TR-CO16.00230

CEHANI E.S.E.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – CEHANI

Arley Realpe Chamorro
Gerente

Centro Integral de Atención Especializada

VIGILADO Supersalud

COPIA CONTROLADA No. COPIA

COPIA NO CONTROLADA

CICLO DE EVALUACIÓN Y MEJORAMIENTO			
REVISIÓN	**FECHA**	**DESCRIPCIÓN DE LA MODIFICACIÓN**	**MEJORAMIENTO**
Actualización del documento	31/01/2019	El cambio se realiza por los requerimientos ante MIPG y por los cambios de la vigencia 2019	Mejoramiento continuo
Actualización del documento	Enero de 2020	Se modificó en el documento los propietarios de los activos de información, se actualizo el cronograma para la vigencia 2020.	Mejoramiento continuo
Actualización del documento	Mayo de 2021	Se revisa el documento en su totalidad, se adicionan en los cronogramas. Responsable, Fecha y observaciones	Mejoramiento Continuo
Actualización del documento	Enero de 2022	Se revisa el documento en su totalidad,	Mejoramiento Continuo

1. INTRODUCCIÓN

El presente documento relacionado con el Plan de Seguridad y Privacidad de la Información contempla las buenas prácticas que la entidad debe adoptar en materia de seguridad, partiendo del hecho de que para CEHANI E.S.E la información es uno de los activos más importante que posee la empresa, puede relacionarse con datos de las partes interesadas y puede llegar a constituirse en un bien de interés público, que por lo tanto merece un tratamiento y consideración especial.

Los esfuerzos realizados por las entidades públicas para afrontar la problemática de la seguridad de la información, relacionada con los riesgos que conlleva la pérdida de cualquiera de sus propiedades como son la confidencialidad, integridad o disponibilidad, ha llevado a que las mismas tengan que hacer esfuerzos para minimizar el nivel de su exposición al riesgo. Estas inversiones se traducen en proyectos que van desde una implementación tecnológica, que constituye un control de seguridad específico para la información, hasta proyectos tendientes a definir e implementar modelos de seguridad que permitan hacer una gestión continua de una estrategia de seguridad de la información, que debe implementarse y mejorarse a través del tiempo.

La norma internacional ISO/IEC 27001:2013 es en sí un modelo para establecer, implementar, operar, hacer seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información. De otro lado la citada norma ISO define la seguridad de la información como: “La Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad”, y también la define desde el punto de vista del negocio como: “La protección de la información contra una serie de amenazas para reducir el daño al negocio y maximizar las oportunidades y utilidades del mismo”. Esta última definición lleva implícito que la seguridad de la información es un tema estratégico y empresarial que debe ser atendido, con compromiso desde la alta dirección.

Teniendo en cuenta lo anterior la gestión de la seguridad de la información requiere de una o varias estrategias alineadas con la plataforma y objetivos, requiere de presupuesto, recursos y de un conjunto de actividades dirigidas y coordinadas por una organización de la seguridad que se extienda a través de toda la organización, desde la alta dirección hasta los usuarios finales.

Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información desarrollado por el MinTic, se trabaja en el fortalecimiento de la seguridad de la información en las entidades públicas, con el fin de garantizar la protección de la misma y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación Colombiana.

2. OBJETIVO

Documentar e implementar el plan de seguridad y privacidad de la información, articulado al modelo de Seguridad y Privacidad de la Información definido por el Ministerio de la información y las comunicaciones MINTIC.

3. ALCANCE

El documento refleja los principales lineamientos para garantizar la seguridad y privacidad de la información, los cuales deben ser divulgados, conocidos y cumplidos por todos los colaboradores de la entidad, contratistas y en general todos los terceros y/o partes interesadas que tengan acceso, almacenen, procesen o transmitan información de la entidad y/o de los usuarios

4. PRINCIPALES DEFINICIONES

- **Activo de Información:** Se considera principalmente a cualquier conjunto de datos creado o utilizado por un proceso de la organización, así como el hardware y el software utilizado para su procesamiento o almacenamiento, los servicios utilizados para su transmisión o recepción y las herramientas y/o utilidades para el desarrollo

y soporte de sistemas de información. En casos particulares, se puede considerar como un activo de información a personas que manejen datos, transacciones o un conocimiento específico muy importante para la organización.

- **Comité de TI:** Este comité es una instancia del nivel superior, que dentro de sus funciones se encuentra la de validar la Política de Información, así como los procesos, procedimientos y metodologías específicas de seguridad de la información para el adecuado uso y administración de los recursos informáticos y físicos, asignados a los servidores públicos de cada ente público, estas funciones pueden ser desempeñadas por el comité de Gestión y Desempeño Institucional.

- **Confidencialidad**: La confidencialidad es la garantía de que la información será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a ésta información. Cada individuo tiene derecho a proteger su información personal.

- **Disponibilidad:** Una vez que la información ha sido capturada en un sistema de cómputo, debe ser almacenada de manera segura y estar disponible para los usuarios cuando la necesiten. La información también debe ser mantenida y utilizada de tal forma que su integridad no se vea comprometida.

- **Evento de seguridad de la información:** un evento de seguridad de la información es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.

- **Incidente de seguridad de la información:** un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de los activos

de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.

- **Integridad:** Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es decir, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- **Propietario/responsable de activo de información:** El cual es una parte designada de la organización, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quiénes tienen acceso, que pueden hacer con la información, y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada y al mismo tiempo de definir qué se hace con la información una vez ya no sea requerida, así como los tiempos de retención asociados a la misma.

- **Servicio:** La razón de ser de toda institución de información es el usuario, es por ello que todas sus funciones se encaminan a la satisfacción de sus necesidades de información. Esta relación usuario/institución se establece a través de los servicios, como actividades identificables e intangibles, que el profesional de la información ofrece al usuario.

- **Usuario:** Persona, grupo o entidad que utiliza la información o los servicios de información. Es un término genérico y abarcador. La educación y formación de usuarios de la información se encuentra estrechamente vinculada con los estudios de usuarios, las necesidades informativas, la psicología, la educación, la divulgación científica y técnica, la caracterización de usuarios, la comunicación científica y otras disciplinas que permiten realizar análisis integrales.

5. DOCUMENTOS RELACIONADOS

Para la construcción del Plan de seguridad y privacidad de la información, se tendrá en cuenta el Modelo de Seguridad y Privacidad de la Información (MSPI) propuesto por el MinTic para entidades de carácter oficial principalmente y la norma ISO-IEC 27001:2013.

6. ROL DE LA ALTA DIRECCIÓN

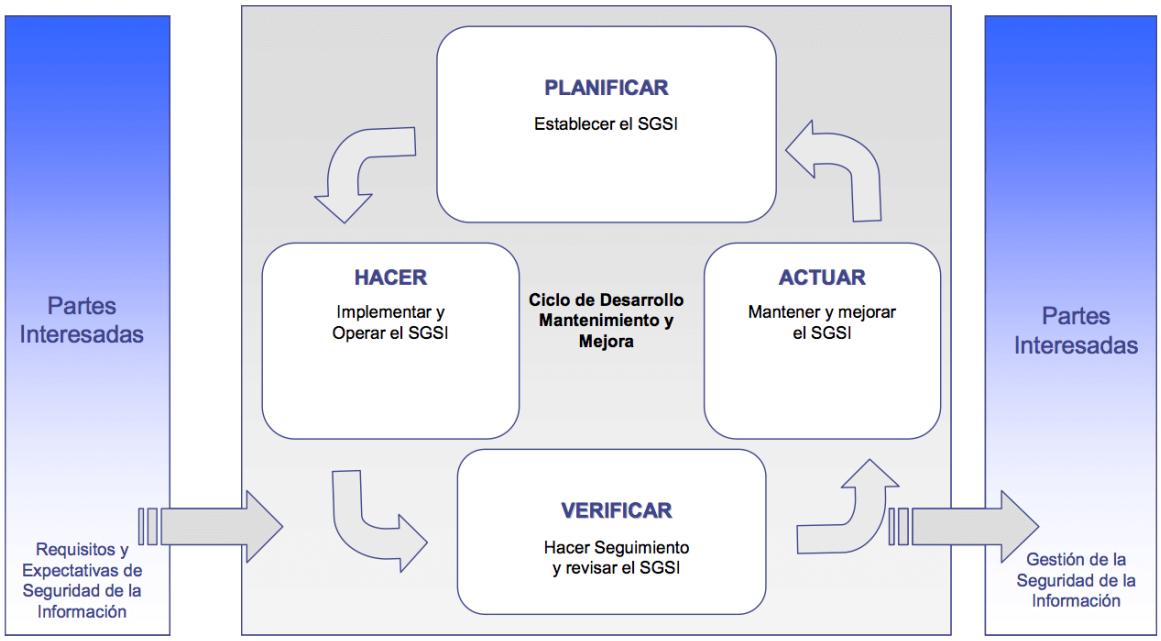
La Alta Dirección de CEHANI E.S.E. Manifiesta el compromiso y apoyo en el diseño, implementación del Modelo de Seguridad y Privacidad de la Información, definiendo la política de seguridad de la información, estableciendo los lineamientos de seguridad, fijando el gobierno de seguridad y la asignación de los recursos necesarios para llevar a feliz término las actividades programadas.

7. REQUISITOS GENERALES

La entidad a través del Comité de Gestión y Desempeño Institucional son los encargados de garantizar e impulsar la articulación del Modelo de Seguridad y Privacidad de la Información (MSPI) definido por el MINTIC en el Plan de seguridad y privacidad de la información, teniendo en cuenta el contexto, el sector salud que la reglamenta, el direccionamiento estratégico y los riesgos a los cuales se encuentra expuesta.

Para poder desarrollar este propósito se basará en el modelo PHVA que se ilustra en el siguiente gráfico.

Modelo PHVA Aplicado al modelo de seguridad y privacidad de la información



SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SEGÚN EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEFINIDO POR EL MINTIC

Guías del MSPI definidas por el Mintic

GUIA	TÍTULO GUIA
Guía 1	Metodología de pruebas de efectividad
Guía 2	Política General MSPI
Guía 3	Procedimientos de Seguridad y Privacidad de la Información
Guía 4	Roles y responsabilidades de seguridad y privacidad de la información
Guía 5	Gestión de Activos
Guía 6	Gestión Documental
Guía 7	Gestión de Riesgos
Guía 8	Controles de Seguridad

GUIA	TÍTULO GUIA
Guía 9	Indicadores Gestión SI
Guía 10	Continuidad de TI
Guía 11	Impacto Negocio
Guía 12	Seguridad en la Nube
Guía 13	Guía De Evidencia Digital
Guía 14	Plan de comunicación, sensibilización y capacitación
Guía 15	Auditoría
Guía 16	Evaluación del Desempeño
Guía 17	Mejora Continua
Guía 18	Lineamientos terminales de áreas financieras entidades públicas
Guía 19	Aseguramiento del protocolo IPV6
Guía 20	Transición IPv4_IPv6
Guía 21	Gestión de Incidentes

8. ESTRATEGIAS - ESTABLECIMIENTO DEL MODELO

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las entidades puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

La seguridad y privacidad de la información, como componente habilitador transversal de la Política Gobierno Digital, permite alinearse a los componentes TIC para el Estado y TIC para la Sociedad y con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

Ciclo de Operación del MSPI

El gráfico anterior muestra las cinco fases del ciclo de operación del MSPI a continuación miraremos en qué consiste cada una de las fases y su corresponsabilidad con el modelo PHVA.

Fase I Diagnóstico: Permite identificar el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información

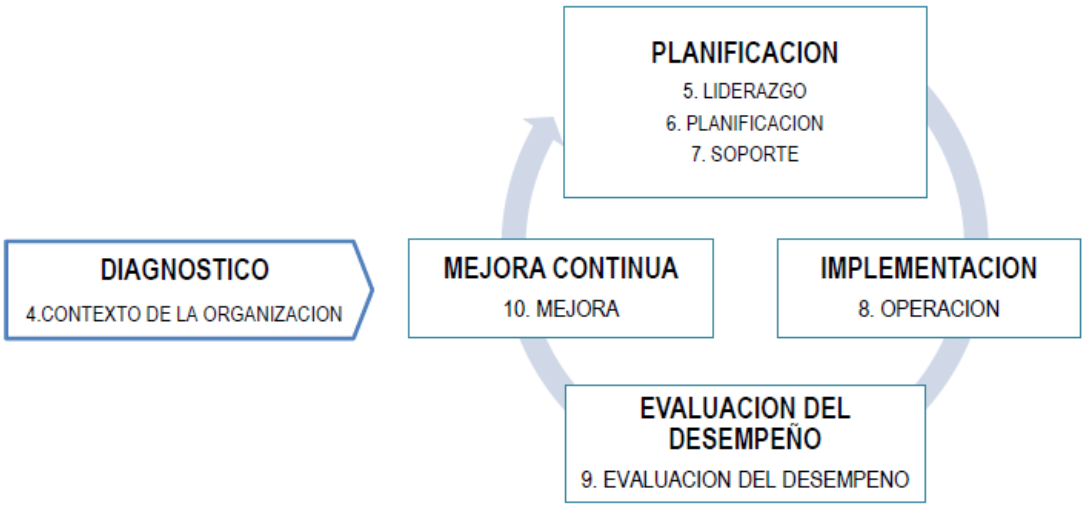
Fase II Planificación (Planear): Que hace referencia a establecer el Modelo de Seguridad y Privacidad de la Información, en esta fase se debe establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para gestionar los activos y el riesgo buscando mejorar la seguridad de la información, con el fin de entregar resultados acordes con las políticas y objetivos globales de la entidad.

Fase III Implementación (Hacer): Que hace referencia a implementar y operar el MSPI, en esta fase se debe implementar y operar la política, los controles y procedimientos del MSPI.

Fase IV Evaluación de Desempeño (Verificar): Que hace referencia a hacer seguimiento y revisión del MSPI, en esta fase se debe evaluar, y, en donde sea aplicable, medir el desempeño del proceso contra la política y los objetivos de seguridad y la experiencia práctica, y reportar los resultados a la dirección, para su revisión.

Fase V Mejora Continua (Actuar): Que hace referencia a mantener y mejorar el MSPI, en esta fase se debe emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del MSPI y la revisión por la dirección, para lograr la mejora continua del MSPI.

Alineación de las Fases Del MSPI Con ISO-IEC 27001: 2013



9. FASES DE IMPLEMENTACIÓN DEL PROYECTO SEGÚN EL CICLO DE OPERACIÓN DEL MSPI

FASES CICLO DE OPERACIÓN MSPI	CORRESPONSABILIDAD CON ISO 27001:2013
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 las necesidades y expectativas de las partes interesadas de la organización en el alcance del SGSI.
PLANIFICACIÓN	En la norma ISO 27001:2013. En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al

FASES CICLO DE OPERACIÓN MSPI	CORRESPONSABILIDAD CON ISO 27001:2013
	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 establecen 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.
IMPLEMENTACIÓN	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.
EVALUACIÓN 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.
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.

9.1. CRONOGRAMA

Fase I diagnóstico

Objetivo: En esta fase lo que se pretende es establecer el estado actual de la entidad con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Metas del Diagnóstico

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS	RESPONSABLE	FECHA	OBSERVACIONES
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad	Diagnóstico nivel de cumplimiento de la entidad frente a los objetivos de control y controles establecidos en el Anexo A de la norma ISO 27001:2013 Herramienta de Diagnóstico del MSPI de MinTic	Herramienta de diagnóstico diligenciada	Profesional universitario GSI	28-02-2022	Se deben realizar autoevaluaciones anuales
Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad	Herramienta de Diagnóstico del MSPI de MinTic	Herramienta de diagnóstico diligenciada Establecimiento del nivel de madurez de la entidad frente al MSPI	Profesional universitario GSI	28-02-2022	Se deben realizar autoevaluaciones anuales
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Herramienta de Diagnóstico del MSPI de MinTic	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Profesional universitario GSI	28-02-2022	Se deben realizar autoevaluaciones anuales

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 Política Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.
- Herramienta de diagnóstico del MSPI de MinTic
- Instructivo para el diligenciamiento de la herramienta de diagnóstico
- Desarrollo de la Guía No 1 - Metodología de Pruebas de Efectividad del MSPI

Una vez se tenga el resultado del diagnóstico inicial y se haya determinado el nivel de madurez de la entidad se procede al desarrollo de la siguiente fase que es la de Planificación.

9.2. Fase II Planificación

Objetivo: Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad de la información, en procura de los resultados que permitan dar cumplimiento con las metas propuestas.

Metas de la Planificación

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS	RESPONSABLE	FECHA	OBSERVACIONES
Política de Seguridad y Privacidad de la Información	Guía No 2 – Política General MSPI	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad Manual con las políticas de seguridad y privacidad de la	Profesional Universitario GSI	IMPLEMENTADA	Implementada

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS	RESPONSABLE	FECHA	OBSERVACIONES
		información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad			
Procedimientos de seguridad de la información	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional	Profesional Universitario GSI	Implementado	Implementada
Roles y responsabilidades de seguridad y privacidad de la información	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad	Profesional Universitario GSI Profesional Universitario SIG	29-04-2022	
Inventario de activos de información	Guía No 5 - Gestión De Activos Guía No 20 - Transición Ipv4 a Ipv6	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de	Profesional Universitario GSI Profesional Universitario SIG	30-06-2022	

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS	RESPONSABLE	FECHA	OBSERVACIONES
		activos de información, que contengan datos personales Inventario de activos de IPv6			
Integración del MSPI con el Sistema de Gestión documental	Guía No 6 - Gestión Documental	Integración del MSPI, con el sistema de gestión documental de la entidad	Profesional Universitario GSI Técnico de Gestión Documental	28-02-2023	
Identificación, Valoración y tratamiento de riesgo	Guía No 7 - Gestión de Riesgos Guía No 8 - Controles de Seguridad	Documento con la metodología de gestión de riesgos Documento con el análisis y evaluación de riesgos Documento con el plan de tratamiento de riesgos Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección	Profesional Universitario GSI Profesional universitario SIG	31-05-2022	
Plan de Comunicaciones	Guía No 14 - Plan de comunicación, sensibilización y capacitación	Documento con el plan de comunicación, sensibilización y capacitación para la entidad	Profesional Universitario GSI Profesional Universitario GTH	30-06-2022	
Plan de diagnóstico de IPv4 a IPv6	Guía No 20 - Transición IPv4 a IPv6	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6	Profesional Universitario GSI	30-06-2022	

9.3. Fase III Implementación

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

Metas de la Implementación

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS	RESPONSABLE	FECHA	OBSERVACIONES
Planificación y Control Operacional	Documento con el plan de tratamiento de riesgos Documento con la declaración de aplicabilidad	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta dirección	Profesional Universitario GSI	31-12-2022	
Implementación del plan de tratamiento de riesgos	Documento con la declaración de aplicabilidad Documento con el plan de tratamiento de riesgos	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso ver matriz de riesgos y oportunidades MA-CDG-003.	Jefe oficina de CDG	30-06-2022	
Indicadores De Gestión	Guía No 9 - Indicadores de Gestión SI	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información. Ver Matriz de aseguramiento MA-GSI-001	Profesional Universitario GSI	30-06-2022	
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6 Guía No 20 - Transición de IPv4 a IPv6 para Colombia Guía No 19 – Aseguramiento del Protocolo IPv6	Profesional Universitario GSI	30-06-2022	

9.4. Fase IV Evaluación De Desempeño

Objetivo: Evaluar el desempeño y la eficacia del SGSI, a través de instrumentos que permitan determinar la efectividad de la implantación del SGSI.

Metas de la Evaluación de Desempeño

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS	RESPONSABLE	FECHA	OBSERVACIONES
Plan de revisión y seguimiento, a la implementación del MSPI	Guía No 16 – Evaluación del desempeño	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección	Jefe oficina CDG	30-03-2023	
Plan de Ejecución de Auditorias	Guía No 15 – Guía de Auditoría	Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección	Jefe oficina CDG	30-03-2023	

9.5. Fase V Mejora Continua

Objetivo: Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad y privacidad de la información, que permita realizar el plan de implementación de las acciones correctivas identificadas para el SGSI.

Meta del Mejoramiento Continuo

METAS	INSTRUMENTOS O HERRAMIENTAS A UTILIZAR	RESULTADOS ESPERADOS	RESPONSABLE	FECHA	OBSERVACIONES
Plan de mejora continua	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI Guía No 17 – Mejora Continua	Documento con el plan de mejoramiento Documento con el plan de comunicación de resultados	Jefe Oficina CDG Profesional Universitario SIG Todos los líderes de procesos y funcionarios	30-01-2022	La mejora continua se realizara según lo descrito en el Procedimiento de mejora continua PR-SIG-005

10. RIESGOS

Los riesgos que se pueden presentar durante la ejecución del plan se encuentran establecidos en la Matriz de Riesgos y Oportunidades (MA-CDG-003), y corresponden a:

- Incumplimiento de metas y objetivos institucionales
- Inoportunidad en las respuestas a PQRSF, derechos de petición, tutelas y fallos judiciales
- Riesgo Psicosocial
- Riesgo Biomecánico
- Riesgo biológico

La implementación del plan disminuye la probabilidad de materializarse en los siguientes riesgos definidos en la Matriz de Riesgos y Oportunidades (MA-CDG-003).

- Pérdida de la integridad de la información
- Pérdida de la confidencialidad de la información
- Pérdida de la disponibilidad de la información

11. INDICADORES

El indicador a establecer con la ejecución del plan de Seguridad y privacidad de la información corresponde a:

Indicador= Grado de implementación de la política de seguridad de la información

Formula=

$$\frac{\text{Número de items del modelo de seguridad de la información cumplidos}}{\text{Numero de items del modelo seguridad de la información requeridos}} \times 100$$

	Actualizado por:	**Revisado por:**	**Aprobado por:**
Firma			
Nombre	JHON JAIRO FIGUEROA	JUAN CARLOS CEBALLOS	ARLEY REALPE CHAMORRO
Cargo / Rol	Profesional universitario - GSI	Subgerente Administrativa y Financiera	Gerente