PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019

Enero 2019

INTRODUCCIÓN

Teniendo en cuenta La Política de Gobierno Digital como un componente del Modelo Integrado de Planeación y Gestión MIPG, la entidad acogiendo los lineamientos y mejores prácticas establecidas en diferente Normatividad, para la Vigencia 2019 realizará las actividades descritas en el presente plan, el cual forma parte integral del Plan de Gestión Institucional de Prosperidad Social.

OBJETIVO

Definir el plan de seguridad y privacidad de la información para el año 2019, el cual forma parte integral del Plan de Gestión Institucional de Prosperidad Social, para preservar los criterios de confidencialidad, integridad, disponibilidad, trazabilidad y privacidad de la información en Prosperidad Social.

IMPLEMENTACIÓN DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para esta etapa del proyecto se pretende de acuerdo al modelo MSPI del Ministerio de Tecnologías de Información, el MIPG del Departamento Administrativo de la Función Pública y basados en la norma ISO 27001:2013, la implementación en el proceso de "Gestión de Información – servicio EQUIDAD DIGITAL" aplicando el ciclo de vida de los procesos - PHVA Planear, Hacer, Verificar y Actuar e incluyendo los Objetivos de Control y controles establecidos en el Anexo A de la referida Norma.

Con el objetivo de continuar con las actividades iniciadas a finales del año 2018 y como parte del alcance de la Fase I en la implementación del sistema de gestión de seguridad en la Entidad, se proyecta para esta vigencia continuar con el nivel de análisis suficiente para realizar la implementación del modelo de seguridad en la Fase II, Para lo cual se realizarán las siguientes acciones:

- Levantamiento y análisis de información del proceso Gestión de Información - Equidad Digital
- Realizar al Análisis GAP de la Norma ISO 27001 con respecto al estado de la Entidad
- Identificación de los activos de información en el alcance establecido
- Aplicar la Metodología para la Valoración de Riesgos
- Identificación de las principales amenazas y riesgos.
- Realizar el análisis del resultado de la Valoración de Riesgos
  Plan de tratamiento de riesgos aprobado por los responsables de los proceso.
- Implementar Controles como pruebas de Ethical Hacking que incluyan Pruebas de Ingeniería Social y pruebas de Vulnerabilidad

- Realizar el análisis del Impacto
- Definir los criterios de identificación y aceptación de niveles de riesgo.
- Identificación y priorización de riesgos asociados a la infraestructura tecnológica y al recurso humano.
- Aprobación del Plan de Tratamiento de Riesgos
- Diagnóstico inicial para la elaboración del Plan de Continuidad del Negocio.

Para ello se ha establecido el siguiente cronograma de actividades:

SEGURIDAD DE LA INFORMACION		E	F	M	A	M	J	J	A	S	O	N	D
Diseñar y Ejecutar las actividades de la fase de planificación para el proyecto Equidad Digital	Levantamiento y análisis de información del proceso Gestión de Información - Equidad Digital												
	Análisis GAP ISO 27002												
	Realizar el inventario de activos de información												
	Identificación y valoración de riesgos												
	Plan de tratamiento de riesgos												
	Plan de acción implementación gestión de seguridad												
	actualización de la Declaración de aplicabilidad SOA												
	Elaboración de procedimientos adicionales												
	Diagnóstico Inicial para la elaboración del Plan de Continuidad del Negocio												
Implementación del SGSI	Implementación de controles de seguridad												
	Realización campaña de concientización en seguridad												

Posteriormente se priorizarán los riesgos, se consolidarán los hallazgos y se plantearán las principales acciones que deben ser realizadas por la Entidad para mitigar de una manera efectiva todo el conjunto de riesgos que pueden materializar afectación a la información sensible manejada por la entidad dentro del alcance definido del sistema. Los posibles elementos que puede contener este plan serán los siguientes:

- Riesgos y/o hallazgos de no cumplimiento que van a ser mitigados
- Selección de controles a aplicar para mitigación del riesgo. Acciones a seguir para llevar a cabo la implementación de los controles.
- Tiempos estimados de implementación

- Recursos necesarios a involucrar en la implementación de los controles
- Costos estimados de implementación

Teniendo en cuenta que ya se establecieron las políticas de seguridad de la información, se elaborarán y actualizarán los procedimientos de seguridad básicos para soportar el SGSI.

Así mismo, se elaborarán procedimientos adicionales y que tienen como objetivo definir lineamientos y flujos de actividades para la implementación de las mejores prácticas en la Entidad, los cuales son:

- Gestión de recursos humanos
- Gestión de terceros
- Control de acceso físico
- Control de acceso lógico
- Mantenimiento, baja y reutilización de equipos y medios
- Capacitación, entrenamiento y concientización en seguridad de la información
- Gestión de la capacidad
- Separación de ambientes
- Control de versiones
- Monitoreo y revisión de logs
- Control de software
- Controles criptográficos
- Control de software malicioso
- Buen uso de los activos

IMPLEMENTACION DEL PLAN DE TRATAMIENTO DE RIESGOS

Una vez definidas las acciones que deben ser llevadas a cabo para mitigar los riesgos que han sido identificados en la fase de diagnóstico y gestionando los recursos necesarios para las tareas de implementación del plan, se realizarán las acciones pertinentes.