

Documentación aplicada a la seguridad digital

Estructura de informe técnico



Estructura de informe técnico

Teniendo en cuenta la definición y características de un informe técnico, en este anexo usted podrá observar algunos ejemplos reales de informes técnicos relacionados con temas de ciberseguridad. Tenga en cuenta que la estructura, forma, cantidad de elementos y presentación visual varían según el contexto y tema del informe; tome los archivos adjuntos como ejemplo, mas no como una estructura fija que deberá implementar en sus documentos y reportes. Al revisar cada uno de los documentos o enlaces adjuntos, tenga en cuenta identificar:

- Aspectos de carácter institucional: nombres, logos, códigos, número de formato y qué incluye cada ejemplo.
- Estructura: introducción, encabezados, objetivos y listado de características, si los hay.
- Contenido: características de los activos, descripciones, etc.
- Lenguaje técnico y términos usados.

Esto le servirá como guía al momento de realizar sus propios informes técnicos:

- Caja de la vivienda popular. (2019). Informe Técnico Diagnóstico del Modelo de Seguridad y Privacidad de la Información - MSPI. Oficina de Tecnologías de la Información y las Comunicaciones.
<https://www.cajaviviendapopular.gov.co/sites/default/files/208-TIC-Mn-11%20INFORME%20TE%CC%81CNICO%20DIAGNO%CC%81STICO%20DEL%20MSPI%20V1.pdf>
- Escuela Superior de Administración Pública. (2021). Plan de privacidad y seguridad de la información 2021. Oficina de Tecnologías de la Información y las Comunicaciones.
<https://www.esap.edu.co/portal/index.php/Descargas/3037/2021/56601/plan-de-seguridad-y-privacidad-de-la-informacion-2021-v1-27-05-2021.pdf>




INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI CAJA DE LA VIVIENDA POPULAR

Oficina de Tecnologías de la Información y las Comunicaciones


Bogotá D.C., agosto de 2019

Versión 1.0

| | | | |
|---|--|--|--------------------------------|
|  <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular</p> | INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI | | Código: 208-TIC-Mn-11 |
| | | | Versión: 1 Página 1 de 11 |
| | Vigente desde: 13-08-2019 | | |

Contenido

| | |
|--|-----------|
| INTRODUCCIÓN | 2 |
| 1. DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI..... | 4 |
| 1.1 EVALUACIÓN DEL ESTADO ACTUAL | 4 |
| 1.1.1 EVALUACIÓN DE EFECTIVIDAD DE CONTROLES | 5 |
| 1.1.2 BRECHA ANEXO A ISO 27001:2013 | 6 |
| 1.1.3 AVANCE DEL CICLO PHVA (PLANEAR-HACER-VERIFICAR-ACTUAR)... | 8 |
| 1.1.4 NIVEL DE MADUREZ | 10 |
| 4. CONTROL DE CAMBIOS..... | 11 |

| | | | |
|--|--|--|--------------------------------|
|  ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular | INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI | | Código: 208-TIC-Mn-11 |
| | | | Versión: 1 Página 2 de 11 |
| | Vigente desde: 13-08-2019 | | |

INTRODUCCIÓN


La fase de diagnóstico de Seguridad y Privacidad de la información se define como la fase inicial del Modelo de Seguridad y Privacidad de la información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC) para todas aquellas entidades que pertenecen al ámbito gubernamental y permite identificar el estado actual de las entidades con respecto a los requerimientos del MSPI. Esta fase pretende alcanzar metas tales como:

- ✓ Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.
- ✓ Determinar el nivel de madurez de los controles de seguridad de la información
- ✓ Identificar el avance de la implementación del ciclo de operación al interior de la entidad
- ✓ Identificar el nivel de cumplimiento con la Normatividades vigente relacionada con protección de datos personales e identificación del uso de buenas prácticas en seguridad de la información.

Los activos de información son lo más importantes en la Entidad que deben ser gestionados para proteger y garantizar la continuidad del negocio. A través de la implantación de un Sistema de Gestión de seguridad de la Información SGSI, se garantiza la gestión y protección eficiente de la información al interior de la entidad que desea asegurar la integridad, confidencialidad y disponibilidad de la misma, siendo esto los tres pilares más importantes de la seguridad de la información.

Según la NTC/ISO-27001, la seguridad de la información preserva la integridad, confidencialidad y disponibilidad, pero para poder considerar que, si es de gran valor, la información debe poseer ciertas características tales como:

- ✓ El ser relevante
- ✓ Estar siempre actualizada
- ✓ Ser altamente confiable
- ✓ Poseer un alto nivel de calidad

| | | | |
|--|--|--|--------------------------------|
|  ALCALDIA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular | INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI | | Código: 208-TIC-Mn-11 |
| | | | Versión: 1 Página 3 de 11 |
| | Vigente desde: 13-08-2019 | | |

✓ Siempre debe ser completa


Lo anterior le permite cumplir eficientemente con el objetivo por el cual fue creada, por ello se hace necesario implementar medidas que permitan salvaguardar de la mejor manera y que al hacerlo cumpla con los tres grandes pilares de la seguridad, evitando que sea usada para fines distintos y pueda afectar de gran manera la operación en la entidad y el cumplimiento de los objetivos institucional.



Fases del Modelo de Seguridad y Privacidad de la Información. MSPI



Objetivos de la Fase Diagnostico MSPI

| | | | |
|--|--|--|--------------------------------|
|  ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular | INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI | | Código: 208-TIC-Mn-11 |
| | | | Versión: 1 Página 4 de 11 |
| | Vigente desde: 13-08-2019 | | |

1. DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

En el primer semestre del año en curso, se recolectó información mediante el diligenciamiento de la herramienta (Instrumento Evaluación-MSPI) proporcionada por el Ministerio de las TIC para determinar el estado actual de gestión de seguridad y privacidad de la información al interior de la Entidad. Para el diligenciamiento de este instrumento (MSPI), se usó como guía el “Instructivo para el Diligenciamiento de la herramienta de Diagnóstico de Seguridad y Privacidad de la Información” el cual proporcionó de manera precisa los pasos a seguir para recolectar toda la información posible y determinar si se cumplen y en qué calificación se encuentran los objetivos.


De acuerdo a esto:

- ✓ Con el diligenciamiento de la herramienta (Instrumento Evaluación MSPI), permitiendo establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de la Caja de la Vivienda Popular, según lo definido en la Política de Seguridad Informática establece como lineamiento y estándar la “Seguridad y Privacidad de la Información”.
- ✓ Se realizó levantamiento de información a nivel de procedimientos, formatos, guías y controles técnicos de acuerdo a los requisitos planteados en el instrumento.

A continuación, se desglosa de manera precisa el proceso realizado y los resultados obtenidos para cada aspecto evaluado e identificado mediante el diagnóstico de seguridad y privacidad de la información.

1.1 EVALUACIÓN DEL ESTADO ACTUAL

Para determinar el estado actual de la implementación de seguridad y privacidad de la información se empleó como herramienta de diagnóstico el Instrumento de Evaluación MSPI. En esta etapa fue necesario identificar cómo se está

| | | | |
|--|--|--|--------------------------------|
|  ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular | INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI | | Código: 208-TIC-Mn-11 |
| | | | Versión: 1 Página 5 de 11 |
| | Vigente desde: 13-08-2019 | | |

asegurando la seguridad de los activos de información al interior de la entidad, verificando la implantación o no de medidas que dan cumplimiento a los requerimientos de las normas sobre la protección de datos personales y que adicionalmente contribuya a la mitigación de riesgos en la información.


1.1.1 EVALUACIÓN DE EFECTIVIDAD DE CONTROLES

El diligenciamiento de la herramienta permitió obtener una calificación calculada para cada dominio y está totalizada a partir del valor registrado y promediado sobre la cantidad de objetivos de control que se establecen, todo esto referenciado desde las hojas nombradas como “ADMINISTRATIVAS y TÉCNICAS” dentro de la Herramienta Instrumento MSPI. El resultado obtenido para la evaluación del estado actual nos refleja los controles y su efectividad según la Normatividad NTC/ISO 27001 del 2013 y lo planteado dentro del desarrollo del modelo de seguridad y privacidad de la información que ha establecido el MinTIC para las entidades públicas de orden territorial, así como el avance del ciclo PHVA (Planear-Hacer-Verificar-Actuar). Con el diligenciamiento de la herramienta MSPI, se obtuvieron los siguientes resultados de los dominios para la EVALUACIÓN Y EFECTIVIDAD DE CONTROLES:

Evaluación de efectividad de Controles - ISO 27001:2013

| No. | Evaluación de Efectividad de controles | | | EVALUACIÓN DE EFECTIVIDAD DE CONTROL |
|---|---|---------------------|-----------------------|--------------------------------------|
| | DOMINIO | Calificación Actual | Calificación Objetivo | |
| A.5 | POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | 90 | 100 | OPTIMIZADO |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 59 | 100 | EFFECTIVO |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 83 | 100 | OPTIMIZADO |
| A.8 | GESTIÓN DE ACTIVOS | 57 | 100 | EFFECTIVO |
| A.9 | CONTROL DE ACCESO | 94 | 100 | OPTIMIZADO |
| A.10 | CRİPTOGRAFÍA | 0 | 100 | İNEXISTENTE |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 82 | 100 | OPTIMIZADO |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 48 | 100 | EFFECTIVO |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 90 | 100 | OPTIMIZADO |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 57 | 100 | EFFECTIVO |
| A.15 | RELACIONES CON LOS PROVEEDORES | 70 | 100 | GESTIONADO |
| A.16 | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 51 | 100 | EFFECTIVO |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | 70 | 100 | GESTIONADO |
| A.18 | CUMPLIMIENTO | 77,5 | 100 | GESTIONADO |
| PROMEDIO EVALUACIÓN DE CONTROLES | | 66 | 100 | GESTIONADO |

Fuente: Herramienta-Instrumento de Evaluación MSPI-Portada


| | | | |
|--|--|--|--------------------------------|
|  ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular | INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI | | Código: 208-TIC-Mn-11 |
| | | | Versión: 1 Página 6 de 11 |
| | Vigente desde: 13-08-2019 | | |

De acuerdo con el análisis y los resultados obtenidos, la calificación promediada de los controles dentro de la entidad fue de **66**, lo cual evidencia que la entidad se encuentra en un proceso inicial de implementación de medidas para la seguridad y privacidad de la información, de los responsables de la misma y los activos que la contienen, actualmente se encuentra en proceso de revisión y mejora de los controles existentes.

Sin embargo, se precisan los dominios que deben ser incluidos entre las acciones de la actual vigencia para su fortalecimiento, son el dominio; A.10 CRIPTOGRAFÍA, A.12 SEGURIDAD DE LAS OPERACIONES, A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN y A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTOS DE SISTEMAS. En estos dominios se evidencia que la calificación obtenida está muy por debajo del promedio total de la evaluación de controles, alcanzando un valor menor a la mitad del promedio.

1.1.2 BRECHA ANEXO A ISO 27001:2013

De acuerdo con la evaluación realizada y el diagnóstico obtenido, la entidad está en un proceso definido con respecto a los aspectos referentes a la implementación de medidas y controles destinados a la privacidad y seguridad de la información así mismo como la protección de los activos que la contienen. La brecha identificada mediante el desarrollo de esta evaluación se puede ver identificada en el siguiente gráfico.


| | | | |
|---|--|----------------|-----------------------|
|  <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular</p> | INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI | | Código: 208-TIC-Mn-11 |
| | Versión: 1 | Página 7 de 11 | |
| | Vigente desde: 13-08-2019 | | |

Brecha Anexo a ISO-27001:2013



Fuente: Instrumento de Evaluación MSPI – Portada

Según fechas establecidas para el desarrollo de las actividades correspondientes a la implementación del modelo de seguridad y privacidad de la información el cual se basa en aspectos del marco 27001:2013, para el año 2018 todas las entidades a nivel nacional deberían cumplir con la meta propuesta la cual está entre el 80% y el 100% de ejecución del MSPI. Como se evidencia en el gráfico anterior, la entidad sobrepasa el 50% en la implementación de sus controles, pero a la fecha debería estar por encima del 80%, para esto se han venido realizando acciones y mejoras frente a la implementación de documentos, formatos y controles al interior de la entidad, con el fin de no poner en riesgo en gran medida cada aspecto relacionado con la información y su valor.

| | | | |
|--|--|--|--------------------------------|
|  ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular | INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI | | Código: 208-TIC-Mn-11 |
| | | | Versión: 1 Página 8 de 11 |
| | Vigente desde: 13-08-2019 | | |

1.1.3 AVANCE DEL CICLO PHVA (PLANEAR-HACER-VERIFICAR-ACTUAR)

Por otra parte, el aspecto que determina la evaluación del estado actual en la entidad es el correspondiente al ciclo del modelo de operación PHVA el cual se encuentra alineado con los plazos para la implementación de las actividades que se establecieron para la Política de Gobierno Digital a través del decreto 1008 de 2018.


La figura que se muestra a continuación, (Avance Ciclo de Funcionamiento Del Modelo De Operación-PHVA), permite visualizar el avance que la Caja de la Vivienda Popular tiene a la fecha con respecto al ciclo PHVA.

Avance Ciclo de Funcionamiento Del Modelo De Operación (PHVA)

| Año | AVANCE PHVA | | |
|--------------|-------------------------|----------------------------|-------------------|
| | COMPONENTE | % de Avance Actual Entidad | % Avance Esperado |
| 2015 | Planificación | 32% | 40% |
| 2016 | Implementación | 16% | 20% |
| 2017 | Evaluación de desempeño | 16% | 20% |
| 2018 | Mejora continua | 12% | 20% |
| TOTAL | | 76% | 100% |

Fuente: Instrumento de Evaluación MSPI – Portada

La figura muestra el estado de avance (columna % de avance actual) frente a cada una de las etapas del ciclo (columna componente), es importante tener en cuenta que de acuerdo al tipo de entidad hay diferentes objetivos (columna % avance objetivo) de avance, así: (Ministerio de Tecnologías de la Información y las Comunicaciones, 2016):

| | | | |
|--|--|--|--------------------------------|
|  ALCALDIA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular | INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI | | Código: 208-TIC-Mn-11 |
| | | | Versión: 1 Página 9 de 11 |
| | Vigente desde: 13-08-2019 | | |


Fechas Límite de Cumplimiento para Entidades Públicas MSPI

| TIPO DE ENTIDAD | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 |
|----------------------------|------|------|------|------|---------------|---------------|
| De Orden Nacional | 40% | 60% | 80% | 100% | Mantener 100% | Mantener 100% |
| De Orden Territorial A | 35% | 50% | 80% | 100% | Mantener 100% | Mantener 100% |
| De Orden Territorial B y C | 10% | 30% | 50% | 65% | 80% | 100% |

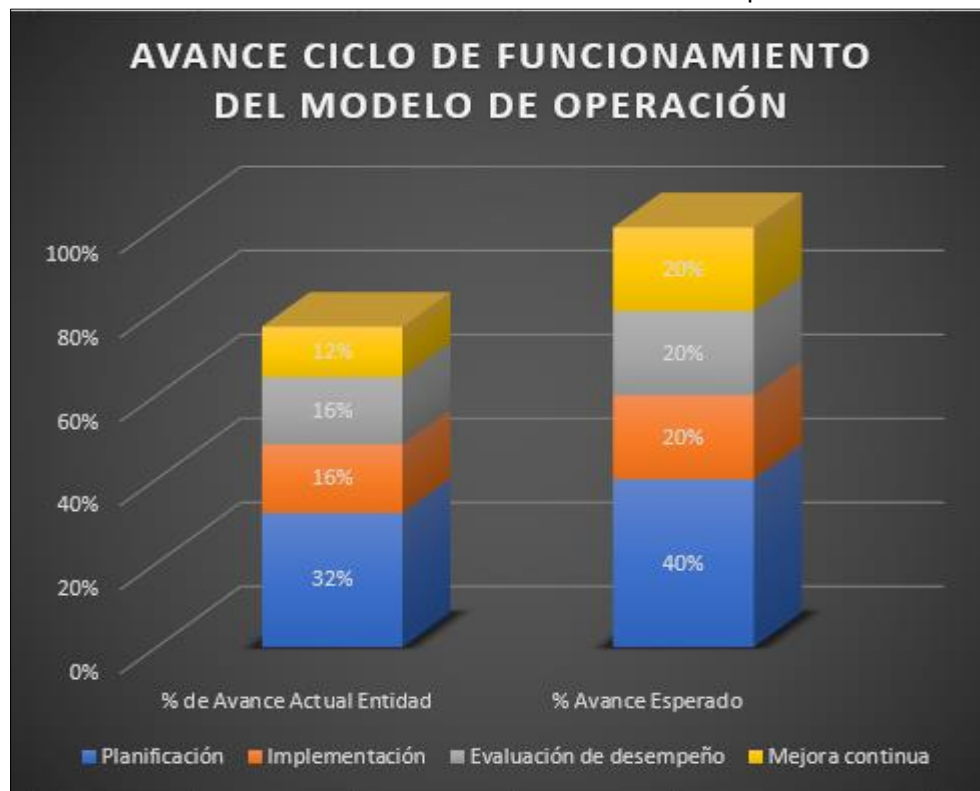
Fuente: Instructivo de Diligenciamiento Herramienta de Evaluación MSPI.

Según el análisis realizado para la figura (Avance Ciclo de Funcionamiento Del Modelo De Operación-PHVA), la entidad se encuentra en un proceso definido de cumplimiento con respecto al PHVA y todo lo referente a la implementación de la Política de Gobierno Digital mediante el MSPI. Para el ítem de planificación la entidad se encuentra en un 32% del 40% que debería presentar par el año 2018, para el ítem de Implementación la entidad se encuentra en un 16% de un total de un 20% que debería presentar para este mismo año, para el ítem de evaluación de desempeño la entidad se encuentra cumpliendo actualmente con un 16% de un total del 20% que debería presentar y para el ítem de mejora continua la entidad ha completado un 12% de un total del 20% que debería presentar para el año 2018.

Lo anterior se puede visualizar de manera precisa en la siguiente figura (Avance Ciclo de Funcionamiento del Modelo de Operación) la cual representa el avance actual en la entidad y lo esperado para el año 2018 mostrando las diferencias de cada fase del ciclo PHVA. La gráfica presenta una comparación entre el avance logrado por la entidad, el avance objetivo y el avance total posible.

| | | |
|--|---------------------------|-----------------|
|  ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular | Código: 208-TIC-Mn-11 | |
| | Versión: 1 | Página 10 de 11 |
| | Vigente desde: 13-08-2019 | |


Avance Ciclo de Funcionamiento del Modelo de Operación



FUENTE: Instrumento de Evaluación MSPI – Portada.

1.1.4 NIVEL DE MADUREZ

La madurez de la seguridad y privacidad de la información incluye los controles tanto administrativos como técnicos, la competencia técnica de los recursos informáticos, los procesos y las prácticas sostenibles, así como la eficiencia de los controles establecidos al interior de la entidad. La madurez de la seguridad se puede medir únicamente a través de la capacidad en que la entidad utiliza de forma eficaz y eficiente los recursos disponibles para el apoyo de las funciones y/o obligaciones laborales de forma que se cree un nivel de seguridad sostenible. Para ello debe establecerse una línea de partida de la madurez de la seguridad y usarse para definir los procesos en las que centra las actividades de seguridad de la información de la entidad, el nivel de madurez se identificó mediante el diligenciamiento del Instrumento de Evaluación MSPI evidenciado en la hoja

| | | | |
|---|--|--|---------------------------------|
|  ALCALDÍA MAYOR DE BOGOTÁ D.C. HABITAT Caja de Vivienda Popular | INFORME TÉCNICO DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN-MSPI | | Código: 208-TIC-Mn-11 |
| | | | Versión: 1 Página 11 de 11 |
| | Vigente desde: 13-08-2019 | | |

llamada madurez MSPI, que permitió identificar el estado actual que cuenta la entidad con respecto al Modelo de Seguridad y Privacidad de la Información y se identificaron requisitos que en su mayoría han sido previamente evaluados en las hojas Administrativas, Técnicas y PHVA.

En el resultado obtenido al diligenciar la herramienta Instrumento de Evaluación MSPI, la Caja de la Vivienda Popular evidencia que la entidad se encuentra en un nivel definido de madurez y de cumplimiento de acuerdo con la implementación del Modelo de Seguridad y Privacidad de la Información. Para alcanzar el nivel de optimizado se debe diseñar un plan de trabajo con las brechas identificadas y así actualizar, diseñar y revisar los controles que actualmente se encuentran en operación.

Descripción Niveles de Madurez y Cumplimiento

| Nivel | Descripción |
|---------------------|---|
| Inicial | En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información |
| Repetible | En este nivel se encuentran las entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI. |
| Definido | En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados. |
| Administrado | En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorías al MSPI, recolectando información para establecer la efectividad de los controles. |
| Optimizado | En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del MSPI, retroalimentando cualitativamente el modelo. |

Fuente: Instrumento de Evaluación MSPI – Madurez.

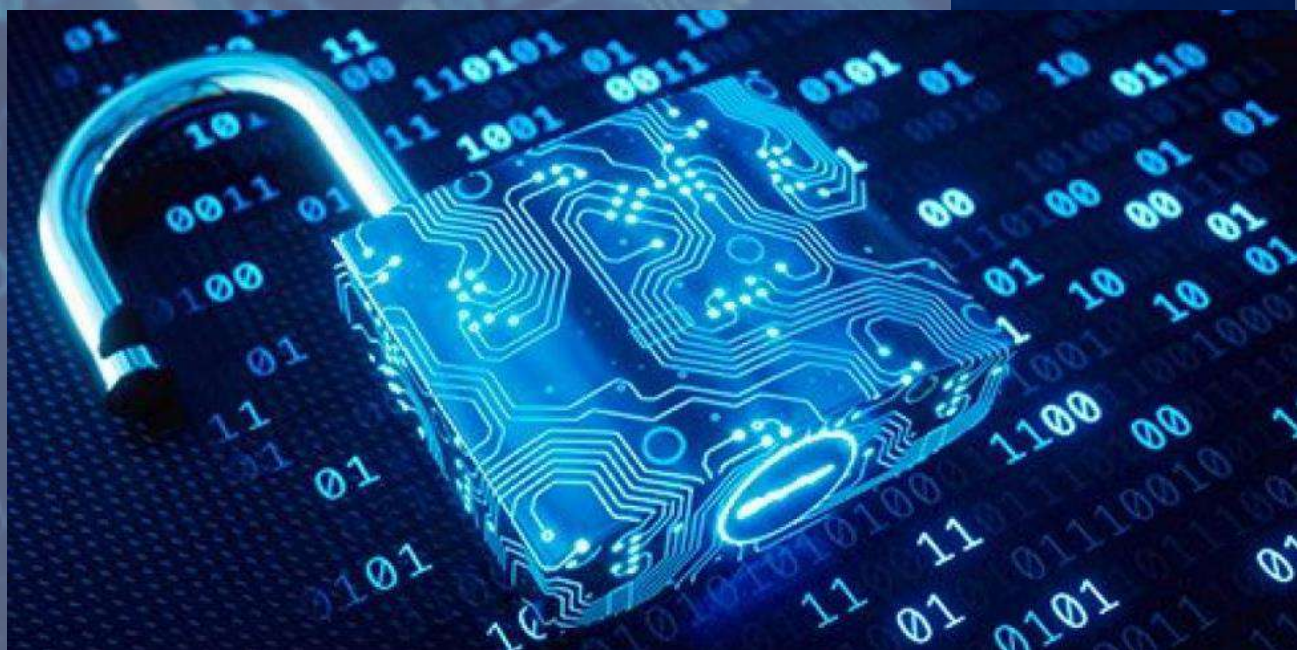
4. CONTROL DE CAMBIOS

| Versión | Fecha Aprobación (dd-mm-aaaa) | Cambios | Revisó (Nombre y Cargo) |
|---------|-------------------------------|------------------------|---|
| 1 | 13-08-2019 | Creación del documento | Andrés Orlando Briceño Díaz Jefe Oficina TIC |



El futuro
es de todos

Gobierno
de Colombia



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021

Imagen capturada de: <https://www.alpeformacion.es/wp-content/uploads/2020/02/curso-seguridad-de-la-informaci%C3%B3n-1024x768.jpg>





Contenido

| | | |
|--------|--|----|
| 1. | INTRODUCCIÓN..... | 3 |
| 2. | OBJETIVO | 3 |
| 3. | ALCANCE | 3 |
| 4. | MARCO NORMATIVO | 4 |
| 5. | RESPONSABLES | 4 |
| 6. | DEFINICIONES | 5 |
| 7. | DESARROLLO DEL PLAN | 6 |
| 7.1. | SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN – SGSI EN LA ESAP | 6 |
| 7.1.1. | POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | 6 |
| 7.1.2. | OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN: | 6 |
| 7.2. | OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI EN LA ESAP | 7 |
| 7.2.1. | COMITÉ DE SEGURIDAD DE LA INFORMACIÓN | 7 |
| 7.2.2. | DIAGNÓSTICO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | 7 |
| 7.3. | PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (ESTRATEGIA DE PLANIFICACIÓN Y CONTROL OPERACIONAL)..... | 10 |
| 7.3.1. | DIRECTRICES DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN | 11 |
| 7.3.2. | CRONOGRAMA..... | 11 |
| 8. | RECURSOS..... | 17 |
| 9. | SEGUIMIENTO Y MEDICIÓN DEL PLAN..... | 17 |
| 9.1. | INDICADORES | 18 |



CONTROL DE CAMBIOS

| Versión | Fecha | Instancia de Aprobación | Descripción |
|---------|------------|---|--|
| 01 | 27/05/2021 | Comité Institucional de Gestión y Desempeño | Formulación del Plan de Seguridad y Privacidad de la Información 2021. Aprobado en sesión del CIGD del 27 de mayo de 2021. |

ARTICULACIÓN MARCO ESTRATÉGICO

| | |
|---------------|---|
| ODS | Objetivo 16. Paz, justicia e instituciones sólidas. |
| PND 2018-2022 | Pacto por la transformación digital de Colombia |
| PES 2019-2022 | Línea 5. Transformación digital y consolidación de una comunicación estratégica del Sector Función Pública. |
| PEI 2021-2022 | Modernizar y fortalecer las capacidades institucionales de la ESAP para agregar mayor valor público a sus tareas. |
| POLÍTICA MIPG | Seguridad Digital |



1. INTRODUCCIÓN

La seguridad y privacidad 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, que en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, y 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.

Teniendo en cuenta lo anterior, se formula el presente Plan, en cumplimiento de la normativa aplicable vigente, y en particular, como parte de los planes institucionales establecidos en el Decreto 612 de 2018.

2. OBJETIVO

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 y 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 Tecnologías de la Información y Comunicaciones - OTIC.

3. ALCANCE

El presente Plan comprende la descripción y programación de las actividades a realizar por la ESAP durante la vigencia 2021, como parte de la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI), de acuerdo con el Modelo de Seguridad y Privacidad



de la Información - MSPI emitido por el Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, y la Norma ISO/IEC 27001:2013. Aplica a todas las sedes, dependencias y procesos de la ESAP.

4. MARCO NORMATIVO

| TIPO DE NORMA | NÚMERO | AÑO | Descripción - Epígrafe |
|---------------------------|--------|------|--|
| Decreto | 1078 | 2015 | Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones |
| Decreto | 1008 | 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 | 2016 | Política Nacional de Seguridad Digital |
| DOCUMENTO TÉCNICO EXTERNO | | 2016 | 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. Versión 3.0.2, julio de 2016. |
| DOCUMENTO TÉCNICO EXTERNO | | 2019 | Manual para la Implementación de la Política de Gobierno Digital Implementación de la Política de Gobierno Digital (Decreto 1008 de 2018). Versión 7, abril de 2019 |
| 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. RESPONSABLES

La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC 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 una 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 Tecnologías de la Información y las Comunicaciones – OTIC hará seguimiento a la implementación del presente Plan, con el fin, de evidenciar en el siguiente ciclo el avance de la madurez del Modelo de Seguridad y Privacidad de la Información.

6. 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).

7. DESARROLLO DEL PLAN

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.

7.1. SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN – SGSI EN LA ESAP

La Escuela Superior de Administración Pública – ESAP creó mediante la Resolución 2823 del 26 de septiembre de 2016, el Sistema de Gestión de Seguridad de la Información – SGSI, como herramienta de gestión para implementar y mantener la política de seguridad de la información. Teniendo en cuenta que la ESAP cuenta con un Sistema Integrado de Gestión – SIG, la operación del SGSI, además de enmarcarse en la normativa aplicable vigente, se integra en las orientaciones del SIG, al tiempo que atiende las disposiciones del Modelo Integrado de Planeación y Gestión MIPG en lo que le es atinente.

7.1.1. POLÍTICA INSTITUCIONAL DE SEGURIDAD 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.

7.1.2. 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.

La Política Institucional de Seguridad de la Información, se complementa con las Políticas de Seguridad y Privacidad de la Información, documentadas en el Manual de Políticas TI DC-A-GT-32.

7.2. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI EN LA ESAP

7.2.1. COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Las funciones del Comité de Seguridad de la Información en la ESAP son asumidas por el Comité Institucional de Gestión y Desempeño según lo dispuesto en el artículo 2 de la Resolución 2823 del 26 de septiembre de 2016.

7.2.2. DIAGNÓSTICO DEL SISTEMA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SGSI

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 2020, el avance general en el ciclo PHVA del Sistema de Gestión de Seguridad y Privacidad de la Información de la ESAP es del 89%, tal como se presenta a continuación:

| AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE SYP | | |
|--|----------------------------|-------------------|
| COMPONENTE | % de Avance Actual Entidad | % Avance Esperado |
| Planificación | 40,0% | 40% |
| Implementación | 16,3% | 20% |
| Evaluación de desempeño | 14,7% | 20% |
| Mejora continua | 18,0% | 20% |
| TOTAL | 89,0% | 100% |

Tabla 1. Avance PHVA del SGSI



La evolución en la implementación en los últimos 4 años es la siguiente:

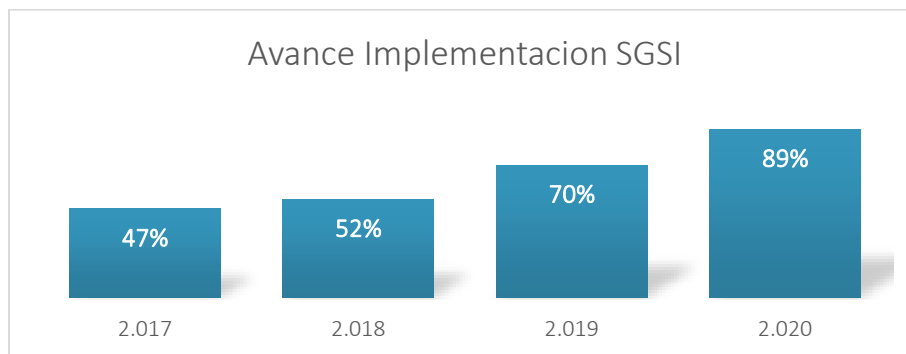


Gráfico 2. Avance implementación - PHVA del SGSI

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 | 98 | 100 | OPTIMIZADO |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 98 | 100 | OPTIMIZADO |
| A.8 | GESTIÓN DE ACTIVOS | 100 | 100 | OPTIMIZADO |
| A.9 | CONTROL DE ACCESO | 78 | 100 | GESTIONADO |
| A.10 | CRIPTOGRAFÍA | 100 | 100 | OPTIMIZADO |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 84 | 100 | OPTIMIZADO |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 85 | 100 | OPTIMIZADO |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 80 | 100 | GESTIONADO |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 81 | 100 | OPTIMIZADO |
| A.15 | RELACIONES CON LOS PROVEEDORES | 70 | 100 | GESTIONADO |
| 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 | 93,5 | 100 | OPTIMIZADO |
| PROMEDIO EVALUACIÓN DE CONTROLES | | 86,7 | 100 | OPTIMIZADO |

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:

- El dominio que se encuentra en el nivel Definido es: Aspectos de seguridad de la información de la gestión de continuidad del negocio, para lo cual se deben

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



establecer las acciones que apoyen la implementación de los controles y lo lleven a un nivel de madurez superior.

- Los demás dominios que se encuentran en el nivel Gestionado requieren la implementación de acciones de automatización de los controles y realizar el monitoreo permanente del control.
- En los dominios que están en nivel Optimizado, se deben implementar acciones de monitoreo y mantenimiento para mantenerlos en un nivel de mejoramiento continuo.

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

| NUMERAL | CLAUSULA | ESTADO ACTUAL | BRECHA | ESTADO ESPERADO | NIVEL |
|---------|---|---------------|--------|-----------------|------------|
| A.9 | CONTROL DE ACCESO | 78% | 22% | 100% | Gestionado |
| A.13 | SEGURIDAD DE LAS COMUNICACIONES | 80% | 20% | 100% | Gestionado |
| A.15 | RELACIONES CON LOS PROVEEDORES | 70% | 30% | 100% | Gestionado |
| A.17 | ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO | 47% | 53% | 100% | 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 | CLAUSULA | ESTADO ACTUAL | BRECHA | ESTADO ESPERADO | NIVEL |
|--------------------|--|---------------|--------|-----------------|------------|
| A.5 | POLITICAS DE SEGURIDAD DE LA INFORMACIÓN | 100% | 0% | 100% | Optimizado |
| A.6 | ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN | 98% | 2% | 100% | Optimizado |
| A.7 | SEGURIDAD DE LOS RECURSOS HUMANOS | 98% | 2% | 100% | Optimizado |
| A.8 | GESTIÓN DE ACTIVOS | 100% | 0% | 100% | Optimizado |
| A.10 | CRİPTOGRAFÍA | 100% | 0% | 100% | Optimizado |
| A.11 | SEGURIDAD FÍSICA Y DEL ENTORNO | 84% | 16% | 100% | Optimizado |
| A.12 | SEGURIDAD DE LAS OPERACIONES | 85% | 15% | 100% | Optimizado |
| A.14 | ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS | 81% | 19% | 100% | Optimizado |
| A.16 | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | 100% | 0% | 100% | Optimizado |
| A.18 | CUMPLIMIENTO | 93,5% | 6% | 100% | Optimizado |
| PROMEDIO CLAUSULAS | | 87% | | | Optimizado |

Tabla 4. Evaluación Dominios Nivel Optimizado

Teniendo en cuenta los anteriores resultados, en la vigencia 2021 se planea llevar a cabo el plan de implementación que se describe a continuación, las cuales serán lideradas por la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC.



7.3. PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (ESTRATEGIA DE PLANIFICACIÓN Y CONTROL OPERACIONAL)

El plan de implementación del Sistema de Seguridad y Privacidad de la Información incluye actividades tendientes a aumentar la gestión de cada uno de los dominios y llevarlos a un nivel Optimizado.

Teniendo en cuenta la brecha de los 14 dominios que se muestra en gráfica, se definieron las actividades que hacen parte de la estrategia de planificación y control operacional y que se relacionan a continuación:

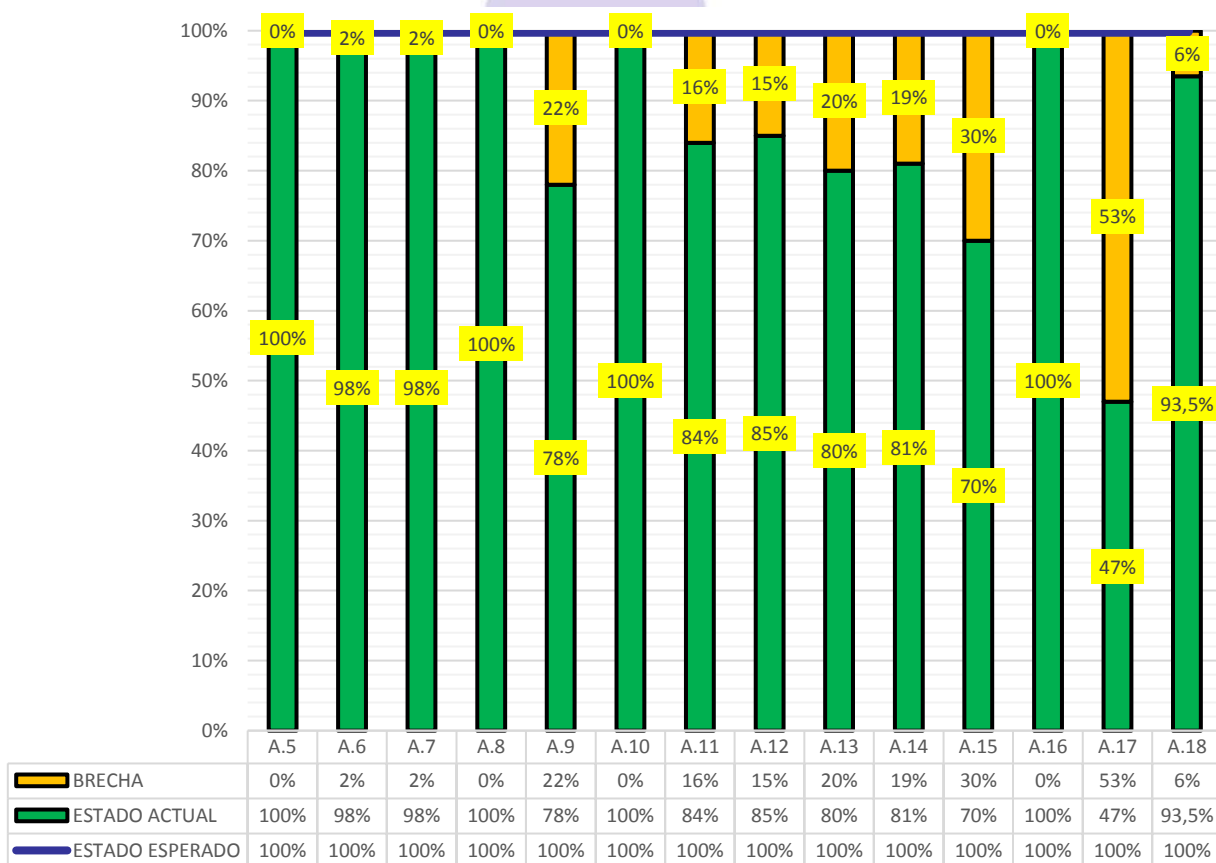


Tabla 5. Brecha Evaluación Dominios



7.3.1. 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 7.2.2. 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 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.

7.3.2. CRONOGRAMA

| Dominios ISO 27001 | Actividades para lograr los objetivos del SGSI 2021 | Responsable | Fechas de Programación | |
|---|---|---|---------------------------|-------------------|
| | | | Fecha Inicio | Fecha Final |
| A.5. Políticas de la seguridad de la información | 1. Se debe realizar la 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 Tecnologías de la Información y las Comunicaciones | MAYO DE 2021 | DICIEMBRE DE 2021 |



| Dominios ISO 27001 | Actividades para lograr los objetivos del SGSI 2021 | Responsable | Fechas de Programación | |
|--|--|--|---------------------------|----------------------|
| | | | Fecha Inicio | Fecha Final |
| A.6. Organización de la seguridad de la información | <ol style="list-style-type: none">1. Realizar la actualización de la resolución 2823 del 2016, en lo que respecta al el Sistema de Gestión de Seguridad de la Información con el fin de incluir los temas de ciberseguridad2. Realizar una correcta segregación de actividades y perfiles a través del levantamiento de roles de los usuarios para cada uno de los procesos, las aplicaciones y la aprobación por parte de los dueños de la información.3. Mantener actualizada la Matriz de contacto con autoridades.4. Mantener contacto con diferentes autoridades, grupos de seguridad nacional e internacionales con el fin de estar actualizado y en contacto con expertos en Seguridad y Ciberseguridad.5. Hacer seguimiento a la implementación de la política para la seguridad en los proyectos6. Incluir en el plan de concientización la divulgación de la guía de uso aceptable de los activos y la declaración de responsabilidad para confirmar el compromiso de la protección de los activos. | Oficina de Tecnologías de la Información y las Comunicaciones | FEBRERO DE 2021 | DICIEMBRE DE 2021 |
| A.7. Seguridad de los recursos humanos | <ol style="list-style-type: none">1. Incluir el plan de concientización en seguridad de la información dentro del proceso de inducción institucional2. Ejecutar el plan de comunicación, sensibilización y capacitación de aspectos de seguridad de la información como; Políticas, procedimientos, cultura de seguridad etc.3. Incluir en el plan de concientización la divulgación de la guía de uso aceptable de los activos y la declaración de responsabilidad para confirmar el compromiso de la protección de los activos.4. Inclusión de los temas de seguridad en el proceso de ingreso de contratistas | Oficina de Tecnologías de la Información y las Comunicaciones | MARZO DE 2021 | DICIEMBRE DE 2021 |
| A.8. Gestión de activos | <ol style="list-style-type: none">1. Realizar la publicación de los instrumentos de la ley 1712 en la página web de la ESAP2. Definir, presentar para aprobación y publicar el plan de tratamiento de riesgos de seguridad y privacidad de la información3. Apoyar a los procesos en la identificación de los riesgos de seguridad de la información y la entrega para consolidación en la matriz de riesgos institucional4. Apoyar a los procesos en la implementación de los controles para cada riesgo no aceptable5. Realizar la actualización anual del registro de activos con cada una de las áreas OCT-DIC-20216. Participar en las mesas de construcción y sensibilización del Modelo Nacional de Gestión de Riesgos de Seguridad Digital - Colcert e Infraestructuras críticas | Oficina de Tecnologías de la Información y las Comunicaciones | ENERO DE 2021 | DICIEMBRE DE 2021 |



| Dominios ISO 27001 | Actividades para lograr los objetivos del SGSI 2021 | Responsable | Fechas de Programación | |
|---|--|---|---------------------------|-------------------|
| | | | Fecha Inicio | Fecha Final |
| A.9. Control de acceso | <ol style="list-style-type: none">1. Hacer seguimiento al cumplimiento de la política de control de acceso2. Publicar y hacer seguimiento al cumplimiento de la guía de conexión y administración de Redes3. Automatizar el proceso de gestión de accesos y de aprovisionamiento para eliminar los errores que pueden surgir por los diferentes actores involucrados4. Hacer seguimiento a través del proceso monitoreo y realizar las capacitaciones pertinentes para controlar los derechos de acceso privilegiado asociados con cada sistema, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación).5. Se debe hacer seguimiento al cumplimiento de los estándares para mantener la robustez de la información de autenticación secreta personal6. Se debe hacer entrega de las responsabilidades que se tienen sobre las contraseñas a cada usuario7. realizar el levantamiento con los propietarios de los activos de la matriz de roles y perfiles de cada sistema de información para tener el control y la segregación de los derechos de acceso a los sistemas de información y aplicaciones.8. Se recomienda definir e implementar un procedimiento de gestión de perfiles y roles de accesos9. Hacer seguimiento a la implementación del ingreso seguro en todas las aplicaciones10. Hacer seguimiento al proceso de instalación del uso de programas utilitarios con la función de anular los controles de sistemas y las aplicaciones y hacer seguimiento al cumplimiento del procedimiento de control de software. | Oficina de Tecnologías de la Información y las Comunicaciones | MARZO DE 2021 | DICIEMBRE DE 2021 |
| A.10. Criptografía | <ol style="list-style-type: none">1. Monitorear 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. | Oficina de Tecnologías de la Información y las Comunicaciones | MARZO DE 2021 | DICIEMBRE DE 2021 |
| A.11. Seguridad física y del entorno | <ol style="list-style-type: none">1. Mantener y monitorear los controles físicos en aquellas áreas donde se contenga información sensible o crítica, e instalaciones de manejo de información.2. Monitorear el cumplimiento de normas de seguridad física.3. Adecuación y mantenimiento del Centro de Datos y centro de cableado.4. Fortalecer el Mantenimiento de planta eléctrica y UPS.5. Realizar la revisión periódica de los servicios de suministro (electricidad, telecomunicaciones, suministro de agua, gas, alcantarillado, ventilación y aire acondicionado).6. Mantener los centros de cableado organizado y con las debidas medidas de seguridad, manejo de llaves para proteger contra interceptación, interferencia o daño. | Oficina de Tecnologías de la Información y las Comunicaciones | MAYO DE 2021 | DICIEMBRE DE 2021 |



| Dominios ISO 27001 | Actividades para lograr los objetivos del SGSI 2021 | Responsable | Fechas de Programación | |
|--|--|--|---------------------------|----------------------|
| | | | Fecha Inicio | Fecha Final |
| A.12. Seguridad de las operaciones | <ol style="list-style-type: none">1. Implementar con el área de infraestructura el procedimiento de gestión de Capacidad2. Monitorear el cumplimiento del procedimiento de asignación de Equipos que incluya el software y aplicaciones base de los equipos y las políticas de seguridad3. Monitorear la implementación en la herramienta Service Manager de los procedimientos de gestión de cambios, la capacidad y disponibilidad de la infraestructura e incidentes.4. Implementar los procedimientos de monitoreo de disponibilidad y seguridad5. Realizar el monitoreo a la remediación de las vulnerabilidades6. Implementar sistema para la gestión de Backups7. Monitorear la administración de herramientas de seguridad como (Antivirus, WSUS, Barracuda, Firewall).8. Separar los ambientes de desarrollo, prueba y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.9. Monitorear las herramientas de código malicioso10. Se debe documentar las guías de reinicio y recuperación del sistema para uso en el caso de falla del sistema de activación del PRD.11. Aprobar y ejecutar el procedimiento de monitoreo para conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información. | Oficina de Tecnologías de la Información y las Comunicaciones | MARZO DE 2021 | DICIEMBRE DE 2021 |
| A.13. Seguridad de las comunicaciones | <ol style="list-style-type: none">1. Aprobar formalmente la guía de conexión y administración de redes e iniciar su implementación y monitoreo al cumplimiento2. Implementar y monitorear la separación de las redes para los diferentes ambientes, usuarios y sistemas de información más críticos.3. Monitorear el cumplimiento de las normas para la transferencia de información4. Ejecutar Migración IPV4-IPV6 | Oficina de Tecnologías de la Información y las Comunicaciones | MARZO DE 2021 | DICIEMBRE DE 2021 |



| Dominios ISO 27001 | Actividades para lograr los objetivos del SGSI 2021 | Responsable | Fechas de Programación | |
|--|---|--|---------------------------|----------------------|
| | | | Fecha Inicio | Fecha Final |
| A.14. Adquisición, desarrollo y mantenimiento de sistemas | <p>1. Definir la protección de los códigos fuentes de los programas que incluya: a) Definir un sitio para mantener las librerías de las fuentes de programas. b) Establecer que el personal de soporte debe tener acceso restringido a las librerías de las fuentes de los programas. c) Definir que la actualización de las librerías de fuentes de programas y elementos asociados, sólo se deben hacer una vez que se haya recibido autorización apropiada. d) Establecer que los listados de programas se deben mantener en un entorno seguro. e) Conservar un registro de auditoría de todos los accesos a las librerías de fuentes de programas. f) Mantener y copiar las bibliotecas de fuentes de programas a través de procedimientos estrictos de control de cambios. g) Se debe monitorear su aplicación y uso del procedimiento definido h) Implementar herramientas para el control de versiones</p> <p>2. Monitorear el cumplimiento de los procedimientos de desarrollo seguro y la verificación de los criterios de seguridad de los programas</p> <p>3. Incluir en los contratos para desarrollos externos el cumplimiento de las políticas y principios de desarrollo seguro de software</p> <p>4. Implementar la protección de datos de prueba para los ambientes diferentes a producción a través de técnicas de ofuscamiento o data scrambling</p> <p>5. Definir técnicas de anonimización de los datos que permitan la preservación de la privacidad de los datos</p> | Oficina de Tecnologías de la Información y las Comunicaciones | MARZO DE 2021 | DICIEMBRE DE 2021 |
| A.15. Relaciones con los proveedores | <p>1. Socializar e implementar la política de seguridad de la información para proveedores y terceras partes.</p> <p>2. Monitoreo al cumplimiento de los controles de seguridad de la información para proveedores existentes.</p> | Oficina de Tecnologías de la Información y las Comunicaciones | MARZO DE 2021 | DICIEMBRE DE 2021 |



| Dominios ISO 27001 | Actividades para lograr los objetivos del SGSI 2021 | Responsable | Fechas de Programación | |
|--|---|---|---------------------------|-------------------|
| | | | Fecha Inicio | Fecha Final |
| A.16. Gestión de incidentes de seguridad de la información | <ol style="list-style-type: none">1. Capacitar a los usuarios en el procedimiento de gestión de incidentes3. Definir las guías de atención para los incidentes comúnmente presentados4. Realizar la medición del procedimiento a través de los indicadores definidos5. 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.6. Realizar el acercamiento con el ColCert, para establecer convenios y o acuerdos de intercambio de información para fomentar la investigación, la innovación y el desarrollo en temas relacionados con la defensa y seguridad nacional en el entorno digital.7. De acuerdo con la caracterización los riesgos cibernéticos e identificar los supuestos (configura el adversario y su entorno), objetivos (establece las motivaciones del adversario), capacidades (identifica el nivel de daño que pueda causar), impactos (analiza las afectaciones claves que pueda ocasionar) y aprendizajes (revela puntos ciegos en el modelo de seguridad informática, implementar los controles para su mitigación) | Oficina de Tecnologías de la Información y las Comunicaciones | ENERO DE 2021 | DICIEMBRE DE 2021 |
| A.17. Aspectos de seguridad de la información de la gestión de continuidad de negocio | <ol style="list-style-type: none">1. Definir, diseñar, implementar y probar los planes de continuidad del negocio que contemplen los procesos críticos de la Entidad y que garanticen la continuidad de estos.2. Definir, diseñar, implementar y probar el Plan de Recuperación ante desastres que permita recuperar la tecnología que soporta los procesos críticos de la Entidad y que garanticen la continuidad de estos.3. Revisión de Sistemas de alta disponibilidad para los procesos críticos4. Revisión de la seguridad para la estrategia de contingencia definida5. Ejecutar pruebas del escenario de simulación y respuesta a ataques cibernéticos6. Implementar la guía para la identificación de infraestructura crítica cibernética7. Realizar la identificación anual de la infraestructura crítica cibernética e Informar al CCOC | Oficina de Tecnologías de la Información y las Comunicaciones | ABRIL DE 2021 | DICIEMBRE DE 2021 |



| Dominios ISO 27001 | Actividades para lograr los objetivos del SGSI 2021 | Responsable | Fechas de Programación | |
|---|---|--|---------------------------|----------------------|
| | | | Fecha Inicio | Fecha Final |
| A.18. Cumplimiento | 1. Actualizar el normograma si es necesario e incluir los cambios en temas de seguridad 2. Realizar el monitoreo al cumplimiento de los procedimientos de administración de software 3. Actualizar los activos de información de acuerdo con lo establecido en la Ley 1712 de 2014 4. Mantener actualizados los lineamientos para la protección de datos personales y monitorear su cumplimiento 5. Monitorear el cumplimiento de las guías definidas para criptografía 6. Continuar con la implementación de los planes de acción para la remediación de las no conformidades. 7. Continuar con las auditorías de control sobre SGSI 8. Ejecutar los análisis de vulnerabilidades mínimo una vez al año | Oficina de Tecnologías de la Información y las Comunicaciones | MARZO DE 2021 | DICIEMBRE DE 2021 |
| A.19 Privacidad y protección de Datos Personales | 1. Realizar la recolección de bases de datos personales de acuerdo con los estándares emitidos por la SIC 2. Registrar o actualizar las bases de datos | Oficina de Tecnologías de la Información y las Comunicaciones | FEBRERO DE 2021 | AGOSTO DE 2021 |

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 funcionamiento de la Oficina de Tecnologías de la Información y las Comunicaciones.

Si la implementación implica la adquisición de herramientas o servicios tecnológicos bajo la responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones, los recursos se tomarán del proyecto de inversión *“Fortalecimiento de las tecnologías de la información y la comunicación en la ESAP a nivel nacional.”*

9. SEGUIMIENTO Y MEDICIÓN DEL PLAN

La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC es la responsable del seguimiento a la implementación del presente Plan, como se estableció en el numeral 5. de este documento.

Toda vez que el presente Plan está integrado al Plan de Acción Institucional de la vigencia, el seguimiento se realizará cuatrimestralmente y se reportará el resultado de cada período, en el instrumento de seguimiento al Plan de Acción, en el compromiso asociado al Plan de Seguridad y Privacidad de la Información.



En atención a lo dispuesto en el Procedimiento para la Gestión de Planes Institucionales PT-S-PE-06, al final de la vigencia se reportará el Informe Anual de Implementación de Planes Institucionales en el formato RE-S-PE-37 establecido para tal fin.

9.1. INDICADORES

La medición se realiza con el indicador “Cumplimiento en la implementación del SGSI”, que está orientado principalmente a aumentar el nivel de madurez de la implementación y operación del SGSI, el cual se encuentra caracterizado en el instrumento PCI-GT-07.

Para este fin, 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 94%.

$$\frac{\text{Porcentaje de cumplimiento del SGSI}}{\text{Meta de cumplimiento programada del SGSI}}$$

Adicionalmente, la Oficina de Tecnologías de la Información y las Comunicaciones medirá el cumplimiento del presente Plan, a través del resultado del siguiente indicador, para el cual la meta es 100%:

$$\frac{\text{N° de Actividades Ejecutadas}}{\text{N° de Actividades Programadas}}$$