PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Oficna de Sistemas e Informática

Escuela Superior de Administración Pública

2020

CONTROL DE CAMBIOS

NOMBRE	VERSIÓN	AUTOR	FECHA
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA ESCUELA SUPERIOR DE ADMINISTRACIÓN PÚBLICA - ESAP	1.0	Oficina de Sistemas e Informática - OSI	JUNIO DE 2020

COMITÉ	ACTA DE APROBACIÓN	FECHA
Comité Institucional de Gestión y Desempeño	No.5	**1 de Julio de 2020**

TABLA DE CONTENIDO

INDICE DE TABLAS

INTRODUCCIÓN

La seguridad de la Información como habilitador transversal de la Política de Gobierno Digital se desarrolla a través del Modelo de Seguridad y Privacidad de la Información -MSPI, orientando la gestión e implementación del Sistema de Gestión de Seguridad de la Información – SGSI, con el fin de incorporar la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de la ESAP, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

En atención a lo anterior, la entidad asumió el reto de implementar el modelo de seguridad y privacidad de la información, a través de la Resolución SC 2823 del 26 de septiembre de 2016, mediante la cual se creó el Sistema de gestión de Seguridad de la información de la Escuela Superior de Administración pública - ESAP siguiendo los lineamientos de la Política de Gobierno Digital, reglamentada a través del Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, los cuales permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital.

El plan de seguridad y privacidad de la información se encuentra alineado con el Plan Decenal de Desarrollo Institucional 2010-2020, dentro del escenario estratégico de Desarrollo Institucional, en la línea de acción Gestión de la Información, cuyo objetivo es disponer de la información apropiada para el desarrollo de las funciones de la ESAP, a través de la estrategia No.1 la cual busca gestionar información confiable, integra y oportuna para el desarrollo de las funciones y actividades de la ESAP.

Así mismo, este plan apoya la implementación de controles y acciones tendientes a la mitigación de los riesgos del proceso de gestión tecnológica como son: "*Detrimento en el desempeño y capacidad de los sistemas de información que afectan su disponibilidad y el desarrollo de las actividades del proceso*", "*apropiación indebida de activos tecnológicos (Impresoras, computadores, teléfono, antenas , cableado, scanner, entre otros*" y "*Desactualización y/o no documentación de procedimientos e instructivos establecidos para el desarrollo de las actividades*

del proceso", hallazgos de auditorías internas y apoya el cumplimiento del Modelo integrado de planeación y gestión del MINTIC, dentro de su política de gobierno Digital.

Teniendo en cuenta lo anterior, se actualiza el presente documento dando cumplimiento a lo establecido en el Decreto 612 de 2018.

1 OBJETIVO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Definir las acciones, tendientes a fortalecer la seguridad y privacidad de la información de la Escuela Superior de Administración pública en adelante ESAP, mediante la planeación de actividades y la implementación de controles de seguridad alineadas con la Norma ISO 27001:2013, la política de gobierno digital, de acuerdo con el alcance definido por la ESAP. Dichas acciones serán gestionadas por los servidores públicos o contratistas asignados de la Oficina de Sistemas e Informática - OSI.

2 POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Escuela Superior de Administración Pública ESAP, en el marco de sus funciones, se compromete a proteger y asegurar la información tanto física como digital, a través de acciones, estrategias y recursos necesarios, con el fin de cumplir con los requisitos legales y de la entidad, en pro del fortalecimiento y mejora del sistema de gestión de seguridad de la información y sus objetivos.

2.1. OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN:

Articulados con la Política de alto nivel del SGSI, la entidad define como objetivos de seguridad de información los siguientes:

- Implementar y fortalecer los controles para la protección de los activos de información.
- Prevenir la materialización de los riesgos de seguridad de la información identificados.
- Controlar y minimizar los incidentes de Seguridad de Información.
- Cumplir los requisitos normativos, legales y de seguridad de la información, a través de políticas, lineamientos, guías y directrices del Sistema de Gestión de Seguridad de la Información SGSI.

- Generar una cultura en seguridad de la información.
- Evaluar y mejorar el Sistema de Gestión de Seguridad de la Información, con el fin de lograr la eficiencia y su mejora continua.

3 ALCANCE DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

Teniendo en cuenta el análisis del contexto externo, interno y las partes interesadas, la ESAP define el alcance de SGSI, en términos de las características de la entidad, su ubicación, sus activos y su tecnología, así: *"La Escuela Superior de Administración Pública ESAP adopta, establece, implementa, opera, verifica y mejora el SGSI para los procesos misionales (4) y los procesos de apoyo (8) que componen el mapa de procesos de la entidad". La ESAP acorde con su naturaleza jurídica, misión y visión, encontró aplicables todos los requisitos de la NTC/ISO 27001:2013 y todos los controles del Anexo A, sin excepción alguna".*

4 MARCO NORMATIVO

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 de 2018	Por medio del cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019
Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales

NORMA	DESCRIPCIÓN
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos.
NTC / ISO 27002:2013	Tecnología de la información. Técnicas de seguridad. Código de Práctica para controles de seguridad de la información.

5 OPERACIÓN DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

5.1 COMITÉ DE SEGURIDAD DE LA INFORMACION:

Las funciones del comité de Seguridad de la Información son asumidas por el Comité institucional de gestión y desempeño mediante Resolución No. 3853 de 2017.

5.2 DIAGNOSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

De acuerdo con la medición del instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones, con corte a diciembre de 2019, el avance general en el ciclo PHVA del Sistema de Gestión de Seguridad y privacidad de la Información de la ESAP es del 70,1%, tal como se presenta a continuación:

AVANCE PHVA		
COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
Planificación	38%	40%
Implementación	16%	20%
Evaluación de desempeño	8%	20%
Mejora continua	8%	20%
TOTAL	70,1%	100%

Tabla 1. Avance PHVA del SGSI

El 100% en el ciclo PHVA se alcanzará cuando se logre un nivel optimizado en el componente de implementación, el cual está relacionado directamente con la evaluación de efectividad de los controles para cada uno de los dominios:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	82	100	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	74	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	98	100	OPTIMIZADO
A.9	CONTROL DE ACCESO	69	100	GESTIONADO
A.10	CRIPTOGRAFÍA	90	100	OPTIMIZADO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	79	100	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	71	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	74	100	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	72	100	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	50	100	DEFINIDO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	100	100	OPTIMIZADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	47	100	DEFINIDO
A.18	CUMPLIMIENTO	91	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**78,3**	**100**	GESTIONADO

Tabla 2. Evaluación Dominios ISO 27001 1

A través del instrumento de identificación de la línea base de seguridad administrativa y técnica suministrada por MINTIC, se realiza la revisión de los avances en la implementación de los controles definidos por la Norma ISO 27001:2013, Anexo A, en cada uno de los dominios, de lo cual se puede concluir que los dominios que se encuentran en el nivel Definido son: Relación con proveedores y Aspectos de Seguridad de la información en la gestión de continuidad del negocio, para lo cual se deben establecer las acciones que apoyen las implementación de los controles y lo lleven a un nivel de madurez superior, los demás dominios se encuentran en los niveles: gestionado y optimizado, en los cuales se debe implementar acciones para llegar al nivel optimizado y realizar un permanente monitoreo para mantenerlos en un nivel de mejoramiento continuo.

[1] Fuente: Instrumento de identificación de la línea base de seguridad administrativa y técnica suministrada por MINTIC

A continuación, se presentan los controles que requieren alcanzar un nivel optimizado en su implementación:

Numeral	Dominio	2019	Nivel
A.11	Seguridad física y del entorno	79%	GESTIONADO
A.7	Seguridad de los recursos humanos	74%	GESTIONADO
A.13	Seguridad de las comunicaciones	74%	GESTIONADO
A.14	Adquisición, desarrollo y mantenimiento de sistemas	72%	GESTIONADO
A.12	Seguridad de las operaciones	71%	GESTIONADO
A.9	Control de acceso	69%	GESTIONADO
A.15	Relaciones con los proveedores	50%	DEFINIDO
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	47%	DEFINIDO

Tabla 3. Evaluación Dominios Inferiores a Nivel Optimizado

Los controles relacionados en la tabla, que se encuentran en un nivel optimizado, requieren de monitoreo permanente para mantenerlos en un nivel de mejoramiento continuo.

Numeral	Dominio	2019	Nivel
A.5	Políticas de la seguridad de la información	100%	OPTIMIZADO
A.16	Gestión de incidentes de seguridad de la información	100%	OPTIMIZADO
A.8	Gestión de activos	98%	OPTIMIZADO
A.18	Cumplimiento	91%	OPTIMIZADO
A.10	Criptografía	90%	OPTIMIZADO
A.6	Organización de la seguridad de la información	82%	OPTIMIZADO

Tabla 4. Evaluación Dominios Nivel Optimizado

Teniendo en cuenta los anteriores resultados, en la vigencia 2020 se planea llevar a cabo las siguientes actividades, las cuales serán lideradas por la Oficina de Sistemas e Informática.

6 PLAN DE IMPLEMENTACION DEL SISTEMA DE GESTION DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

De acuerdo con lo estipulado en el numeral 2.1.3 del Manual de Gobierno Digital, el plan de seguridad y privacidad de la información debe establecer los detalles de cómo se realizará la implementación de la seguridad de la información en cada uno de los procesos de la entidad, estipulando directrices, tiempo y responsables para lograr un adecuado proceso de gestión, administración y evaluación.

6.1 DIRECTRICES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

- Para cada uno de los dominios se definirán actividades tendientes a dar cumplimiento al establecimiento de los controles para los dominios que se encuentra en estado Definido y gestionado, según lo expuesto en el numeral 5.2 del presente documento.
- Los dominios que se encuentra en estado optimizado, serán monitoreados para garantizar su cumplimiento y actualizados periódicamente para lograr el mejoramiento continuo.
- Las estrategias de sensibilización, con base en la caracterización de grupos focales (Usuarios, Directivos, Técnicos y Terceros), se definirán en el Plan de Sensibilización en seguridad y privacidad de la información.
- La mitigación de los riesgos de seguridad de la información y seguridad digital hacen parte del plan de tratamiento de riesgos de seguridad y privacidad e la información.

6.2 PLAN DE IMPLEMENTACION

El plan de implementación para la dimensión de Seguridad y Privacidad de la Información comprende el siguiente cronograma:

Dominios ISO 27001	Actividades para lograr los objetivos de SGSI 2020	RESPONSABLE	FECHAS DE PROGRAMACION	
			FECHA INICO	FECHA FINAL
A.5. Políticas de la seguridad de la información	1. Se debe realizar la actualización y aprobación y divulgación del Manual de las políticas de TI, el cual incluye las políticas de seguridad de la información. 2. Solicitar la actualización del manual de sistemas integrados, el cual incluye el contexto interno y externo, los objetivos de seguridad, roles, responsabilidades y organigrama del SGSI y las resoluciones requeridas para la actualización de las responsabilidades en seguridad del equipo que conforma el SGSI.	OFICINA DE SISTEMAS E INFORMATICA	MAYO DE 2020	AGOSTO DE 2020
A.6. Organización de la seguridad de la información	1. Implementación de DMZ y VPN'S en Teletrabajo 2. Desarrollar el plan de actualización de la documentación del SGSI 3. Contratación del equipo de trabajo para mantenimiento del SGSI, Oficial de Seguridad y los profesionales de apoyo 4. Realizar la actualización del plan de seguridad y privacidad de la Información	OFICINA DE SISTEMAS E INFORMATICA	ENERO DE 2020	JUNIO DE 2020
A.7. Seguridad de los recursos humanos	1. Realizar sensibilización en seguridad para el personal 2. Establecimiento de la guía ara el uso aceptable de los activos de información y la declaración de responsabilidad 3. Inclusión de los temas de seguridad en el proceso de inducción 4. Inclusión de los temas de seguridad en el proceso de ingreso de contratistas 5. Establecer los lineamientos y el procedimiento para la gestión de los equipos de cómputo, propios de terceros y alquilados	OFICINA DE SISTEMAS E INFORMATICA	ENERO DE 2020	DICIEMBRE DE 2020
A.8. Gestión de activos	1. Realizar la entrega formal de los activos a cada uno de los procesos. 2. Realizar la publicación de los instrumentos de la ley 1712 en la página web de la ESAP 3. Realizar la actualización anual del registro de activos con cada una de las áreas. 4. Apoyar a los procesos en la identificación de los riesgos de seguridad digital y la entrega para consolidación en la matriz de riesgos institucional 5. Apoyar a los procesos en la implementación de los controles para cada riesgo no aceptable 6. Definir, presentar para aprobación y publicar el plan de tratamiento de riesgos de seguridad y privacidad de la información	OFICINA DE SISTEMAS E INFORMATICA Y ENLACES DE CADA PROCESO	ENERO DE 2020	DICIEMBRE DE 2020

Dominios ISO 27001	Actividades para lograr los objetivos de SGSI 2020	RESPONSABLE	FECHAS DE PROGRAMACION	
			FECHA INICO	FECHA FINAL
A.9. Control de acceso	1. Actualizar el manual de Administración de usuarios 2. Construir los procedimientos para la gestión de perfiles 3. Realizar el levantamiento de perfiles y roles de todos los procesos para las aplicaciones y sistemas de la ESAP 4. Implementar el procedimiento de gestión de los perfiles 5. Desarrollar el proyecto de centralización de los accesos a las diferentes aplicaciones. 6. Construir el flujo de aprovisionamiento de usuarios 7. Realizar la centralización de autenticación a través del DA y realizar la integración de las aplicaciones que lo permitan. 8. Ejecutar la revisión y publicación de los procedimientos de áreas seguras	OFICINA DE SISTEMAS E INFORMATICA	MARZO DE 2020	DICIEMBRE DE 2020
A.10. Criptografía	1. Realizar el proceso de aseguramiento de los sitios que requieran autenticación a través de certificados digitales 2. Realizar el proceso para la adquisición de los certificados y firmas digitales que se requieran para la operación. 3. Seguimiento a la aplicación de controles criptográficos para la protección de la información	OFICINA DE SISTEMAS E INFORMATICA	MARZO DE 2020	DICIEMBRE DE 2020
A.11. Seguridad física y del entorno	1. Mejora de controles de acceso y protección contra amenazas en: - Datacenter y centros de cableado - Áreas con servidores, ya sean de procesamiento o dispositivos de comunicación - Áreas donde se encuentren concentrados dispositivos de información - Áreas donde se almacenen y guarden elementos de respaldo datos (CD, Discos, Cintas etc.) 2. Monitoreo de los controles de accesos biométricos 3. Cumplimiento de normas de seguridad física 4. Adecuación y mantenimiento del Centro de Datos y centro de cableado 5. Fortalecer el Mantenimiento de planta eléctrica y UPS	OFICINA DE SISTEMAS E INFORMATICA	MAYO DE 2020	DICIEMBRE DE 2020

Dominios ISO 27001	Actividades para lograr los objetivos de SGSI 2020	RESPONSABLE	FECHAS DE PROGRAMACION	
			FECHA INICO	FECHA FINAL
A.12. Seguridad de las operaciones	1. Diseñar en conjunto con el área de infraestructura el procedimiento de gestión de Capacidad 2. Diseñar en conjunto con el área de servicios le procedimiento de asignación de Equipos que incluya el software y aplicaciones base de los equipos y las políticas de seguridad 3. Implementar en la herramienta de gestión de servicios los procedimientos de gestión de cambios, la capacidad y disponibilidad de la infraestructura e incidentes 4. Diseñar los procedimientos de monitoreo de disponibilidad y seguridad 5. Realizar el monitoreo y análisis de vulnerabilidades 6. Implementar sistema para la gestión de Backups 7. Realizar la administración de herramientas de seguridad de manera centralizada como (Antivirus, WSUS, Barracuda, Firewall, IBOSS) 8. Ejecutar la separación de ambientes (físicos y lógicos) 9. Realizar la revisión de código malicioso 10. Operar el procedimiento de control de cambios	OFICINA DE SISTEMAS E INFORMATICA	MARZO DE 2020	DICIEMBRE DE 2020
A.13. Seguridad de las comunicaciones	1. Implementación de Switches de nivel 4. 2. Fortalecimiento de Sistemas de protección Firewall 3. Balanceadores de carga 4. Analizadores de tráfico en tiempo real 5. Optimizadores en el uso de anchos de banda 6. Canales redundantes de comunicaciones 7. Adquisición de un NAC 8. Ejecutar Plan de migración IPv4 a IPv6	OFICINA DE SISTEMAS E INFORMATICA	MARZO DE 2020	DICIEMBRE DE 2020
A.14. Adquisición, desarrollo y mantenimiento de sistemas	1. Actualización de políticas y principios de desarrollo seguro 2. Implementar procedimiento de desarrollo 3. Implementar controles de código fuente, gestión de requerimientos y gestión de pruebas 4. Implementar controles para la revisión de código seguro. 5. Pruebas de vulnerabilidad Ethical Hacking (OWASP)	OFICINA DE SISTEMAS E INFORMATICA	MARZO DE 2020	DICIEMBRE DE 2020

Dominios ISO 27001	Actividades para lograr los objetivos de SGSI 2020	RESPONSABLE	FECHAS DE PROGRAMACION	
			FECHA INICO	FECHA FINAL
A.15. Relaciones con los proveedores	1. Definir, publicar, aprobar y socializar una política de seguridad de la información para proveedores y terceras partes. 2. Monitoreo al cumplimiento de procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, los incidentes de seguridad de la información y la revaloración de los riesgos.	OFICINA DE SISTEMAS E INFORMATICA	MARZO DE 2020	JUNIO DE 2020
A.16. Gestión de incidentes de seguridad de la información	1. Implementar el procedimiento de Gestión de Incidentes en la herramienta correspondiente 2. Capacitaciones en el procedimiento de gestión de incidentes 3. Definir las guías de atención para los incidentes comúnmente presentados 4. Realizar la medición del procedimiento a través de los indicadores definidos 5. Definir el alcance de los incidentes cometidos para saber si obedece a un proceso disciplinario formal establecido para ocuparse de los empleados que cometen violaciones a la seguridad; 6. Se deben realizar los procesos de retroalimentación adecuados para asegurar que las personas que reportan eventos de seguridad de la información sean notificadas de los resultados después de que la cuestión haya sido tratada y cerrada.	OFICINA DE SISTEMAS E INFORMATICA	ENERO DE 2020	DICIEMBRE DE 2020
A.17. Aspectos de seguridad de la información de la gestión de	1. Actualización del Planes de Continuidad del Negocio (BCP) 2. Actualización Planes de recuperación ante desastres (DRP) 3. Revisión de Sistemas de alta disponibilidad para los procesos críticos 4. Revisión de la seguridad para la estrategia de contingencia definida	OFICINA DE SISTEMAS E INFORMATICA	JULIO DE 2020	DICIEMBRE DE 2020

Dominios ISO 27001	Actividades para lograr los objetivos de SGSI 2020	RESPONSABLE	FECHAS DE PROGRAMACION	
			FECHA INICO	FECHA FINAL
A.18. Cumplimiento	1. Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información 2. Actualización de las políticas para el cumplimiento de los requisitos y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados. 3. Aprobación de la política publicada sobre el cumplimiento de derechos de propiedad intelectual que defina el uso legal del software y de productos informáticos, esta política debe estar orientada no solo al software, sino también a documentos gráficos, libros, etc. 4. Monitoreo del cumplimiento de la instalación de software 5. Monitoreo al inventario de software instalado y se compara con el número de licencias adquiridas para asegurar que no se incumplen los derechos de propiedad intelectual. 6. Atención de las auditorias de Seguridad de la información programadas por Control Interno. 7. 8. Actualizar el plan de seguridad y privacidad de la información. 9. Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente. 10. Revisar el avance de implementación del Plan de Seguridad Digital de la ESAP 11. Aplicar el Instrumento de identificación de la línea base de seguridad administrativa y técnica suministrada por MINTIC. 12. Hacer seguimiento a los hallazgos, acciones correctivas y oportunidades de mejora de las evaluaciones de seguridad realizadas.	OFICINA DE SISTEMAS E INFORMATICA	MARZO DE 2020	DICIEMBRE DE 2020
18.1.4. Privacidad y protección de Datos Personales	1. Realizar la recolección de bases de datos personales de acuerdo a los estándares emitidos por la SIC 2. Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos 3. Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	OFICINA DE SISTEMAS E INFORMATICA / LIDERES DE PROCESO	FEBRERO DE 2020	JULIO DE 2020

7 DEFINICIONES

- **Activo**: En cuanto a la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).
- **Confidencialidad:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- **Control**: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- **Criptografía:** Arte y técnica de escribir con procedimientos o claves secretas o de un modo enigmático, de tal forma que lo escrito solamente sea inteligible para quien sepa descifrarlo.
- **Disponibilidad:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **Guía**: documento técnico que describe el conjunto de normas a seguir en los trabajos relacionados con los sistemas de información.
- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- **Norma**: Principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.
- **Política**: Es la orientación o directriz que debe ser divulgada, entendida y acatada por todos los miembros de la entidad.
- **Privacidad de datos:** La privacidad de datos, también llamada protección de datos, es el aspecto de la tecnología de la información (TI) que se ocupa de la capacidad que una organización o individuo tiene para determinar qué datos en un sistema informático pueden ser compartidos con terceros
- **Procedimiento**: Los procedimientos constituyen la descripción detallada de la manera como se implanta una política.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

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

8. RECURSOS

- La estimación y asignación de los recursos para la implementación del plan de seguridad y privacidad de la información, hacen parte del presupuesto de la Oficina de Sistemas e informática.
- Si la implementación implica la adquisición de herramientas o servicios tecnológicos bajo la responsabilidad de la Oficina de sistemas e informática, los recursos de inversión se tomarán del proyecto *"Fortalecimiento de las tecnologías de la información y la comunicación en la ESAP a nivel nacional."*

9. INDICADORES

La medición se realiza con un indicador de gestión que está orientado principalmente a aumentar el nivel de madurez de la implementación y operación del SGSI, para lo cual se utilizará el Instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las Comunicaciones.

El avance en ciclo PHVA del sistema debe aumentar en 5 puntos frente al diagnóstico actual, para lograr un avance del 75%.

10. RESPONSABLES

La Oficina de sistemas e Informática asesora a las áreas en el proceso de implementación de controles de seguridad para la protección de la información, y realiza el proceso de sensibilización en Seguridad y privacidad de la información, con el fin de crear un cultura en seguridad que

permita minimizar los riesgos a los que está expuesta la información, así mismo los líderes de las áreas cumplen con los procedimientos establecidos para la clasificación y protección de los activos de información que hacen parte de los procesos de cada una de las áreas.

La oficina de sistemas e informática hará seguimiento a la implementación del plan, con el fin, de evidenciar en el siguiente ciclo el avance de la madurez del modelo de Seguridad y privacidad de la información.

Los activos de información de la ESAP se encuentran disponibles para consulta en la página web https://www.esap.edu.co/portal/index.php/transparencia-2/ en la opción Instrumentos de gestión de Información de gestión pública.