1. DEFINICIÓN

Establecer, asegurar y gestionar los activos de información mediante acciones que permitan proteger a la Universidad del Tolima frente a amenazas y riesgos que pueden poner en peligro los niveles de competividad, rentabilidad y conformidad necesarios para cumplir con los objetivos estratégicos y misionales, permitiendo preservar la confidencialidad, integridad y disponibilidad de la información.

2. ALCANCE

Inicia desde el establecimiento de los activos de información de la institución, hasta la declaración, implementación, generación de controles, verificaciones y evaluaciones de medidas de seguridad que permitan garantizar la seguridad de la información.

3. ESTRUCTURA

3.1. GENERALIDADES

La gestión de la seguridad de la información es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información, permitiendo conocer y minimizar los posibles riesgos que atenten contra la seguridad de la información de la Institución.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Confidencialidad: Garantizar que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: Mantener de forma completa y exacta la información y los métodos de proceso.

Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.

Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

No Repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Legalidad: Referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

Vulnerabilidad: Una vulnerabilidad es una debilidad que puede ser 'activada' de forma accidental o intencionadamente. Es un factor de riesgo interno de un elemento expuesto a una amenaza de ser susceptible a sufrir un daño y de encontrar dificultades en recuperarse posteriormente.

Amenaza: Una amenaza es la posibilidad de que se produzca una determinada vulnerabilidad de forma satisfactoria. Una fuente de amenazas no plantea un riesgo cuando no hay vulnerabilidades que puedan ser 'activadas'.

Impacto: El impacto es la materialización de un riesgo; una medida del grado de daño o cambio sobre un activo, entendiendo como riesgo la probabilidad de que un evento desfavorable ocurra y que tendría un impacto negativo si se llegase a materializar
Políticas de Seguridad: Es un conjunto de leyes, reglas y prácticas que regulan la manera de dirigir, proteger y distribuir recursos en una organización para llevar a cabo los objetivos de seguridad informática dentro de la misma.

Seguridad Informática: Se refiere a protección de las infraestructuras de las tecnologías de la información y comunicación que soportan el Core del negocio de las empresas.

Copias de Seguridad (Backups): Es la operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático.

CIGD: Comité Institucional de Gestión y Desempeño de la Universidad del Tolima.

3.2. DESCRIPCIÓN

3.2.1 Activos de Información.

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
1		Inicio de actividades
2	Profesional Universitario	Realizar diagnóstico de la infraestructura de TI de la Universidad del Tolima.
3	Profesional Universitario	Realizar la identificación de los activos de información, con sus respectivas fuentes de información y soportes de la Universidad del Tolima.
4	Profesional Universitario	Se remite el inventario de activos de información al comité ….
5	Profesional Universitario	Revisar y analizar el inventario de activos de información para su aprobación
6	Profesional Universitario	Aprobar inventario de activos de información. Si: Continua paso No.7 No: Regresa al Paso No. 2
7	Profesional Universitario	Realizar la clasificación de los activos de información en grupos de servicios, datos e información, aplicaciones, equipos informáticos, redes de comunicaciones, soportes de información y equipamiento auxiliar.
8	Profesional Universitario	Realizar análisis de dependencia de activos de información, para determinar en caso de fallas de un activo que otros activos se ven perjudicados o involucrados.
9	Profesional Universitario	Generar diagrama de árbol de dependencias de activos donde se observaran as relaciones existentes
10	Profesional Universitario	Realizar valoración de los activos de información en función de la relevancia, criticidad y nivel de impacto.
11	Profesional Universitario	Establecer el ciclo de vida de cada uno de los activos de información, para su gestión efectiva.
12	Profesional Universitario	Seguimiento, verificación, evaluación y emisión de reporte periódico del estado de los activos de información.
13	Profesional Universitario	¿Existen modificaciones a los activos de información o existen nuevos activos de información? Sí: continua al paso 3 No: continua al paso 6
14		Fin del Procedimiento

3.2.2 Gestión de riesgos de seguridad de la Información.

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
1		Inicio de actividades
2	Profesional Universitario	Realizar la identificación los riesgos de seguridad de la información en cada uno de los activos de información.
3	Profesional Universitario	Realizar clasificación de los riesgos de la seguridad de la información.
4	Profesional Universitario	Establecer las amenazas y o eventos que pueden desencadenar un incidente de seguridad informática.
5	Profesional Universitario	Establecer vulnerabilidades y o debilidades que tienen los activos de información.
6	Profesional Universitario	Establecer los riesgos intrínsecos que tiene la posibilidad de producir un impacto sobre activos de información.
7	Profesional Universitario	Realizar y establecer controles que reduzcan los riesgos de seguridad de la información sobre los activos de información disminuyendo el impacto y la probabilidad de ocurrencia.
8	Profesional Universitario	Aplicar controles sobre los riesgos de seguridad de la información a los activos de información.
9	Profesional Universitario	Establecer los riesgos residuales de los activos de información, los cuales deben ser asumibles y vigilados.
10	Profesional Universitario	Generar matriz de riegos de todos los activos de información y documentación
11	Profesional Universitario	Seguimiento, verificación, evaluación y emisión de reporte periódico del estado de la aplicación de los controles sobre los riesgos de seguridad de la información
12	Profesional Universitario	¿Existen modificación o adecuación sobre los controles aplicados a los riesgos? Si: continua al paso 7 No: continua al paso 12
13	Profesional Universitario	Seguimiento, verificación, evaluación de los riegos existentes a los activos de información.
14	Profesional Universitario	¿Existen nuevos riesgos de seguridad de la información? Sí: continua al paso 2 No: continua al paso 15
15		Fin del procedimiento

3.2.3 Políticas de Seguridad de la Información.

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
1		Inicio de actividades
2	Profesional Universitario	Elaborar y describir las políticas de seguridad de la información de acuerdo con las necesidades, activos de información, objetivos misionales y visiónales de la institución.
3	Profesional Universitario	Emisión documentación con las políticas de seguridad de la información para aprobación por parte del Comité de gestión tecnológica.
4	Comité CIGD	Revisa y analiza las políticas de seguridad de la información.
5	Comité CIGD	¿Viabilidad de las políticas de seguridad de la información? Si: continúa al paso No. 2 No: continúa al paso No. 6
6	Profesional Universitario	Realizar comunicación y publicación oficial para dar a conocer a toda la comunidad universitaria las políticas de seguridad de la información aprobadas.
7	Profesional Universitario	Realizar seguimiento continuo a la aplicación y cumplimiento de las políticas de seguridad de la información
8	Profesional Universitario	Evaluación y diagnostico periódico de eficiencia de las políticas de seguridad de la información.
9	Profesional Universitario	Emisión del informe de diagnóstico y evaluación de las políticas de seguridad de la información, para modificación y/o mejora continua de las mismas.
10	Profesional Universitario	¿Existen modificaciones y/o mejora continua de las políticas de seguridad de la información? **Sí**: Se envían las modificaciones y/o actualizaciones de las políticas de seguridad de la información al Comité de Gestión Tecnología para su evaluación (paso 3) **No**: continúa al paso No 11
11		Fin del Procedimiento

3.2.4 Copias de Seguridad

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
1		Inicio de actividades
2	Profesional Universitario	Establecer los activos de información a los cuales se le realizara copias de seguridad.
3	Profesional Universitario	Establecer los dispositivos y tecnologías de almacenamiento para las copias de seguridad.
4	Profesional Universitario	Establecer los riesgos a los que se enfrenta la integridad y conservación de la información. Comunica Subproceso **2.2.2** *Gestión de riesgos de seguridad de la Información*
5	Profesional Universitario	Crear y establecer controles sobre los riesgos de la integridad y conservación de la información. Comunica Subproceso *2.2.2 Gestión de riesgos de seguridad de la Información*
6	Profesional Universitario	Aplicar los controles sobre la integridad y conservación de la información. Comunica Subproceso *2.2.2 Gestión de riesgos de seguridad de la Información*
7	Profesional Universitario	Evaluación y diagnostico periódico de eficiencia de los controles sobre la integridad y conservación de la información. Comunica Subproceso *2.2.2 Gestión de riesgos de seguridad de la Información*
8	Profesional Universitario	¿Existen modificaciones y/o mejora continua a los controles sobre la integridad y conservación de la información? **Sí** continua al paso No. 5 **No**: continua al paso No. 9
9	Profesional Universitario	Crear y establecer reglas de seguridad y reglas de acceso a la información guardada en copias de seguridad.
10	Profesional Universitario	Aplicar las reglas de seguridad y reglas de acceso a la información guardada en copias de seguridad.
11	Profesional Universitario	Evaluación y diagnostico periódico de eficiencia de las reglas de seguridad y reglas de acceso a la información guardada en copias de seguridad.

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
12	Profesional Universitario	¿Existen modificaciones y/o mejora continua a las reglas de seguridad y reglas de acceso a la información guardada en copias de seguridad? **Sí**: continúa al paso No. 9 **No**: continúa al paso No. 13
13	Profesional Universitario	Establecer el tipo de copia de seguridad y periodicidad de acuerdo a la clasificación de cada uno de los activos de información.
14	Profesional Universitario	Elaborar manuales de creación y ejecución de copia de seguridad de cada uno de los activos de información.
15	Profesional Universitario	Ejecución de las copias de seguridad a los activos de información de acuerdo a los manuales.
16	Profesional Universitario	Verificación de la ejecución e integridad de las copias de seguridad realizadas a cada activo de información.
17	Profesional Universitario	¿Se realizó correctamente la copia de seguridad? Sí: continúa al paso No. 18 No: continúa al paso No. 15.
18	Profesional Universitario	Evaluación y diagnostico periódico de eficiencia de los tipos de copia de seguridad, periodicidad y ejecución de las copias de seguridad.
19	Profesional Universitario	¿Existen modificaciones y/o mejora continua a los tipos de copia de seguridad, periodicidad y ejecución de las copias de seguridad? **Sí**: continúa al paso No. 13 **No**: continúa al paso No. 20
20		Fin de procedimiento

3.2.5 Recuperación de Desastres

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
1		Inicio de actividades

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
2	Profesional Universitario	Establecer los tipos de riesgos que se pueden materializar en desastres en cada uno de los activos de información. Comunica Subproceso *2.2.2 Gestión de riesgos de seguridad de la Información*
3	Profesional Universitario	Realizar clasificación de los activos de información con cada uno de los riesgos de ocurrencia de desastres que puede afectarle. Comunica Subproceso *2.2.2 Gestión de riesgos de seguridad de la Información*
4	Profesional Universitario	Crear y establecer controles sobre los riesgos de ocurrencia de desastres de cada uno de los activos de información. Comunica Subproceso *2.2.2 Gestión de riesgos de seguridad de la Información*
5	Profesional Universitario	Aplicar los controles sobre los riesgos de ocurrencia de desastres a cada uno de los activos de información. Comunica Subproceso *2.2.2 Gestión de riesgos de seguridad de la Información*
6	Profesional Universitario	Evaluación y diagnostico periódico de la eficiencia de los controles sobre los riesgos de ocurrencia de desastres de cada uno de los activos de información. Comunica Subproceso *2.2.2 Gestión de riesgos de seguridad de la Información*
7	Profesional Universitario	¿Existen modificaciones y/o mejora continua a los controles sobre los riesgos de ocurrencia de desastres? **Sí**: continúa al paso No. 3 **No**: continúa al paso No. 8
8	Profesional Universitario	Crear y establecer puntos de restauración en caso de ocurrencia de desastres según la clasificación de los activos de información de acuerdo a su nivel de criticidad e importancia.
9	Profesional Universitario	Elaborar manuales ejecución de restauración, recuperación de información y servicios de cada uno de los activos de información.

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
10	Profesional Universitario	Realizar pruebas periódicas de restauración en ambientes controlados para la verificación de la efectividad de la restauración, recuperación de los activos de información y servicios.
11	Profesional Universitario	¿Existen modificaciones y/o mejora continua a las actividades restauración y recuperación? **Sí**: continúa al paso No. 8 **No**: continúa al paso No. 12
12	Profesional Universitario	En caso de ocurrencia de desastres realizar labores de restauración y recuperación de acuerdo a los manuales del activo o activos de información.
13	Profesional Universitario	Verificación y validación de la ejecución de la recuperación de desastres e integridad de la información, activos de información y prestación de servicios.
14	Profesional Universitario	¿Se realizó correctamente restauración y recuperación de los activos de información? Sí: continúa al paso No. 15 No: continúa al paso No. 12
15	Profesional Universitario	Informar a las dependencias y/o comunidad universitaria la correcta restauración y recuperación de los activos de información y/o servicios
16		Fin del procedimiento.

3.2.6 Seguridad de la informática perimetral

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
1		Inicio de actividades
2	Profesional Universitario	Establecer los servicios informáticos, zonas y redes a asegurar conforme a las políticas seguridad y activos de información establecidas en la Universidad del Tolima.
3	Profesional Universitario	Realizar la clasificación de los servicios informáticos y acceso a estos de acuerdo a su nivel de criticidad, e importancia para la Universidad del Tolima.
4	Profesional Universitario	Elaborar reglas genéricas de protección informática de acuerdo a la clasificación de servicios informáticos y activos de información.

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
5	Profesional Universitario	Ejecutar, aplicar y administrar las reglas genéricas de protección informática a cada uno de servicios informáticos y activos de información.
6	Profesional Universitario	Seguimiento y manteamiento a las reglas genéricas de protección informática.
7	Profesional Universitario	Evaluación y diagnostico diario de eficiencia de las reglas genéricas de seguridad informática y activos de información.
8	Profesional Universitario	¿Existen modificaciones y/o mejora continua a las reglas de seguridad informática? **Sí**: continúa al paso No 4 **No**: continúa al paso No 9
9	Profesional Universitario	Creación de reglas de niveles de acceso y de navegación sobre cada activo de información y servicio establecido
10	Profesional Universitario	Aplicar las reglas de niveles de acceso y de navegación a cada activo de información y servicio establecido.
11	Profesional Universitario	Evaluación y diagnostico diario de eficiencia de las de accesibilidad y navegación a los activos de información.
12	Profesional Universitario	¿Existen modificaciones y/o mejora continua a las reglas de accesibilidad y navegación a los activos de información? **Sí**: continúa al paso No 9 **No**: continúa al paso No 13
13	Profesional Universitario	Realizar monitoreo y análisis constante para prevenir ataques informáticos.
14	Profesional Universitario	Crear medidas de protección de activos de información ante ataque informáticos que se presenten.
15	Profesional Universitario	Evaluar, analizar y diagnosticar la eficiencia de las medidas implementadas ante ataques informáticos.
16	Profesional Universitario	¿Existen modificaciones y/o mejora continua a las medidas implementadas ante ataques informáticos? **Sí**: continúa al paso No 14 **No**: continúa al paso No 17
17	Profesional Universitario	Realizar monitoreo constante del estado de los equipos y herramientas encargados de dar seguridad perimetral a los activos de información
18	Profesional Universitario	Realizar actualización de las bases de datos de los módulos de protección de los equipos de seguridad informática perimetral.
19	Profesional Universitario	Realizar evaluación del estado de funcionamiento de los equipos de seguridad informática perimetral.

Nº	RESPONSABLE	DESCRIPCIÓN DE LA ACTIVIDAD
20	Profesional Universitario	Estado de funcionamiento de los equipos de seguridad perimetral. ¿El equipo no funciona correctamente y cumplió su ciclo de vida útil? **Sí**: Se comunica con el proceso de Proyectos de TI. **No**: continúa al paso No 21
21		Fin de procedimiento.

4. BASE LEGAL

- Ley de transparencia 1712: “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones."
- ISO 27000.
- Estrategia Gobierno Digital.
- Metodología MAGERIT (metodología para gestionar los riesgos derivados del uso de las tecnologías y comunicaciones).
- Ley 1273 de 2009 (ley de delitos informáticos).

5. REGISTROS

No	IDENTIFICACIÓN		ALMACENAMIENTO		PROTECCIÓN	TRD	
	Código Formato	Nombre	Lugar Archivo	Medio de archivo	Responsable de Archivarlo	Tiempo de Retención	Disposición Final

6. ANEXOS

Anexo 1.

REGISTRO DE MODIFICACIONES

VERSIÓN	FECHA	ÍTEM MODIFICADO	DESCRIPCIÓN