional, una adecuada lista de políticas de seguridad informática y las revisiones periódicas de su cumplimiento ayudan a mantener bajo control los riesgos de seguridad informática que tanto los usuarios, personal técnico, coordinadores y autoridades están expuestos a diario.

- Las políticas que se diseñaron son consideradas como las más adecuadas para mejorar los porcentajes de cumplimiento "bajo", ya que al establecer políticas de seguridad informática clasificadas para cada Unidad que conforma la DTIC, se va a conseguir una mejor seguridad, organización, concienciación, desempeño laboral y el resultado va a ser la obtención de una mejora en la seguridad de la información.

  Los funcionarios de la DTIC como los usuarios finales van a tener el conocimiento de sus obligaciones, responsabilidades, prohibiciones, consecuencias y tareas que tienen que desempeñar a diario en sus puestos de trabajo, también se va a conseguir la concientización tanto del personal técnico como de los usuarios finales, ya que el incumplimiento de alguna política de seguridad puede desencadenar un riesgo a la seguridad de la

información, además el desconocimiento no exime de responsabilidad.

- Como se indicó en el alcance de la presente trabajo de tesis, se estableció unas políticas de seguridad informática más relevantes para la DTIC basado en el análisis de la información proporcionada por los funcionarios que allí laboran, se pudo identificar algunos controles que no se aplican por la naturaleza de la Universidad de Cuenca, como por ejemplo: Servicios de Comercio Electrónico.

  Además recordamos que la norma ISO 27002 está diseñada para aplicarla en cualquier tipo de empresa de cualquier magnitud, donde va a depender de los objetivos, modelo de negocio, metas, naturaleza de cada una de las empresas en aplicar o no cierto control de seguridad informática, por ese motivo el porcentaje de cumplimiento total estimado para la DTIC no sería del 100%.

- Se tiene la confianza que la implementación de las políticas de seguridad informática definidas en el presente documento van a ayudar en primer lugar a la concientización de todos los funcionarios que laboran en la DTIC, ya que el incumplimiento de alguna política de seguridad informática puede poner en riesgo a la información, equipos informáticos de toda la comunidad Universitaria. En segundo lugar se va a conseguir un mejoramiento sustancial en aquellos puntos débiles de la seguridad informática que tiene actualmente la DTIC, como por ejemplo se conseguirá un fortalecimiento en la seguridad de los sistemas informáticos institucionales, en los equipos informáticos y en los equipos de comunicación que administran los funcionarios de la DTIC, también se dispondrá de documentación técnica y de adiestramiento actualizado, se elaborará y se realizará revisiones periódicas de los planes de contingencia.

5.2. Recomendaciones

Como punto final se citan algunas recomendaciones:

- Para aprender de los incidentes que se suscitan a menudo es recomendable documentar, revisar, actualizar la Base del Conocimiento de la herramienta Proactiva Net, ya que con una adecuada documentación y procedimientos a seguir se optimiza el tiempo y se da soluciones inmediatas a los incidentes.
- Para garantizar el acceso tanto a la información, sistemas informáticos y a los planes de contingencia se recomienda tener servidores réplica en otro lugar físico de la Universidad de Cuenca y disponer de un segundo enlace de internet con otro proveedor, ya que ante un desastre natural que afecte al Data Center ubicado en la Administración Central, se garantiza la continuidad de los servicios que brinda la DTIC y poner en marcha los planes de contingencia para solucionar los problemas que se tenga en Data Center principal.
- Conformar un CSIRT "Computer Security Incident Response Team" (equipo de respuesta a incidentes de seguridad informática) interno, con el personal adecuado e idóneo de las tres Unidades que conforman la DTIC, Mantener contacto con grupos de especial interés como por ejemplo: consultores de seguridad informática, expertos en Ciberseguridad, para estar actualizados en nuevas amenazas de seguridad, ataques, vulnerabilidades, etc.
- Realizar frecuentemente auditorías informáticas internas a los sistemas informáticos, equipos de comunicación y estaciones de trabajo y contratar auditores informáticos externos para garantizar que los controles, procedimientos y políticas de seguridad informática implementados sean cumplidos de forma adecuada por los funcionarios y los usuarios.

ANEXOS

ANEXO A

5. POLÍTICA DE SEGURIDAD

5.1 Política de seguridad de la información

5.1.1 Documento de la política de seguridad de la información

Control:

"La Dirección debería aprobar y publicar un documento de la política de seguridad de la información y comunicar la política a todos los empleados y las partes externas relevantes"

Análisis:

No se tiene establecido documentos de políticas de seguridad informática, tampoco existe una socialización adecuada al personal que labora en la DTIC y a toda la comunidad Universitaria, por lo general se indica algunas normas de seguridad de forma verbal al personal que labora en la DTIC.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

5.1.2 Revisión de la política de seguridad de la información

Control:

"La política de seguridad de la información se debería revisar a intervalos planificados (o en caso que se produzcan cambios significativos) para garantizar que es adecuada, eficaz y suficiente"

Análisis:

Al no disponer de políticas establecidas no se considera que se realicen revisiones en intervalos de tiempo planificados, cuando existe un problema de seguridad informática se toma las medidas correctivas lo antes posible y se analiza la causa del incidente para evitar que se vuelva a repetir.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

6.1. Organización interna

6.1.1 Compromiso de la gerencia con la seguridad de la información

Control:

"Los miembros de la Dirección deberían respaldar activamente las iniciativas de seguridad demostrando su claro apoyo y compromiso, asignando y aprobando explícitamente las responsabilidades en seguridad de la información dentro de la Organización"

Análisis:

Existe el interés por parte de la dirección de la DTIC pero formalmente no se encuentra nada establecido, muchos de los compromisos se los tiene solo en palabras, las responsabilidades son establecidas al inicio de la relación laboral y cuando existe una reorganización interna en cada Unidad.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

6.1.2 Coordinación de la seguridad de la información

Control:

"Las actividades para la seguridad de la información deberían ser coordinadas por representantes que posean de cierta relevancia en su puesto y funciones de los distintos sectores que forman la Organización"

Análisis:

Los coordinadores de cada Unidad que conforman la DTIC establecen roles y responsabilidades para el personal que allí laboran, pero no se especifican formalmente las actividades para asegurar la seguridad informática.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

6.1.3 Asignación de las responsabilidades de la seguridad de la información

Control:

"Se deberían definir claramente todas las responsabilidades para la seguridad de la información"

Análisis:

Las responsabilidades, deberes y obligaciones son definidos de acuerdo al cargo del personal que labora en cada Unidad, todo el personal tiene claro el rol que desempeña, en el transcurso del tiempo los roles pueden cambiar según las exigencias o reorganización interna de cada Unidad de la DTIC.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

6.1.4 Proceso de autorización de recursos para el tratamiento de la información

Control:

"Se debería definir y establecer un proceso de gestión de autorizaciones para los nuevos recursos de tratamiento de la información"

Análisis:

Existe un procesamiento de la información especialmente la generada por los sistemas de informáticos universitarios con el afán de determinar inconsistencias, evaluar datos erróneos. Por parte de la Dirección de la DTIC no existe autorización para procesar nueva información de los sistemas informáticos hasta el momento.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

6.1.5 Acuerdos de confidencialidad

Control:

"Se deberían identificar y revisar regularmente en los acuerdos aquellos requisitos de confidencialidad o no divulgación que contemplan las necesidades de protección de la información de la Organización"

Análisis:

Al inicio de la relación laboral cuando se firma un contrato de trabajo se explica pocos detalles sobre temas relacionados con normas, pero no se tiene bien definido cuales son las prohibiciones, compromisos, y sanciones

al faltar a un acuerdo de confidencialidad, sobre todo cuando un funcionario deja de prestar sus servicios en la DTIC.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

6.1.6 Contacto con las autoridades

Control:

"Se deberían mantener los contactos apropiados con las autoridades pertinentes"

Análisis:

Se tiene conocimiento que el director de la DTIC está en contacto directo con las autoridades universitarias por varios temas, pero en pocas ocasiones se tocan temas relacionados con políticas de seguridad informática, las reuniones son más orientadas a la adquisición de nuevas soluciones informáticas, dotación de infraestructura, equipos de comunicación, rendición de cuentas, etc.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

6.1.7 Contacto con grupos de especial interés

Control:

"Se debería mantener el contacto con grupos o foros de seguridad especializados y asociaciones profesionales"

Análisis:

De lo que se tiene conocimiento es que se mantiene contacto con consultores externos por ejemplo: Cobit, ITIL, pero contacto con consultores de relacionados con aspectos de seguridad informática muy poco.

Según los datos obtenidos se considera un cumplimiento del 20% de este control.

6.1.8 Revisión independiente de la seguridad de la información

Control:

"Se deberían revisar las prácticas de la Organización para la gestión de la seguridad de la información y su implantación (por ej., objetivos de control, políticas, procesos y procedimientos de seguridad) de forma independiente y a intervalos planificados o cuando se produzcan cambios significativos para la seguridad de la información"

Análisis:

De lo que se tiene conocimiento se revisa y analiza por separado los incidentes generados y registrados en el sistema Help Desk, pero no se revisa los objetivos de control, políticas, procesos relacionados con la seguridad informática.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

6.2. Terceros

6.2.1 Identificación de los riesgos derivados de terceros

Control:

"Se deberían identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso"

Análisis:

Se tiene permisos de acceso para los sistemas como por ejemplo el eSIUC para los docentes, estudiantes, el acceso es limitado a las bases de datos, solo el personal autorizado tiene acceso a la información, no se tiene identificado los riesgos que puede tener la información de la DTIC y no están establecidos los controles necesarios.

Según los datos obtenidos se considera un cumplimiento del 60% de este control.

6.2.2 Tratamiento de la seguridad en la relación con los clientes

Control:

"Se deberían anexar todos los requisitos identificados de seguridad antes de dar a los clientes acceso a la información o a los activos de la organización"

Análisis:

Por lo general solo se da acceso a los estudiantes y docentes para que puedan usar los sistemas académicos institucionales, solo el personal de la

DTIC tiene acceso remoto a los servidores, no se tiene identificado de forma clara aspectos de seguridad, riesgos, consecuencias, vulnerabilidades.

Según los datos obtenidos se considera un cumplimiento del 60% de este control.

6.2.3 Tratamiento de la seguridad en contratos con terceros

Control:

"Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes"

Análisis:

Por lo general los accesos a los sistemas universitarios son enteramente permitidos para estudiantes y docentes, existen sistemas informáticos adquiridos por terceras partes y tiene establecido el acceso a la información de forma local, no existe un procedimiento para que terceras partes tengan acceso a la información universitaria.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

7. GESTIÓN DE ACTIVOS

7.1 Responsabilidad sobre los activos

7.1.1 Inventario de los activos

Control:

"Todos los activos deberían estar claramente identificados, confeccionando y manteniendo un inventario con los más importantes"

Análisis:

Existe una identificación de los activos que utilizan el personal de la DTIC, tanto de los equipos informáticos, como de muebles y enseres; en ocasiones no se tiene actualizada la información cuando existen cambios internos de custodios de los bienes asignados.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

7.1.2 Propiedad de los activos

Control:

"Toda la información y activos asociados a los recursos para el tratamiento de la información deberían pertenecer a una parte designada de la Organización"

Análisis:

La información relacionada con la DTIC que se encuentra en los equipos informáticos es responsabilidad de cada funcionario sobre la correcta manipulación, uso, seguridad e integridad de los datos.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

7.1.3 Uso aceptable de los activos

Control:

"Se deberían identificar, documentar e implantar regulaciones para el uso adecuado de la información y los activos asociados a recursos de tratamiento de la información"

Análisis:

Los procedimientos para el uso correcto de los activos se lo realiza al inicio de la entrega de los equipos informáticos de forma verbal, no existe documentación al respecto sobre el uso correcto, prevenciones, problemas, consecuencias, sanciones, etc.

Según los datos obtenidos se considera un cumplimiento del 60% de este control.

7.2 Clasificación de la información

7.2.1 Directrices de clasificación

Control:

"La información debería clasificarse en relación a su valor, requisitos legales, sensibilidad y criticidad para la Organización"

Análisis:

Por lo general la información digital se encuentra clasificada por carpetas en las estaciones de trabajo, pero no se tiene una clasificación por valor, sensibilidad y criticidad, para delegar permisos de acceso.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

7.2.2 Etiquetado y manipulado de la información

Control:

"Se debería desarrollar e implantar un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo con el esquema de clasificación adoptado por la Organización"

Análisis:

La información física (documentos, certificados, contratos, etc.) de la DTIC, se encuentra clasificada y etiquetada por carpetas, la información digital no cuenta con algún etiquetado para el correcto tratamiento, no existe un esquema de clasificación de la información por parte de la dirección de TI.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

8. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

8.1 Antes del empleo

8.1.1 Funciones y responsabilidades

Control:

"Se deberían definir y documentar los roles y responsabilidades de la seguridad de los empleados, contratistas y terceros en concordancia con la política de seguridad de la información de la organización"

Análisis:

Se encuentra establecido los roles y responsabilidades para el nuevo personal que se integra a la Universidad, en los contratos de trabajo que son firmados en la Unidad de Talento Humano, no existe documentación en la DTIC sobre roles y responsabilidades en temas se seguridad informática y seguridad física.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

8.1.2 Investigación de antecedentes

Control:

"Se deberían realizar revisiones de verificación de antecedentes de los candidatos al empleo, contratistas y terceros y en concordancia con las regulaciones, ética y leyes relevantes y deben ser proporcionales a los requerimientos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos"

Análisis:

Lo que se evalúa es la experiencia, recomendaciones del nuevo personal que se integra a la DTIC, se tiene conocimiento que el tema de los antecedentes lo revisa la Unidad de Talento Humano, en el caso de terceros como empresas proveedoras, se analiza los antecedentes y reputación en la página web de compras públicas.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

8.1.3 Términos y condiciones de contratación

Control:

"Como parte de su obligación contractual, empleados, contratistas y terceros deberían aceptar y firmar los términos y condiciones del contrato de empleo, el cual establecerá sus obligaciones y las obligaciones de la organización para la seguridad de información"

Análisis:

Los términos y condiciones para la contratación del nuevo personal que se integra a la DTIC lo maneja la Unidad de Talento Humano, se tiene conocimiento que en la firma del contrato se encuentran establecidas algunas cláusulas de obligaciones y prohibiciones, pero no están del todo claras.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

8.2 Durante el empleo

8.2.1 Responsabilidades de la Dirección

Control:

"La Dirección debería requerir a empleados, contratistas y usuarios de terceras partes aplicar la seguridad en concordancia con las políticas y los procedimientos establecidos de la organización"

Análisis:

La Dirección de la DTIC delega la responsabilidad de dar el seguimiento para el correcto desarrollo de las tareas diarias a los Coordinadores de cada

Unidad. No se tiene establecido políticas en temas se seguridad informática dentro de cada Unidad.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

8.2.2 Concienciación, formación y capacitación en seguridad de la información

Control:

"Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deberían recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo"

Análisis:

El personal que labora en la DTIC ha recibido capacitación en temas de nuevas herramientas de desarrollo, soluciones informáticas, talleres para gestión de proyectos, ITIL, Cobit, pero no ha existido capacitación en temas de seguridad informática.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

8.2.3 Proceso disciplinario

Control:

"Debería existir un proceso formal disciplinario para empleados que produzcan brechas en la seguridad"

Análisis:

No se tiene establecido un procedimiento y medidas a tomar cuando el personal ha cometido algún acto voluntario e involuntario que ponga en riesgo a la seguridad de la información, hasta el momento no se tiene noticias de problemas se seguridad informática por factor humano.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

8.3 Cese del empleo o cambio de puesto de trabajo

8.3.1 Responsabilidades del cese o cambio

Control:

"Las responsabilidades para ejecutar la finalización de un empleo o el cambio de éste deberían estar claramente definidas y asignadas"

Análisis:

Se tiene un procedimiento para llevar a cabo la finalización de la relación de dependencia con el personal que va a dejar de laborar en la DTIC, que consiste básicamente en deshabilitar el acceso a los sistemas institucionales a los cuales tenía permisos, cuando se trata de cambio de funciones o dependencias, se sigue el mismo procedimiento, este procedimiento lo administra los administradores de los sistemas informáticos, en algunos casos no se lo realiza de forma oportuna ya que la orden de des habilitación y permisos de acceso viene desde la Unidad de Talento Humano.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

8.3.2 Devolución de los activos

Control:

"Todos los empleados, contratistas y terceros deberían devolver todos los activos de la organización que estén en su posesión a la finalización de su empleo, contrato o acuerdo"

Análisis:

Cuando el personal que deja de prestar sus servicios está obligado a realizar los trámites para finalización de la relación de dependencia, entre ellos está la entrega de los bienes asignados a la persona que lo va a reemplazar o al feje inmediato, el trámite se lo realiza con la Unidad de Activos Fijos, es un requisito para recibir la liquidación.

Según los datos obtenidos se considera un cumplimiento del 90% de este control.

8.3.3 Retiro de los derechos de acceso

Control:

"Se deberían retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisada en caso de cambio"

Análisis:

En el último día de labores del personal que deja de prestar los servicios en la DTIC se ejecuta el cese de funciones y permisos de acceso a los sistemas

informáticos que tenía permisos, en el caso de cambio de funciones del personal, se lo realiza el primer día de trabajo en el nuevo cargo.

Según los datos obtenidos se considera un cumplimiento del 90% de este control.

9. SEGURIDAD FÍSICA Y DEL ENTORNO

9.1 Áreas seguras

9.1.1 Perímetro de seguridad física

Control:

"Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento"

Análisis:

Existe protección para las puertas de acceso a las tres unidades de la DTIC mediante tarjetas magnéticas, por lo general se utiliza cuando las puertas se cierran, en la jornada diaria laboral no se aplica porque las puertas permanecen abiertas, el acceso al Data Center es muy seguro, se tiene una seguridad con autenticación de huella, tarjeta magnética, barrera de protección.

Según los datos obtenidos se considera un cumplimiento del 60% de este control.

9.1.2 Controles físicos de entrada

Control:

"Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado"

Análisis:

No se tiene un control de acceso adecuado para personal no autorizado hacia las tres Unidades de la DTIC, el control es más estricto al Data Center de la Universidad, el acceso a la oficina del director de TI está controlado por una recepcionista.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

9.1.3 Seguridad de oficinas, despachos e instalaciones

Control:

"Se debería asignar y aplicar la seguridad física para oficinas, despachos y recursos"

Análisis:

Existe medidas de seguridad en especial para la mayoría de tomacorrientes eléctricos los cuales tienen conexiones a tierra, la mayoría del cableado informático cumple normas y certificaciones de seguridad, la mayoría de los equipos informáticos cuentan con reguladores de voltaje.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

9.1.4 Protección contra amenazas externas y de origen ambiental

Control:

"Se debería designar y aplicar medidas de protección física contra incendio, inundación, terremoto, explosión, malestar civil y otras formas de desastre natural o humano"

Análisis:

Existen medidas se seguridad contra incendios, la mayoría de las oficinas de las oficinas de la DTIC cuentan con extintores de fuego, al estar ubicada la DTIC en el último piso de la administración Central de la Universidad, se reduce la probabilidad por inundaciones, el Data Center dispone de sistemas contra incendios, generador de energía, no se tiene rutas de evacuación adecuadas, no existe planes de contingencia cuando exista un desastre natural.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

9.1.5 Trabajo en áreas seguras

Control:

"Se debería diseñar y aplicar protección física y pautas para trabajar en las áreas seguras"

Análisis:

De lo que se tiene conocimiento las tres unidades que conforman la DTIC cuentan con las seguridades parciales para realizar el trabajo en un ambiente seguro en lo referente a la seguridad física, existen algunos aspectos de

seguridad que se deben tener en cuenta, como por ejemplo: mejorar el control del personal no autorizado, hace falta definir rutas de evacuación adecuadas.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

9.1.6 Áreas de acceso público y de carga y descarga

Control:

"Se deberían controlar las áreas de carga y descarga con objeto de evitar accesos no autorizados y, si es posible, aislarlas de los recursos para el tratamiento de la información"

Análisis:

De lo que se tiene conocimiento el acceso a los sistemas universitarios es otorgado solo a los estudiantes y docentes, no se tiene acceso al público en general para carga y descarga de información, la página web universitaria es solo un medio informativo, la VLAN de invitados está debidamente aislada de la información confidencial universitaria, no se realiza una revisión adecuada de que información que se carga y descarga dentro de las oficinas de la DTIC.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

9.2 Seguridad de los equipos

9.2.1 Emplazamiento y protección de equipos

Control:

"El equipo debería situarse y protegerse para reducir el riesgo de materialización de las amenazas del entorno, así como las oportunidades de acceso no autorizado"

Análisis:

Los equipos informáticos son ubicados en lugares seguros, cuentan con claves de acceso al sistema operativo, no se tiene una protección adecuada en el caso de existir una amenaza de desastre natural.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

9.2.2 Instalaciones de suministro

Control:

"Se deberían proteger los equipos contra fallos en el suministro de energía u otras anomalías eléctricas en los equipos de apoyo"

Análisis:

La mayoría de equipos informáticos de la DTIC disponen de reguladores de voltaje y de equipos UPS, existen algunos UPS que no están funcionando de forma adecuada, debido al mal estado de las baterías.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

9.2.3 Seguridad del cableado

Control:

"Se debería proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles interceptaciones o daños"

Análisis:

El cableado externo de la red LAN es de fibra óptica utilizado para interconectar los edificios, el cableado es subterráneo y cuando la fibra óptica sufre algún daño por factores externos, se contrata a una empresa externa que solucione el problema, no existe un plan de contingencia para reestablecer los servicios lo ante posible. El cableado interno de la DTIC en su gran mayoría se encuentra instalado bajo normas y certificación, existen pocos cables que no cumplen las normas.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

9.2.4 Mantenimiento de los equipos

Control:

"Se deberían mantener adecuadamente los equipos para garantizar su continua disponibilidad e integridad"

Análisis:

Existe un plan de mantenimiento preventivo anual para los equipos informáticos de la DTIC y de la Administración Central de la Universidad, se crea un cronograma de mantenimiento y se lo realiza de acuerdo a las

fechas establecidas, el plan se cumple casi en su totalidad ya que existen usuarios que no dan las facilidades para cumplir con este proceso.

Según los datos obtenidos se considera un cumplimiento del 95% de este control.

9.2.5 Seguridad de los equipos fuera de las instalaciones

Control:

"Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización considerando los diversos riesgos a los que están expuestos"

Análisis:

No se aplica el control debido a que según la información receptada, no se utilizan los equipos informáticos fuera de las instalaciones de la Universidad, los equipos informáticos son de uso exclusivo para el personal que labora dentro de la DTIC, los equipos portátiles son de entera responsabilidad del custodio.

Según los datos obtenidos se considera un cumplimiento del 0% de este control.

9.2.6 Reutilización o retirada segura de equipos

Control:

"Debería revisarse cualquier elemento del equipo que contenga dispositivos de almacenamiento con el fin de garantizar que cualquier dato sensible y software con licencia se haya eliminado o sobrescrito con seguridad antes de la eliminación"

Análisis:

Cuando los equipos informáticos son retirados, enviados a la bodega, o se cambian de usuario, por lo general se realiza un respaldo de la información por parte del propietario y se realiza otro respaldo adicional por parte del personal de soporte de primera línea de la DTIC, en la mayoría de casos los equipos son formateados y se vuelven a instalar el sistema operativo.

Según los datos obtenidos se considera un cumplimiento del 95% de este control.

9.2.7 Retirada de materiales propiedad de la empresa

Control:

"No deberían sacarse equipos, información o software fuera del local sin una autorización"

Análisis:

De lo que se tiene conocimiento los equipos informáticos son de uso exclusivo para el personal de la DTIC, el software instalado en los equipos tienen licenciamiento y control de instalaciones, el personal tiene la prohibición de utilizar los equipos fuera de las instalaciones de la Universidad, solo el Director de la DTIC y algunos los Coordinadores tienen autorización de trabajar con los equipos portátiles fuera de las oficinas, cada uno es responsable del equipo, además existe la prohibición de sacar la información confidencial de la DTIC, pero no existe una adecuada revisión de la extracción de la información.

Según los datos obtenidos se considera un cumplimiento del 60% de este control.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.1 Responsabilidades y procedimientos de operaciones

10.1.1 Documentación y procedimientos de operación

Control:

"Se deberían documentar y mantener los procedimientos de operación y ponerlos a disposición de todos los usuarios que lo necesiten"

Análisis:

De lo que se tiene conocimiento existen pocos procedimientos que son documentados, actualmente se están elaborando los documentos técnicos para algunos sistemas informáticos, se tiene documentación sobre configuraciones de algunos equipos de comunicación, los manuales de usuario son pocos y en muchos casos incompletos.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

10.1.2 Gestión de cambios

Control:

"Se deberían controlar los cambios en los sistemas y en los recursos de tratamiento de la información"

Análisis:

La mayoría de controles de cambios se lo realiza cuando se está desarrollando, modificando o actualizando los sistemas informáticos institucionales, en las pruebas de escritorio y pruebas piloto por parte de los usuarios, la mayor parte de cambios son notificados al personal de desarrollo, no existe una política formal para el control de cambios, ni revisiones de su cumplimiento.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

10.1.3 Segregación de tereas

Control:

"Se deberían segregar las tareas y las áreas de responsabilidad con el fin de reducir las oportunidades de una modificación no autorizada o no intencionada, o el de un mal uso de los activos de la organización"

Análisis:

Las tareas y responsabilidades son separadas de acuerdo al perfil del personal que labora en la DTIC, existe un coordinador de cada Unidad quien está al tanto del correcto desempeño laboral del personal que allí labora, existen tareas que son compartidas entre el personal, los administradores de los sistemas tienen acceso a revisar, modificar la información.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

10.1.4 Separación de los recursos de desarrollo, prueba y operación

Control:

"La separación de los recursos para el desarrollo, prueba y producción es importante para reducir los riesgos de un acceso no autorizado o de cambios al sistema operacional"

Análisis:

En la Unidad de Sistemas de Información se encuentra separado el tratamiento a los sistemas informáticos, existe personal que se encarga del desarrollo de nuevos sistemas, otro personal para modificaciones en los sistemas existentes, se cuenta con personal que se encarga de las pruebas y de poner en operación a los sistemas nuevos y modificados.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

10.2 Gestión de la provisión de servicio por terceros

10.2.1 Provisión de servicios

Control:

"Se debería garantizar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el acuerdo de entrega de servicio externo sean implementados, operados y mantenidos por la parte externa"

Análisis:

Cuando existe una implementación de un nuevo sistema informático por parte de terceros, existen cláusulas de controles de seguridad que se cumplen como está definido en la documentación, en ocasiones suele fallar

los tiempos de entrega o implementación por factores externos, dependiendo de las cláusulas establecidas en los contratos se lleva a cabo penalidades.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

10.2.2 Supervisión y revisión de los servicios prestados por terceros

Control:

"Los servicios, informes y registros suministrados por terceros deberían ser monitoreados y revisados regularmente, y las auditorías se deberían realizar a intervalos regulares"

Análisis:

La revisión, supervisión y cumplimiento de los servicios prestados por terceros se lo realiza de acuerdo a las cláusulas establecidas en los contratos, por lo general existe un administrador de contrato designado, quien es el responsable de verificar el correcto cumplimiento del contrato, auditorias son efectuadas ocasionalmente.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

10.2.3 Gestión del cambio en los servicios prestados por terceros

Control:

"Se deberían gestionar los cambios en la provisión del servicio, incluyendo mantenimiento y mejoras en las políticas de seguridad de información existentes, en los procedimientos y los controles teniendo en cuenta la

importancia de los sistemas y procesos del negocio involucrados, así como la reevaluación de los riesgos"

Análisis:

De lo que se tiene conocimiento existe un administrador de contrato, quien es el responsable de verificar que se cumplan las cláusulas establecidas en cada contrato, por ejemplo en la dotación de equipos informáticos cuando se realiza la recepción, se verifica el correcto funcionamiento de los equipos, en caso de existir algún problema se notifica al proveedor el cambio de algún equipo, hasta que no esté todo funcionando de forma adecuada no se firma el acta de recepción, este control no es cumplido en su totalidad.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

10.3 Planificación y aceptación del sistema

10.3.1 Gestión de capacidades

Control:

"Se debería monitorizar el uso de recursos, así como de las proyecciones de los requisitos de las capacidades adecuadas para el futuro con objeto de asegurar el funcionamiento requerido del sistema"

Análisis:

El personal que labora en la unidad de Redes y Comunicaciones por lo general realiza el monitoreo permanente de los estados de los servidores, el consumo de memoria, procesamiento, espacio de almacenamiento, en caso de existir algún inconveniente se notifica a los responsables de la

administración de los respectivos servidores para que tomen las medidas necesarias, en algunos casos no se toman las medidas correctivas de forma inmediata.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

10.3.2 Aceptación del sistema

Control:

"Se deberían establecer criterios de aceptación para nuevos sistemas de información, actualizaciones y versiones nuevas. Se deberían desarrollar las pruebas adecuadas del sistema durante el desarrollo y antes de su aceptación"

Análisis:

En la Unidad de Sistemas de Información se delega a un supervisor de sistemas, quien conjuntamente con los usuarios finales lleva a cabo todas las evaluaciones para los nuevos sistemas, modificación de sistemas existentes, dependiendo de los resultados el usuario acepta o no el sistema informático.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

10.4 Protección contra el código malicioso y descargable

10.4.1 Controles contra código malicioso

Control:

"Se deberían implantar controles de detección, prevención y recuperación contra el software malicioso, junto a procedimientos adecuados para la concienciación de los usuarios"

Análisis:

En la Unidad de Servicios Informáticos existe un delegado que administra el servidor del antivirus Kaspersky, que continuamente lleva un control y monitoreo de virus, spyware, gusanos, troyanos, en las estaciones de trabajo semanalmente, en caso de existir algún equipo infectado la consola de administración del antivirus identifica el equipo y reporta al administrador para las acciones necesarias, en ocasiones se realiza campañas de concienciación a los usuarios en temas de virus informáticos, existen equipos informáticos que no están debidamente configurados con el antivirus, otros equipos tienen vencida la licencia de antivirus, existe poca información y capacitación a los usuarios finales para concientizar sobre las amenazas de software malicioso .

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

10.4.2 Controles contra códigos descargados en el cliente

Control:

"Cuando se autoriza la utilización de código móvil, la configuración debería asegurar que dicho código móvil opera de acuerdo a una política de seguridad definida y se debería evitar la ejecución de los códigos móviles no autorizados"

Análisis:

La solución de antivirus Kaspersky tiene la opción de antivirus para dispositivos móviles, es responsabilidad del propietario del dispositivo la información que descarga, las aplicaciones móviles universitarias son solo de consulta y la mayoría cumplen con controles de seguridad.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

10.5 Copias de seguridad

10.5.1 Copias de seguridad de la información

Control:

"Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, de acuerdo con la política acordada de recuperación"

Análisis:

El personal de la Unidad de Redes y Comunicaciones es el encargado de realizar los respaldos de la información generada por los sistemas

informáticos, los respaldos se los realiza diariamente en las noches y luego se realiza respaldos en cinta.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

10.6 Gestión de la seguridad de las redes

10.6.1 Controles de red

Control:

"Se deberían mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito"

Análisis:

El personal de la Unidad de Redes y Comunicaciones aplica controles de seguridad a la red LAN, las redes están segmentadas mediante VLANs, la red de invitados tiene restricciones para acceder a la red administrativa, así mismo la red inalámbrica WIFI tiene acceso solo al internet, en ocasiones se analiza el tráfico de información en la red de invitados y WIFI, no se tiene mecanismos para proteger la información que viaja por la red LAN, y no se tiene control de la información que circula por la red de invitados.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

10.6.2 Seguridad de los servicios de red

Control:

"Se deberían identificar e incluir, en cualquier acuerdo sobre servicios de red, las características de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, independientemente de que estos servicios sean provistos desde la propia organización o se contratan desde el exterior"

Análisis:

Los servicios que brinda la DTIC cuentan con las seguridades para garantizar el adecuado acceso y trabajo en los sistemas informáticos institucionales tanto en el acceso interno y externo, en ocasiones suele existir problemas en algún sistema informático lo que impide el adecuado trabajo diario, no existe un plan de contingencia contra interrupciones de servicio, cuando existe alguna falla se trata de volver a reestablecer los servicios lo antes posible en el menor tiempo.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

10.7 Manipulación de los soportes

10.7.1 Gestión de soportes extraíbles

Control:

"Se deberían establecer procedimientos para la gestión de los medios informáticos removibles"

Análisis:

En la actualidad se emplea muy poco el uso de dispositivos extraíbles para compartir información, la única protección que se tiene es el uso del antivirus para los medios extraíbles utilizados en los equipos informáticos de la DTIC, no existe mecanismos para proteger los dispositivos extraíbles y la información que transportan.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

10.7.2 Retirada de soportes

Control:

"Se deberían eliminar los medios de forma segura y sin riesgo cuando ya no sean requeridos, utilizando procedimientos formales"

Análisis:

Cuando ya no se utilizan los medios por ejemplo medios extraíbles se envía a la bodega, por lo general no se tiene la precaución de eliminar de forma segura la información que contiene dichos medios, en el caso de los CDs que tienen información relacionada con la institución, no se tiene la precaución de destruir los discos que ya no se ocupan o están defectuosos, no existe un procedimiento formal para este control.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

10.7.3 Procedimientos de manipulación de la información

Control:

"Se deberían establecer procedimientos para la manipulación y almacenamiento de la información con el objeto de proteger esta información contra divulgaciones o usos no autorizados o inadecuados"

Análisis:

La manipulación de información por lo general lo realiza el personal autorizado, la información personal es entera responsabilidad del propietario, existe una prohibición del uso indebido y de fuga de la información confidencial universitaria, por lo general este control no es aplicado de forma correcta, pero no existe una política y sanciones para aquellos colaboradores que utilizan de forma indebida la información.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

10.7.4 Seguridad de la documentación del sistema

Control:

"Se debería proteger la documentación de los sistemas contra accesos no autorizados"

Análisis:

El acceso a la documentación de los sistemas informáticos institucionales solo está permitido para los administradores de los diferentes sistemas, cada uno es responsable del correcto uso y de la seguridad de cada documento

físico y digital, no se tiene un control adecuado del uso y manipulación de la información almacenada en los computadores.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

10.8 Intercambio de información

10.8.1 Políticas y procedimientos de intercambio de información

Control:

"Se deberían establecer políticas, procedimientos y controles formales de intercambio con objeto de proteger la información mediante el uso de todo tipo de servicios de comunicación"

Análisis:

La información que se intercambia en la DTIC se lo realiza en formatos: (docx, xlsx, pdf), se envía por correo electrónico como archivo adjunto a los coordinadores de cada Unidad, en ocasiones se utilizan medios extraíbles, no se tienen definidos controles adicionales para asegurar la seguridad de la información, no se tiene control ni registro de la información que se pueda intercambiar entre el personal de la DTIC.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

10.8.2 Acuerdos de intercambio

Control:

"Se deberían establecer acuerdos para el intercambio de información y software entre la organización y las partes externas"

Análisis:

Por lo general los acuerdos de intercambio de información están establecidos en las cláusulas de los contratos de trabajo para el personal que se va a integrar a la DTIC, pero no siempre se cumple lo estipulado en los contratos, no existe un seguimiento y verificación del cumplimiento de los acuerdos, para la prestación de servicios con terceros existe acuerdos de intercambio de información definidos en las cláusulas de los contratos entre la Universidad y la entidad que presta sus servicios.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

10.8.3 Soportes físicos en tránsito

Control:

"Se deberían proteger los medios que contienen información contra acceso no autorizado, mal uso o corrupción durante el transporte fuera de los límites físicos de la organización"

Análisis:

La DTIC aplica mecanismos para proteger los equipos informáticos y así garantizar el acceso adecuado a los sistemas institucionales, solo los usuarios autenticados tienen acceso de acuerdo al perfil establecido, pero no existe una verificación del adecuado cumplimiento, no existe seguridades como por ejemplo: protección de cifrado de información en el acceso web.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

10.8.4 Mensajería electrónica

Control:

"Se debería proteger adecuadamente la información contenida en la mensajería electrónica"

Análisis:

Existe protección física para los servidores de correo electrónico institucional, adicional se cuenta con software anti spam, se tiene definido un límite para envío de archivos adjuntos, permanentemente se está monitoreando los buzones de correo electrónico, se realizan pocas campañas informativas vía correo electrónico sobre amenazas como por ejemplo: ingeniería social, no se cuenta con protección para la información que viaja en los correos electrónicos, no existe una concientización de los usuarios sobre el uso correcto de la contraseña, ni los controles adecuados.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

10.8.5 Sistemas de información empresarial

Control:

"Se deberían desarrollar e implementar políticas y procedimientos con el fin de proteger la información asociada con la interconexión de sistemas de información del negocio"

Análisis:

No se aplica el control ya que la Universidad es un establecimiento de Educación Superior Público sin fines de lucro, todos los sistemas

informáticos institucionales están relacionados con las actividades diarias de los estudiantes y docentes, la página web institucional es de carácter informativo.

Según los datos obtenidos se considera un cumplimiento del 0% de este control.

10.9 Servicios de comercio electrónico

10.9.1 Comercio electrónico

Control:

"Se debería proteger la información involucrada en el comercio electrónico que pasa por redes públicas contra actividades fraudulentas, disputas por contratos y divulgación o modificación no autorizadas"

Análisis:

No se aplica el control ya que la Universidad es un establecimiento de Educación Superior Público sin fines de lucro, no existe comercio electrónico, los sistemas web son básicamente relacionados con labores académicas.

Según los datos obtenidos se considera un cumplimiento del 0% de este control.

10.9.2 Transacciones en línea

Control:

"Se debiera proteger la información involucrada en las transacciones en línea para evitar una transmisión incompleta, alteración no autorizada del

mensaje, divulgación no autorizada, duplicación o repetición no autorizada del mensaje"

Análisis:

No se aplica el control ya que la Universidad es un establecimiento de Educación Superior Público sin fines de lucro, los pagos por algún servicio, capacitación, horas de clases, etc., son cancelados en las ventanillas de la Tesorería de la Administración Central y otros pagos se realizan en las ventanillas de los bancos donde se tiene la apertura de las cuentas de la Universidad.

Según los datos obtenidos se considera un cumplimiento del 0% de este control.

10.9.3 Información públicamente disponible

Control:

"Se debería proteger la integridad de la información que pone a disposición en un sistema de acceso público para prevenir modificaciones no autorizadas"

Análisis:

La DTIC tiene implementado algunas seguridades en el servidor Web, pero no se realiza una validación y verificación frecuente para determinar si existen vulnerabilidades en la aplicación web, no existe un plan de contingencia en caso de una caída del sitio web. La administración de la página web institucional está a cargo del personal de la Unidad de Redes y Comunicaciones, existe un operador de la página web en la Unidad de

Relaciones Publicas y Comunicación, quien es el encargado de subir la información universitaria.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

10.10 Supervisión

10.10.1 Registros de auditoría

Control:

"Se deberían producir y mantener durante un periodo establecido los registros de auditoria con la grabación de las actividades de los usuarios, excepciones y eventos de la seguridad de información, con el fin de facilitar las investigaciones futuras y el monitoreo de los controles de acceso"

Análisis:

De lo que se tiene conocimiento se realiza un chequeo permanente de las actividades, rendimiento, espacios de almacenamiento de los servidores, no se revisa los registros de los logs de las aplicaciones, tiempo de conexión de las sesiones de usuario, tampoco existe controles de auditoria en temas de controles de acceso, seguridad de la información, no se lleva acabo grabaciones y registros de las actividades de usuarios y de los administradores de los sistemas informáticos.

Según los datos obtenidos se considera un cumplimiento del 60% de este control.

10.10.2 Supervisión del uso del sistema

Control:

"Se deberían establecer procedimientos para el uso del monitoreo de las instalación de procesamiento de información y revisar regularmente los resultados de las actividades de monitoreo"

Análisis:

Existe un monitoreo del rendimiento de los servidores, en pocas ocasiones se realiza un monitoreo de los registros, logs en los servidores y de los sistemas informáticos institucionales, no se revisa y analiza con frecuencia los resultados de las actividades de monitoreo, en pocas ocasiones se guardan los resultados de monitoreo para futuras evaluaciones.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

10.10.3 Protección de la información de los registros

Control:

"Se deberían proteger los servicios y la información de registro de la actividad contra acciones forzosas o accesos no autorizados"

Análisis:

Por lo general los servicios que brinda la DTIC a la comunidad Universitaria están protegidos contra accesos no autorizados, pero no se realiza una verificación del adecuado cumplimiento, en ocasiones los reportes de actividades y de los sistemas informáticos son enviados vía

correo electrónico y en físico a cada coordinador de la respectiva Unidad, no se tiene protección de los registros de monitoreo y auditoria.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

10.10.4 Registros de administración y operación

Control:

"Se deberían registrar las actividades del administrador y de los operadores del sistema"

Análisis:

En los logs de los servidores existe registro de las actividades que realizan a diario los administradores y operadores de los sistemas informáticos, pero casi nunca se revisa y analiza allí almacenada, tampoco se tiene un registro detallado de las actividades de los administradores y operadores en formato digital o físico y almacenado en lugares seguros.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

10.10.5 Registro de fallos

Control:

"Se deberían registrar, analizar y tomar acciones apropiadas de las averías"

Análisis:

Por lo general las fallas en los sistemas informáticos son detectados por los operadores, administradores y los usuarios finales, cuando existe una falla por lo general se crea una incidencia en el sistema de Help Desk, el personal de soporte de primera línea revisa y analiza la incidencia, en caso de no poder revolver se escala la incidencia al personal de soporte de segunda línea para dar la respectiva solución.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

10.10.6 Sincronización del reloj

Control:

"Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información dentro de la organización o en el dominio de seguridad, con una fuente acordada y exacta de tiempo"

Análisis:

La gran mayoría de equipos informáticos de la DTIC trabajan dentro del dominio de Microsoft Active Directory, la fecha y hora es sincronizado de forma automática con el controlador de dominio Windows Server 2008 R2.

Según los datos obtenidos se considera un cumplimiento del 90% de este control.

11. CONTROL DEL ACCESO

11.1 Requisitos de negocio para el control del acceso

11.1.1 Política de control de acceso

Control:

"Se debería establecer, documentar y revisar una política de control de accesos en base a las necesidades de seguridad y de negocio de la Organización"

Análisis:

Los controles de acceso a los sistemas informáticos institucionales son supervisados por los administradores de cada sistema informático, los permisos para los usuarios son solicitados al director de la DTIC, en base al rol de cada usuario se habilita el permiso de acceso, no se realiza una verificación del adecuado cumplimiento y tampoco se encuentra definida una adecuada política de control de acceso.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

11.2 Gestión de acceso de usuario

11.2.1 Registro de usuario

Control:

"Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información"

Análisis:

Por lo general existe un control de usuarios, en especial cuando se existen cambios de roles o cuando se integra un nuevo funcionario a la Universidad, el jefe inmediato del usuario en mención solicita vía Quipux la creación o modificación del nuevo perfil al Director de la DTIC, cuando un funcionario deja de laborar por algún motivo en la Universidad, el Director de la DTIC notifica a los administradores de los sistemas para que den de baja al usuario que está dejando de prestar sus servicios, pero en algunas ocasiones no existe un adecuado control del correcto cumplimiento de éste control ya que en ocasiones siguen activas algunas cuentas de usuarios que dejaron de laborar en la Universidad.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

11.2.2 Gestión de privilegios

Control:

"Se debería restringir y controlar la asignación y uso de los privilegios"

Análisis:

Por lo general existe una unificación de permisos y roles para usar algunos sistemas informáticos institucionales, con la misma clave se tiene acceso al perfil establecido para el usuario de acuerdo a la solicitud enviada al Director de la DTIC, pero no existe una restricción total ni la respectiva verificación del adecuado cumplimiento.

Según los datos obtenidos se considera un cumplimiento del 90% de este control.

11.2.3 Gestión de contraseñas de usuario

Control:

"Se debería controlar la asignación de contraseñas mediante un proceso de gestión formal"

Análisis:

La Unidad de Servicios Informáticos genera las cuentas para los nuevos usuarios que se van a integrar a la Universidad, los usuarios tienen la obligación de cambiar la clave generada de forma automática y personalizarla de acuerdo a los parámetros establecidos y las recomendaciones de seguridad, se recuerda a los usuarios que el uso de las claves son de entera responsabilidad del propietario.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

11.2.4 Revisión de los derechos de acceso de usuario

Control:

"El órgano de Dirección debería revisar con regularidad los derechos de acceso de los usuarios, siguiendo un procedimiento formal"

Análisis:

El coordinador de la Unidad de Sistemas de Información delega la responsabilidad a los administradores de los sistemas informáticos sobre la gestión de usuarios como por ejemplo: revisión de perfiles, permisos de

acceso, la gestión se lo realiza de forma rutinaria pero no como un procedimiento formal establecido en alguna política.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

11.3 Responsabilidades del usuario

11.3.1 Uso de contraseñas

Control:

"Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad en la selección y uso de las contraseñas"

Análisis:

Existe una campaña informativa vía correo electrónico sobre información y consejos para el correcto uso de las contraseñas, requisitos de complejidad, etc. Por lo general las campañas se las realiza cada dos meses.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

11.3.2 Equipo del usuario desatendido

Control:

"Los usuarios deberían garantizar que los equipos desatendidos disponen de la protección apropiada"

Análisis:

No se aplica el control ya que la todos los equipos informáticos de la DTIC son ocupados por el personal de cada Unidad, se tiene conocimiento que no existen equipos desatendidos.

Según los datos obtenidos se considera un cumplimiento del 0% de este control.

11.3.3 Política de puesto de trabajo y pantalla limpios

Control:

"Políticas para escritorios y monitores limpios de información"

Análisis:

Según se tiene conocimiento no existe una política para el uso de escritorios y pantallas limpias, es responsabilidad de cada usuario saber cómo se organiza en su puesto de trabajo, como administra su información digital.

Según los datos obtenidos se considera un cumplimiento del 10% de este control.

11.4 Control de acceso a la red

11.4.1 Política de uso de los servicios en red

Control:

"Se debería proveer a los usuarios de los accesos a los servicios para los que han sido expresamente autorizados a utilizar"

Análisis:

Por lo general los jefes de cada Unidad de la DTIC avalan los perfiles y roles para el personal que allí laboran, el mismo procedimiento lo realiza los jefes de cada dependencia de la Universidad, la generación de los nuevos usuarios los realiza el personal de la Unidad de Servicios Informáticos, después de la aprobación de la solicitud enviada al Director de la DTIC, pero en ocasiones existen usuarios sin los permisos adecuados, hay otros usuarios con permisos adicionales especialmente en los sistemas informáticos para los cuales no están autorizados, no se realiza una verificación frecuente de todos los perfiles de usuario.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

11.4.2 Autenticación del usuario para las conexiones externas

Control:

"Se deberían utilizar métodos de autenticación adecuados para el control del acceso remoto de los usuarios"

Análisis:

Por lo general el acceso remoto hacia los sistemas informáticos institucionales cuenta con los controles y métodos de autenticación adecuados para garantizar que solo el personal autorizado, estudiantes y docentes ingresen de acuerdo a su perfil. Pero no se realiza una revisión frecuente del adecuado uso de los controles de acceso, tampoco se revisa los registros de acceso en los servidores.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

11.4.3 Identificación del equipo en las redes

Control:

"Se debería considerar la identificación automática de los equipos como un medio de autenticación de conexiones procedentes de lugares y equipos específicos"

Análisis:

La gran mayoría de los equipos informáticos de la DTIC trabajan bajo un dominio de Microsoft Active Directory, el nombre del equipo en la red está delimitado por las iniciales de la Dependencia o Unidad y las iniciales del nombre y apellido del usuario, no existe una revisión y actualización frecuente de los equipos en la red, existe equipos con otras credenciales en la red LAN lo que dificulta su ubicación.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

11.4.4 Diagnostico remoto y protección de los puertos de configuración

Control:

"Se debería controlar la configuración y el acceso físico y lógico a los puertos de diagnóstico"

Análisis:

El personal de la Unidad de Redes y Comunicaciones administra todos los servidores de la Universidad, habilita solo los puertos necesarios de acuerdo

a cada sistema informático, cuando se adiciona un nuevo sistema informático o alguna aplicación, se emite una solicitud al coordinador de la Unidad de Redes, indicando las funciones de la nueva aplicación y los puertos que necesita.

Según los datos obtenidos se considera un cumplimiento del 100% de este control.

11.4.5 Segregación en redes

Control:

"Se deberían segregar los grupos de usuarios, servicios y sistemas de información en las redes"

Análisis:

Como la gran mayoría de equipos que se utilizan en la DTIC y en la Administración Central trabajan bajo un dominio de Microsoft Active Directory, en donde se tiene clasificado a los usuarios por Unidades Organizacionales de acuerdo a cada dependencia, la red universitaria interna se encuentra segregada por medio de VLANs.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

11.4.6 Control de la conexión a la red

Control:

"En el caso de las redes compartidas, especialmente aquellas que se extienden más allá de los límites de la propia Organización, se deberían restringir las competencias de los usuarios para conectarse en red según la

política de control de accesos y necesidad de uso de las aplicaciones de negocio"

Análisis:

Tanto las redes LAN internas y externas son controladas por el personal de la Unidad de Redes y Comunicaciones, la red interna tiene acceso por autenticación a los sistemas internos de la Universidad, la red externa tiene restricción de acceso a los sistemas internos, el control se lo realiza por VLANs, no se realiza una revisión periódica de los controles de acceso.

Según los datos obtenidos se considera un cumplimiento del 90% de este control.

11.4.7 Control de encaminamiento (routing) de red

Control:

"Se deberían establecer controles de enrutamiento en las redes para asegurar que las conexiones de los ordenadores y flujos de información no incumplen la política de control de accesos a las aplicaciones de negocio"

Análisis:

El personal de la Unidad de Redes y Comunicaciones realizan la administración de las redes informáticas Universitarias, por lo general se monitorea el correcto funcionamiento de los equipos de comunicación informáticos como son: switches, routers, APs, etc, en ocasiones cuando se realizan cambios o modificaciones en los equipos de comunicación, no existe documentación de estos cambios.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

11.5 Control del acceso al sistema operativo

11.5.1 Procedimientos seguro de sesión

Control:

"Debería controlarse el acceso al sistema operativo mediante procedimientos seguros de conexión"

Análisis:

El acceso a las sesiones de usuario en los equipos informáticos y el uso de los sistemas institucionales requieren por lo general una autenticación, las sesiones de los usuarios en los sistemas informáticos en ocasiones son revisadas y monitoreadas, no se tiene una revisión o monitoreo del acceso a los sistemas operativos.

Según los datos obtenidos se considera un cumplimiento del 90% de este control.

11.5.2 Identificación y autenticación de usuario

Control:

"Todos los usuarios deberían disponer de un único identificador propio para su uso personal y exclusivo. Se debería elegir una técnica de autenticación adecuada que verifique la identidad reclamada por un usuario2.

Análisis:

Por lo general se tiene un único identificador para el uso de los diferentes sistemas informáticos, la clave de acceso a la sesión de usuario en los equipos informáticos es personalizada por cada usuario, es de entera responsabilidad del propietario de la clave el uso correcto de la misma, no existe una revisión frecuente en los registros de los servidores para determinar el correcto uso del identificador único.

Según los datos obtenidos se considera un cumplimiento del 90% de este control.

11.5.3 Sistema de gestión de contraseñas

Control:

"Los sistemas de gestión de contraseñas deberían ser interactivos y garantizar la calidad de las contraseñas"

Análisis:

En las opciones de cambio de claves en algunos sistemas informáticos, existe mensajes con consejos, requisitos y recomendaciones que debe cumplir la nueva clave, si la clave ingresada no cumple con los requisitos mínimos de seguridad, por lo general el sistema genera una alerta para que el usuario vuelva a ingresar una nueva clave, este control no se aplica para todos los sistemas informáticos.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

11.5.4 Uso de los recursos del sistema

Control:

"Se debería restringir y controlar muy de cerca el uso de programas de utilidad del sistema que pudieran ser capaces de eludir los controles del propio sistema y de las aplicaciones"

Análisis:

La mayoría de los equipos informáticos que se usan en la DTIC está bajo un controlador de dominio Microsoft Active Directory, pero no está definido los permisos de los usuarios en su totalidad, existen algunos perfiles de usuario con permisos para agregar o quitar aplicaciones, por lo que en ocasiones resulta dificultoso revisar los programas y aplicaciones instaladas en los equipos.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

11.5.5 Desconexión automática de sesión

Control:

"Se deberían desconectar las sesiones tras un determinado periodo de inactividad"

Análisis:

De lo que se tiene conocimiento se desconectan las sesiones de usuario que no están activas por un lapso de tiempo determinado en algunos sistemas informáticos, en el caso de las sesiones de usuario inactivas en algunos

equipos informáticos, se reactiva el uso de la sesión por medio de la clave de usuario, pero no se realiza este proceso en todos los equipos.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

11.5.6 Limitación del tiempo de conexión

Control:

"Se deberían utilizar limitaciones en el tiempo de conexión que proporcionen un nivel de seguridad adicional a las aplicaciones de alto riesgo"

Análisis:

La limitación de tiempo de conexión está definida por defecto en los sistemas informáticos, en el caso de los equipos informáticos no se cumple este control en su totalidad.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

11.6 Control de acceso a las aplicaciones y a la información

11.6.1 Restricción del acceso a la información

Control:

"Se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos definida"

Análisis:

El acceso a las sesiones de usuario en algunos equipos informáticos está permitida por el uso obligatorio de la clave del sistema operativo, no está formalizada una política de control de acceso a las estaciones de trabajo.

Según los datos obtenidos se considera un cumplimiento del 90% de este control.

11.6.2 Aislamiento de sistemas sensibles

Control:

"Los sistemas sensibles deberían disponer de un entorno informático dedicado (propio)"

Análisis:

El aislamiento de los sistemas sensibles como por ejemplo: sistema financiero, contable, etc. Se lo realiza por medio de VLANs en la red LAN interna, solo tiene acceso el personal autorizado de acuerdo a su perfil, el uso de las claves es de responsabilidad del propietario de la cuenta de usuario, no se revisa el cumplimiento de este control con frecuencia.

Según los datos obtenidos se considera un cumplimiento del 90% de este control.

11.7 Ordenadores portátiles y teletrabajo

11.7.1 Ordenadores portátiles y comunicaciones móviles

Control:

"Se debería establecer una política formal y se deberían adoptar las medidas de seguridad adecuadas para la protección contra los riesgos derivados del uso de los recursos de informática móvil y las telecomunicaciones"

Análisis:

Los equipos móviles por ejemplo: notebooks que se usan en la red interna tienen el mismo control de acceso que las estaciones de trabajo fijas, no está disponible el acceso a los sistemas informáticos internos por medio de un Smartphone, existe control de acceso externo para los sistemas institucionales.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

11.7.2 Teletrabajo

Control:

"Se debería desarrollar e implantar una política, planes operacionales y procedimientos para las actividades de teletrabajo"

Análisis:

De lo que se tiene conocimiento no existe una política formal para actividades de teletrabajo en la DTIC, y el toda la Universidad, actividades

de teletrabajo existen en pocas cantidades en la DTIC y en diferentes dependencias de la Universidad.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

12.1 Requerimientos de seguridad de los sistemas de información

12.1.1 Análisis y especificación de los requisitos de seguridad

Control:

"Las demandas de nuevos sistemas de información para el negocio o mejoras de los sistemas ya existentes deberían especificar los requisitos de los controles de seguridad"

Análisis:

De lo que se tiene conocimiento el coordinador de la Unidad de Sistemas de Información se reúne con el personal de desarrollo, para analizar los requisitos de los nuevos sistemas informáticos o mejora de los ya existentes, se analiza ciertos aspectos que tienen que ver con los controles de acceso y seguridad, no existe un procedimiento formal para modificaciones o actualizaciones en los sistemas que se encuentran en producción, tampoco se realizan verificaciones del cumplimiento de este control.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

12.2 Tratamiento correcto en las aplicaciones

12.2.1 Validación de los datos de entrada

Control:

"Se deberían validar los datos de entrada utilizados por las aplicaciones para garantizar que estos datos son correctos y apropiados"

Análisis:

En algunas ocasiones se realiza validaciones de los datos de entrada para los sistemas informáticos, la mayoría de veces se trabaja a partir de la identificación y corrección de los errores receptados, no se realiza un control del cumplimiento de este control.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

12.2.2 Control del procesamiento interno

Control:

"Se deberían incluir chequeos de validación en las aplicaciones para la detección de una posible corrupción en la información debida a errores de procesamiento o de acciones deliberadas"

Análisis:

De lo que se tiene conocimiento en pocas ocasiones se realiza chequeos de validación en los sistemas informáticos, más se trabaja con la corrección de errores recibidos y detectados en las fases de pruebas.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

12.2.3 Integridad de los mensajes

Control:

"Se deberían identificar los requisitos para asegurar la autenticidad y protección de la integridad del contenido de los mensajes en las aplicaciones, e identificar e implantar los controles apropiados"

Análisis:

Por lo general los mensajes y alertas de los sistemas informáticos son revisados y valorados por el personal que realiza las pruebas, si existe una incoherencia entre los controles y los mensajes del sistema, se notifica al personal de desarrollo para su respectiva revisión y corrección, pero no siempre se realiza una evaluación del correcto cumplimiento de este control.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

12.2.4 Validación de los datos de salida

Control:

"Se deberían validar los datos de salida de las aplicaciones para garantizar que el procesamiento de la información almacenada es correcto y apropiado a las circunstancias"

Análisis:

Se realiza verificaciones periódicas de los datos de salida en las pruebas de escritorio, también se verifican los datos de salida cuando se pone en producción los sistemas informáticos y se trabaja con la corrección de errores al recibir reportes de incidencias y problemas en los sistemas.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

12.3 Controles criptográficos

12.3.1 Política sobre el uso de controles criptográficos

Control:

"Se debería desarrollar e implantar una política de uso de controles criptográficos para la protección de la información"

Análisis:

De lo que se tiene conocimiento existen definidos controles criptográficos para proteger la información en algunos sistemas informáticos, no existe una política formal para la protección de la información por medio de seguridad criptográfica, por lo general no se revisa el cumplimiento de este control.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

12.3.2 Gestión de claves

Control:

"Se debería establecer una gestión de las claves que respalde el uso de las técnicas criptográficas en la Organización"

Análisis:

En la mayoría de sistemas informáticos están definido las técnicas criptográficas para la gestión de claves de acceso, en especial en los sistemas académicos internos y externos, pero no siempre se utilizan las técnicas criptográficas.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

12.4 Seguridad de los archivos del sistema

12.4.1 Control del software en explotación

Control:

"Se deberían establecer procedimientos con objeto de controlar la instalación de software en sistemas que estén operativos"

Análisis:

De lo que se tiene conocimiento en algunos equipos informáticos de la DTIC y de la Administración Central se monitorea el software instalado, la mayoría de equipos trabajan bajo un controlador de dominio, no se puede supervisar todas las instalaciones de software porque hay equipos que tienen permisos para instalar y desinstalar programas.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

12.4.2 Protección de datos de prueba del sistema

Control:

"Se deberían seleccionar, proteger y controlar cuidadosamente los datos utilizados para las pruebas"

Análisis:

La información utilizada para realizar pruebas en los diferentes sistemas informáticos tiene acceso solo el personal de la Unidad de Sistemas de Información.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

12.4.3 Control de acceso al código fuente de los programa

Control:

"Se debería restringir el acceso al código fuente de los programas"

Análisis:

El acceso a los servidores en donde se alojan los diferentes sistemas informáticos es exclusivamente para el personal de la Unidad de Sistemas de Información, el acceso al código fuente lo tiene el personal de desarrollo quienes son los responsables del uso correcto del código.

Según los datos obtenidos se considera un cumplimiento del 100% de este control.

12.5 Seguridad en los procesos de desarrollo y soporte

12.5.1 Procedimientos de control de cambios

Control:

"Se debería controlar la implantación de cambios mediante la aplicación de procedimientos formales de control de cambios"

Análisis:

Los cambios se los realiza en los sistemas informáticos según exista la necesidad, en especial cuando se está en fase de pruebas, no existen procedimientos formales para la gestión de cambios y establecer responsables.

Según los datos obtenidos se considera un cumplimiento del 60% de este control.

12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema

Control:

"Se deberían revisar y probar las aplicaciones críticas de negocio cuando se realicen cambios en el sistema operativo, con objeto de garantizar que no existen impactos adversos para las actividades o seguridad de la Organización"

Análisis:

Las pruebas a los sistemas informáticos luego de hacer algún cambio se lo realiza antes de poner en producción al sistema, para garantizar que no existan inconvenientes al momento de trabajar con la aplicación.

Según los datos obtenidos se considera un cumplimiento del 60% de este control.

12.5.3 Restricciones sobre los cambios en los paquetes de software

Control:

"Se debería desaconsejar la modificación de los paquetes de software, restringiéndose a lo imprescindible y todos los cambios deberían ser estrictamente controlados"

Análisis:

Por lo general se realizan cambios a los sistemas informáticos cuando el usuario necesita adicionar alguna funcionalidad en particular, no se tiene

definido un versionamiento de los sistemas, se trabaja directamente en la aplicación y se va modificándole según los requerimientos,

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

12.5.4 Fugas de información

Control:

"Se debería prevenir las posibilidades de fuga de información"

Análisis:

Por lo general al momento de firmar el contrato de trabajo, se establecen las prohibiciones que tiene el personal con respecto a la confidencialidad de la información Universitaria, no existe una política de seguridad y tampoco un control adecuado para garantizar que no exista fuga de información.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

12.5.5 Externalización del desarrollo de software

Control:

"Se debería supervisar y monitorizar el desarrollo del software subcontratado por la Organización"

Análisis:

No se aplica el control ya que la todos los sistemas informáticos institucionales son desarrollados en la Unidad de Sistemas de Información, en el caso de adquirir una aplicación de terceros se instala el software ejecutable y no se dispone del código fuente.

Según los datos obtenidos se considera un cumplimiento del 0% de este control.

12.6 Gestión de la Vulnerabilidad Técnica

12.6.1 Control de las vulnerabilidades técnicas

Control:

"Se debería obtener información oportuna sobre la vulnerabilidad técnica de los sistemas de información que se están utilizando, evaluar la exposición de la organización ante tal vulnerabilidad y tomar las medidas adecuadas para hacer frente a los riesgos asociados"

Análisis:

Los programadores de los sistemas informáticos están capacitados para el correcto desarrollo, cambios o modificación de las aplicaciones, no existe un control para determinar si existe una vulnerabilidad técnica por parte de los desarrolladores.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

13. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

13.1 Notificación de eventos y puntos débiles de seguridad de la información

13.1.1 Notificación de eventos de seguridad de la información

Control:

"Se deberían comunicar los eventos en la seguridad de información lo más rápido posible mediante canales de gestión apropiados"

Análisis:

De lo que se tiene conocimiento cuando existe un inconveniente en los sistemas informáticos el usuario crea un incidente en el sistema de Help Desk, el personal de soporte de primera línea revisa y evalúa el inconveniente, en caso de no poder resolver, la incidencia se escala a la segunda línea de soporte para dar solución, están definidos tiempos de respuesta y responsables para los incidentes reportados, no se tiene definido un agente u oficial de seguridad de la información en la DTIC, no se tiene definido y conformado un equipo de CSIRT.

Según los datos obtenidos se considera un cumplimiento del 70% de este control.

13.1.2 Notificación de puntos débiles de seguridad

Control:

"Todos los empleados, contratistas y terceros que son usuarios de los sistemas y servicios de información deberían anotar y comunicar cualquier debilidad observada o sospechada en la seguridad de los mismos"

Análisis:

Cuando existe alguna debilidad de seguridad o problema de funcionamiento en algún sistema informático, por lo general algunos usuarios reportan el incidente de manera verbal, en ocasiones por correo electrónico al Director de Tecnología. Cuando algún funcionario de la DTIC detecta un problema en algún sistema, crea un incidente en el sistema de Help Desk para su revisión y corrección lo antes posible.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

13.2 Gestión de incidentes de seguridad de la información y mejoras

13.2.1 Responsabilidades y procedimientos

Control:

"Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, efectiva y ordenada a los incidentes en la seguridad de información"

Análisis:

De lo que se tiene conocimiento la estructura de trabajo de la DTIC está organizada bajo las mejores prácticas de ITIL, se tiene implementado un sistema de Help Desk, el personal de la DTIC tiene definido sus roles y funciones, cuando se crea un ticket de alguna incidencia, el personal de primera línea tiene establecido tiempos de respuesta para atender y resolver los problemas reportados, los incidentes de seguridad tienen un tratamiento diferente comparado con otros tipos de incidentes, pero en ocasiones no se da el seguimiento adecuado para encontrar las soluciones oportunas.

Según los datos obtenidos se considera un cumplimiento del 90% de este control.

13.2.2 Aprendizaje de los incidentes de seguridad de la información

Control:

"Debería existir un mecanismo que permitan cuantificar y monitorear los tipos, volúmenes y costes de los incidentes en la seguridad de información"

Análisis:

De lo que se tiene conocimiento el sistema de Help Desk permite monitorear el estado de los tickets creados, resueltos, pendientes; en ocasiones se genera reportes de los tickets con sus respectivos estados, para dar seguimiento y presentar los respectivos informes al Director de la DTIC, por lo general el personal de primera línea no revisa, actualiza, ni modifica la base del conocimiento el sistema de Help Desk para aprender de los incidentes y dar soluciones en el menor tiempo.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

13.2.3 Recopilación de evidencia

Control:

"Cuando una acción de seguimiento contra una persona u organización, después de un incidente en la seguridad de información, implique acción legal (civil o criminal), la evidencia debe ser recolectada, retenida y presentada conforme a las reglas para la evidencia establecidas en la jurisdicción relevante"

Análisis:

De lo que se tiene conocimiento los registros que se tiene almacenado son los relacionados con los logs de los sistemas informáticos, no existe una política para el registro formal de antecedentes de seguridad informática, hasta el momento no se tiene conocimiento de que se ha utilizado algún registro de los sistemas para tomar acciones civiles contra algún funcionario que haya cometido algún incidente de seguridad.

Según los datos obtenidos se considera un cumplimiento del 20% de este control.

14. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

14.1 Aspectos de la seguridad de la información en la gestión de la continuidad del negocio

14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de continuidad del negocio

Control:

"Se debería desarrollar y mantener un proceso de gestión de la continuidad del negocio en la organización que trate los requerimientos de seguridad de la información necesarios para la continuidad del negocio"

Análisis:

De lo que se tiene conocimiento existe pocos planes de contingencia para algunos sistemas informáticos, en ocasiones los planes están solo definidos pero no están revisados ni evaluados, existen pocas pruebas para determinar si los planes de contingencia cumplen con los objetivos planteados, la mayoría de las ocasiones se trata de dar continuidad del negocio con soluciones puntuales en el sistema informático, equipo de comunicación, equipo informático que presente inconvenientes.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

14.1.2 Continuidad del negocio y evaluación de riesgos

Control:

"Se deberían identificar los eventos que puedan causar interrupciones a los procesos de negocio junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información"

Análisis:

De lo que se tiene conocimiento se realiza un monitoreo frecuente a las actividades de los sistemas informáticos, la actividad de la red LAN, estado de los servidores; cuando se genera un evento que interrumpa el correcto funcionamiento de los sistemas, se detecta la falla y se toman las medidas correctivas lo antes posible para superar los inconvenientes, no se tiene una estimado de cálculo de probabilidad e impacto cuando surge una interrupción del servicio.

Según los datos obtenidos se considera un cumplimiento del 80% de este control.

14.1.3 Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

Control:

"Se deberían desarrollar e implantar planes de mantenimiento o recuperación de las operaciones del negocio para asegurar la disponibilidad de la información en el grado y en las escalas de tiempos requeridos, tras la interrupción o fallo de los procesos críticos de negocio"

Análisis:

De lo que se tiene conocimiento no existe un plan de mantenimiento o recuperación formal cuando existe un fallo o interrupción del servicio para algunos sistemas informáticos, por lo general se toman medidas correctivas a penas se tenga una interrupción de un determinado servicio.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

14.1.4 Marco de Referencia para la planeación de la continuidad del negocio

Control:

"Se debería mantener un esquema único de planes de continuidad del negocio para garantizar que dichos planes son consistentes, para tratar los requisitos de seguridad y para identificar las prioridades de prueba y mantenimiento"

Análisis:

No se tiene un esquema definido para revisar, analizar, mejorar los planes de continuidad del negocio, por lo general se tiene un procedimiento a seguir cuando existe una interrupción del servicio.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

14.1.5 Prueba, mantenimiento y reevaluación de los planes de continuidad del negocio

Control:

"Se deberían probar regularmente los planes de continuidad del negocio para garantizar su actualización y eficacia"

Análisis:

Como se había dicho anteriormente, no existen muchos planes para la continuidad del negocio, se aplican los procedimientos necesarios ante una interrupción de algún servicio en particular, se documenta el inconveniente suscitado para tener una base del conocimiento, los pocos planes de contingencia no son revisados de forma oportuna.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

15. CUMPLIMIENTO

15.1 Cumplimiento de los requisitos legales

15.1.1 Identificación de la legislación aplicable

Control:

"Todos los requisitos estatutarios, de regulación u obligaciones contractuales relevantes, así como las acciones de la Organización para cumplir con estos requisitos, deberían ser explícitamente definidos, documentados y actualizados para cada uno de los sistemas de información y la Organización"

Análisis:

Por lo general se tiene definido los reglamentos, estatutos, obligaciones contractuales al inicio del desarrollo de algún sistema informático, en el análisis de requisitos que debe cumplir el programa, cuando se adquiere un sistema informático de terceros se definen los requerimientos en las cláusulas del contrato.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

15.1.2 Derechos de propiedad intelectual (DPI)

Control:

"Se deberían implantar procedimientos adecuados que garanticen el cumplimento de la legislación, regulaciones y requisitos contractuales para el uso de material con posibles derechos de propiedad intelectual asociados y para el uso de productos software propietario"

Análisis:

Existe procedimientos definidos que garanticen los cumplimientos y que protejan los derechos de propiedad intelectual tanto con el software adquirido por terceros, como el desarrollado en la Unidad de Sistemas de Información; estos procedimientos son definidos en los contratos y en la definición de requerimientos del proyecto a desarrollar.

Según los datos obtenidos se considera un cumplimiento del 50% de este control.

15.1.3 Protección de los documentos de la organización

Control:

"Los registros importantes se deberían proteger de la pérdida, destrucción y falsificación, de acuerdo a los requisitos estatutarios, regulaciones, contractuales y de negocio"

Análisis:

De lo que se tiene conocimiento, existe poca documentación de los diferentes sistemas informáticos institucionales, la poca documentación existente es almacenada en archivos físicos, y la documentación digital se encuentra en los equipos informáticos de los responsables de cada aplicación, no existe controles adecuados para proteger la documentación.

Según los datos obtenidos se considera un cumplimiento del 20% de este control.

15.1.4 Protección de datos y privacidad de la información de carácter personal

Control:

"Se debería garantizar la protección y privacidad de los datos y según requiera la legislación, regulaciones y, si fueran aplicables, las cláusulas relevantes contractuales"

Análisis:

De lo que se tiene conocimiento la información de carácter personal es entera responsabilidad del propietario ante pérdidas, extracción, modificación; la DTIC aplica pocos controles para proteger la información

relevante y que tiene relación directa con la Universidad de Cuenca, no existe un control adecuado sobre la información relacionada con la Universidad.

Según los datos obtenidos se considera un cumplimiento del 20% de este control.

15.1.5 Prevención del uso indebido de los recursos de tratamiento de la información

Control:

"Se debería disuadir a los usuarios del uso de los recursos dedicados al tratamiento de la información para propósitos no autorizados"

Análisis:

No existe una política de seguridad que prohíba el uso indebido de los sistemas informáticos, tampoco existe una sanción para los usuarios que utilicen de forma indebida los equipos y sistemas informáticos institucionales.

Según los datos obtenidos se considera un cumplimiento del 20% de este control.

15.1.6 Regulación de controles criptográficos

Control:

"Se deberían utilizar controles cifrados en conformidad con todos acuerdos, leyes y regulaciones pertinentes"

Análisis:

De lo que se tiene conocimiento los controles cifrados son utilizados solo en algunos sistemas informáticos, no está definida una política de seguridad que defina qué tipo de controles son de uso obligatorio para garantizar la seguridad en la información generada por los sistemas informáticos, falta de implementar más controles para el resto de sistemas informáticos, definir las claves de acceso con controles criptográficos.

Según los datos obtenidos se considera un cumplimiento del 20% de este control.

15.2 Cumplimiento de las políticas y normas de seguridad, y cumplimiento técnico

15.2.1 Cumplimiento con las políticas y normas de seguridad

Control:

"Los directivos se deberían asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad se realizan correctamente y cumplen con los estándares y políticas de seguridad"

Análisis:

De lo que se tiene conocimiento el director de la DTIC no realiza chequeos frecuentes de los estándares y políticas de seguridad informática, no existen muchas políticas de seguridad informática establecidas para provenir algún inconveniente de seguridad en los sistemas informáticos, por lo general los Coordinadores realizan un seguimiento y verificación del trabajo realizado por el personal de sus respectivas Unidades.

Según los datos obtenidos se considera un cumplimiento del 20% de este control.

15.2.2 Comprobación del cumplimiento técnico

Control:

"Se debería comprobar regularmente la conformidad de los sistemas de información con los estándares de implantación de la seguridad"

Análisis:

Se realizan chequeos a los sistemas informáticos en especial cuando se realizan modificaciones, en ocasiones algunos administradores no aplican regularmente medidas correctivas o preventivas en las observaciones realizadas por los usuarios.

Según los datos obtenidos se considera un cumplimiento del 40% de este control.

15.3 Consideraciones de auditoria de los sistemas de información

15.3.1 Controles de auditoría de los sistemas de información

Control:

"Se deberían planificar y acordar cuidadosamente los requisitos y actividades de auditoría que impliquen comprobaciones en los sistemas en activo con objeto de minimizar el riesgo de interrupciones de los procesos de negocio"

Análisis:

No se realiza controles de auditoria de forma regular en los respetivos sistemas informáticos, es responsabilidad de cada Coordinador realizar controles de auditoría en los sistemas informáticos que administra.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

15.3.2 Protección de las herramientas de auditoría de los sistemas de información

Control:

"Se deberían proteger los accesos a las herramientas de auditoría de los sistemas de información con objeto de prevenir cualquier posible mal uso o compromiso"

Análisis:

No existen herramientas informáticas definidas para realizar auditorías en los sistemas informáticos, se realiza chequeos regulares de la información que genera los sistemas institucionales.

Según los datos obtenidos se considera un cumplimiento del 30% de este control.

5.3. Bibliografía

ISO/IEC 27002. (2005). Obtenido de http://www.iso27000.es/download/ControlesISO27002-2005.pdf

INEN 27002. (05 de 2009). Obtenido de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/EXTRACTO_2014/GAN/nte_inen_iso_iec_27002extracto.pdf

Dirección TI. (2013). Obtenido de http://www.ucuenca.edu.ec/sobre-uc/administracion-central/direccion-de-tic/la-direccion

EGSI. (09 de 2013). Obtenido de http://www.planificacion.gob.ec/wp-content/uploads/downloads/2013/12/Esquema-Gubernamental-de-Seguridades-de-la-Informaci%C3%83%C2%B3n.pdf

Implementación EGSI. (marzo de 2014). Obtenido de http://www.puertodemanta.gob.ec/wp-content/uploads/2015/02/15-de-marzo-2014.pdf

ucuenca. (2014). Obtenido de http://www.ucuenca.edu.ec/images/DTIC/DOCUMENTOS/poa_dtic_2014.pdf

ISO27002 . (2015). Obtenido de https://iso27002.wiki.zoho.com/

Díaz, M., & Navarro, J. (2011). *Planificación de Políticas de Seguridad.* Obtenido de http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-91112.pdf

Lanche, D. (2015). *Diseño de un sistema de seguridad de la información para la compañía acotecnic cía. ltda. basado en la norma nte inen iso/iec 27002.* Obtenido de http://dspace.ucuenca.edu.ec/handle/123456789/22371

Luján, U. (Febrero de 2015). Obtenido de http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

Mifsud, E. (marzo de 2012). Obtenido de http://recursostic.educacion.es/observatorio/web/gl/software/software-general/1040-%20introduccion-a-la-seguridad-informatica?start=1

Romo, D., & Valarezo, J. (2012). *ANÁLISIS E IMPLEMENTACIÓN DE LA NORMA ISO 27002 PARA EL DEPARTAMENTO DE SISTEMAS DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL.* Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/3163/1/UPS-GT000319.pdf

WOOD, C. C. (2002). *Políticas de Seguridad Informática-Mejores Prácticas Internacionales.* NetIQ.