PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

BOGOTÁ

Enero de 2024

CONTROL DE CAMBIOS

VERSION	FECHA	DESCRIPCIÓN DEL CAMBIO
1	Enero / 2021	Elaboración del documento “Plan de Seguridad y privacidad de la Información”.
2	Enero /2022	Modificación Generalidades del Plan – Situación actual - Actividades del plan (Cronograma)
3	Enero /2023	Actualización del Plan por cambio de vigencia Modificación Generalidades del Plan – Situación actual - Actividades del plan (Cronograma)
4	Enero /2024	Actualización del Plan por cambio de vigencia Modificación Generalidades del Plan

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Computadores para Educar, reconoce la seguridad de la información como un pilar fundamental para el fortalecimiento de los procesos internos y como habilitador estratégico para la eficiencia administrativa, en este sentido la entidad se encuentra comprometida con la implementación de mecanismos que permitan preservar la confidencialidad, integridad, disponibilidad y privacidad de la información de CPE.

Computadores para Educar ha adoptado el Modelo de Seguridad de la Información 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. En el mismo sentido el Decreto 2106 de 2019, en el parágrafo del artículo 16 indica que las entidades deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones, en cumplimiento de este Decreto se emite la Resolución 500 de 2021, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

En atención a lo anterior y dando cumplimiento al Decreto 612 de 2018, se actualiza el plan estratégico de seguridad y privacidad de la Información de Computadores para Educar alineado con el Modelo de seguridad de la Información de MinTIC, la NTC/IEC ISO 27001, la Política de Gobierno Digital, el Modelo integrado de planeación y gestión (MIPG) y demás políticas y lineamientos establecidas por el Gobierno Nacional a través del Ministerio de Tecnologías de la Información (MinTIC).

2. OBJETIVO

Definir las acciones tendientes a fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables a partir de la implementación de las estrategias de seguridad digital definidas en este documento para la vigencia 2024.

3. ALCANCE

El Plan Estratégico de Seguridad y Privacidad de la Información comparte el alcance definido dentro de la Política General de Seguridad de la Información, en la que se indica que se tendrán en cuenta todos los procesos y el personal que por el desarrollo de sus funciones realicen acciones de recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información.

4. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- Decreto 612 de 2018, “Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado”, donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021. “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Computadores para Educar reconoce la información como un activo estratégico fundamental para consecución de los objetivos misionales institucionales por lo que existe el compromiso expreso de la entidad de gestionar de forma responsable la información mediante la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), garantizando relaciones de confianza con sus grupos de interés y la preservación de los principios de confidencialidad, integridad y disponibilidad de la información, todo enmarcado en el estricto cumplimiento de los requisitos normativos, legales y contractuales aplicables.

5.1 Objetivo General

Establecer los lineamientos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de Computadores para Educar, teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la entidad.

5.1.1 Objetivos específicos

Objetivo 1. Definir los principios y las reglas básicas para la gestión de la seguridad de la información

Objetivo 2. Fortalecer la cultura de seguridad de la información en los colaboradores, así como en contratistas o tercero involucrado en manejo de información de CPE.

Objetivo 3. Mejorar la confianza de las partes interesadas en el compromiso institucional de preservar adecuadamente la confidencialidad, integridad y disponibilidad de la información bajo responsabilidad de la entidad.

Objetivo 4. Implementar los controles tecnológicos necesarios para la protección de los activos de la entidad y para la mitigación de los riesgos.

6. GENERALIDADES DEL PLAN

6.1 Situación Actual

Para establecer el estado actual de la implementación de la seguridad y privacidad de la información, Computadores para Educar aplicó el “instrumento de evaluación del Modelo de Seguridad y Privacidad de la Información de la Política Nacional de Gobierno Digita-MSPI” emitido por el MINTIC, con el que se identifica el porcentaje de efectividad en la implementación de los controles de la Norma NTC/ISO 27001:2013.

Basado en el nivel de madurez alcanzado por cada uno de los dominios de la escala de evaluación y el grado de cumplimiento de controles que establece el instrumento del MSPI, se definieron las actividades dentro del Plan estratégico de seguridad que permitirán reducir la brecha hacia el nivel de cumplimiento optimizado de todos los controles.

No.	DOMINIO	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	**OPTIMIZADO**
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	**OPTIMIZADO**
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	**OPTIMIZADO**
A.8	GESTIÓN DE ACTIVOS	**OPTIMIZADO**
A.9	CONTROL DE ACCESO	**GESTIONADO**
A.10	CRIPTOGRAFÍA	**EFECTIVO**
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	**GESTIONADO**

A.12	SEGURIDAD DE LAS OPERACIONES	**GESTIONADO**
A.13	SEGURIDAD DE LAS COMUNICACIONES	**OPTIMIZADO**
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	**EFECTIVO**
A.15	RELACIONES CON LOS PROVEEDORES	**GESTIONADO**
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	**GESTIONADO**
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	**EFECTIVO**
A.18	CUMPLIMIENTO	**GESTIONADO**
EVALUACIÓN DE CONTROLES		**GESTIONADO**

Los dominios que se encuentran en nivel más alto es decir “Optimizado”, son los que han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua, según los resultados arrojados estos dominios son:

- POLITICAS DE SEGURIDAD DE LA INFORMACIÓN
- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- SEGURIDAD DE LOS RECURSOS HUMANOS
- GESTIÓN DE ACTIVOS

Estos dominios se seguirán monitoreando para garantizar su cumplimiento y actualizados periódicamente para lograr el mejoramiento continuo.

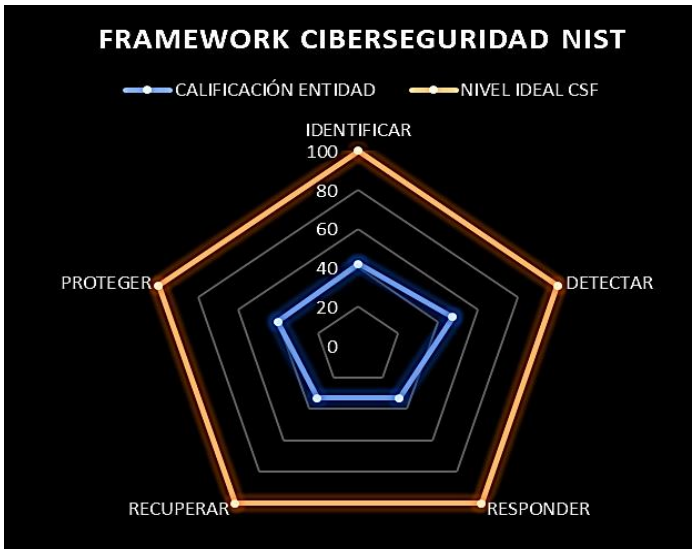
En el nivel “Gestionado”, están aquellos dominios que tienen implementados controles que se pueden monitorear constantemente en pro de tomar medidas de acción en caso de que no funcionen de manera eficiente, en este nivel de efectividad se encuentran los dominios:

- CONTROL DE ACCESO
- SEGURIDAD FÍSICA Y DEL ENTORNO
- SEGURIDAD DE LAS OPERACIONES
- SEGURIDAD DE LAS COMUNICACIONES
- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
- RELACIONES CON LOS PROVEEDORES
- GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN
- CUMPLIMIENTO

Por último, se encuentran los dominios cuyo estado está en “efectivo” es decir, se han implementado acciones y controles, pero es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada. Los Siguientes dominios en estado efectivo son los siguientes:

- CRIPTOGRAFÍA
- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
- ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

6.2 calificación frente a mejores prácticas en ciberseguridad (NIST)



El avance en aspectos de Ciberseguridad requeridos en Computadores para Educar oscila entre el 33% y el 48%, aunque la entidad tiene un avance proporcional en sus categorías.

ESTRATEGIA DE SEGURIDAD DIGITAL

COMPUTADORES PARA EDUCAR establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes.

Por tal motivo, COMPUTADORES PARA EDUCAR define los siguientes 6 ejes, que permitirán establecer el conjunto una estrategia de seguridad de la Información:

6.2 Conformación del equipo y responsabilidades

El proceso de Gestión de Tecnologías de la Información liderará la implementación del presente plan, no obstante, la seguridad de la información es un componente transversal que requiere el apoyo de todas las áreas de Computadores para educar.

Es importante resaltar que en Computadores para Educar, con fundamento en lo establecido en la norma ISO 27001: “Aspectos organizativos para la Seguridad de la Información” y las directrices fijadas en la Guía No. 4 de Seguridad y Privacidad de la Información del MinTIC, las funciones del Comité de seguridad de la información están en cabeza del Comité Institucional de Gestión y Desempeño, según lo establecido en numeral

6 de la GUÍA DE CONFORMACIÓN Y FUNCIONES DEL COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO.

7. DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

ESTRATEGIA / EJE	DESCRIPCIÓN/OBJETIVO
Activos de Información	Determinar que activos posee la entidad, de cómo deben ser utilizados, los roles y responsabilidades que tienen los colaboradores sobre los mismos y, reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele. El sistema de clasificación definido se basa en la confidencialidad como principio rector en la selección e incluye el tratamiento de la información en cuanto a la Confidencialidad, la Integridad y la Disponibilidad de cada activo. Asimismo, contempla el impacto que causaría la pérdida de alguna de estas propiedades.
Gestión de riesgos	Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.
Gestión de incidentes	Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.
Cultura de Seguridad	Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.

Implementación de controles	Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.
Continuidad del Negocio	Planificar e implementar acciones que permitan la continuidad de las principales funciones misionales de la entidad en el caso de un adverso, así como documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información.

7.1 PORTAFOLIO DE INICIATIVAS / ACTIVIDADES

No.	Actividad	Inicio	Final	Responsable
1.	**Activos De Información**			
1.1	Realizar actualización de la información del registro de activos de información por novedades en la vigencia	02/2024	02/2024	Enlace de cada proceso, Equipos SGSI
1.2	Validar, consolidar y aceptar los activos de información	02/2024	02/2024	Equipo SGSI
1.3	Consolidar y revisar los activos de información de los procesos	02/2024	03/2024	Equipo SGSI
1.4	Aprobar y publicar el versionamiento de activos de acuerdo a los lineamientos de la ley 1712 de 2014	03/2024	03/2024	Equipo de Activos, Oficina de planeación y oficina de comunicaciones
2.	**Gestión de Riesgos**			
2.1	Revisar y actualizar los lineamientos de riesgos de seguridad de la información	02/2024	06/2024	Equipo SGSI, Subdirección TI y Oficina asesora de planeación
2.2	Socializar manual de riesgos de seguridad de la información	04/2024	05/2024	Equipo SGSI
2.3	Identificar y Analizar Riesgos Seguridad de la información	04/2024	05/2024	Subdirección TI, Oficina Asesora de Planeación
2.4	Consolidar matriz de riesgos de seguridad de la Información	05/2024	06/2024	Equipo SGSI, Oficina asesora de planeación
2.5	Definir el plan de Tratamiento de riesgos	05/2024	06/2024	Equipo SGSI, Oficina asesora de planeación
2.6	Aceptar y aprobar matriz de riesgos	06/2024	07/2024	Comité de Gestión y desempeño

2.7	Realizar seguimiento, monitoreo de los riesgos identificados	01/2024	12/2024	Subdirección de TI, Oficina Asesora de Planeación
2.8	Actualizar y socializar los procedimientos de seguridad cuando se requiera	01/2024	12/2024	Equipo SGSI y Subdirección de TI
3.	**Gestión de Incidentes**			
3.1	Gestionar Incidentes de seguridad de la información	01/2024	12/2024	Equipo SGSI
3.2	Socializar formato de registro de incidentes de seguridad digital y procedimiento de reporte	04/2024	04/2024	Equipo SGSI
3.3	Ejecutar actividades de remediación	01/2024	12/2024	Subdirección de TI
3.4	Socializar novedades y boletines del CSIRT relacionados con recomendaciones de incidentes de seguridad	02/2024	12/2024	Subdirección de TI
4.	**Cultura de seguridad**			
4.1	Actualizar Plan de Cultura y Apropiación de la Seguridad de la Información	02/2024	02/2024	Subdirección de TI
4.2	Diseñar contenido para la comunicación y sensibilización de riesgos de Seguridad	02/2024	03/2024	Subdirección de TI, Oficina Asesora de comunicaciones
4.3	Ejecución del Plan de Cultura y Apropiación de la Seguridad de la Información	03/2024	12/2024	Equipo SGSI, Oficina de Talento humano
4.5	Informe de resultados del plan de cultura y apropiación de la seguridad de información	11/2024	11/2024	Equipo SGSI
5.	**Implementación de controles**			
5.1	Diligenciar la herramienta de evaluación de cumplimiento de los controles del Anexo A de la norma ISO 27001:2013 del MinTIC,	01/2024	02/2024	Equipo SGSI
5.2	Actualizar la declaración de aplicabilidad de controles de acuerdo a la norma ISO 27001:2022	03/2024	05/2024	Equipo SGSI
5.3	Actualizar la matriz de requisitos legales referentes a seguridad de la información	03/2024	05/2024	Equipo SGSI, Oficina Jurídica
5.4	Identificar acciones de mejoramiento para fortalecer la implementación y cumplimiento de los controles de seguridad y Ciberseguridad	02/2024	02/2024	Equipo SGSI
5.5	Implementación y afinamiento de las herramientas de seguridad – Controles de Ciberseguridad	01/2024	08/2024	Subdirección de TI
5.6	Participar y apoyar la ejecución de la auditoria internas y externas de seguridad de la Información	11/2024	12/2024	Subdirección de TI
5.7	Realizar actividades para atención de observaciones o recomendaciones	01/2024	12/2024	Subdirección de TI

	producto de las auditorías internas o externas			
6.	**Continuidad de TI**			
6.1	Realizar Mantenimiento preventivo de la plataforma tecnológica	5/2024	08/2024	Subdirección de TI
6.2	Realizar seguimiento a ANS de Conectividad	01/2024	12/2024	Subdirección de TI
6.3	Gestionar riesgos asociados a la continuidad	02/2024	12/2024	Subdirección de TI

8. SEGUIMIENTO Y CONTROL

El seguimiento y monitoreo a la ejecución de las actividades del Plan de Seguridad de la Información, se realizará trimestralmente en cabeza del líder del proceso de Gestión de Tecnologías de la Información, de igual forma se rendirá un reporte periódico del avance de la ejecución al Comité de Gestión y despeño.

Una vez finalice la ejecución de actividades del plan, se realizará la medición del nivel de madurez de la implementación del Modelo de seguridad y privacidad de la información (MSPI) a través del instrumento de identificación de la línea base de seguridad administrativa y técnica suministrada por MINTIC; de acuerdo con los resultados de los indicadores, el proceso de Gestión de Tecnologías de la Información, se encargará de actualizar el plan de seguridad, adicionando actividades que propicien la mejora continua y sostenibilidad del MSPI

9. NORMATIVIDAD ASOCIADA

- Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.
- CONPES 3995 Política Nacional de Confianza y Seguridad Digital.
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.
- Ley 1955 de 2019 “Por la cual se expide el Plan Nacional de Desarrollo 2018-2022 “Pacto por Colombia, pacto por la Equidad”.
- Decreto 1499 de 2017, el cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.

- Decreto 1083 de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, ("11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital).
- Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital del Departamento Administrativo para la Función Pública (DAFP) año 2018.
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 728 de 2017. Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
- Decreto 1499 de 2017. Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.