PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

OFICINA DE TECNOLOGIA DE INFORMACIÓN

Encargado:

Ing. Carlos Alberto Rodríguez

Tabla de Contenido

Pág.

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia

Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220

PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co

SC-CER 115543

Lista de Tablas

Pág.

Lista de Gráficas

Pág.

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia

Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220

PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co

2. Introducción.

Hoy en día, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma adecuada, integra, oportuna, responsable y segura, lo que implica, que es necesario que las organizaciones tengan una adecuada gestión de sus recursos y activos de información con el objetivo de asegurar y controlar el debido acceso, tratamiento y uso de la información. El aseguramiento y la protección de la seguridad de la información de las organizaciones y de los datos de carácter personal de los usuarios, representan un reto al momento de pretender garantizar su confidencialidad, integridad, disponibilidad y privacidad, razón por la cual, la seguridad de la información se ha convertido en uno de los aspectos de mayor preocupación a nivel mundial. Cualquier tipo de organización independiente de su tamaño y naturaleza, debe ser consciente que la diversidad de amenazas existentes que actualmente atentan contra la seguridad y privacidad de la información, representan un riesgo que al materializarse no solo les puede acarrear costos económicos, sanciónales legales, afectación de su imagen y reputación, sino que pueden afectar la continuidad y supervivencia del negocio. Lo anterior, sumando a un entorno tecnológico en donde cada día se hace más complejo de administrar y asegurar, genera que cada vez más la seguridad de la información forme parte de los objetivos y planes estratégicos de las organizaciones. Por lo tanto, es indispensable que los responsables dentro de las organizaciones encargadas de velar por la protección y seguridad de sus recursos, infraestructura e información, constantemente estén adoptando, implementando y mejorando medidas de seguridad orientadas a prevenir y/o detectar los riesgos que pueden llegar a comprometer la disponibilidad, integridad y confidencialidad de los activos de información a través de los cuales se gestiona la información del negocio, independientemente si está es de carácter organizacional o personal, o de tipo pública o privada. En la medida que la organización tenga una visión general de los riesgos que pueden afectar la seguridad y privacidad de la información, podrán establecer controles y medidas efectivas, viables y transversales con el propósito de salvaguardar la disponibilidad, integridad y confidencialidad tanto de la información del negocio como los datos de carácter personal de sus empleados, usuarios y partes interesadas. Es indispensable que las organizaciones realicen una adecuada identificación, clasificación, valoración, gestión y tratamiento de los riegos que pueden afectar su seguridad, con

el propósito de implementar medidas y controles efectivos que les permitan estar preparados ante situaciones adversas que puedan comprometer tanto la seguridad física y lógica de sus instalaciones, personas, recursos y sistemas, como la seguridad de su información. Las entidades del sector educación están en la obligación de garantizar la debida seguridad, protección y privacidad de la información de la comunidad Universitaria y personal de los usuarios que residen en sus bases de datos, lo que implica, que deben contar con los más altos estándares y niveles de seguridad con el propósito de asegurar la debida recolección, almacenamiento, respaldo, tratamiento, uso, intercambio y distribución de esta información. Debido a los múltiples riesgos y amenazas que hoy en día atentan contra la seguridad de la información y la protección y privacidad de los datos, es fundamental que las organizaciones establezcan, implementen, mantengan y mejoren continuamente un sistema de gestión de seguridad de la información basado en los riesgos y a su vez, alineado con los objetivos estratégicos y necesidades tanto del negocio como de sus partes interesadas. La oficina de Tic es consciente que la protección y aseguramiento de su información es fundamental para garantizar su debida gestión financiera, administrativa y operativa, razón por la cual debe establecer un marco normativo de Seguridad de la Información que contemple políticas, límites, responsabilidades y obligaciones frente a la seguridad y privacidad de la información de la entidad. El presente documento contiene el plan de seguridad y privacidad de la información para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de la organización, el cual tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno en Línea y la norma ISO 27001[1], los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de un modelo de Gestión de Seguridad y Privacidad de la Información en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

[1] Es una norma internacional que permite el asegur amiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

3. Marco de Referencia

3.1 Marco Normativo

Un listado de las diferentes leyes que son el punto de partida para la elaboración de planes, guías y documentos organizacionales.

Tabla 1 Leyes (2020-2021)

2020	**LEY 2069 DE 2020**	**Por medio de la cual se impulsa el emprendimiento en Colombia; Art. 82 Par. 2l.**
	LEY 2066 DE 2020	Por medio de la cual se establecen condiciones especiales para la normalización de cartera por única vez para los concesionarios de los servicios de radiodifusión sonora de interés público y comunitario y para los operadores del servicio de televisión comunitaria.
	LEY 2063 DE 2020	Por la cual se decreta el presupuesto de rentas y recursos de capital y ley de apropiaciones para la vigencia fiscal del 1 de enero al 31 de diciembre de 2021; arts. 52, 105.
	LEY 2056 DE 2020	Por la cual se regula la organización y el funcionamiento del Sistema General de Regalías; Art. 35.
	LEY 2055 DE 2020	Por medio de la cual se aprueba la "convención interamericana sobre la protección de los derechos humanos de las personas mayores", adoptada en Washington, el 15 de junio de 2015.
	LEY 2052 DE 2020	Por medio de la cual se establecen disposiciones transversales a la rama ejecutiva del nivel nacional y territorial y a los particulares que cumplan funciones públicas y-o administrativas, en relación con la racionalización de trámites y se dictan otras disposiciones.
	LEY 2050 DE 2020	Por medio de la cual se modifica y adiciona la Ley 1503 de 2011 y se dictan otras disposiciones en seguridad vial y tránsito; Art. 4o.
	LEY 2047 DE 2020	Por la cual se prohíbe en Colombia la experimentación, importación, fabricación y comercialización de productos cosméticos, sus ingredientes o combinaciones de ellos que sean objeto de pruebas con animales y se dictan otras disposiciones; Art. 7o.
	LEY 2043 DE 2020	Por medio de la cual se reconocen las prácticas, laborales como experiencia profesional y-o relacionada y se dictan otras disposiciones; Art. 1o.
	LEY 2040 DE 2020	Por medio de la cual se adoptan medidas para impulsar el trabajo para adultos mayores y se dictan otras disposiciones; Art. 8o.
	LEY 2016 DE 2020	Por la cual se adopta el Código de Integridad del Servicio Público Colombiano y se dictan otras disposiciones; Art. 3 Par.
2021	LEY 2153 DE 2021	Por la cual se crea un sistema de información, registro y monitoreo que permita controlar, prevenir y evitar el tráfico ilegal de fauna y flora silvestre en el territorio nacional y se dictan otras disposiciones; Art. 3 Inc. 2
	LEY 2132 DE 2021	Por medio del cual se establece el Día Nacional de la Niñez y Adolescencia Indígena colombiana y se dictan otras disposiciones; Art. 5

	LEY 2127 DE 2021	Por medio de la cual se erigen los municipios de Pisba, Paya y Labranza grande - departamento de Boyacá, como "Triángulo de la Libertad" en reconocimiento del Bicentenario de Independencia y se dictan otras disposiciones; Art. 5
	LEY 2126 DE 2021	Por la cual se regula la creación, conformación y funcionamiento de las Comisarías de Familia, se establece el órgano rector y se dictan otras disposiciones; Art. 30 Par. 2
	LEY 2108 DE 2021	Ley de internet como servicio público esencial y universal" o por medio de la cual se modifica la ley 1341 de 2009 y se dictan otras disposiciones
	LEY 2101 DE 2021	Por medio de la cual se reduce la jornada laboral semanal de manera gradual, sin disminuir el salario de los trabajadores y se dictan otras disposiciones.
	LEY 2097 DE 2021	Por medio de la cual se crea el registro de deudores alimentarios morosos (redan) y se dictan otras disposiciones.
	LEY 2089 DE 2021	Por medio de la cual se prohíbe el uso del castigo físico, los tratos crueles, humillantes o degradantes y cualquier tipo de violencia como método de corrección contra niñas, niños y adolescentes y se dictan otras disposiciones; Art. 5.
	LEY 2085 DE 2021	Por medio de la cual se adopta la figura de la Depuración Normativa, se decide la pérdida de vigencia y se derogan expresamente normas de rango legal; Art. 7 Inc. 3.
	LEY 2080 DE 2021	Por medio de la cual se reforma el código de procedimiento administrativo y de lo contencioso administrativo -ley 1437 de 2011- y se dictan otras disposiciones en materia de descongestión en los procesos que se tramitan ante la jurisdicción; arts. 1, 8, 9, 10, 12 a 15.

Fuente: (MinTIC, 2021)

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia

Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220

PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co

3.2 Contexto Histórico

Los recursos informáticos y de telecomunicaciones de la Institución son administrados por la oficina de Tecnologías de Información y Comunicaciones (DTIC) adscrita a la Rectoría de la UNIAJC. Esta oficina contribuye en la gestión de actividades académicas, investigativas y administrativas de la Institución a través del diseño, el desarrollo y la prestación de servicios de informática y telecomunicaciones, alineado con el objetivo estratégico de "modernizar la infraestructura física y tecnológica que garantice el adecuado servicio educativo" y con los objetivos estratégicos por área de desempeño de "infraestructura y equipamiento", y cumplir con los objetivos de las políticas gubernamentales como lo son la política del gobierno digital, las directrices del Conpes (3701, 3854, 2018 incluyendo la directriz 2021, 2022) que incentiva la confianza en el comercio electrónico y la interoperabilidad de datos entre las instituciones.

4. Caracterización de la infraestructura tecnológica

La institución garantiza a la comunidad universitaria condiciones que favorezcan el acceso permanente a la información, experimentación y práctica docente, necesarios para apoyar los procesos misionales, docencia, investigación y proyección social.

Actualmente, la configuración de los canales de Internet de la Institución cuenta con las siguientes características:

- Internet dedicado (1024Mb Emcali)
- Enlace de Backup redundante (258 Megas).
- Internet dedicado (300Mb Claro como Backup Activo)
- Nap Colombia 30 MB
- Sede Parquesoft 500 MB internet dedicado
- Edificios Sur Alameda Canal de datos 150 MB
- Red Metro (Casa Proyección Social, canal de datos 70 MB)
- Conexión con Data Center Netgroup (Edificio Ermita) 20 MB (canal de datos). Conexión por 1.2 Km mono-modo de fibra óptica propia, entre el edificio Principal y los edificios Estación I y Estación II. Interconexión de centros de cómputo por 350 metros de Fibra óptica propia multi-modo.
- Dos canales de datos nuevos, 50 MB para la sede Estación 1 y 10 MB para la sede Estación 2.

5. Objetivos.

5.1 Objetivo General.

Establecer un Plan de Seguridad y Privacidad de la Información que apoye el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de UNIAJC, acorde a los requerimientos del modelo de seguridad de la estrategia de gobierno en línea, los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

5.2 Objetivos Específicos

- Definir las etapas para establecer la estrategia de seguridad de la información de la entidad.
- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno en Línea.
- Establecer lineamientos para la implementación y/o adopción de mejores prácticas de seguridad en la entidad.
- Optimizar la gestión de la seguridad de la información al interior de la entidad.

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia

Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220

PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co

SC-CER 115543

6. Políticas actuales de seguridad de la información

Propósito: Proteger la información estratégica de la Institución y formar sus niveles de acceso y confidencialidad.

Exposición de la política

- Los dueños de la información nominados por autoridad competente deben ser funcionarios que estén completamente familiarizados con el segmento de información que les corresponde, así como con todos los procesos que interactúan con esta información.
- Los dueños de la información serán los responsables de verificar que existan procedimientos y procesos de seguridad para asegurar el manejo y la integridad de la información que reside en medios magnéticos o en documentos.
- El uso de los recursos lógicos de la institución deberá ser destinados para uso exclusivo de la UNIAJC.
- Toda información que viaje en un ambiente público deberá ser previamente encriptada.
- Los permisos de acceso a todos los sistemas de información, sean estos aplicativos del ERP y/o tendrán un tiempo de expiración de tres meses como mínimo y máximo cuatro meses.
- Se debe aplicar estándares y buenas prácticas de seguridad sobre el manejo de un modelo seguro de datos.
- Toda alta o baja del archivo maestro de personal debe ser oportuna y adecuadamente informado para una correcta administración de las claves de acceso.
- La entrega y/o acceso a la información de la institución, así como el acceso a su infraestructura tecnológica por parte de terceros se realizará en base a la suscripción de convenios de confidencialidad o a la existencia de cláusulas de confidencialidad en los contratos u órdenes de trabajo respectivos.
- Todos los funcionarios que manejan información sensible de la compañía deberán firmar un acuerdo de confidencialidad.
- Será responsabilidad de la Oficina de tecnologías de la información, mantener vigente y actualizado el licenciamiento de software para la institución, tal como antivirus, licencias de firewall, destinados a proteger las instalaciones y activos informáticos de la Institución, así como también procurar una operación sin sobre cargas en la red de datos.

6.1 Políticas de manejo de cuentas de correo y uso de la red

Propósito: Para el manejo del uso de red se ha establecido las siguientes políticas:

- La instalación de puntos de red LAN Y WAN se realizará con contratación externa y/o personal directo de la Institución Universitaria Antonio José Camacho.
- La Oficina de tecnologías de la información y Comunicaciones, tendrá la responsabilidad de llevar un control de inventario de los puntos de red instalados en todos los edificios y oficinas de la Institución. Esto incluye la certificación, rotulación de los mismos de acuerdo al estándar previamente establecido, y el uso de un sistema informático de control de este inventario.

- Todas las unidades de la institución que tengan necesidad de instalar puntos de red deberán canalizar y sustentar sus requerimientos ante su correspondiente responsable de área. Encontrar justificada la necesidad, cada responsable deberá hacer llegar a DTIC para ser atendidos.

Para el manejo del correo electrónico y el internet, la UNIAJC ha establecido las siguientes políticas:

- Para la utilización de los diferentes servicios de red a través de las cuentas creadas, se deben acatar las normas obligatorias, cuyo incumplimiento acarreará sanciones de acuerdo con el reglamento interno de trabajo, según sea el caso.
- La cuenta electrónica es personal e intransferible. El usuario es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre. La Institución Universitaria Antonio José Camacho no se hace responsable por lo que se haga o diga en nombre de una cuenta particular, y por lo tanto, está prohibido el uso de cuentas por personas ajenas a su titular.
- La UNIAJC podrá suspender o cancelar cuentas por mal manejo, sin perjuicios de imponer las sanciones correspondientes, según la gravedad de la falla.

Se consideran como conductas de mal manejo de las cuentas personales: Usos inaceptables tales como:

- Exceder los servicios para la cual se creó la cuenta.
- Intentar apoderarse de claves de acceso de otros usuarios acceder y/o modificar archivos de otro usuario y en especial los pertenecientes a la UNIAJC.
- Enviar mensajes para la difusión de mensajes o correos electrónicos sin identificar plenamente a su autor o enviar anónimos.
- Usar los servicios de red para propósitos no investigativos o usuarios para propósitos fraudulentos, comerciales o publicitarios o para propagación de mensajes destructivos u obscenos.
- Difundir cadena de mensajes.
- Perturbar el trabajo de los demás enviando mensajes que pueden interferir con su trabajo.
- Violar o intentar violar los sistemas de seguridad de la red y servidores académicos y administrativos a los cuales se tenga acceso de manera local o externamente.
- Violar los derechos de privacidad de terceras partes.
- Violación de los derechos de propiedad intelectual de terceras partes.
- Usar la red para propósitos recreativos.
- Violar las reglas y restricciones impuestas por el administrador de red y la política de seguridad de la información de cualquier equipo que tenga una conexión a la red.
- No hacer uso racional del ancho de banda, espacio en disco, memoria, disco duro y unidades de almacenamiento.

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia
Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220
PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co
SC-CER 115543

- No salirse de una cuenta ajena cuando por circunstancia accidental se conecte a una.
  Se consideran como conductas de buen manejo de las cuentas personales: Usos aceptables:
- Uso para propósitos educativos y de investigación.
- Uso para propósitos de administración de la infraestructura educativa y para investigación.
- Uso para acceso a bibliotecas.
- Uso para desarrollar proyectos de instituciones educativas o de un sector privado de proyectos de investigación.

6.2 Custodia y tenencia de activos informáticos.

• Los activos informáticos corporativos y centralizados serán custodiados por DTIC En caso de que se requiere equipo especializado, estos serán custodiados por el área donde se encuentre la operación.

• Los activos informáticos de usuarios finales (Mouse, Teclado y Diademas, sonido), serán custodiados por el responsable de su operación.

• Los custodios deberán ser funcionarios nombrados por la institución, a quienes se asignan los activos informáticos y son responsables pecuniariamente de su buen uso e integridad. Los usuarios son quienes utilizan para su labor diaria o eventual el activo informático y pueden ser empleados regulares de la institución o no (empleados de outsourcing, contratistas externos, consultores, entre otros).

• Cuando el usuario es un empleado regular de la institución, es a su vez un custodio. Cuando el usuario no es un empleado regular, el equipo debe estar a cargo de un funcionario nombrado de la Institución.

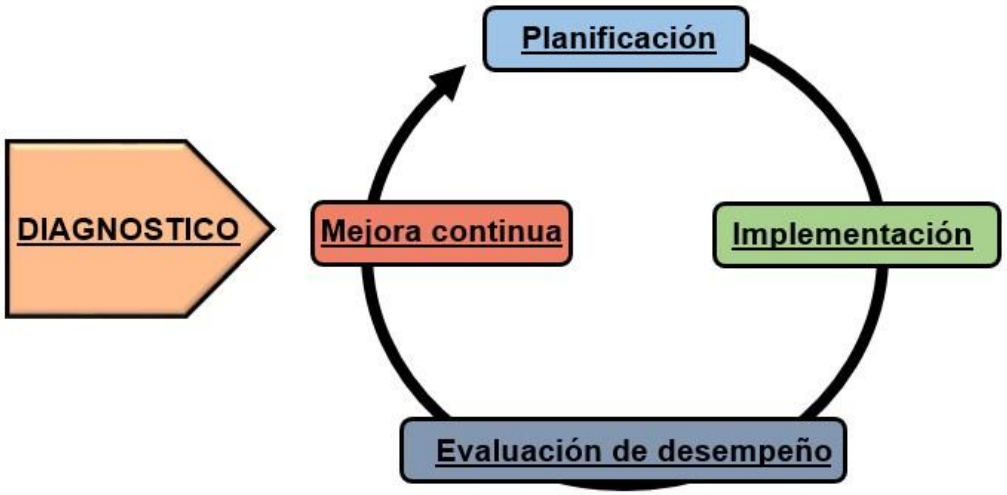
• La asignación de equipos de cómputo se realiza por la DTIC a los funcionarios custodios, después de la solicitud del jefe de área, una vez asignado el recurso a un funcionario este no puede asignarse a ningún otro empleado.

7. Metodología e implementación del modelo de seguridad

7.1 Ciclo Operación.

El Modelo de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea contempla el siguiente ciclo de operación que contempla cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

Grafica 1. Ciclo operación.



Fuente: (MinTIC, s.f.)

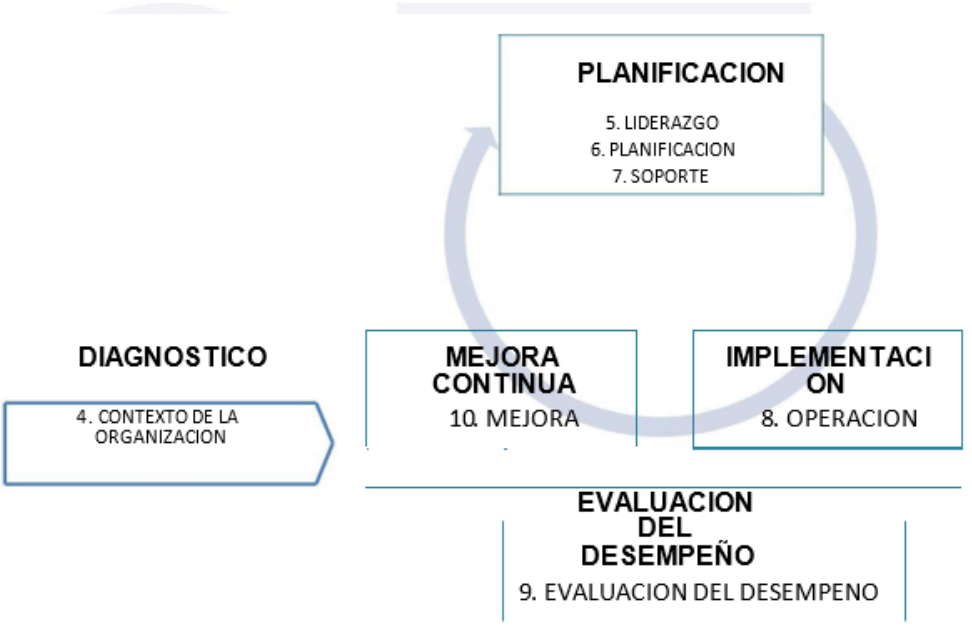
- Fase Diagnostico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- Fase Planificación (Planear): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.
- Fase Implementación (Hacer): En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.
- Fase Evaluación de desempeño (Verificar): Una vez implantada la mejora, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones implementadas.
- Fase Mejora Continua (Actuar): Se analizan los resultados de las acciones implementadas y si estas no se cumplen los objetivos definidos se analizan las causas de las desviaciones y se generan los respectivos planes de acciones.

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia
Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220
PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co
SC-CER 115543

7.2 Alineación norma ISO 27001:2013 vs ciclo de operación.

Aunque en la norma ISO 27001:2013 no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:

Grafica 2. Norma ISO 27001:2013 alineado al Ciclo de mejora continua.



Fuente: (Gutiérrez, 2013)

El siguiente cuadro muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnostico, Planificación, Implementación, Evaluación, Mejora Continua) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Tabla 1. Fases Ciclo Operación vs Estructura ISO 27001:2013.

FASES	CAPITULO ISO 27001:2013	CUMPLIMIENTO												
		2021	2022											
			01	02	03	04	05	06	07	08	09	10	11	12
Diagnostico	Contexto de la organización	50%	5%	5%	5%	5%	5%	5%	5%	5%	10%			

Fuente: (Gutiérrez, 2013)

- Fase DIAGNÓSTICO en la norma ISO 27001:2013.

En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestiones externas e internas de la organización y de su contexto, con el propósito de incluir la necesidad, es y expectativas de las partes interesas de la organización en el alcance del SGSI.

- Fase PLANEACIÓN en la norma ISO 27001:2013.

En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.
En el capítulo 6 - Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.
En el capítulo 7 - Soporte se establece que la organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua Sistema de Gestión de Seguridad de la Información.

- Fase IMPLEMENTACION en la norma ISO 27001:2013.

En el capítulo 8 - Operación de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

- Fase EVALUACION DEL DESEMPEÑO en la norma ISO 27001:2013.

En el capítulo 9 - Evaluación del desempeño, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información.

- Fase MEJORA CONTINUA en la norma ISO 27001:2013.

En el capítulo 10 - Mejora, se establece para el proceso de mejora del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, las organizaciones deben establecer las acciones más efectiva para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia
Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220
PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co
SC-CER 115543

7.3 Fases del ciclo operativo.

7.3.1 Fase I: diagnostico.

Identificar el estado de la Entidad con respecto a los requerimientos del SGSI.

Tabla 2. Metas VS Actividades, Instrumentos y Resultados.

Metas	Actividades \ Instrumentos \ Resultados	2021	CUMPLIMIENTO												META
			2023												
			01	02	03	04	05	06	07	08	09	10	11	12	
Perfilar la gestión de seguridad y privacidad de la información al interior de la Entidad, a la luz de la ISO270001	Recibir la asesoría de implementación de ISO 270001.	50%													50%
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Valoración del nivel de madurez de la entidad frente a la seguridad de la información a la luz de la ISO27001.	50%													50%
	Valoración del nivel de madurez de la privacidad de la información en la entidad a la luz de la ISO27001.	50%													50%
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Actualización con nuevas herramientas para la mitigación de vulnerabilidades.	50%													50%

Fuente: (Gutiérrez, 2013)

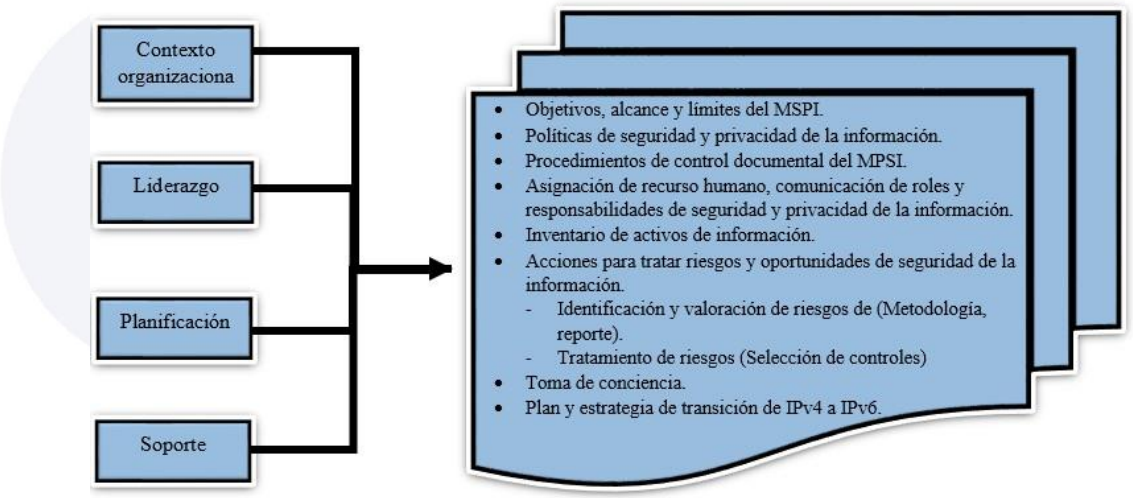
Para la recolección de la información, en esta fase se utilizarán mecanismo como:

- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de la entidad con relación a los dominios de la norma ISO/IEC 27001:2013.
- Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.
- Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la estrategia de gobierno en línea Ministerio de Tecnologías de la Información y las Comunicaciones.

7.3.2 Fase II: planificación.

Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la mejora de seguridad de la información, en procura de los resultados.

Grafica 3. Planificación modelo de seguridad.



Fuente: (MinTIC)

Tabla 3. Metas VS Actividades, Instrumentos y Resultados.

Metas	Actividades \ Instrumentos \ Resultados	CUMPLIMIENTO													
		2021	2022												
			01	02	03	04	05	06	07	08	09	10	11	12	
Realizar un análisis de Contexto y factores externos e internos de la Entidad en torno a la seguridad de la información junto con el asesor ISO27001.	Realizar un Análisis de Contexto de la entidad entorno a la seguridad	80%													85%
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información con las modificaciones y nuevos activos de información.	Adicionar las funciones de seguridad de la información al personal de la oficina de Tic.	80%													95%
	Establecer nuevos Roles de Seguridad de la información a la luz de los nuevos cambios que traen los nuevos activos de información.	80%													80%
Elaborar los procedimientos, manuales de seguridad y privacidad de la información de la entidad.	Elaborar nuevos procedimientos generales para la seguridad, privacidad y buenas prácticas de la información al interior de la Entidad.	80%													80%
Identificar y valorar activos de información.	Realizar una actualización y valoración de los activos de información de la entidad de acuerdo con su	100%													100%

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia

Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220

PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co

SC-CER 115543

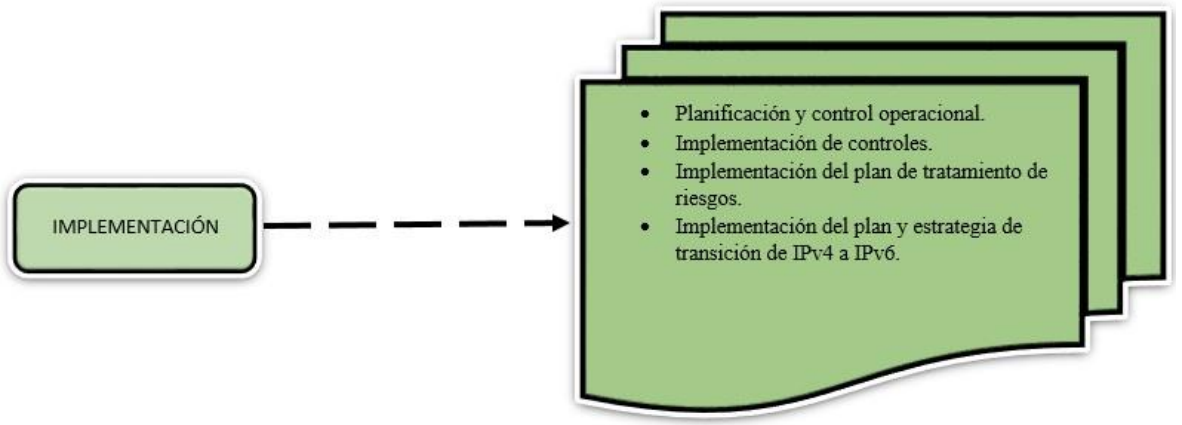
	nivel de criticidad de acuerdo con el alcance del SGSI.														
Establecer capacitaciones, y sensibilización de seguridad de la información.	Dictar mínimo dos capacitaciones al año, sobre sensibilización en el ámbito de seguridad de la información.	50%													50%

Fuente: (Gutiérrez, 2013)

7.3.3 Fase III: implementación.

Llevar a cabo la implementación de la fase de planificación del SGSI, teniendo en cuenta para esto los aspectos más relevantes en los de implementación del Sistema de Gestión de Seguridad.

Grafica 4. Fase de implementación modelo de seguridad.



Fuente: (MinTIC)

Tabla 4. Metas VS Actividades, Instrumentos y Resultados.

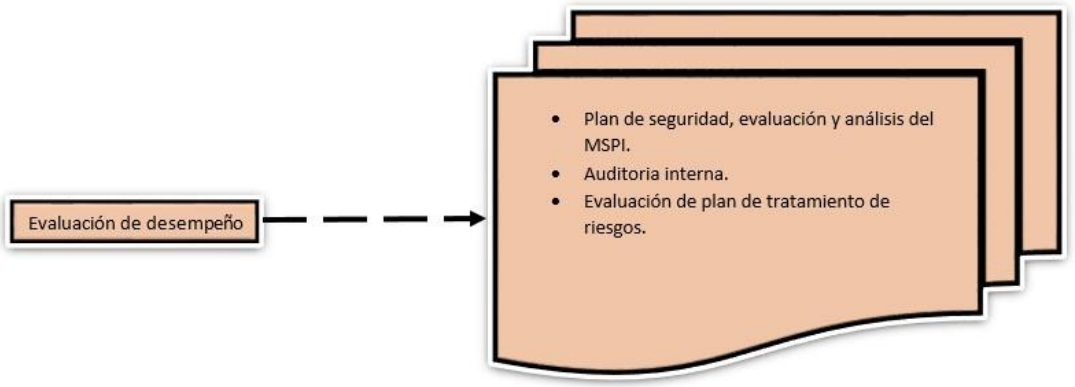
Metas	Actividades \ Instrumentos \ Resultados	2021	CUMPLIMIENTO 2022											META
			01	02	03	04	05	06	07	08	09	10	11	12	
Establecer controles a la seguridad de la información y los riesgos.	Realizar análisis exhaustivos con equipos de seguridad perimetral	100%													100%
Ejecutar pruebas anuales de vulnerabilidades e intrusión.	Ejecutar pruebas de vulnerabilidad e intrusión con el objetivo de identificar el nivel de protección de los activos de información de la entidad.	80%													80%

Fuente: (Gutiérrez, 2013)

7.3.4 Fase IV: evaluación de desempeño.

Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos.

Grafica 5. Fase Evaluación Desempeño modelo de seguridad.



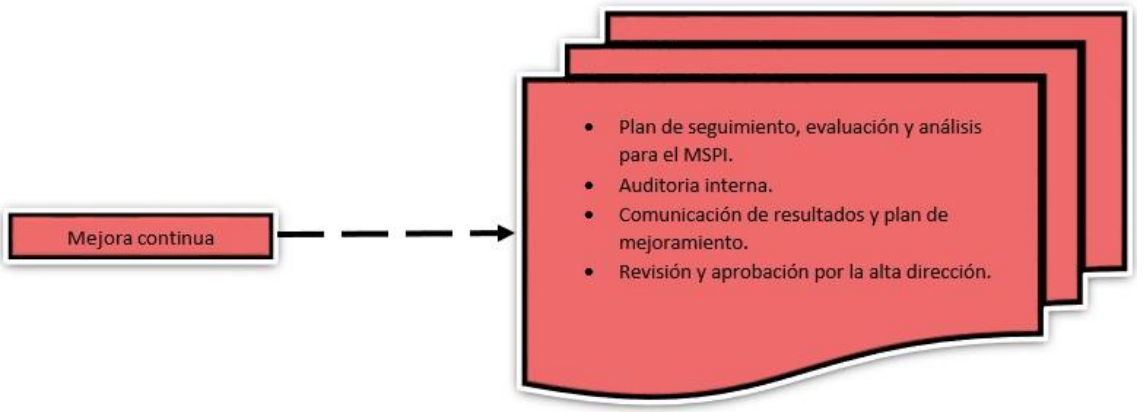
Fuente: (MinTIC)

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia
Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220
PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co

7.3.5 Fase V: mejora continua.

Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento y privacidad de la información, que permita realizar el plan.

Grafica 6. Fase Mejora Continua modelo de seguridad.



Fuente: (MinTIC)

Tabla 6. Metas VS Actividades, Instrumentos y Resultados.

METAS	ACTIVIDADES \ INSTRUMENTOS \ RESULTADOS	CUMPLIMIENTO												META
		2023	2023											
			01	02	03	04	05	06	07	08	09	10	11	12	
Diseñar plan de mejoramiento.	Aplicar acciones correctivas que permitan mejorar la seguridad perimetral de equipos, servidores y dispositivos.	90%												90%

Fuente: (Gutiérrez, 2013)

7.4 Mapa de Riesgos.

Una gran variedad de riesgos amenaza la infraestructura de tecnología de la información en la organización, por esta razón los riesgos de seguridad se clasifican en tres grandes tipos con diferentes consecuencias y probabilidades agrupados en la siguiente tabla:

Tabla 7. Tipo de riesgos.

TIPO DE RIESGO	DESCRIPCION
R. Estratégico	Este tipo de riesgo obedece a todo lo que la organización no puede controlar. Ej. Desastres naturales, redes eléctricas externas, asonadas.
R. Corrupción	Este tipo de riesgo está asociado con el indebido con personas dentro de la organización.
R. Digital	todas aquellas amenazas que afectan el buen funcionamiento de las tecnologías de información que soportan las actividades académico administrativos

Fuente: (Gutiérrez, 2013)

Tabla 8. Mapa de riesgo.

MAPA DE RIESGOS						V - 3.0 - 2015 DIR-F-7
MEDIDAS DE MITIGACIÓN			ANÁLISIS			
TIPO DE RIESGO	AMENAZAS	CONSECUENCIA	PROBABILIDAD	CONTROLES	IMPACTO	ZONA RIESGO RESIDUAL
R. Seguridad Digital	Evadir los dispositivos y controles que cuidan la seguridad perimetral.	Perdida de la continuidad de negocio.	4	Generación periódica de los informes pertenecientes a los equipos y sistemas de seguridad perimetral.	1	Moderada
R. Seguridad Digital	Saltar controles de usuarios, roles, permisos, perfiles, restricciones y contraseñas.	Falla en el control de acceso a activos de información.	2	Generación periódica de los informes pertenecientes a los equipos y sistemas de seguridad perimetral.	3	Moderada
R. Estratégico	Sobrepasar la capacidad contingencia.	Atención parcial de los servicios de tecnología.	3	Actualización de contratos de tecnologías con diferentes proveedores tecnológicos.	3	Alta
R. Corrupción	Falta de normas, manuales y procedimientos.	Asumir el Riesgo	2	Capacitación y charlas permanentes al personal interno de la oficina.	2	Baja

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia
Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220
PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co
SC-CER 115543

R. Corrupción	Falta de normas, manuales y procedimientos.	Asumir el Riesgo	1	Actualización permanente en documentos del sistema de calidad institucional.	2	Baja
R. Corrupción	- Procedimientos formales aplicados - Dispositivos de seguridad física y electrónica.	Perdida o daños a la infraestructura tecnológica	5	Gestión periódica de los inventarios y activos.	4	Extrema

7.5 Seguimiento al Plan de Seguridad.

La tabla número 9 describe cada una de las actividades que soportan el plan de seguridad de la información, además se describe el presupuesto promediado mensual.

Tabla 9. Fuente de elaboración propia, matriz de seguimiento.

CRONOGRAMA DE EJECUCIÓN															
		2024													
Proyectos	DESCRIPCION	01	02	03	04	05	06	07	08	09	10	11	12	Objetivo	Meta %
Aplicativos y sistemas de información	Gestión y mantenimiento de sistemas de información Académico y administrativo	12.5%												90%	80%
Seguridad perimetral, sistemas de prevenciónn y sistemas detección	Gestión y mantenimientode sistemas de seguridad	12.5%												95%	95%
Análisis de vulnerabilidad, se evidencian reportes de análisis de seguridad.	SOC de 4 reportes para el análisis de vulnerabilidad (https://repo.triara.co/repositori o/index.php)	12.5%												95%%	95%
Gestión de servidores	Gestión de servidores Data-Center	12.5%												95%	95%
Seguridad firewall perimetral.	Gestión de 7 equipos de seguridad perimetral	12.5% .												100%	100%

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia
Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220
PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co
SC-CER 115543

Implantación de controles de acceso en los diferentes edificios		125. %												90%	85%
Induccioness	Sensibilizar y educar a la comunidad académica en el manejo, rol y seguridad de lossistemas de información y dispositivos que les prestan Servicios.	20%												80%	85%

7.6 Términos y Referencias.

- Activo de información: aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.
- Amenaza: Es la causa potencial de un daño a un activo de información.
- Anexo SL: Nuevo esquema definido por International Organización de estándares - ISO para todos los Sistemas de Gestión acorde al nuevo formato llamado “Anexo SL”, que proporciona una estructura uniforme como el marco de un sistema de gestión genérico.
- Análisis de riesgos: Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.
- Causa: Razón por la cual el riesgo sucede.
- Ciclo de Deming: Modelo mejora continua para la implementación de un sistema de mejora continua.
- Colaborador: Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, Trabajadores de Planta, Trabajadores Temporales, Contratistas, Proveedores y Practicantes.
- Confidencialidad: Propiedad que determina que la información no esté disponible a personas no autorizados.
- Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

- Disponibilidad: Propiedad se determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.
- Dueño del riesgo sobre el activo: Persona responsable de gestionar el riesgo.
- Impacto: Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.
- Incidente de seguridad de la información: Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.
- Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.
- Oficial de Seguridad: Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.
- Probabilidad de ocurrencia: Posibilidad de que se presente una situación o evento específico.
- Responsables del Activo: Personas responsables del activo de información.
- Riesgo: Grado de exposición de un activo que permite la materialización de una amenaza.
- Riesgo Inherente: Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.
- Riesgo Residual: Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.
- PSE: Proveedor de Servicios Electrónicos, es un sistema centralizado por medio del cual las empresas brindan a los usuarios la posibilidad de hacer sus pagos por Internet.
- SARC: Siglas del Sistema de Administración de Riesgo Crediticio.
- SARL: Siglas del Sistema de Administración de Riesgo de Liquidez.
- SARLAFT: Siglas del Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo.
- SARO: Siglas del Sistema de Administración de Riesgos Operativos.
- Seguridad de la Información: Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).
- SGSI: Siglas del Sistema de Gestión de Seguridad de la Información.

- Sistema de Gestión de Seguridad de la información SGSI: permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.
- Vulnerabilidad: Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad se caracteriza por ausencia en controles de seguridad que permite ser explotada.

Resolución MEN No. 963
Exp. el 02 de marzo de 2007
Cali - Colombia

Norte: Av. 6N #28N-102
Sur: Km.7 vía Cali-Jamundí · Calle 25 #127-220

PBX: +57(2) 665 2828 Opc.1
mercadeo@admon.uniajc.edu.co
www.uniajc.edu.co

SC-CER 115543

Bibliografía

- Gutiérrez Amaya, H. C. (09 de Octubre de 2013). *Publicada ISO 27000:2013, cambios en la norma para gestionar la seguridad de la información.* Obtenido de www.welivesecurity.com: https://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

- MinTIC. (s.f.). *El Modelo de Seguridad y Privacidad de la Información (MSPI).* Obtenido de www.mintic.gov.co: http://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

- MinTIC. (s.f.). *Modelo de Seguridad y Privacidad de la Información.* Obtenido de https://mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf