



PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

BOGOTÁ

Enero de 2022

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)

Tabla de Contenido

1. INTRODUCCIÓN..... 1

2. OBJETIVO 1

3. ALCANCE 1

4. GENERALIDADES DEL PLAN 2

4.1 Situación Actual..... 2

4.2 Conformación del equipo y responsabilidades 4

5. ACTIVIDADES DEL PLAN 4

6. SEGUIMIENTO Y CONTROL 6

7. NORMATIVIDAD ASOCIADA 7

1. INTRODUCCIÓN

Computadores para Educación, 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 Educación 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.

El presente documento establece las actividades del habilitador transversal “Seguridad de la Información” en el marco de la implementación del MSPI, el presente plan se encuentra alineado con la NTC/IEC ISO 27001:2013, la Política de Gobierno Digital, el Modelo integrado de planeación y gestión (MIPG) adoptado por CPE 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 seguridad y privacidad de la información en el marco de la implementación del Modelo de Seguridad de la Información, alineadas con la Norma ISO 27001:2013, la política de Gobierno Digital y de acuerdo con el alcance establecido por Computadores para Educación.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información de Computadores para Educación contempla actividades que impactan todos los niveles y dependencias en las que por el desarrollo de sus funciones se realizan acciones de recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información.

4. GENERALIDADES DEL PLAN

4.1 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 MSPI” suministrado por MINTIC, con el que se identifica de forma específica los controles implementados y faltantes y así tener insumos fundamentales para establecer la línea base para esta vigencia.

Para poder realizar el Plan de Seguridad y Privacidad de la Información es indispensable que se tenga en cuenta los niveles de madurez alcanzados por cada uno de los dominios, la escala de evaluación que establece el instrumento del MSPI es la siguiente:

Descripción
No Aplica
Inexistente
Inicial
Repetible
Efectivo
Gestionado
Optimizado

A continuación se observa el resultado de la revisión de los avances en Computadores para Educar de la implementación de los controles definidos por la Norma ISO 27001:2013, Anexo A, en cada uno de los siguientes dominios:

No.	DOMINIO	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	GESTIONADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	OPTIMIZADO
A.9	CONTROL DE ACCESO	GESTIONADO
A.10	CRIPTOGRAFÍA	EFFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	OPTIMIZADO
A.12	SEGURIDAD DE LAS OPERACIONES	EFFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	OPTIMIZADO

A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	GESTIONADO
A.15	RELACIONES CON LOS PROVEEDORES	OPTIMIZADO
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	EFFECTIVO
A.18	CUMPLIMIENTO	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:

- SEGURIDAD DE LOS RECURSOS HUMANOS
- GESTIÓN DE ACTIVOS
- SEGURIDAD FÍSICA Y DEL ENTORNO
- SEGURIDAD DE LAS COMUNICACIONES
- RELACIONES CON LOS PROVEEDORES

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

El presente plan prioriza aquellas actividades que impacten a los dominios cuya evaluación de madurez haya arrojado un estado de “Gestionado” y “efectivo”.

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:

- POLITICAS DE SEGURIDAD DE LA INFORMACIÓN
- ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN
- CONTROL DE ACCESO
- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS
- 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 Siguietes dominios en estado efectivo son los siguientes:

- CRIPTOGRAFÍA
- SEGURIDAD DE LAS OPERACIONES
- ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

Es de anotar que el presente plan es complementario a otras estrategias implementadas por CPE en el habilitador transversal de seguridad de la información, como son: el plan de cultura de seguridad de la información, el plan de continuidad de operación y el plan de recuperación de desastres de las operaciones de TI.

4.2 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.

5. ACTIVIDADES DEL PLAN

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

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2022				
Eje	Marco Legal	Actividades	programación	
			Fecha Inicio	Fecha Final
Gestión de la Documentación del Sistema de gestión de seguridad de la información	Ley 1581/2012 Decreto 1078/2015, Política de gobierno Digital Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y	Documento de autoevaluación de la Entidad en la Implementación de Seguridad y Privacidad de la Información	ene-22	ene-22
		Actualizar el manual de Políticas específicas de seguridad de la información (seguridad de teletrabajo, seguridad de recursos humanos - Control de acceso- A6)	ene-22	dic-22

**PLAN DE SEGURIDAD Y PRIACIDAD
DE LA INFORMACIÓN**

	herramientas que permitan la adecuada gestión de riesgos de seguridad digital	Apoyar el ajuste de la documentación de la gestión de proyectos institucionales para integrar los riesgos de seguridad de la información - A6	abr-22	abr-22
		Validación con contratación de cláusulas de transferencia de información y propiedad intelectual	abr-22	may-22
		Actualizar el normograma con normatividad de seguridad de la información que le aplique a la entidad	mar-22	abr-22
		Revisar y Actualizar documentos de SGSI de acuerdo a Norma ISO 27001 y el MSPI	feb-22	nov-22
		Apoyar diseño de instrumentos para control documental del SGSI	mar-22	jun-22
Gestión de Riesgos	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. CONPES 3995 Política Nacional de Confianza y Seguridad Digital	Actualización de riesgos de seguridad Digital	jun-22	dic-22
		Revisión y seguimiento a los controles y tratamientos de riesgos de seguridad Digital	ene-22	dic-22
		Identificar oportunidades de mejora en la gestión de riesgos residuales	ene-22	dic-22
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información	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.	Actualizar el plan de cambio y cultura de seguridad de la información	mar-22	mar-22
		Realizar inducción y reinducción en seguridad de la información a empleados y contratistas	may-22	jul-22
		Elaborar contenidos de sensibilización y divulgación de los componentes del SGSI	abr-22	abr-22
		Realizar sesiones de sensibilización sobre seguridad de la información y ciberseguridad	may-22	ago-22
		Enviar boletines de sensibilización de riesgos y tips de seguridad de la información	ene-22	dic-22
		Participar en las estrategias de acompañamiento y/o capacitaciones del Mintic para temas relacionados con seguridad de la información	mar-22	dic-22

Ciberseguridad y gestión de incidentes	Documento CONPES 3854 Política Nacional de Ciberseguridad	Participar en Workshop Ciberseguridad Azure (Equipo de TI) para fortalecimiento de capacidades	feb-22	ago-22
		Administrar y realizar reportes de las soluciones adquiridas de protección perimetral y de ciberseguridad	mar-22	dic-22
		Actualizar el procedimiento de gestión de incidentes para incluir la actividad de la documentación de las lecciones aprendidas	may-22	may-22
		Monitorear vulnerabilidades Informáticas desde paneles de administración de las diferentes plataformas tecnológicas	ene-22	dic-22
		Realizar un ejercicio de simulación de ataque Cibernético	sep-22	oct-22
		Coordinar una acción proactiva y una reactiva para el manejo de incidentes de seguridad de la información con CSIRT Gobierno	ago-22	ago-22
Plan de Continuidad de la Operación	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.	Actualizar el plan de continuidad del negocio y DRP	may-22	jun-22
		elaborar propuesta de plan de pruebas de continuidad	jul-22	jul-22
		Ejecutar actividades priorizadas en el plan de pruebas	sep-22	nov-22
Protección de datos personales	Ley 1581 de 2012, por la cual se dictaron disposiciones generales para la protección de datos personales	Apoyar la consolidación de la información para reporte de Bases de datos de CPE para SIC	feb-22	mar-22
		Realizar registro de las bases de Datos de Computadores para Educar ante SIC	abr-22	abr-22

6. 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
 EN CASO DE REPRODUCCIÓN, SE CONSIDERA COMO COPIA NO CONTROLADA

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

7. 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.