PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

BOGOTÁ

Enero de 2021

CONTROL DE CAMBIOS

VERSION	FECHA	DESCRIPCIÓN DEL CAMBIO
1	Enero / 2021	Elaboración del documento "Plan de Seguridad y privacidad de la Información".

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.

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 Educar.

3. ALCANCE

El Plan de Seguridad y Privacidad de la Información de Computadores para Educar 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

Conocer el estado actual de la entidad en el componente de Seguridad de la Información, es de vital importancia para establecer una priorización adecuada de actividades que incrementen el nivel de madurez del MSPI.

Computadores para Educar a través del instrumento de identificación de la línea base de seguridad administrativa y técnica suministrada por MINTIC, se realizó 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 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	OPTIMIZADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	GESTIONADO
A.9	CONTROL DE ACCESO	GESTIONADO
A.10	CRIPTOGRAFÍA	EFECTIVO
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	GESTIONADO
A.12	SEGURIDAD DE LAS OPERACIONES	EFECTIVO
A.13	SEGURIDAD DE LAS COMUNICACIONES	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	EFECTIVO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	GESTIONADO
A.18	CUMPLIMIENTO	GESTIONADO

Como se puede observar los dominios que se encuentran en nivel optimizado, es decir, los que han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua son: ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN y SEGURIDAD DE LOS RECURSOS HUMANOS. Por otro lado, se observan los dominios en nivel gestionado, que son aquellos dominios que se monitorean 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 de POLITICAS DE SEGURIDAD DE LA INFORMACIÓN, GESTIÓN DE ACTIVOS CONTROL DE ACCESO, SEGURIDAD FÍSICA Y DEL ENTORNO, SEGURIDAD DE LAS COMUNICACIONES, ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO y CUMPLIMIENTO.

Por último, los dominios de CRIPTOGRAFÍA, SEGURIDAD DE LAS OPERACIONES, ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS, RELACIONES CON LOS PROVEEDORES y GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN, se encuentran en un estado efectivo, es decir que estos dominios, aunque los controles son efectivos y se aplican casi siempre, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.

Considerando el resultado anterior se definirán actividades que impacten en el cumplimiento de los controles para los dominios que se encuentra en estado efectivo y gestionado. Para aquellos dominios que se encuentra en estado optimizado, se seguirán monitoreando para garantizar su cumplimiento y actualizados periódicamente para lograr el mejoramiento continuo. 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 DE LA INFORMACIÓN 2021

Eje	Marco Legal	Actividades	Fechas Programación Tareas	
			Fecha Inicio	Fecha Final
Gestión de Riesgos	Ley 1581/2012 Decreto 1078/2015, Politica de gobierno	Enviar Boletines mensuales para la sensibilización y prevención de riesgos de Seguridad Digital a los colaboradores de CPE	ene-21	dic-21
		Realizar la Identificación, Análisis y Evaluación de Riesgos Seguridad Digital	ene-21	dic-21

	Digital Plan Nacional de desarrollo Art. 147. 2. Aplicación y aprovechamiento de estándares, modelos, normas y herramientas que permitan la adecuada gestión de riesgos de seguridad digital	Actualizar Matriz de riesgos de seguridad Digital	mar-21	abr-21
		Realizar monitoreo a los planes de tratamiento de riesgos	ene-21	dic-21
		Identificar riesgos residuales	mar-21	abr-21
		Identificar oportunidades de mejora en la gestión de riesgos residuales	mar-21	abr-21
		Administrar y realizar reportes de las soluciones adquiridas de protección perimetral y de ciberseguridad	ene-21	dic-21
		Documentar controles de desarrollo seguro de sistemas de Información	jul-21	ago-21
Gestión de Incidentes de Seguridad 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. CONPES 3995 Política Nacional de Confianza y Seguridad Digital	Socializar y articular el Procedimiento de gestión de incidentes de seguridad con el proveedor de la mesa de servicios de TI y con los colaboradores de CPE.	mar-21	mar-21
		Gestionar eventos e incidentes de seguridad de la información	ene-21	dic-21
		Realizar informes de atención a los eventos o incidentes de seguridad de la información (En caso de que existan reportes)	ene-21	dic-21
		Monitorear vulnerabilidades Informáticas desde paneles de administración de las diferentes plataformas tecnológicas (implementación de controles de seguridad de la información de la suite de Office 365 adquirida por la entidad.)	ene-21	dic-21
		Coordinar una acción proactiva y una reactiva para el manejo de incidentes de seguridad de la información con CSIRT Gobierno	may-21	jun-21
		Realizar un ejercicio de simulación de ataque Cibernetico	sep-21	sep-21
Activos de Información	La 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 Ley 1581 de 2012, por la cual se dictaron disposiciones generales para la protección de datos personales	Validación del Instrumento de levantamiento de activos de información	jun-21	ago-21
		Realizar la Valoración y clasificación de activos de información	jun-21	ago-21
		Validar con el área jurídica de valoración y clasificación de activos	jun-21	ago-21
		Publicar en el sitio web institucional el inventario de activos de información	jun-21	ago-21
		Formalizar y socializar el procedimiento de clasificación y etiquetado de activos de información	jun-21	ago-21
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad	Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018 - Política de	Actualizar actividades del Plan de Cultura de Seguridad de la Información	feb-21	feb-21

Digital y Continuidad de la Operación	Gobierno Digital que contiene el Modelo de Seguridad y Privacidad - MSPI de MINTIC.	Implementar y evaluar el desempeño de las estrategias del Plan de cultura de Seguridad de la información	mar-21	dic-21
		Participar en los comités sectoriales de seguridad de la información	feb-21	dic-21
		Participar en las estrategias de acompañamiento y/o capacitaciones del Mintic para temas relacionados con seguridad de la información	feb-21	dic-21
		Socializar Políticas específicas de seguridad con proveedores de servicios	feb-21	dic-21
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Revisar la Matriz de verificación de Requisitos Legales de Seguridad de la Información	abr-21	abr-21
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.	Estructurar y liberar curso virtual de Continuidad de la Operación	mar-21	mar-21
		Publicar plan de continuidad y DRP	mar-21	mar-21
		Elaborar plan de pruebas de continuidad	jun-21	jul-21
SGSI	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 Documento de autoevaluación de la Entidad en la Implementación de Seguridad y Privacidad de la Información	ene-21	ene-21
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	abr-21	may-21
		Elaborar instrumentos de seguimiento de SGSI	abr-21	may-21
Protección de datos personales	Ley 1581 de 2012, por la cual se dictaron disposiciones generales para la protección de datos personales	Consolidar reporte de Bases de datos de CPE para SIC	feb-21	mar-21
		Realizar registro de las bases de Datos de Computadores para Educar ante SIC	mar-21	abr-21

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 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.