UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"PROPUESTA DE UN PLAN DE ASEGURAMIENTO DE LA INFORMACIÓN DIGITAL BASADO EN LA NORMA TÉCNICA PERUANA ISO/IEC 27001:2014 PARA LAS OFICINAS ADMINISTRATIVAS DE LA UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR"

TRABAJO DE SUFICIENCIA PROFESIONAL
Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

GONZALES ROJAS, ANDRES PEDRO

Villa El Salvador
2016

DEDICATORIA

A mi familia, por el apoyo incondicional durante todo este tiempo, por los consejos y las enseñanzas brindadas.

AGRADECIMIENTOS

Agradezco a mi familia por apoyarme y no dejarme caer en los momentos difíciles y mis amigos y profesores que me apoyaron en estos años.

INDICE

LISTA DE FIGURAS

LISTADO DE TABLAS

INTRODUCCIÓN

El presente documento tiene como finalidad proponer un plan de aseguramiento de la información digital para las oficinas administrativas de la UNTELS.

Actualmente la universidad no cuenta con un plan de seguridad ni políticas para resguardar la información digital que se almacena, crea y comparte a través de sus redes de información en las diferentes oficinas administrativas, esto representa un gran problema para la institución pues no tiene conocimiento de las amenazas y vulnerabilidad a los cuales están expuestos sus activos de información digital y que de explotar en riesgos podrían en peligro la continuidad del negocio.

El proyecto clasifica la información que se maneja en las diferentes oficinas administrativas para luego hacer una valoración de los activos de información digital que se encuentra en cada oficina, la valoración se realiza en base a los criterios claves de información, los cuales son: integridad, disponibilidad y confidencialidad.

Posterior a la clasificación de las oficinas administrativas se detectan las amenazas, vulnerabilidades y el riesgo al que están expuesto cada oficias tomando como criterios su ubicación, niveles de seguridad física y el tipo de información que maneja, de esta manera podemos tratar los riesgos encontrados

proponiendo controles y políticas para reducir, evitar, mitigar o transferir los riesgos.

1. CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

En la actualidad la Universidad Nacional Tecnológica de Lima Sur (UNTELS) no cuenta con un plan de seguridad de la información “debido a la falta de personal permanente en la Oficina de Desarrollo de Tecnologías de la Información y Comunicación (ODTIC) y las constantes rotaciones de los mismo, este problema se debe al cambio de jefe de esta oficina que se realiza muchas veces por problemas de índole administrativo”. (Juan Ibarra, comunicación personal, 18 de Julio de 2016). Esta situación no permite cumplir con lo establecido por la ONGEI en la **Resolución Ministerial Nº 004-2016-PCM**, donde se hace obligatorio el uso de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

Así también, El ambiente donde se encuentra el Data Center (Centro de Datos) no es un lugar adecuado, “los ambientes donde se encuentran los servidores no fueron construidos para esa finalidad, son aulas adaptadas para cumplir otro propósito, por este motivo es difícil contar con las medidas de seguridad convenientes, e implementarlas resulta costoso, sin embargo se trata de cumplir con las medidas de seguridad necesarias.” (Juan Ibarra, comunicación personal, 18 de Julio de 2016).

Respecto de la seguridad de la información digital, “el control de los equipos de las oficinas administrativas se realiza mediante el antivirus GDATA, sin embargo no existen políticas dirigidas al personal, además de esto la información digital de cada oficina esta almacenada en cada computadora, a excepción de algunas oficinas que comparten un espacio en el servidor para su almacenamiento”. (Juan Ibarra, comunicación personal, 18 de Julio de 2016), dejando así la información vulnerable a pérdida, robo, alteración o publicación desautorizada.

Se observó que tampoco se bridan capacitaciones constantes al personal administrador y usuario para concientizar en uso de medidas de seguridad de la información digital, “usualmente existen capacitaciones brindadas por parte del proveedor pero son limitadas, para un máximo de tres personas”. (Juan Ibarra, comunicación personal, 18 de Julio de 2016).

1.2. Justificación del proyecto

La información digital es un activo muy importante en una organización como la UNTELS, sin ella no podría funcionar poniendo en riesgo a la institución e impidiendo lograr sus metas, para evitar que esto pueda suceder es necesario hacer uso de la Norma Técnica Peruana ISO/IEC: 27001:2014 con el objetivo de asegurar la información digital en la institución. La aplicación de esta norma es recomendada por la ONGEI y adopta un carácter obligatorio en la **Resolución Ministerial Nº 004-2016-PCM**.

Mediante este plan se busca reducir el alto grado de vulnerabilidad de la información digital que existe en la UNTELS, descrita en el punto 1.1 de este mismo documento, de esta manera se podrá capacitar al personal usuario y administrador de la información digital en la Norma Técnica Peruana ISO/IEC 27001:2014, la cual nos dice cómo proteger los activos de la información digital y brinda técnicas para la correcta manipulación de los mismo, evitando daños que puedan perjudicar a la universidad.

Las políticas de aseguramiento de la información digital que describen la forma de empleo, responsabilidades y derechos que los usuarios y administradores poseen, además de medidas preventivas y correctivas para asegurar la información digital. Estas políticas se comunicaran, cumplirán y evaluaran para una mejora constante.

Es necesario contar con controles para mitigar los riesgos a los que se encuentran expuestos los activos de información digital de la universidad porque estas amenazan podrían detener parcial o totalmente las funciones críticas de la universidad impidiendo la continuidad del negocio, es por esto que es necesario proponer un plan de aseguramiento de la información digital basado en la Norma Técnica Peruana “NTP ISO/IEC 27001:2014” para las oficinas administrativas de la UNTELS.

1.3. Delimitación del proyecto

El plan de aseguramiento de la información digital basado en la Norma Técnica Peruana ISO/IEC 27001:2014 será realizado para la UNTELS, su implementación estará cargo de ODTIC y será aplicado en todos los equipos de las oficinas administrativas en un tiempo de 4 meses.

1.4. Formulación del problema

¿La inexistencia de un plan de aseguramiento de la información digital basado en la Norma Técnica Peruana ISO/IEC 27001:2014 para las oficinas administrativas de la UNTELS pone en riesgo los activos de información?

1.5. Objetivos

1.5.1. Objetivo general

1.5.1.1. Propuesta de un plan de aseguramiento de la información digital basado en la Norma Técnica Peruana ISO/IEC 27001:2014 para las oficinas administrativas de la UNTELS.

1.5.2. Objetivos Específicos

1.5.2.1. Realizar una valoración de los activos de información digital por oficinas administrativa.

1.5.2.2. Identificar los riesgos de los activos de información digital por oficina administrativa.

1.5.2.3. Proponer controles asociados a los riesgos identificados, empleando la Norma Técnica Peruana ISO/IEC 27002: 2014.

2. CAPITULO II: MARCO TEORICO

2.1. Antecedentes de la investigación

“DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION PARA UN INSTITUTO EDUCATIVO” realizado por Luis Carlos Aliaga Flores, facultad de ciencias e ingeniería. PUCP Febrero del 2013, en este trabajo se concluye lo siguiente: “Un sistemas de Gestión de Seguridad de Información (SGSI) establecido en una institución educativa se muestra como la solución para que el flujo de información que se da entre los procesos críticos y los activos involucrados dentro de dichos procesos, logren el nivel de seguridad adecuado para garantizar el cumplimiento de los objetivos de TI y, en consecuencia lo objetivos organizacionales.”

2.2. Bases teóricas

2.2.1. Normas y regulaciones

- **LEY N° 29733 – LEY DE TRANSPARENCIA Y ACCESO A LA INFORMACION PUBLICA**

En el 2003 se aprobó la ley de transparencia y acceso a la información pública en el Perú, la cual tiene como finalidad promover la transparencia de los actos del estado y regular el derecho fundamental del acceso a la información consagrado en el numeral 5 del Artículo 2 de la Constitución Política del Perú.

La ley consta de 4 títulos y 2 capítulos en los que se indica los derechos que otorga esta ley a los ciudadanos para acceder a la información, las responsabilidades del funcionario público y las excepciones de la ley.

2.2.2. Conceptos generales

- **Alta dirección**

Dentro de los niveles jerárquicos de una organización, la alta dirección es la encargada de tomar las decisiones estratégicas más importantes relacionadas con productos y servicios, esto garantiza el buen desempeño de la organización. (Laudon Kenneth y Laudon Jane, 2012)

- **Compromiso de la dirección**

Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. (Agustín López, 2012)

- **Políticas de seguridad**

Las políticas de seguridad de una organización están compuestas por las normas y procedimientos internos que deben seguir los miembros de la organización para respetar los requerimientos de seguridad establecidos. Debe describirse la criticidad de los sistemas y de la información, los roles de cada puesto de trabajo y mecánica de acceso a los sistemas, herramientas, documentación y cualquier otro componente del sistema de información. (Pablo Galdámez, 2003)

- **Activo de información**

Los activos de información están compuestos por todos los recursos que tienen valor o utilidad para la organización, estos recursos son necesarios para que las operaciones de la organización no se detengan y alcance sus objetivos. (Fernández, Eduardo y Mario Piattini, 2003).

Los activos son aquellos elementos relacionados con el entorno, como son el personal, los edificios, instalaciones, los equipos o los suministros; los relacionados con los sistemas de TIC, como el hardware y software, los componentes de comunicaciones de datos. (Javier Areitio Bertolin, 2008)

- **ISO**

Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo

objetivo es establecer, promocionar y gestionar estándares. (Agustín López, 2012)

- **Riesgo**

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (Agustín López, 2012)

- **Seguridad de la información**

Preservación de la confidencialidad, integridad y disponibilidad de la información. (Agustín López, 2012)

- **Gestión de riesgos**

Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos. (Agustín López, 2012)

- **Codificación**

Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad, El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no

autorizado a los repositorios de información. (Fernández, Eduardo y Mario Piattini, 2003).

- **Confidencialidad**

Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (Agustín López, 2012)

- **Disponibilidad**

Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (Agustín López, 2012)

- **Integridad**

Propiedad de la información relativa a su exactitud y completitud. (Agustín López, 2012)

- **Software Malicioso**

Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información. (Agustín López, 2012)

- **DHCP**

El protocolo de configuración de host dinámico (DHCP) automatiza el proceso de configurar las interfaces de redes y asegura eliminar la duplicación de direcciones mediante el uso de la base de datos de dirección administrada de forma central. (Natalia y Víctor Olifer, 2009)

2.3. Marco conceptual

- **Activo de información digital**

Los activos de información digital de la UNTELS son todos los equipos de cómputo y de telecomunicaciones que se encuentran en las oficinas administrativas, además de los equipos ubicados en el Data Center.

- **Alta dirección**

La alta dirección en la UNTELS está conformada por la Asamblea Universitaria, Consejo Universitario y el Rectorado. Son ellos quienes pueden actuar con autonomía absoluta y plena responsabilidad sobre los objetivos generales de la universidad y están únicamente limitados por órganos de gobierno superiores.

3. CAPITULO III: DISEÑO DE MODELO

3.1. Pasos

3.1.1. Alcance del plan de seguridad de la información digital

El plan de seguridad de la información digital basado en la NTP ISO/IEC 27001:2014 solo se enfocara en las oficinas administrativas de la UNTELS descritas en la resolución de comisión organizadora número 072-2015-UNTELS y que se encuentren operativas a la fecha del proyecto.

3.1.2. Presupuesto del proyecto

Tabla 1
Presupuesto del proyecto

Recursos Utilizados	Costos	
Material de impresión	S/.	120.00
Licencia Office 2013	S/.	230.00
Humano	S/.	3,600.00
Equipo de Computo	S/.	1,500.00
		Otros Servicios
Luz	S/.	100.00
Internet	S/.	400.00
Alimentos	S/.	800.00
Total	S/.	6,750.00

Fuente: Elaboración Propia.
Los costos del proyecto fueron asumidos por el proyectista en su totalidad.

3.1.3. Clasificación de la información

La información digital puede ser clasificada según el nivel de sensibilidad o grado de importancia para la organización, la clasificación nos permite limitar el acceso a clases particulares de personas, de esta manera se puede evitar fugas de información, alteración de información o eliminación por el acceso no autorizado de terceros.

Sin embargo una entidad del estado se ve afectada por la ley N 27806, Ley de transparencia y acceso a la información pública, la cual menciona que toda información que posea el estado se presume publica, salvo las excepciones expresamente previstas por el artículo 15 de la presente ley. La excepción que se aplica a la universidad está en la letra h del artículo 15, La información referida a los datos personales cuya publicidad constituya una invasión de la intimidad

personal y familiar. La información referida a la salud personal, se considera comprendida dentro de la intimidad personal.

Bajo estas consideraciones se clasifico la información de la UNTELS de la siguiente manera:

Tabla 2
Clasificación de la información

Clasificación	Descripción
Información Publica	Es toda información de carácter administrativo que se genere por la UNTELS
Información Restringida	Es toda información que comprometa datos personales de los empleados de la universidad o terceros cuya publicación constituya la invasión de la intimidad personal y familiar.

Fuente: Elaboración propia.

3.1.4. Valoración de activos de información digital por área administrativa

En base a los activos identificados por área administrativa, ver Anexo B, se realizó una valoración al área mediante la relación de los criterios claves de información:

- Disponibilidad
- Integridad
- Confidencialidad

En este proyecto se valorara una escala cuantitativa de acuerdo a los criterios antes mencionados, teniendo al número 1 con menor relevancia y el 4 con la

relevancia más alta. En las siguientes tablas se muestran los criterios con sus valores respectivos.

Tabla 3
Valoración de la disponibilidad de un activo de información digital

Disponibilidad	
Valor	Criterio
1	Debe estar disponible por lo menos 25% del tiempo
2	Debe estar disponible por lo menos 50% del tiempo
3	Debe estar disponible por lo menos 75% del tiempo
4	Debe estar disponible el 100% del tiempo

Fuente: Elaboración propia.

Tabla 4
Valoración de la integridad de un activo de información digital

Integridad	
Valor	Criterio
1	Tiene que estar correcto y completo al menos en un 25%
2	Tiene que estar correcto y completo al menos en un 50%
3	Tiene que estar correcto y completo al menos en un 75%
4	Tiene que estar correcto y completo en un 100%

Fuente: Elaboración propia.

Tabla 5
Valoración de la confidencialidad de un activo de información digital

Confidencialidad	
Valor	Criterio
1	Daños muy bajos, el incidente no trascendería del área afectada
2	Daños relevantes, el incidente implicaría a otras áreas
3	Daños muy relevantes La información es sensible, puede contener información financiera, personal entre otros.
4	Daños catastróficos La información contenida es altamente sensible, la reputación y la imagen de la organización se verían comprometidas

Fuente: Elaboración propia.

Luego de la valoración de disponibilidad, integridad, confidencialidad a cada oficina administrativa de la UNTELS se obtuvo un valor final para determinar la criticidad de cada área respecto a la información digital.

Tabla 6
Valor promedio de los activos de información digital

Valor	Descripción
1	Bajo
2	Medio
3	Alto
4	Muy Alto

Fuente: Elaboración propia

Para ver la criticidad de activos de información digital por área administrativa, consultar el Anexo C.

3.1.5. Identificación de los riegos de los activos de información digital por área administrativa

Una vez identificadas los activos de información se procedió a asociar las amenazas, de acuerdo al Anexo C de la ISO 27005, y las vulnerabilidades, de acuerdo al Anexo D de la ISO 27005, a cada activo.

Para analizar el riesgo se estableció la posibilidad de ocurrencia de las amenazas y el impacto de las vulnerabilidades a la universidad, de acuerdo a los siguientes valores:

Tabla 7
Probabilidad de ocurrencia de las amenazas

Probabilidad	Descripción
5	Extremadamente Probable
4	Muy probable
3	Probable
2	Poco Probable
1	Improbable

Fuente: Elaboración propia.

Tabla 8
Impacto de la vulnerabilidad en la universidad

Impacto	Descripción
1	Insignificante
2	Menor
3	Medio
4	Critico
5	Catastrófico

Fuente: Elaboración propia.

En la Figura 1, se observa la relación que existe entre la probabilidad y el impacto, esta relación permitirá medir el riesgo de los activos de información digital por área.

Probabilidad						
	Extremadamente Probable	A	A	E	E	E
	Muy probable	M	A	A	E	E
	Probable	B	M	A	A	E
	Poco Probable	B	B	M	A	E
	Improbable	B	B	M	M	A
		Insignificante	Menor	Medio	Critico	Catastrofico
		Impacto				

Figura 1 *Matriz de calor para analizar los riegos*
Fuente: Elaboración propia.

B	Riesgo Bajo
M	Riesgo Moderado
A	Riesgo Alto
E	Riesgo Extreno

Figura 2 *Valores cualitativos encontrados en la matriz de calor*
Fuente: Elaboración propia.

En el Anexo D, se observa la asociación de los activos de información digital por área administrativa a las amenazas y sus respectivas vulnerabilidades, y al tipo de riesgo.

3.1.6. Tratamiento del riesgo

Luego de identificar los tipos de riesgos por cada amenaza y vulnerabilidad, se procedió a definir un tratamiento, control y responsable.

Para el tratamiento del riesgo se tienen las siguientes acciones.

- **Evitar,** se ve como opción más conveniente retirar la fuente de riesgo.
- **Aceptar,** luego de realizar el análisis de riesgo se concluye que no es posible mitigar el riesgo y la única opción es continuar con la actividad.
- **Reducir,** usar controles para reducir la probabilidad o el impacto del riesgo y así reducir las consecuencias.
- **Transferir,** cuando el riesgo es muy complicado de tratar se comparte con una o varias partes, estas partes pueden pertenecer o no a la organización.

En el Anexo E, se observan los riesgos identificados en todas las áreas con su tratamiento, control y responsable.

3.1.7. Propuesta de políticas para la seguridad de la información digital

Adicionalmente a los controles y el tratamiento de riesgo, se propusieron políticas para la seguridad de la información digital, estas políticas se pueden observar en el Anexo F.

3.1.8. Plan de elaboración del proyecto

La elaboración de este proyecto tomo un tiempo aproximado de 3 meses para el levantamiento de la información, análisis y propuesta se controles y política.

En el Anexo G, se puede observar el plan de elaboración del proyecto.

CONCLUSIONES

Es vital el desarrollo e implementación de un plan de seguridad de la información que complemente al presente proyecto para poder lograr el aseguramiento de toda la información en la UNTELS.

Los activos de información digital más importantes, se encuentran ubicados en el Data Center según el nivel de criticidad identificado en la valoración de activos de información digital, estos activos están expuestos a múltiples amenazas que de no ser tratadas a tiempo podrían explotar riesgos que afecten directamente a la universidad, para cumplir con los controles y políticas propuestas el papel de la alta dirección es muy importante debido a que es imprescindible su compromiso para la implementación de los controles y políticas.

Es importante el cumplimiento de las políticas propuestas para una correcta administración de la información digital, a fin de garantizar la continuidad del negocio asegurando la disponibilidad, integridad y confidencialidad de la información digital. Por este motivo la alta dirección debe publicar y difundir estas políticas a todo el personal que labora en la universidad.

Implementar un plan de seguridad de la información digital en la UNTELS es un proceso complicado por el personal nombrado que muchas veces no está acostumbrado al cambio, lo cual generara demoras en una futura implementación.

RECOMENDACIONES

Se recomienda hacer un trabajo muy intenso en la concientización a los empleados que están relacionados con la información digital de la universidad, este trabajo no se logra de manera rápida, debido a que muchas personas no aceptan el cambio en las organizaciones y esto puede traer problemas para hacer efectivo el plan de seguridad de la información digital. El principal objetivo de la concientización debe ser la alta dirección, de esta manera se tendrá el apoyo total para llevar a cabo el plan de seguridad, por este motivo se recomienda realizar capacitaciones a todo el personal para que sepan la importancia de su participación en la seguridad de la información digital.

Realizar estudios de software que puedan satisfacer los requerimientos de la UNTELS en seguridad de la información y realizar su implementación para apoyar al aseguramiento de la información digital.

Analizar, diseñar e implementar una nueva red de información, que cumpla con las políticas propuestas en este proyecto y cuente con todas las medidas de seguridad necesarias para desempeño confiable y seguro.

También es muy importante comunicar que la seguridad total de la información digital no existe, las políticas y controles propuestas buscan reducir y controlar los riesgos, para esto es importante analizar y actualizar los riesgos y controles de

manera periódica a fin de tener una mejora continua en el plan de seguridad de la información digital.

Por último es necesario realizar auditorías internas para conocer los problemas de seguridad y tener una mejor continua en los controles y políticas, se recomienda que el equipo auditor sea externo a la universidad para evitar un conflicto de intereses.

BIBLIOGRAFIA

- Agustín López (2012). ISO 27000.ES El portal de ISO 27001 en Español. Recuperado de: http://www.iso27000.es/iso27000.html

- Fernández, Eduardo y Mario Paittini (2003), Seguridad de las tecnologías de la información: La construcción de la confianza para una sociedad conectada. Madrid, España.

- INDECOPI (2014), Norma Técnica Peruana ISO/IEC 27001:2014. 2nd Edición.

- ISO/IEC (2011), ISO/IEC 27005:2011 Information technology – Security techniques – Information security risk management. 2nd Edition.

- ISO/IEC (2013), ISO/IEC 27002:2013 Information technology - Security techniques – Code of practice for information security management. 2nd Edition.

- Javier Areitio Bertolin (2008), Seguridad de la Información, Redes, Informática y sistemas de información. Madrid, España.

- Laudon Kenneth y Laudon Jane (2012), Sistemas de información gerencial, Duodécima edición. México.

- Ley N° 27806, Diario Oficial el Peruano, Perú, 7 de Agosto de 2003.

- Natalia y Víctor Olifer (2009), Redes de Computadoras: Principios, tecnología y protocolos para el diseño de redes. México D.F, México.

- Pablo Galdámez (2013), Seguridad Informática. Recuperado de: http://web.iti.upv.es/actualidadtic/2003/07/2003-07-seguridad.pdf

ANEXO A: ENTREVISTA AL JEFE DE ODTIC

Juan Ibarra, Jefe de ODTIC

Realidad de la seguridad de la información en la UNTELS

¿La UNTELS esta tiene un plan de seguridad de la información o tiene alguna implementado?

En cada gestión de esta oficina se realizan plan de seguridad, pero no se terminan debido a la falta de personal permanente en la Oficina de Desarrollo de Tecnologías de la Información y Comunicación y las constantes rotaciones de los mismo, este problema se debe al cambio de jefe de esta oficina que se realiza muchas veces por problemas de índole administrativo, en la actualidad lo que se está desarrollando es un plan de auditoria para el 2017 que esperamos dejar terminado para su implementación.

¿Cuentan con políticas sobre la información digital?

No existen políticas de seguridad de la información en la universidad, sin embargo el control de los equipos de las oficinas administrativas se realiza mediante el antivirus GDATA, sin embargo no existen políticas dirigidas al personal, además de esto la información digital de cada oficina esta almacenada en cada computadora, a excepción de algunas

oficinas que comparten un espacio en el servidor para su almacenamiento como la de recursos humanos, tesorería, contabilidad.

¿Existe un plan de capacitaciones para los usuarios finales y los administradores en la ISO 27001?

La universidad no da ningún tipo de capacitación al personal, usualmente existen capacitaciones brindadas por parte del proveedor pero son limitadas, para un máximo de tres personas y no son suficientes para lo que realmente se necesita.

¿Cuál es la situación actual del Data Center?

Los ambientes donde se encuentran los servidores no fueron construidos para esa finalidad, son aulas adaptadas para cumplir otro propósito, por este motivo es difícil contar con las medidas de seguridad convenientes, e implementarlas resulta costoso, sin embargo se trata de cumplir con las medidas de seguridad necesarias

ANEXO B: IDENTIFICACION DE ACTIVOS DE INFORMACION DIGITAL POR AREA ADMINISTRATIVA

Oficina Administrativa	Cantidad	Equipo
Rectorado	2	PC
	2	Impresora
Órgano de Control Institucional	5	PC
	3	Impresora
Tribunal de Honor	1	PC
	1	Impresora
Secretaria General	3	PC
	2	Impresora
Oficina de Certificación Grados y Títulos	2	PC
	2	Impresora
Oficina de Tramite Documentario y Archivo Central	2	PC
	1	Impresora
	1	Escáner
Oficina de Comunicación, Imagen Institucional y Protocolo	3	PC
	2	Impresora
Oficina Central de Calidad y Acreditación	2	PC
	2	Impresora
Oficina de Cooperación Técnica y Relaciones Internacionales	2	PC
	1	Impresora
Oficina de Desarrollo de Tecnologías de Información y Telecomunicaciones	4	PC
	2	Impresora
Data Center	4	Servidor
	1	Router
	1	Swtich
	1	Balanceador de ancho de banda

Oficina Administrativa	Cantidad	Equipo
Oficina Central de Planificación y Presupuesto	2	PC
	2	Impresora
Oficina de Racionalización y Estadística	1	PC
Oficina de Presupuesto	3	PC
	1	Impresora
Oficina Central de Asesoría Legal	3	PC
	1	Impresora
Dirección General de Administración	2	PC
	1	Impresora
Oficina de Abastecimiento	5	PC
	4	Impresora
Oficina de Control Patrimonial	2	PC
	1	Impresora
Oficina de Contabilidad	3	PC
	1	Impresora
Oficina de Recursos Humanos	5	PC
	2	Impresora
Oficina de Tesorería	5	PC
	2	Impresora
Oficina de Bienestar Universitario	5	PC
	4	Impresora
Oficina Central de Proyectos e Infraestructura y Servicios Generales	2	PC
	2	Impresora
Oficina de Operación y Mantenimiento	4	PC
	3	Impresora
Oficina de Proyectos e Inversiones	3	PC
	2	Impresora

Oficina Administrativa	Cantidad	Equipo
Oficina de Seguridad	1	PC
Oficina de Infraestructura y Obras	2	PC
	2	Impresora
Vicerrectorado Académico	2	PC
	2	Impresora
Oficina Central de Registro Académicos	3	PC
	3	Impresora
Oficina de Registros Académicos e Informáticos	9	PC
	6	Impresora
Oficina Central de Extensión y Proyección Social	2	PC
	2	Impresora
Oficina Central del Centro de Admisión	2	PC
	1	Impresora
Oficina Central del Centro Pre Universitario	2	PC
	1	Impresora
Oficina Central del Centro de Idiomas	3	PC
	2	Impresora
Vicerrectorado de Investigación y Responsabilidad Social Universitaria	2	PC
	2	Impresora
Oficina Centro de Planeamiento Estratégico y Desarrollo	1	PC
Oficina de Coordinación Académica y Administrativa	1	PC
	1	Impresora
Oficina Central de Investigación Transferencia e Innovación	1	PC
Oficina Central de Gestión de la Investigación	1	PC
Oficina de Biblioteca Central	3	PC
	2	Impresora
Oficina Central de Responsabilidad Social Universitaria y Centros de Producción	1	PC

Oficina Administrativa	Cantidad	Equipo
	1	Impresora
Oficina Producción de Bienes y Servicios	1	PC
	1	Impresora
Oficina Central de Institutos y Centros de Investigación	2	PC
	1	Impresora
Centro de Investigación Servicios de Salud Publica	2	PC
	1	Impresora
Oficina Central de Estado Empresa y Sociedad Civil	2	PC
	1	Impresora
Decanato Facultad de Ingeniería de Sistemas y Administración de Empresas	2	PC
	2	Impresora
Oficina de Tutoría y Practicas Pre Profesionales	3	PC
	1	Impresora
Escuela Profesional de Ingeniería de Sistemas	2	PC
	2	Impresora
Escuela Profesional de Administración de Empresas	2	PC
	2	Impresora
Decanato Facultad de Ingeniería Mecánica, Electrónica y Ambiental	2	PC
	2	Impresora
Oficina de Tutoría y Practicas Pre Profesionales	3	PC
	1	Impresora
Escuela Profesional de Ingeniería Electrónica y Telecomunicaciones	2	PC
	2	Impresora
Escuela Profesional de Ingeniería Ambiental	3	PC
	2	Impresora
Escuela Profesional de Ingeniería Mecánica y Eléctrica	2	PC
	2	Impresora

ANEXO C: LISTADO DE VALORACION DE ACTIVOS AGRUPADOS POR AREA ADMINISTRATIVA

Activos de Información digital por oficina administrativa	Tipo de Información	Valorización			
		Criterios			Valor
		Disponibilidad	Integridad	Confidencialidad	
Rectorado	Publica	4	4	2	3
Órgano de Control Institucional	Restringida	4	4	3	4
Tribunal de Honor	Restringida	4	4	3	4
Secretaria General	Publica	4	4	2	3
Oficina de Certificación Grados y Títulos	Publica	4	4	2	3
Oficina de Tramite Documentario y Archivo Central	Publica	4	4	2	3
Oficina de Comunicación, Imagen Institucional y Protocolo	Publica	4	4	2	3
Oficina Central de Calidad y Acreditación	Publica	4	4	2	3
Oficina de Cooperación Técnica y Relaciones Internacionales	Publica	4	4	2	3
Oficina de Desarrollo de Tecnologías de Información y Telecomunicaciones	Publica	4	4	2	3
Data Center	Restringida	4	4	3	4
Oficina Central de Planificación y Presupuesto	Publica	4	4	2	3
Oficina de Racionalización y Estadística	Publica	4	4	2	3
Oficina de Presupuesto	Publica	4	4	2	3
Oficina Central de Asesoría Legal	Restringida	4	4	3	4
Dirección General de Administración	Publica	4	4	2	3
Oficina de Abastecimiento	Restringida	4	4	2	3
Oficina de Control Patrimonial	Publica	4	4	2	3
Oficina de Contabilidad	Restringida	4	4	3	4
Oficina de Recursos Humanos	Restringida	4	4	3	4
Oficina de Tesorería	Restringida	4	4	3	4

Activos de Información digital por oficina administrativa	Tipo de Información	Valorización			
		Criterios			Valor
		Disponibilidad	Integridad	Confidencialidad	
Oficina de Bienestar Universitario	Restringida	4	4	3	4
Oficina Central de Proyectos e Infraestructura y Servicios Generales	Publica	4	4	2	3
Oficina de Operación y Mantenimiento	Publica	4	4	2	3
Oficina de Proyectos e Inversiones	Publica	4	4	2	3
Oficina de Seguridad	Publica	4	4	2	3
Oficina de Infraestructura y Obras	Publica	4	4	2	3
Vicerrectorado Académico	Publica	4	4	2	3
Oficina Central de Registro Académicos	Restringida	4	4	3	4
Oficina de Registros Académicos e Informáticos	Restringida	4	4	3	4
Oficina Central de Extensión y Proyección Social	Restringida	4	4	3	4
Oficina Central del Centro de Admisión	Publica	4	4	1	3
Oficina Central del Centro Pre Universitario	Publica	4	4	1	3
Oficina Central del Centro de Idiomas	Publica	4	4	1	3
Vicerrectorado de Investigación y Responsabilidad Social Universitaria	Publica	4	4	1	3
Oficina Centro de Planeamiento Estratégico y Desarrollo	Publica	4	4	1	3
Oficina de Coordinación Académica y Administrativa	Publica	4	4	1	3
Oficina Central de Investigación Transferencia e Innovación	Publica	4	4	1	3
Oficina Central de Gestión de la Investigación	Publica	4	4	1	3
Oficina de Biblioteca Central	Publica	4	4	1	3
Oficina Central de Responsabilidad Social Universitaria y Centros de Producción	Publica	4	4	1	3
Oficina Producción de Bienes y Servicios	Publica	4	4	1	3
Oficina Central de Institutos y Centros de Investigación	Publica	4	4	1	3

Activos de Información digital por oficina administrativa	Tipo de Información	Valorización			
		Criterios			Valor
		Disponibilidad	Integridad	Confidencialidad	
Centro de Investigación Servicios de Salud Publica	Restringida	4	4	3	4
Oficina Central de Estado Empresa y Sociedad Civil	Publica	4	4	1	3
Decanato Facultad de Ingeniería de Sistemas y Administración de Empresas	Publica	4	4	1	3
Oficina de Tutoría y Practicas Pre Profesionales	Publica	4	4	1	3
Escuela Profesional de Ingeniería de Sistemas	Publica	4	4	1	3
Escuela Profesional de Administración de Empresas	Publica	4	4	1	3
Decanato Facultad de Ingeniería Mecánica, Electrónica y Ambiental	Publica	4	4	1	3
Oficina de Tutoría y Practicas Pre Profesionales	Publica	4	4	1	3
Escuela Profesional de Ingeniería Electrónica y Telecomunicaciones	Publica	4	4	1	3
Escuela Profesional de Ingeniería Ambiental	Publica	4	4	1	3
Escuela Profesional de Ingeniería Mecánica y Eléctrica	Publica	4	4	1	3

ANEXO D: EVALUACION DE RIESGOS POR OFICINA ADMINISTRATIVA

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
Rectorado	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	3	2	Moderado
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	2	3	Moderado
	Uso no autorizado del equipo	Conexiones de red pública sin protección	4	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	3	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	4	2	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	2	Moderado
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	2	Moderado
Órgano de Control Institucional	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		hardware			
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	2	Moderado
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	5	Extremo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	4	Alto
Tribunal de Honor	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no	3	3	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		controlados de software			
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	2	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	5	Extremo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	4	Alto
Secretaria General	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	3	Moderado
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	2	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	4	Alto
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	2	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	2	Moderado
Oficina de Certificación Grados y Títulos	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	3	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	2	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	4	Alto
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	2	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	2	Moderado
Oficina de Tramite Documentario y Archivo Central	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	3	Moderado
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	2	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		mensajería			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	2	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	2	Moderado
Oficina de Comunicación, Imagen Institucional y Protocolo	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	1	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	1	Bajo
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	1	Bajo
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina Central de Calidad y Acreditación	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	3	Moderado
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	2	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	2	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	2	Moderado
Oficina de Cooperación Técnica y Relaciones Internacionales	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	3	Moderado
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	2	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	4	Alto
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	2	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los	3	2	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		derechos intelectuales			
Oficina de Desarrollo de Tecnologías de Información y Telecomunicaciones	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	2	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	2	3	Moderado
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	2	3	Moderado
	Error en el uso	Uso incorrecto de software y hardware	2	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	2	3	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a	2	3	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		las edificaciones y los recintos			
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	2	3	Moderado
	Falla del equipo	Falta de planes de continuidad	3	4	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto
Data Center	Destrucción del equipo o los medios. Polvo, corrosión, congelamiento.	Falta de esquemas de reemplazo periódico. Susceptibilidad a la humedad, el polvo y la suciedad.	2	4	Alto
	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	2	5	Extremo
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	3	4	Alto
	Falla del equipo de	Conexión deficiente de los	3	5	Extremo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	telecomunicaciones	cables			
	Falla del equipo de telecomunicaciones	Punto único de falla	4	5	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	2	4	Alto
	Incumplimiento en la disponibilidad del personal	Ausencia del personal	4	5	Extremo
	Espionaje remoto	Transferencia de contraseñas autorizadas	4	5	Extremo
	Error en el uso	Entrenamiento insuficiente en seguridad	2	3	Moderado
	Error en el uso	Uso incorrecto de software y hardware	2	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	2	3	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	2	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	2	5	Extremo
	Daños por agua	Ubicación en un área susceptible de aniego	4	5	Extremo
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	2	5	Extremo
	Falla del equipo	Falta de planes de	3	5	Extremo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		continuidad			
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	4	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	5	Extremo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	4	Alto
Oficina Central de Planificación y Presupuesto	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	3	Moderado
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de	3	2	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		la seguridad			
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	4	Alto
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	2	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	2	Moderado
Oficina de Racionalización y Estadística	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin	2	3	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		protección			
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	2	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	4	Alto
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	2	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	2	Moderado
Oficina de Presupuesto	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	3	Moderado
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	2	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		mensajería			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	2	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	2	Moderado
Oficina Central de Asesoría Legal	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	2	Moderado
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	5	Extremo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	4	Alto
Dirección General de Administración	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	2	Moderado
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	5	Extremo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	4	Alto
Oficina de Abastecimiento	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	3	Moderado
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	2	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	4	Alto
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	2	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los	3	2	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		derechos intelectuales			
Oficina de Control Patrimonial	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	3	Moderado
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	2	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	4	Alto
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a	3	2	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		las edificaciones y los recintos			
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	2	Moderado
Oficina de Contabilidad	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		autorizadas			
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	2	Moderado
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	5	Extremo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
Oficina de Recursos Humanos	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	3	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	4	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	5	Extremo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	3	Alto
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	2	2	Bajo
	Robo de equipo	Falta de protección física de las puertas y ventanas de la	2	3	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		edificación			
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	2	3	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto
Oficina de Tesorería	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	2	Moderado
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	4	Alto
Oficina de Bienestar Universitario	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto
Oficina Central de Proyectos e Infraestructura y Servicios Generales	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	4	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto
Oficina de Operación y Mantenimiento	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	4	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto
Oficina de Proyectos e Inversiones	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	2	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	1	Moderado
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		mensajería			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	1	Bajo
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	1	Bajo
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina de Seguridad	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	2	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	1	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	1	Bajo
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	1	Bajo
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina de Infraestructura y Obras	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	3	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	2	Moderado
	Espionaje	Líneas de comunicación sin protección	2	3	Moderado
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	3	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	3	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	2	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	3	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	2	Moderado
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	2	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	2	Moderado
	Falla del equipo	Falta de planes de continuidad	3	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	2	Moderado
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	2	Moderado
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	2	Moderado
Vicerrectorado Académico	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		autorizadas			
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto
Oficina Central de Registro Académicos	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		continuidad			
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto
Oficina de Registros Académicos e Informáticos	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de	3	3	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		la seguridad			
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	4	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto
Oficina Central de Extensión y Proyección Social	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin	2	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		protección			
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	4	Alto
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	4	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto
Oficina Central del Centro de Admisión	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		mensajería			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina Central del Centro Pre Universitario	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina Central del Centro de Idiomas	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Vicerrectorado de Investigación y Responsabilidad Social Universitaria	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	3	Alto
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		autorizadas			
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	3	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto
Oficina Centro de Planeamiento Estratégico y	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
Desarrollo	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		continuidad			
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina de Coordinación Académica y Administrativa	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		la seguridad			
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina Central de Investigación Transferencia e Innovación	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin	2	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		protección			
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina Central de Gestión de la Investigación	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		mensajería			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina de Biblioteca Central	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina Central de Responsabilidad Social Universitaria y Centros de Producción	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina Producción de Bienes y Servicios	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		derechos intelectuales			
Oficina Central de Institutos y Centros de Investigación	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a	4	1	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		las edificaciones y los recintos			
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Centro de Investigación Servicios de Salud Publica	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	5	Extremo
	Manipulación con software	Falta de copias de respaldo	3	4	Alto
	Manipulación con software	Descarga y uso no controlados de software	3	3	Alto
	Espionaje	Líneas de comunicación sin protección	2	4	Alto
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	4	4	Extremo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	4	Alto
	Espionaje remoto	Transferencia de contraseñas	3	4	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		autorizadas			
	Error en el uso	Entrenamiento insuficiente en seguridad	4	3	Alto
	Error en el uso	Uso incorrecto de software y hardware	3	4	Alto
	Error en el uso	Falta de conciencia acerca de la seguridad	3	3	Alto
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	5	Extremo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	3	3	Alto
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	3	3	Alto
	Falla del equipo	Falta de planes de continuidad	3	4	Alto
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	3	Alto
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	3	Alto
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	3	Alto

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
Oficina Central de Estado Empresa y Sociedad Civil	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la	4	1	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		edificación			
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Decanato Facultad de Ingeniería de Sistemas y Administración de Empresas	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina de Tutoría y Practicas Pre Profesionales	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Escuela Profesional de Ingeniería de Sistemas	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Escuela Profesional de Administración de Empresas	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Decanato Facultad de Ingeniería Mecánica, Electrónica y Ambiental	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		mensajería			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Oficina de Tutoría y Practicas Pre Profesionales	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Escuela Profesional de Ingeniería Electrónica y Telecomunicaciones	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo
Escuela Profesional de Ingeniería Ambiental	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	4	1	Moderado
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los	3	1	Bajo

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		derechos intelectuales			
Escuela Profesional de Ingeniería Mecánica y Eléctrica	Perdida del suministro de energía	Susceptibilidad a las variaciones de tensión	5	1	Alto
	Manipulación con software	Falta de copias de respaldo	3	1	Bajo
	Manipulación con software	Descarga y uso no controlados de software	3	1	Bajo
	Espionaje	Líneas de comunicación sin protección	2	1	Bajo
	Falla del equipo de telecomunicaciones	Conexión deficiente de los cables	3	1	Bajo
	Uso no autorizado del equipo	Conexiones de red pública sin protección	3	1	Bajo
	Espionaje remoto	Transferencia de contraseñas autorizadas	3	1	Bajo
	Error en el uso	Entrenamiento insuficiente en seguridad	4	1	Moderado
	Error en el uso	Uso incorrecto de software y hardware	3	1	Bajo
	Error en el uso	Falta de conciencia acerca de la seguridad	3	1	Bajo
	Uso no autorizado del equipo	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	3	1	Bajo
	Destrucción de equipos o medios	Uso inadecuado o descuidado del control de acceso físico a	4	1	Moderado

Identificación de Riegos			Evaluación de los Riesgos		
Activos de Información digital por oficina administrativa	Riesgo		Probabilidad de Ocurrencia	Impacto	Tipo de Riesgo
	Amenaza	Vulnerabilidad			
		las edificaciones y los recintos			
	Robo de equipo	Falta de protección física de las puertas y ventanas de la edificación	4	1	Moderado
	Falla del equipo	Falta de planes de continuidad	3	1	Bajo
	Error en el uso	Falta de procedimientos para la introducción del software en los sistemas operativos	3	1	Bajo
	Robo de medios o documentos	Falta o insuficiencia de la política sobre limpieza	3	1	Bajo
	Uso de software falso o copiado	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	3	1	Bajo

ANEXO E: TRATAMIENTO DE LOS RIESGOS

Código	Riesgo	Tratamiento	Control	Clausula ISO/IEC 27002	Responsable del Control
RR-01	Susceptibilidad a las variaciones de tensión	Evitar	Implementar un sistema generador de energía eléctrica automático	11. Seguridad física y del entorno	Jefe de Operación y Mantenimiento
RR-02	Falta de copias de respaldo	Reducir	Establecer políticas de copias de seguridad	12. Seguridad de la operaciones	Jefe de ODTIC
RR-03	Descarga y uso no controlados de software	Reducir	Establecer políticas de instalación de software y acceso a la internet	12. Seguridad de la operaciones	Jefe de ODTIC
RR-04	Líneas de comunicación sin protección	Evitar	Establecer un sistema de cifrado para las redes de telecomunicaciones	13. Seguridad de las comunicaciones	Administrador de Red y Data Center
RR-05	Conexión deficiente de los cables	Evitar	Establecer políticas para las conexiones de red en las oficinas	13. Seguridad de las comunicaciones	Administrador de Red y Data Center
RR-06	Punto único de falla	Reducir	Implementar un sistema de redundancia en los equipos críticos de telecomunicación	13. Seguridad de las comunicaciones	Administrador de Red y Data Center
RR-07	Conexiones de red pública sin protección	Evitar	Establecer políticas para el control de las redes publicas	13. Seguridad de las comunicaciones	Administrador de Red y Data Center
RR-08	Ausencia del personal	Reducir	Contratar personal estable para los puestos de trabajo en el área de ODTIC	7. Seguridad de los recursos humanos	Jefe de RRHH
RR-09	Transferencia de contraseñas autorizadas	Reducir	Establecer políticas de control de acceso	9. Control de acceso	Jefe de ODTIC
RR-10	Entrenamiento insuficiente en seguridad	Reducir	Realizar capacitaciones para el personal en la norma ISO 27001	7. Seguridad de los recursos humanos	Jefe de ODTIC
RR-11	Uso incorrecto de software y hardware	Reducir	Realizar capacitaciones al personal en el uso de sus equipos	7. Seguridad de los recursos	Jefe de ODTIC

Código	Riesgo	Tratamiento	Control	Clausula ISO/IEC 27002	Responsable del Control
			de computo	humanos	
RR-12	Falta de conciencia acerca de la seguridad	Reducir	Incentivar y fomentar prácticas de seguridad de la información digital	7. Seguridad de los recursos humanos	Jefe de ODTIC
RR-13	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Reducir	Realizar capacitaciones al personal en el uso de sus equipos de telecomunicaciones	7. Seguridad de los recursos humanos	Jefe de ODTIC
RR-14	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Reducir	Registrar el acceso de visitantes a la universidad	9. Control de acceso	Jefe de Seguridad
RR-15	Ubicación en un área susceptible de aniego	Evitar	La ubicación del Data Center debe ser es un lugar seguro de aniegos o inundaciones	11. Seguridad física y del entorno	Jefe de ODTIC
RR-16	Falta de protección física de las puertas y ventanas de la edificación	Reducir	Mejorar protección física de los pabellones administrativos	9. Control de acceso	Jefe de Operación y Mantenimiento
RR-17	Falta de planes de continuidad	Evitar	Establecer un servicio de almacenamiento en la nube	17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	Jefe de ODTIC
RR-18	Falta de procedimientos para la introducción del software en los sistemas operativos	Reducir	La instalación de software solo será realizada por el usuario administrador o personal de ODTIC	9. Control de acceso	Jefe de ODTIC
RR-19	Falta o insuficiencia de la política sobre limpieza	Reducir	Realizar un registro del personal de limpieza por pabellón administrativo	9. Control de acceso	Jefe de Operación y Mantenimiento

Código	Riesgo	Tratamiento	Control	Clausula ISO/IEC 27002	Responsable del Control
RR-20	Falta de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales	Evitar	Establecer políticas para para la instalación solo de software licenciado o distribuciones de código abierto	9. Control de acceso	Jefe de ODTIC

ANEXO F: POLITICAS PARA LA SEGURIDAD DE LA INFORMACION

POLITICAS GENERALES

Código	Políticas Generales
PG-01	Los nombres de usuarios y contraseñas asignados a los empleados para el acceso a los sistemas, aplicaciones y recursos de cómputo de la universidad, son personales e intransferibles. La persona asignada a este usuario y contraseña es responsable del uso que se haga con ellos, así como la información y ventajas que se obtengan por ellos, para sí o para terceros y los daños que se ocasiones sin reducir las responsabilidades y sanciones organizacionales, civiles y penales que resulten.
PG-02	Se considera una falta grave el uso o ejecución de programas, aplicaciones u otros medios que puedan dañar, modificar o reducir el desempeño de los componentes de software de un equipo de cómputo o telecomunicaciones de propiedad de la universidad con el fin de perjudicar a la universidad o molestar a otros usuarios, así como también intentar violar los controles y medidas de seguridad de información digital definidos por la universidad.
PG-03	Los usuarios de los sistemas de la universidad deben reportar a ODTIC cualquier violación a las políticas, control o medidas de seguridad de información digital de la universidad.
PG-04	Está prohibido la instalación o ejecución de software no autorizado por ODTIC o sin licencia en cualquiera de los equipos de las oficinas administrativas de la universidad.
PG-05	Está prohibido la instalación o conexión de hardware no autorizado por ODTIC a los equipos de cómputo o instalación de telecomunicación.
PG-06	Se almacenará un registro de operación transaccionales (archivo log) de los sistemas por un periodo no menor a seis meses.
PG-07	La custodia de los equipos de almacenamiento de información interno y externo estará a cargo del personal asignado a su uso, los cuales deberán informar a su inmediato superior si estos equipos sufren daño alguno.
PG-08	Es responsabilidad de todo miembro de la universidad con personal a cargo (contratado o no), que este conozca la presente normativa y cumpla las disposiciones que requieren aprobación o supervisión previa al inicio de sus labores, especialmente las que necesiten conectar equipos ajenos a las redes de la universidad.

Código	Políticas Generales
PG-09	El uso de equipos que sean de propiedad de docentes y administrativos, en las instalaciones de la universidad deberán contar con la autorización de su respectiva jefatura o decanato. • Los miembros de la universidad solo podrán usar sus equipos de cómputo, dispositivos periféricos, o software en las instalaciones de la universidad si no cuentan con la autorización correspondiente. • Los dispositivos de almacenamiento externo deben ser revisados por ODTIC, con la finalidad de garantizar su limpieza de posible software malicioso y virus, antes de ser empleados en los equipos e instalación de la universidad. • Las computadoras portátiles usadas en las oficinas o ambientes de la universidad, a excepción de los ambientes con redes inalámbricas designados por ODTIC, deberán ser revisadas en ODTIC por el motivo señalado en el punto anterior. • El incumplimiento de alguna de estas políticas será tomado como una violación a los protocolos de seguridad y será motivo de sanción.
PG-10	Está totalmente prohibido el uso de software de seguridad por parte de los usuarios en los equipos de cómputo: • A menos que cuenten con la autorización de ODTIC, el personal de la universidad no debe emplear o poseer software o hardware que pueda romper, o aprovechar vulnerabilidades de seguridad. • El incumplimiento de esta política será tomado como una violación de protocolo de seguridad y será motivo de sanción.
PG-11	En caso de la promoción, rotación, vacaciones y/o cese del personal docentes y administrativo de la universidad • Los accesos de seguridad serán reevaluado o revocado de manera temporal o indefinidamente cuando un docente o administrativo es promovido, hace uso de sus vacaciones o pide licencia, es despedido o transferido, esta política se aplica a toda la comunidad universitaria que cuenten con acceso a los sistemas de información, equipos de cómputo o telecomunicaciones.
PG-12	Cada puesto dentro de la universidad estará completamente descrito y el personal que lo desarrolla debe conocer las responsabilidades propias de su puesto. • Se debe contar con una descripción formal del puesto y las responsabilidades asociadas (MOF). • Esta descripción debe ser proporcionada al personal cuando inicie sus funciones en la universidad.

Código	Políticas Generales
PG-13	Las copias de seguridad de la información académica y otros sistemas será almacenada con una antigüedad no mayor a un mes y se redundara en un servicio de almacenamiento en la nube o en un equipo que se encuentre en una ubicación diferente a del Data Center. • Las copias de seguridad se realizaran diariamente de manera automática y a la media noche. • Las copias de seguridad de las bases de datos serán totales. • Durante los periodos de registro de notas, matrículas, rectificaciones y mayor actividad en los sistemas académicos, las copias de seguridad se realizaran cuatro veces al día cada seis horas a partir de la media noche. • Se mantendrá un chequeo constante del nivel de almacenamiento en los discos duros para evitar la saturación de los mismos. • Se manejara un inventario de la realización de copias de seguridad de bases de datos detallando la fecha de backup, la hora, el tamaño, el responsable y las observaciones en el caso que existan.
PG-14	Todas las responsabilidades de seguridad de la información deben ser definidas e informadas a cada empleado al inicio de sus funciones.
PG-15	Los equipos de cómputo por parte de los proveedores que vayan a acceder a la infraestructura de la universidad y conectarse a una red deberá tener instalado y configurado un antivirus homologado por la universidad, para un monitoreo constante por el personal del ODTIC
PG-16	Se debe contar con personal estable en los puestos de trabajo de ODTIC a fin de asegurar su continuidad en la organización y el mantenimiento adecuado de los equipos de cómputo y telecomunicación
PG-17	Estará a cargo de ODTIC incentivar a los usuarios en la importancia de la seguridad de la información digital, se deben brindar continuas capacitaciones y charlas para que el usuario tenga presente lo importante que es mantener la seguridad de la información digital.
PG-18	Los usuarios de las oficinas administrativas de la universidad deberán contar con capacitaciones anualmente sobre la importancia de la seguridad de la información. Un resumen escrito de la información básica debe de ser entrega a cada empleado y una copia firmada será agregada como parte de sus archivos del empleado.
PG-19	Las claves de los servidores y equipos de telecomunicación deberán ser cambiadas cada seis meses o a la terminación o cambio de empleo del personal que interactúa con estas claves.

Código	Políticas Generales
PG-20	La responsabilidad de los activos de información de los cargos de ODTIC estarán detallada en el MOF, serán indicadas al personal a contratar durante su entrevista y entregadas luego de su contratación por escrito además de las medidas básicas de seguridad de la información, una copia firmada de las políticas de seguridad de información se guardara como parte del archivo del empleado.
PG-21	El incumplimiento por parte del empleado a lo establecido en las políticas de seguridad de la información digital, da causa a: • Que la universidad aplique las medidas disciplinarias correspondientes, incluyendo en su caso la baja de la(s) clave(s) de acceso a los sistemas, aplicaciones o equipos involucradas de la institución. • Si el caso lo amerita la baja de la institución. • Indemnizar de manera económica los daños y perjuicios que le ocasione a la universidad el problema ocasionado, independientemente a que se ejecuten las acciones legales de carácter civil, laboral y penal.
PG-22	Todos los procedimientos de manipulación de los equipos de cómputo y telecomunicación relevantes deberán ser documentados, además deben incluir información del personal clave a ser contactado en caso de fallas no contempladas en los procedimientos de la documentación.
PG-23	Los usuarios deberán estar restringidos de poder instalar programas que puedan pasar por alto los controles del sistema y aplicaciones.
PG-24	El usuario y contraseña asignada al trabajador es personal e intransferible.
PG-25	El acceso a internet será bloqueado desde las 5:00 pm hasta las 7:30 am para oficinas administrativas, sábados y domingos durante todo el día, Solo las oficinas de la alta dirección y unidades críticas contaran con el servicio ininterrumpido, salvo indicación contraria de las mismas, cualquier excepción será autorizada por la alta dirección de la universidad. • Los días en que realicen exámenes de admisión, simulacros o exámenes del centro PRE todas las redes serán bloqueadas, para asegurar la información digital y el ingreso de intrusos.
PG-26	Los usuarios del sistema informático tienen un firme compromiso de mantener en secreto sus contraseñas personales y las compartidas por un grupo al cual pertenece, este compromiso estará contemplado en los términos y condiciones del contrato o resolución.
PG-27	Las claves usadas en los servidores y equipos de telecomunicación deberán contar con al menos 8 caracteres, incluirán números, letras mayúsculas y minúsculas, símbolos, y serán diferentes por cada equipo.
PG-28	Los equipos deben contar con sistemas de alimentación ininterrumpida para evitar la pérdida o daño de información durante un corte de energía eléctrica

Código	Políticas Generales
PG-29	La universidad debe contar con generador de energía eléctrica automático, que permita reestablecer el suministro eléctrico en un tiempo menor al de la duración de los sistemas de alimentación ininterrumpida para evitar la pérdida de los o daño de la información.
PG-30	Implementar un plan de mantenimiento de servidores y equipos de telecomunicación de manera periódica, a fin de asegurar su operatividad y buen desempeño.
PG-31	Los dispositivos de almacenamiento externo que contengan copias de seguridad, deberán estar resguardados mediante el uso de cerradura u otro sistema de acceso al cual solo tendrá acceso solo el personal de ODTIC.
PG-32	El Data Center debe contar con un sistema de seguridad biométrico, para el cual solo tendrá acceso personal de ODTIC que interactúe con los equipos ubicados dentro.
PG-33	Los equipos de telecomunicación sensibles que se encuentren ubicados fuera del data center deberán estar en un lugar seguro y protegido por medio de una cerradura o u otros sistemas de acceso al cual solo tendrá acceso el personal de ODTIC.
PG-34	El Data Center debe estar ubicado en un ambiente construido para esta finalidad y que cuente con todas las medidas de seguridad y prevención necesarias.
PG-35	La limpieza dentro del Data Center o de los equipos de telecomunicación sensibles fuera del mismo se realizara bajo la presencia de algún trabajador encargado de ODTIC
PG-36	La ubicación del data center o equipos de telecomunicación sensibles debe ser en lugares seguros de aniegos o inundaciones
PG-37	Se debe establecer un registro de control de entrada y salida a las oficinas administrativas.
PG-38	Cada vez que los usuarios de los equipos de cómputo se alejen momentáneamente de sus respectivos equipos, deberá asegurarse de bloquear el equipo.
PG-39	Por ningún motivo, ninguna persona podrá retirar un equipo o componente de computo o telecomunicación de propiedad de la universidad, sin una guía de salía previamente autorizada por la dependencia en cuestión.
PG-40	Apagar los equipos de cómputo cuando no se usaran por un largo periodo de tiempo.
PG-41	Los equipos de cómputo y telecomunicación deben estar inventariados, los riesgos de inventario deben mantenerse actualizados.
PG-42	La pérdida o robo de hardware debe ser reportada inmediatamente.
PG-43	Las autorizaciones de ingreso al Data Center las deberá hacer la jefatura de ODTIC o el responsable que se designe.
PG-44	La puerta del Data Center deberá permanecer cerrada permanentemente, tanto en el día como en la noche.

Código	Políticas Generales
PG-45	El Data Center es una zona donde está terminantemente prohibido fumar, así como ingresar o transportar material inflamable.
PG-46	Se deben realizar copias de seguridad de bases de datos e imágenes de los sistemas de manera periódica, estas copias deben ser probadas regularmente para comprobar su integridad
PG-47	Se deben implementar medidas de protección contra la instalación de software sin la previa autorización de ODTIC en los equipos informáticos
PG-48	Es responsabilidad del DBA el cuidado y la integridad de la información almacenada en la estructura de las bases de datos
PG-49	La ODTIC bloqueara los accesos de ingreso o salida de información a través de medios de almacenamiento, a excepción de las áreas y/o unidades autorizadas por la alta dirección de la universidad
PG-50	La ODTIC mantendrá una bitácora actualizada de los virus encontrados y una descripción de los métodos usados para su eliminación y recuperación de archivos
PG-51	La ODTIC deberá capacitar al personal y hacerse cargo de eliminar la existencia de virus que se presenten en la organización con apoyo de las diferentes herramientas que se disponen
PG-52	Cada pabellón o ambiente de la universidad debe contar con una red diferente para protegerla de cualquier intruso.
PG-53	Cada punto de red debe tener asignado una IP estático para evitar accesos no autorizados y tener un mejor control sobre las redes.
PG-54	Las líneas de energía y de telecomunicaciones en los servicios de procesamiento de información deberían ser subterráneas, cuando sea posible, o tener protección alterna adecuada
PG-55	Todo punto de red que no esté en uso deberá ser desactivado para evitar el acceso no autorizado a la red.
PG-56	Deberá existir un oficial de seguridad de la información, quien administrara las claves de los servidores y equipos de telecomunicación
PG-57	No deben existir conexiones expuestas en las oficinas administrativas o sus exteriores, todas las conexiones deberán estar protegidas
PG-58	Se debe procurar que todos los componentes de la red deben ser redundados para evitar el colapso de toda la red por el fallo en un equipo vital.
PG-59	Los rangos de red asignados en el protocolo DHCP a un punto de acceso inalámbrico deberán ser denegados de todas las otras redes, para impedir el acceso de personas no autorizadas.

Código	Políticas Generales
PG-60	El Administrador red y Data Center deberá revisar constantemente el tráfico o flujo de información de la red, además de revisar el nivel de congestión y las causas probables del mismo, también revisara periódicamente de manera integral el estado de los componentes y enlaces de comunicación.
PG-61	Nunca Se deben ejecutar ni descargar programas o archivos adjuntos en correo electrónicos cuya procedencia y fiabilidad no ofrezca todas las garantías.
PG-62	En caso de recibir un mensaje de correo sospechoso, por el contenido o por incluir archivos adjuntos que se consideren extraños, aun en el caso de tener como procedencia personas conocidas, se deberá informar de forma inmediata a ODTIC para que se tomen las medidas correspondientes.
PG-63	Se deberían utilizar rótulos de equipo y de cables claramente identificables para minimizar los errores en el manejo, tales como conexiones accidentales de cables erróneos a la red
PG-64	Los cables de energía deberían estar separados de los cables de comunicaciones para evitar interferencia
PG-65	Las empresas proveedoras que interactúen con la información de la universidad recibirán una copia del acuerdo de no divulgación, este debe ser firmado por la universidad y por el proveedor de servicios.
PG-66	Luego de reportado un incidente de seguridad, este debe ser investigado por el personal técnico de ODTIC de forma rápida y confidencial. Se debe identificar la severidad del incidente para la toma de medidas correctivas, además de documentar los métodos de mitigación del incidente.
PG-67	Se debe mantener una documentación de todos los incidentes de seguridad ocurridos en la universidad.
PG-68	Se debe mantener intacta la evidencia que prueba la ocurrencia de una violación de seguridad producida, tanto por entes internos o externos, para su posterior utilización en procesos legales de ser caso.
PG-69	Implementar un servicio de almacenamiento en la nube, para asegurar las copias de seguridad en caso de crisis o desastre.
PG-70	Los servidores deben contar con un sistema de redundancia en un ambiente externo de la ubicación actual del Data Center o en una nube, para asegurar la continuidad del negocio en caso de crisis o un desastre.

POLITICAS ESPECIFICAS PARA LAS AREAS QUE MANIPULEN INFORMACION RESTRINGIDA

Código	Políticas específicas para áreas que manipulen información restringida
PE-01	Los equipos de cómputo designados a los jefes de área deberán contar con acceso total a internet, mientras que los designados a los demás empleados tendrá el acceso restringido a páginas que no aporten al desarrollo de sus funciones, cualquier excepción será comunicada por el jefe de área correspondiente.
PE-02	Aplicar técnicas de cifrado sobre la información que viaja a través de las redes de comunicación de las oficinas que manejen información restringida.
PE-03	Las oficinas que manejen información restringida contaran con una red independiente del resto de oficinas en su mismo pabellón
PE-04	Toda información personal de los trabajadores de la universidad que sea manipulada por el personal de las áreas que manejan información restringida no podrá ser revelada o divulgada.
PE-05	Los usuarios pertenecientes a estas áreas tendrán el acceso a sus terminales de trabajo restringido a su horario de labores, salvo una previa coordinación con la alta dirección y el personal de ODTIC
PE-06	Los equipos de cómputo de estas áreas contaran con una partición personal donde almacenaran toda su información, esta partición estará ubicada en los servidores de la universidad, cualquier archivo que no sea guardado en esta partición corre el riesgo de ser borrada del sistema.
PE-07	Esta extremadamente prohibió el uso de dispositivos de almacenamiento externo.
PE-08	Cada área contara con una partición que será visible por todo el personal perteneciente a dicha área, esta partición será usada para compartir archivos entre los usuarios.
PE-09	El usuario no podrá copiar información de su equipo de cómputo para trabajar desde su hogar. Toda manipulación de la información será desde su terminal de trabajo en la universidad.

ANEXO G: PLAN DE ELABORACION DEL PROYECTO

Nro.	Actividades	Mayo			Junio				Julio				Agosto		Total de Semanas
		2	3	4	1	2	3	4	1	2	3	4	1	2	
1	Identificación de activos por oficina administrativa		X	X	X										3
2	valoración de activos de información digital por oficina administrativa			X	X	X									3
3	Identificación de amenazas					X	X	X	X						4
4	Identificación de vulnerabilidades						X	X	X	X					4
5	Análisis del riesgo								X	X	X	X			4
6	Tratamiento del riesgo								X	X	X	X			4
7	Propuesta de políticas de seguridad de la información digital									X	X	X	X		4