Hoja de Ruta
IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN

UNIVERSIDAD DEL QUINDÍO

Elaborado por:	Revisado por:	Aprobado por:
José E. García Castro	**Martha C. Sánchez**	**John E. Martínez García**
Consultor	Gerente del Proyecto	Consultor Senior

CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio
0.0	28/09/2017	Emitido para aprobación
1.0	29/09/2017	Revisado
2.0	30/09/2017	Aprobado

Contenido

1 DEFINICIONES A TENER EN CUENTA

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000). • Análisis de Riesgo Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000). • Auditoría Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Son las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

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. (ISO/IEC 27000).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

2 HOJA DE RUTA

La implementación del Sistema de Gestión de Seguridad de la Información - SGSI en La Universidad del Quindío, se debe definir por las fases: Planear, Hacer, Verificar y Actuar (PHVA), ver figura 1, y las cuales son correspondientes con la norma NTC:ISO/IEC 27001:2013.

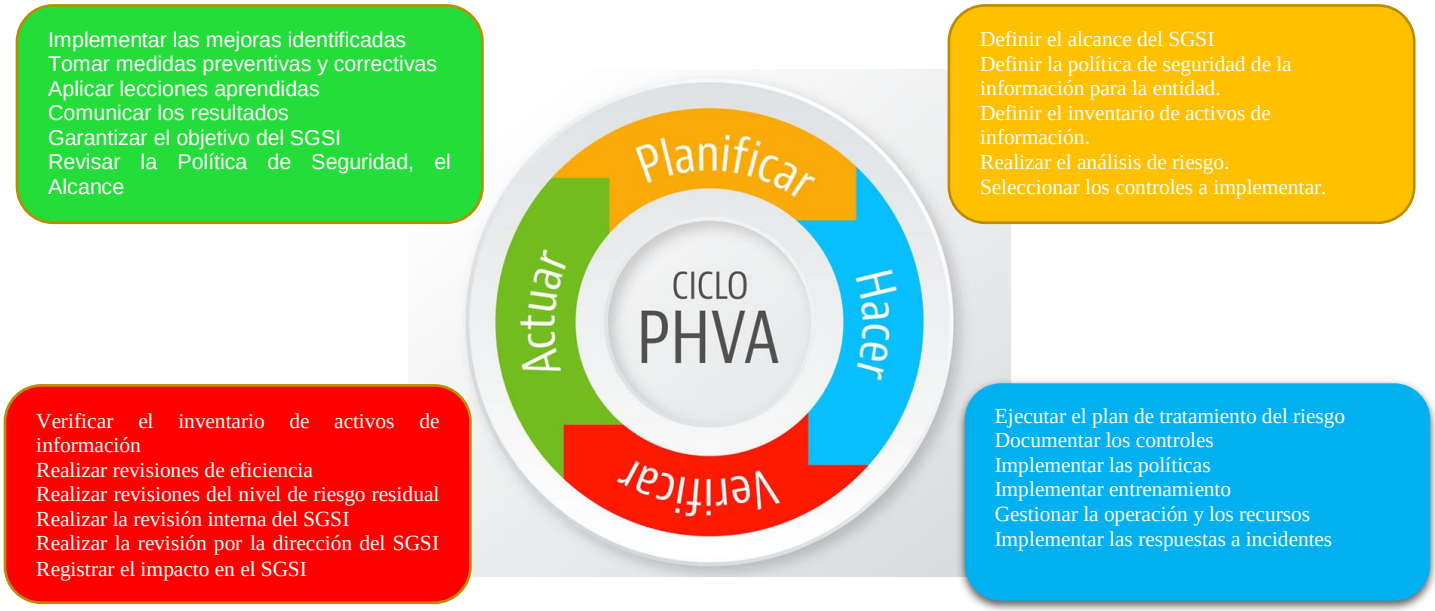

Figura 1. ISO27001:2013 marco del ciclo PHVA

La seguridad de la información debe contar con aprobación y apoyo sostenido de la dirección de La Universidad del Quindío. Esto permitirá que la gestión del riesgo (lo cual incluye el análisis, la identificación de controles adecuados, su implementación, su medición y mejora continua), sea aprobada y apoyada con los recursos necesarios a través de todas las etapas e instancias del sistema.

Este estándar internacional se complementa de manera armónica con otras iniciativas y estándares nacionales e internacionales, tales como MECI (Modelo Estándar de Control Interno), COBIT, ITIL, etc…

3 CONCEPTOS GENERALES DE UN SGSI

ISO 27001:2013 es un Sistema de Gestión de la Seguridad de la Información (SGSI).

La seguridad de la información queda definida por tres atributos:

a. **Confidencialidad:** Información disponible exclusivamente a personas autorizadas.

b. **Integridad:** Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas. Contra la integridad la información puede parecer manipulada, corrupta o incompleta.

c. **Disponibilidad:** Acceso y utilización de los servicios sólo y en el momento de ser solicitado por una persona autorizada.

La seguridad de la información (SI) es la protección de la información contra una amplia gama de amenazas respecto a:

a. Minimizar daños;
b. Oportunidades del negocio;
c. Retorno de la inversión;
d. Continuidad del negocio;
e. Cultura ética.

El SGSI garantiza la SI mediante una estructura de buenas prácticas, definidas por:

a. Gestión de riesgos;
b. Políticas;
c. Procesos;
d. Procedimientos;
e. Controles;
f. Revisiones;
g. Mejoras.

4 IMPLEMENTACIÓN DE LAS POLITICAS DE SEGURIDAD DE INFORMACIÓN

Se debe definir como estrategia para la implementación del Modelo de seguridad de información en La Universidad del Quindío, cumplir con una serie de fases que se sugieren en esta hoja de ruta, las cuales tienen como objetivo que la Universidad, desarrolle, apruebe, implemente y socialice e interiorice las políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de la Universidad.

Revisar con la alta dirección y acordar el compromiso con el cumplimiento y preparación de los prerrequisitos para iniciar la implementación del SGSI, y así mismo de los requisitos los cuales La Universidad del Quindío debe cumplir de acuerdo con manual de Gobierno en línea, una vez el SGSI está implementado y en operación.

Para la Universidad del Quindío es importante contar con políticas de seguridad ya que son ellas quienes guiaran el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la Universidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales a los cuales esté obligada a cumplir la Universidad.

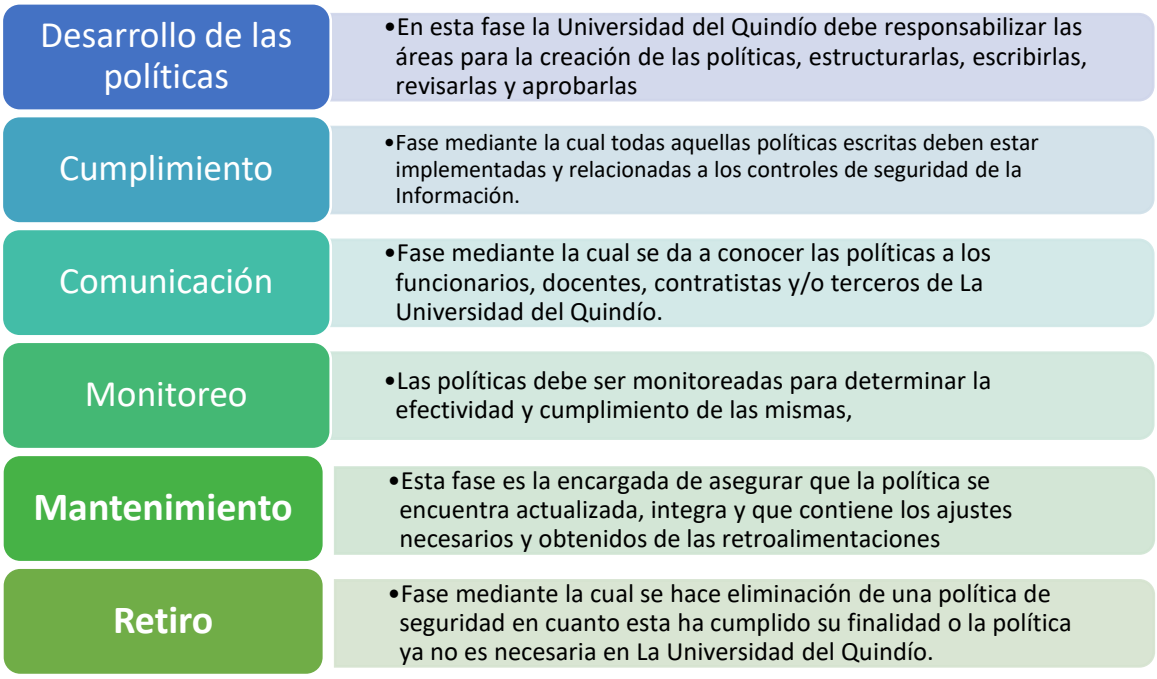

Figura 2. Fases de implementación de las políticas de seguridad de información

5 IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACION

La intención es presentar las recomendaciones de políticas de seguridad de la información para el Modelo de Seguridad y privacidad de la Información para la Universidad del Quindío. A continuación se agruparan las políticas con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad.

ORGANIZACIÓN: Esta política tiene como finalidad establecer el comité directivo de la seguridad de la información

Se debe conformar el comité directivo de seguridad de la información. Se debe especificar los objetivos del comité. Debe establecerse que dicho comité verifique el cumplimiento de las políticas.

GESTION DE ACTIVOS: Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios y contratistas

los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información.

En la elaboración de esta política debe tenerse en cuenta las leyes y normatividades actuales que afecten a la Universidad, ejemplo: Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo a la naturaleza de la Universidad.

CONTROL DE ACCESO: Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales la Universidad determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos.

Esta política debe determinar el seguimiento que se debe realizar para garantizar el cumplimiento de dicha política y sus correspondientes responsables.

NO REPUDIO: La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción. La política deberá incluir mínimo los siguientes aspectos:

a. **Trazabilidad:** La política hará que por medio de la trazabilidad de las acciones se haga seguimiento a la creación, origen, recepción, entrega de información y otros.

b. **Retención:** La política debe incluir el periodo de retención o almacenamiento de las acciones realizadas por los usuarios, el cual deberá ser informado a los funcionarios, contratistas, estudiantes y/o terceros de la Universidad.

c. **Auditoría:** La política incluirá la realización de auditorías continuas, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción.

d. **Intercambio electrónico de información**: La política incluirá en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

PRIVACIDAD Y CONFIDENCIALIDAD: Esta política debe contener una descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente. La política de privacidad debe contener los requerimientos dados en la Ley 1581 de 2012.

La política deberá indicar desde cuando se firma el acuerdo de confidencialidad, así como la vigencia del mismo.

INTEGRIDAD La política de integridad debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que hagan parte de la Universidad, la cual se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los mismos. Debe ser complementaria al Código de Ética y Buen Gobierno emitido por Resolución de Rectoria.

En el caso de vinculación contractual, el Compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de Cláusula de integridad de la información. La política de integridad, deberá establecer asimismo la vigencia de la misma acorde al tipo de vinculación del personal al cual aplica el cumplimiento.

DISPONIBILIDAD DEL SERVICIO E INFORMACIÓN La Universidad, deberá contar con un plan de continuidad del negocio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Universidad, ante el evento de un incidente de seguridad de la información.

REGISTRO Y AUDITORÍA: Esta política vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.

Esta política deberá incluir la responsabilidad de la Oficina de Control Interno acerca de la responsabilidad de llevar a cabo las auditorías periódicas a los sistemas y actividades relacionadas a la gestión de activos de información, así como la responsabilidad de dicha Oficina de informar los resultados de las auditorías.

Se debe tener en cuenta lo establecido por La Ley 87 de 1993 por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado, así como las previsiones de la ley 489 de 1998.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: La Universidad, deberá documentar una política general de gestión de eventos, incidentes y vulnerabilidades de seguridad de la información. Debe ir dirigida a todos los usuarios que tienen un acceso autorizado a cualquier sistema de información.

CAPACITACIÓN Y SENSIBILIZACIÓN EN SEGURIDAD DE LA INFORMACIÓN: Esta política se centra en la formación del personal en temas relacionados con la seguridad de la información, cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

IDENTIFICAR LOS RIESGOS: La Universidad debe realizar la identificación de amenazas potenciales y vulnerabilidades para cada activo y los niveles de confidencialidad, integridad y disponibilidad de los activos.

Se deben analizar el riesgo o los riesgos, en contexto de los objetivos de la entidad y de las partes interesadas, se asignarán valores a los riegos para poder saber cuáles son los más relevantes, los más críticos, los más prioritarios y cuales se pueden tolerar de acuerdo a su impacto y otras métricas.

Enumerar las opciones para el tratamiento/reducción del riesgo (selección de controles).

Es posible utilizar el conjunto de controles de la norma NTC/ISO 27002, NIST SP-800-53.

PLAN DE TRATAMIENTO DEL RIESGO En esta etapa se debe aprobar los objetivos de control y controles a implementar con el fin de tratar los riesgos identificados.

El Plan de tratamiento del riesgo debe tener:

- ✓ El método aplicable para cada riesgo: aceptar, reducir, transferir o eliminar.

- ✓ Listado de controles actualmente implementados.
- ✓ Controles adicionales propuestos
- ✓ Espacio de tiempo en el cual los controles propuestos serán implementados.

Los ajustes que considere necesarios, previos a la aprobación, se realizará por la dirección, quien será la responsable de la aceptación del riesgo residual y de suministrar los recursos para la implementación del plan de tratamiento del riesgo.

GENERAR EL DDA - DECLARACIÓN DE APLICABILIDAD: La declaración de aplicabilidad es un documento orientado a dar cumplimiento al estándar NTC:ISO/IEC 27001:2013, y optar por una futura certificación. Este documento debe tener el compromiso aceptado por la dirección con respecto a los controles que serán aplicados, respecto al total de controles existentes en el conjunto de controles utilizados y justificar cada una de las excepciones.

Este proceso ayuda a que la auditoría tenga un sólido punto de partida en la verificación de controles y de compromisos aceptados por la entidad y su dirección.

6 LINEAMIENTOS POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta que se observó en el Diagnostico, que el Macroproceso de Gestión de TICs tiene el documento Políticas de Seguridad de la Información, se sugiere verificar el cumplimiento de los siguientes lineamientos:

Lineamiento	Tipo	Descripción
1	Uso de contraseñas y usuarios	Debe definir las condiciones, normas y procedimientos necesarios para fijar los requisitos que se deben cumplir por cualquier funcionario, contratista o estudiante de la Universidad para obtener acceso a los sistemas de información, hardware y software propiedad de la Universidad del Quindío
2	Uso del servicio de correo electrónico	Debe generar conciencia a los funcionarios, contratistas o estudiantes de la Universidad de los riesgos asociados

		con el uso de correo electrónico y presenta las normas y protocolos a seguir para el buen uso de este servicio.
3	Uso del servicio de internet / intranet	Concientizar a los funcionarios, contratistas o estudiantes de la Universidad de las buenas prácticas a seguir sobre las normas de uso del servicio de Internet/Intranet, así como el conocimiento de los riesgos asociados por el uso indebido de los mismos.
4	Uso de servicio de mensajería instantánea	Concientizar a los funcionarios, contratistas o estudiantes de la Universidad de las buenas prácticas a seguir sobre las normas y el uso del servicio de mensajería instantánea, así como el conocimiento de los riesgos asociados por el uso indebido de los mismos.
5	Uso de dispositivos de almacenamiento externo	Describir el uso permitido de los dispositivos de almacenamiento externo en la Universidad y las restricciones en su empleo al interior de la institución.
6	Uso de dispositivos de captura de imágenes y/o grabación de video	Definir el acceso y el uso de cámaras fotográficas, cámaras de video y demás dispositivos que permitan el registro de imágenes, fotografías y/o video
7	Uso de escritorios y pantallas despejadas	Definir los mecanismos necesarios que se deben aplicar en el Instituto con el fin de proteger la información física residente en los escritorios y puestos de trabajo y la información digital almacenada en los computadores e infraestructura técnica a disposición de todos los funcionarios, contratistas o estudiantes para el normal desarrollo de las actividades.
8	Uso de dispositivos móviles (Tablets, Celulares)	Define los mecanismos necesarios que se deben aplicar en la Universidad, con el fin de proteger la confidencialidad de la información mediante el uso de los dispositivos móviles personales o de la Universidad. Se deben definir en qué áreas o para que macroprocesos se restringe o no el uso de los dispositivos personales móviles y cuales son las medidas de seguridad para el transporte de estos fuera de las instalaciones en caso de los dispositivos móviles de la Universidad.
9	Conexiones remotas / teletrabajo	Definir los requisitos y los casos en los cuales se concede acceso remoto a las plataformas tecnológicas de la Universidad y las medidas de seguridad que se establece para la garantizar la integridad, confidencialidad y disponibilidad de la información que es accedida por este medio o teletrabajo.

Tabla 1. Lineamientos

7 PLAN DE ACCIÓN GENERAL GOBIERNO DE TECNOLOGIA

INICIATIVAS	PROPUESTAS
Modificar la visión de TI, pasando de administradores de dispositivos a administradores de servicios de TI como apoyo al cumplimiento de los objetivos estratégicos de la La Universidad del Quindío.	Adoptar un Framework de arquitectura empresarial (ejemplo TOGAF), que permita alinear los procesos, datos, aplicaciones e infraestructura con los objetivos estratégicos de la La Universidad del Quindío. El estado Colombiano define un marco de referencia que puede ser adoptado y se conoce como arquitectura de TI, la cual es la estructura que ordena los conceptos y las estrategias, la columna vertebral del uso de tecnología, sobre la que las instituciones y los gobiernos soportan la gestión de TI. Es la estructura sobre la que el Estado colombiano organiza la tecnología en las Áreas de TI para alinearse con la Estrategia GEL.
	Evaluar, Seleccionar e implementar un estándar, regulación y/o mejores prácticas para Gobierno de TI como: ITIL, ISO-20000, CobiT, SOX, ISO-27001, PCI.
	Definir y ejecutar un Plan de capacitación especializada y/o certificaciones relacionado con el estándar seleccionado.
	Definir y ejecutar un Plan de Socialización y adaptación al cambio para toda la La Universidad del Quindío.
	Evaluar, seleccionar e implementar una herramienta de gestión de servicios de TI que facilite la implementación del estándar seleccionado.
	Generar y/o actualizar los procedimientos de TI acorde al estándar seleccionado.
Implementar acciones transversales de Seguridad de la Información.	Establecer formalmente un Sistema de Gestión de Seguridad de la Información ya sea en desarrollo propio o con el acompañamiento especializado.
	Implementar los planes de transición de los Protocolos IPv4 a IPv6. Ya está documentado, es llevarlo a la práctica.
	Diseñar y ejecutar planes de pruebas a la implementación de la transición IPv4 a IPv6.
	Implementar buenas prácticas de ciberseguridad.
	Establecer una estrategia para la implementación del tratamiento de riesgos de seguridad de la información.
	Implementar la Política de Protección de Datos Personales para dar cumplimiento a la legislación vigente relacionada con protección de datos personales.
	Implementar el Principio de Responsabilidad Demostrada (Accountability)

	Planificar e implementar del Modelo de Seguridad y Privacidad de la Información – MSPI. El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.
Implementar el Plan Estratégico de TI (PETI)	Definir las estrategias en cuanto a TI, sistemas de información, servicios tecnológicos y del uso y apropiación de los anteriores.
	Garantizar el valor estratégico de la capacidad y la inversión en tecnología.
	Definir la estrategia organizacional y las necesidades del negocio de TI.
	Definir la Planeación estratégica de gestión de TI
	Definir el Portafolio de planes, servicios y proyectos de TI
	Definir las Políticas de TI en cuanto a seguridad, información, acceso y uso, etc.
	Reforzar el Plan de Continuidad de TI.

Tabla 2. Iniciativas a realizar en marco del cumplimiento componente Seguridad.