PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2022

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

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 encargados 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 aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

3. Objetivos.

3.1 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.

3.2 Objetivos Específicos

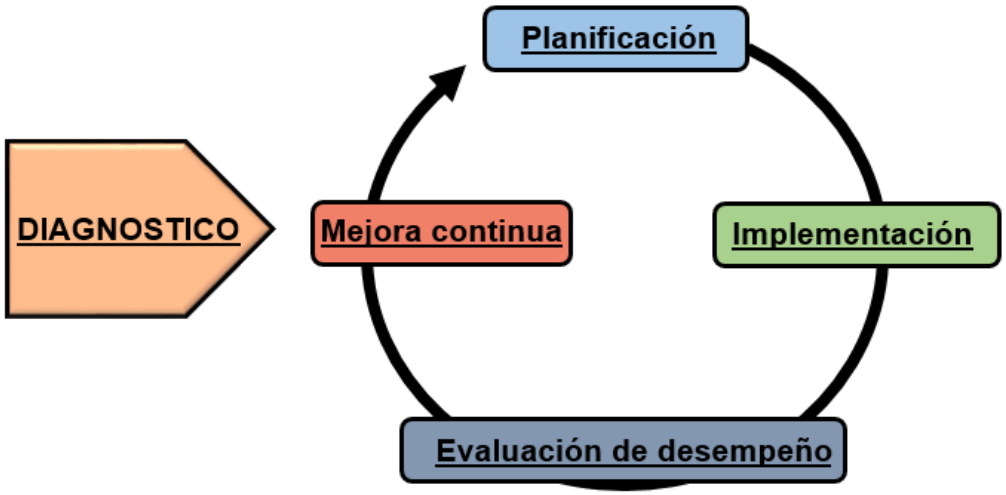
- Definir las etapas para establecer la estrategia de seguridad de la información de la entidad.
- Apalancar la implementación del Sistema de Gestión de Seguridad de la Información de la entidad de acuerdo con los requerimientos establecidos en el modelo de seguridad de la estrategia de Gobierno en Línea.
- 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.

4. Metodología e implementación del modelo de seguridad.

4.1 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.)

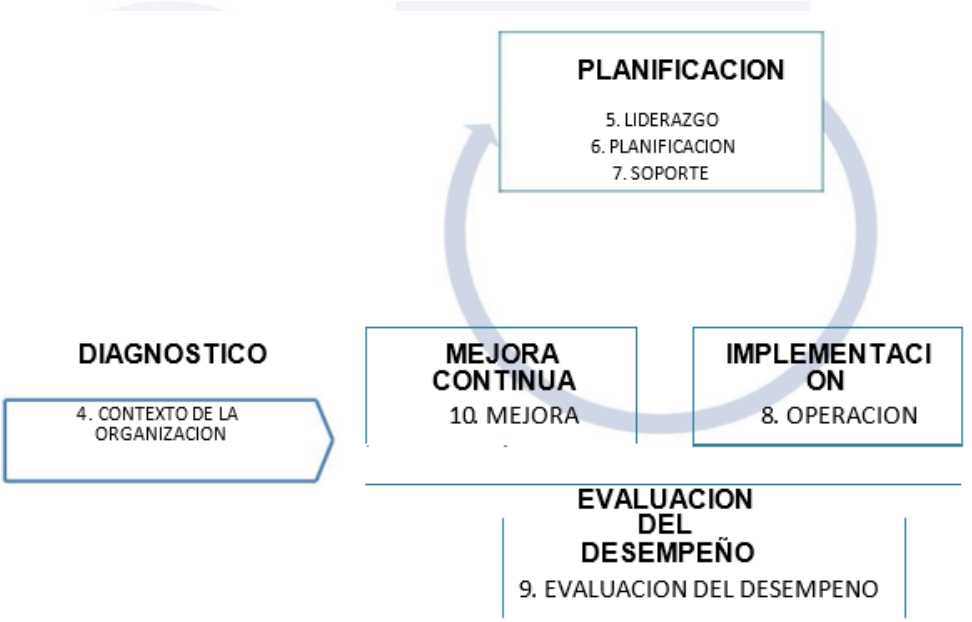
- Fase Diagnostico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.
- Fase Planificación (Planear): En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así 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

4.2 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 DIAGNOSTICO 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 cuestionas 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 PLANEACION 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

4.3 Fases del ciclo operativo.

4.3.1 Fase I: diagnostico.

Identificar el estado de la entidad con respecto a los requerimientos del SGSI, para la presente se realizó un pre-diagnóstico junto con un proveedor especializado de seguridad, donde se describió un estado inicial de condiciones mínimas para la implementación de seguridad ISO 27001.

Tabla 2. Metas VS Actividades, Instrumentos y Resultados.

Metas	Actividades \ Instrumentos \ Resultados	2021	CUMPLIMIENTO												META
			2022												
			01	02	03	04	05	06	07	08	09	10	11	12	
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad	Diagnóstico de la situación actual de la entidad con relación a la gestión de seguridad de la información, basado en ISO - 27001	80%										10%			90%
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad, a la luz de la ISO27001	Valoración del nivel de estratificación de la entidad frente a la seguridad de la información.	80%										5%			85%
	Valoración del nivel de madurez de seguridad y privacidad de la información en la entidad.	80%										10%			90%
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Ejecución prueba de vulnerabilidades con el fin de identificar el nivel de seguridad y protección de los activos de información de la entidad y definición de planes de mitigación. (Resultados Adquisición de un EDR como herramienta complementaria)	90%										5%			95%

Fuente: (Gutiérrez, 2013)

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

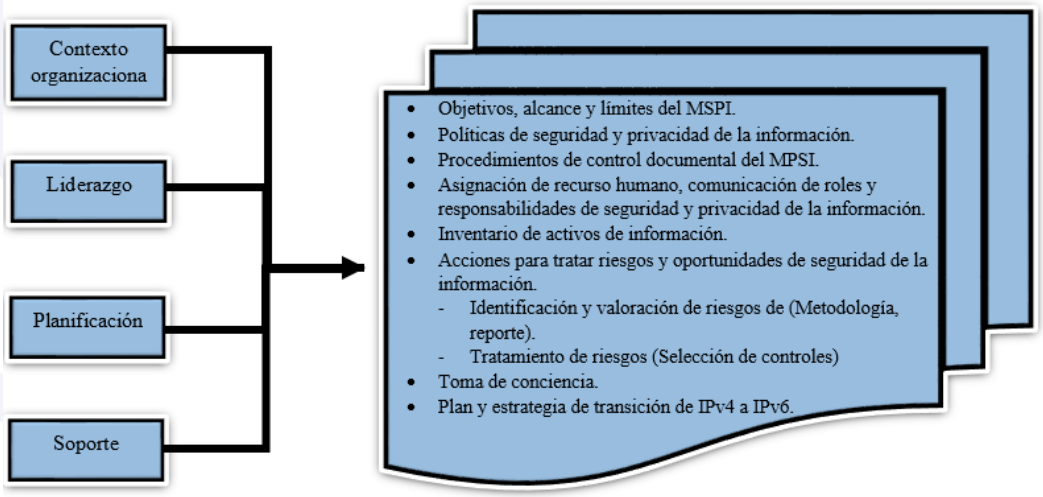
- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de le entidad con relación a los dominios de la norma ISO/IEC 27001:2013.
- Documentación existente en el sistema de calidad de la entidad relacionada con la información de las partes interesadas de la entidad 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.

4.3.2 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.	Realizar un Análisis de Contexto de la entidad entorno a la seguridad	80%										5%			85%
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información	Adicionar las funciones de seguridad de la información al personal de la oficina de Tic.	80%										15%			95%
	Establecer el Rol de Oficial de Seguridad de la información. Definir un marco de gestión que contemple roles y responsabilidades para la implementación, administración, operación y gestión de la seguridad de la información en la entidad. Definir la	80%										5%			85%

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

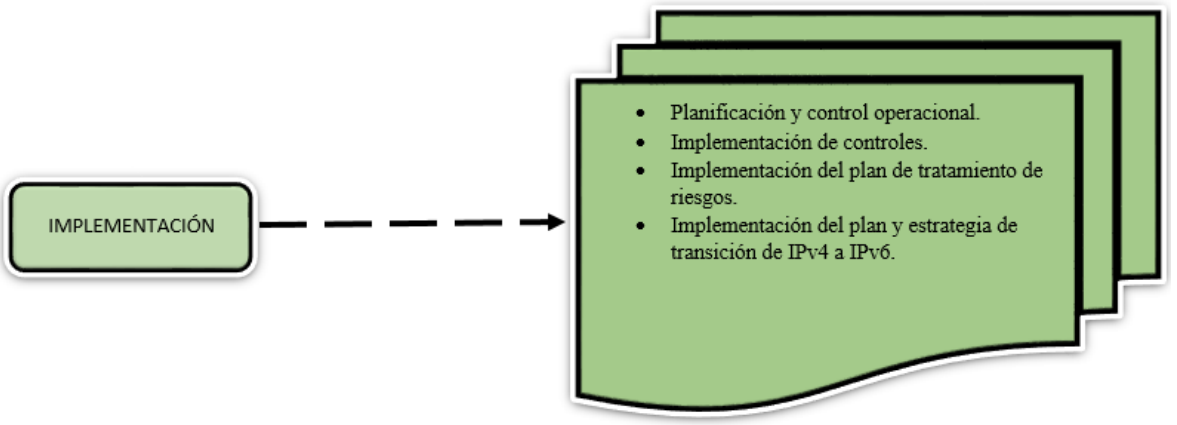
	estructura organizacional de la Entidad que contendrá los roles y responsabilidad pertinentes a la seguridad de la información.														
Elaborar los procedimientos, manuales de seguridad y privacidad de la información de la entidad.	Elaborar procedimientos generales para la seguridad, privacidad y buenas prácticas de la información al interior de la Entidad.	90%										5%			95%
Identificar y valorar activos de información.	Realizar una actualización y valoración de los activos de información de la entidad de acuerdo con su nivel de criticidad de acuerdo con el alcance del SGSI.	100%										100%			100%
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.	75%													100%

Fuente: (Gutiérrez, 2013)

4.3.3 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.

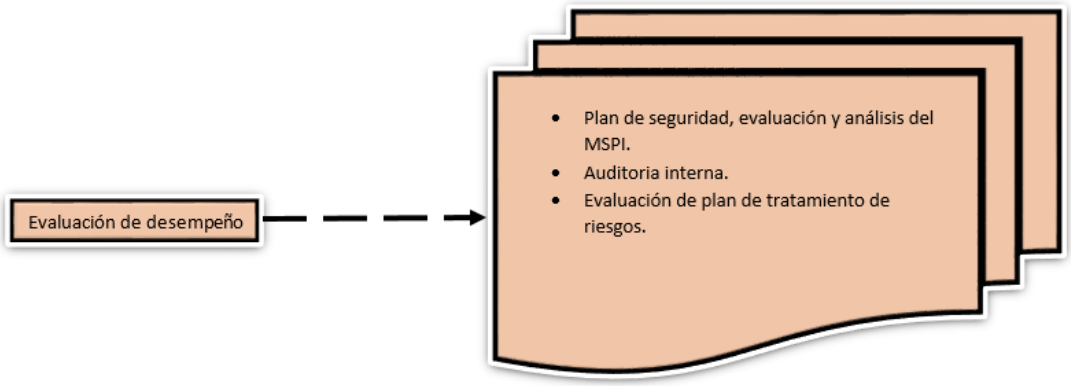
Metas	Actividades \ Instrumentos \ Resultados	2021	CUMPLIMIENTO 2022												META
			01	02	03	04	05	06	07	08	09	10	11	12	
Establecer controles a la seguridad de la información y los riesgos.	Realizar análisis exhaustivos con equipos de seguridad perimetral	100%			25%			25%			25%			25%	100%
Ejecutar 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.	85%						40%				45%			90%

Fuente: (Gutiérrez, 2013)

4.3.4 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.



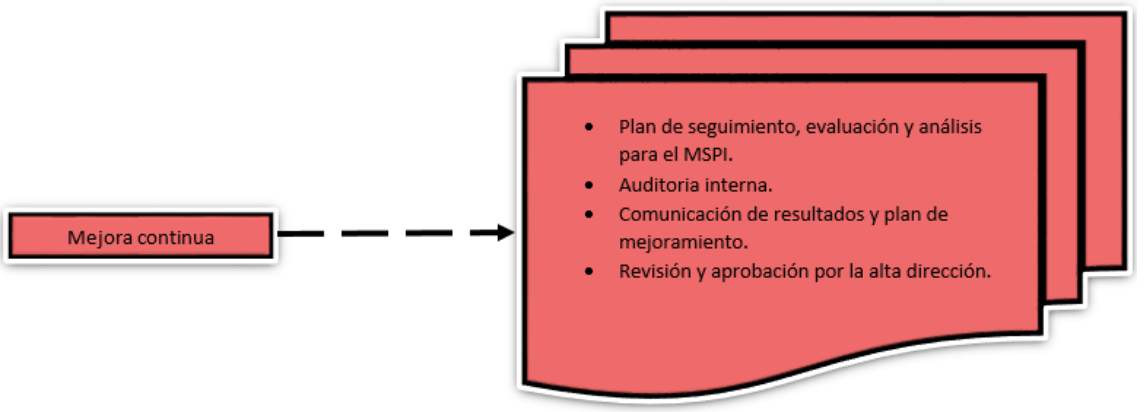
Fuente: (MinTIC)

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
SC-CER 115543

4.3.5 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
		2021	2022												
			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.	95%	8%	8%	8%	8%	8%	8%	8%	8%	8%	8%	8%	8 %	96%

Fuente: (Gutiérrez, 2013)

4.3.6 Implementación modelo de seguridad alineado a riesgos.

Grafica 7. Productos.

Fuente: (Gutiérrez, 2013)

4.4 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)

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

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
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

4.5 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.

PLAN DE SEGURIDAD DE LA INFORMACION						
CDP	PROVEEDOR	ACTIVIDAD / DESCRIPCIÓN DE PROYECTO	PRESUPUESTO ANUAL DE FUNCIONAMIENTO	ENERO-OCTUBRE PRESUPUESTO MES	ACTIVIDADES DE AVANCE EN LA EJECUCIÓN	EVIDENCIAS
	Claro	Actualización de servicios, para aumentar el canal dedicado de Wifi.	30.240.000	2.520.000	Ampliación del ancho de banda	Ordenes de servicio
	Claro	Actualización de servicios, para aumentar el canal dedicado.	50.400.000	4.200.000	Ampliación del ancho de banda	Ordenes de servicio
	Claro	Soporte a los diferentes sistemas de seguridad perimetral	91.096.380	7.591.365	Renovación de los servicios	Ordenes de servicio
	Moodle	Baja de servidores	59.000.000	4.916.000	Recofiguración de recursos en el datacenter	Contrato NetgroupSA
	RUAV	Petición de informe trimestral	60.262.353	5.021.862	Solicitud de informes trimestrales de utilización de salones virtuales	Informe trimestral de utilización de salones virtuales

Fuente: (Gutiérrez, 2013)

4.6 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.

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

- 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 de 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 de 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

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