PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIDAD DE SERVICIOS PENITENCIARIOS Y CARCELARIOS

2019

1. Introducción

A través del decreto 1008 del 14 de junio de 2018 se establecieron los lineamientos generales de la política de Gobierno Digital. En el mismo se establecen dos componentes o líneas de acción de esta política: TIC para el estado y TIC para la sociedad y establece tres habilitadores transversales que permitirán el cumplimiento de los logros establecidos en el decreto mencionado, estos habilitadores son Arquitectura de TI, Servicios ciudadanos digitales y Seguridad y privacidad.

Desde el año 2015 la entidad ha venido implementando el Sistema de Gestión de Seguridad de Información en sus procesos institucionales. Como parte de los logros alcanzados se han definido inventario de activos, riesgos de seguridad de información, planes de tratamiento para mitigar los riesgos. Así mismo se ha buscado fortalecer otros aspectos relevantes como lo son la sensibilización y formación del personal que labora en la entidad y el fortalecimiento de la seguridad informática a través de nuevos controles de la infraestructura tecnológica de la entidad.

En tal sentido se hace necesario continuar con la implementación y apropiación de lineamientos en materia de seguridad de información que permitan fortalecer los tres pilares de la seguridad de información como lo son la confidencialidad, integridad y disponibilidad de la información institucional, así como la gestión y operación asociada con el suministro de bienes y la prestación de los servicios, la infraestructura y brindar el apoyo logístico y administrativo requeridos para el adecuado funcionamiento de los servicios penitenciarios y carcelarios a cargo del Instituto Nacional Penitenciario y Carcelario – INPEC, los cuales tienen como beneficiarios a las Personas Privadas de la Libertad.

2. Objetivo general

Fortalecer la implementación del Sistema de Gestión de Seguridad de la Información con el fin de establecer controles que permitan proteger la información institucional de riesgos asociados a la confidencialidad, integridad y disponibilidad de los activos de información de la USPEC.

2.1 Objetivos Específicos

- ✓ Identificar, clasificar y valorar los activos de información que soportan los procesos institucionales con el fin de establecer su importancia para la entidad.
- ✓ Identificar, analizar, valorar los riesgos de seguridad de información con el propósito de definir las amenazas a las que se encuentran expuestos los activos de información de la entidad.
- ✓ Definir planes de tratamiento de riesgos con la intención de establecer controles que permitan mitigar los riesgos de seguridad de información.

- ✓ Socializar directrices en materia de seguridad de información con el fin de sensibilizar al personal de la USPEC frente a la aplicación de controles.

3. Alcance

El presente plan de seguridad de información aplica para los procesos incluidos en el mapa de procesos institucional de la USPEC, así como todo el personal que forma parte del mismo.

4. Plan de Seguridad y Privacidad de la Información

Este plan cuenta con una serie de actividades enmarcadas dentro del ciclo PHVA que se desarrollarán en el transcurso del 2019. Cabe mencionar que para el desarrollo de estas actividades se requiere contar con el apoyo de los líderes de cada proceso institucional y cada uno de sus delegados. A continuación se detalla cada una de las fases, actividades, fechas y responsables.

FASE PLANEAR				
PRODUCTO	**ACTIVIDAD**	**METODOLOGÍA**	**FECHA INICIO / FECHA FIN**	**RESPONSABLE**
Inventarios de activos de información actualizados. (1 por cada proceso).	Actualizar el inventario de activos de información de cada proceso.	La Oficina de Tecnología convocará a mesas de trabajo a cada uno de los líderes de proceso y delegados con el fin de apoyar a cada proceso en la actualización de su inventario de activos de información. Se deberá tomar como referencia el Manual de Clasificación de Activos.	01/05/2019 al 31/05/2019	Líder de cada proceso. Funcionario delegado por la dependencia.
	Aprobar inventarios de activos de información.	NA	04/06/2019 al 07/06/2019	Líder de cada proceso.

Manual de riesgos institucional	Actualizar manual de riesgos institucional (Contiene riesgos de gestión, riegos de corrupción y riesgos de seguridad digital) **Nota**: La oficina de Tecnología definirá los lineamientos de riesgos de seguridad de información	Se realizarán mesas de trabajo entre la OAPLA y la OTEC con el fin de definir los lineamientos para actualizar la metodología de riesgos de seguridad digital. OTEC llevará a cabo la actualización del manual en el tema referente a seguridad digital y la OAPLA en cuanto a riesgos de gestión y riesgos de corrupción. Posteriormente OAPLA revisará y aprobará los cambios realizados y solicitará a OTEC la respectiva publicación.	01/03/2019 al 12/04/2019	Oficina Asesora de Planeación Oficina de Tecnología
	Aprobar Manual de riesgos institucional		22/04/2019 al 26/04/2019	Oficina Asesora de Planeación
	Publicar Manual de riesgos institucional		26/04/2019	Oficina de Tecnología
Matrices de riesgos de seguridad de información y planes de tratamiento de riesgos – PTR actualizados. (1 por cada proceso).	Actualizar la matriz de riesgos de seguridad de información y el respectivo plan de tratamiento de riesgos.	La Oficina de Tecnología convocará a mesas de trabajo a cada uno de los líderes de proceso y delegados con el fin de apoyar a cada proceso en la actualización de sus matrices de riesgos de seguridad de información y sus respectivos planes de tratamiento. Se deberá tomar como base el Manual de riesgos institucional y las matrices vigentes de riesgos.	04/06/2019 al 31/07/2019	Líder de cada proceso. Funcionario delegado por la dependencia.

	Aprobar matriz de riesgos de seguridad de información y PTR		01/08/2019 al 09/08/2019	Líder de cada proceso.
Plan de pruebas de vulnerabilidad y ethical hacking	Contratar las pruebas de vulnerabilidad y ethical hacking.	A través de la contratación de un servicio se ejecutarán todas las actividades concernientes para determinar y mitigar las vulnerabilidades de la plataforma tecnológica.	01/07/2019 al 30/08/2019	Oficina de Tecnología Dirección de Gestión Contractual
	Definir plan de pruebas de vulnerabilidad y ethical hacking		01/09/2019 al 25/09/2019	Contratista
Plan de comunicación, sensibilización y capacitación en seguridad de información.	Definir plan de comunicación, sensibilización y capacitación en seguridad de información.	Se realizarán mesas de trabajo entre las áreas involucradas con el fin de definir el plan de comunicación, sensibilización y capacitación en seguridad de información.	18/02/2019 al 29/03/2019	Grupo Talento Humano Prensa (Dirección General) Oficina de Tecnología
	Aprobar el plan de comunicación, sensibilización y capacitación en seguridad de información.	El Grupo de Talento Humano y la Oficina de Tecnología gestionará ante el Comité Institucional de Gestión y Desempeño la aprobación de este plan.	01/04/2019 al 05/04/2019	Comité Institucional de Gestión y Desempeño

FASE HACER				
PRODUCTO	**ACTIVIDAD**	**METODOLOGÍA**	**FECHA INICIO / FECHA FIN**	**RESPONSABLE**

Seguimiento periódico a los PTR .	Realizar seguimiento a la ejecución de los planes de tratamiento de riesgos de seguridad de información. (PTR actuales - 2018)	Inicialmente se realizará seguimiento a los planes de tratamiento de riesgos de seguridad definidos en el 2018. Una vez se cuente con la actualización de los PTR se deberá realizar de igual forma el respectivo seguimiento para determinar la ejecución frente a las acciones propuestas. La periodicidad de este seguimiento dependerá de la definición que se realice en la metodología de riesgos institucional.	02/01/2019 al 30/05/2019	Oficina de Tecnología
	Realizar seguimiento a la ejecución de los planes de tratamiento de riesgos de seguridad de información. (PTR actualizados - 2019)		01/09/2019 al 31/12/2019	
Informe con el resultado de las pruebas de vulnerabilidad y el detalle de la ejecución	Ejecutar el plan de pruebas de vulnerabilidad y ethical hacking	El contratista deberá ejecutar las pruebas de vulnerabilidad y hacking ético de acuerdo al plan propuesto con el acompañamiento del personal de seguridad de la entidad.	01/10/2019 al 31/10/2019	Contratista
Documento con el plan para mitigar los riesgos producto de las vulnerabilidades.	Definir el plan para mitigar los riesgos producto de las vulnerabilidades detectadas.	Una vez se ejecuten las pruebas de vulnerabilidad, el contratista deberá evaluar un plan para llevar a cabo la mitigación de las mismas.	01/11/2019 al 05/11/2019	Contratista

Seguimiento al plan para mitigar riesgos de vulnerabilidades tecnológicas.	Ejecutar plan para mitigar los riesgos de vulnerabilidades tecnológicas.	Teniendo en cuenta el plan de mitigación para vulnerabilidades tecnológicas establecidas, la OTEC llevará a cabo la ejecución de acciones requeridas con el apoyo del contratista.	06/11/2019 al 31/12/2019	Contratista
Seguimiento al plan de comunicación, sensibilización y capacitación.	Ejecutar el plan de comunicación, sensibilización y capacitación.	Se llevarán a cabo las acciones definidas en el plan de comunicación, sensibilización y capacitación.	01/05/2019 al 31/13/2019	Grupo Talento Humano

FASE VERIFICAR				
PRODUCTO	**ACTIVIDAD**	**METODOLOGÍA**	**FECHA INICIO / FECHA FIN**	**RESPONSABLE**
Informe del estado general del SGSI.	Elaborar el informe del estado general del SGSI.	De acuerdo a la información reportada por cada uno de los procesos institucionales se elaborará este informe como insumo para las tomas de decisiones en materia de seguridad de información.	01/11/2019 al 20/11/2019	Oficina de Tecnología
	Aprobar informe del estado general del SGSI.	Se realizará presentación a la Dirección General del informe del estado general del SGSI.	21/11/2019 al 30/11/2019	Dirección General

Informe con el resultado del retest de las pruebas de vulnerabilidad y ethical hacking.	Realizar retest a los activos evaluados en las pruebas de vulnerabilidad y Ethical Hacking	Después de ejecutar el plan para el cierre de las vulnerabilidades tecnológicas se deberá realizar nuevamente una prueba a las mismas IP´s con el propósito de determinar si realmente se cerraron.	10/12/2019 al 31/12/2019	Contratista
Plan de Auditoria. Informe con el resultado de la auditoria.	Definir el plan de auditoria en seguridad de información.	La Oficina de Control Interno coordinará la auditoria al SGSI y se ejecutará teniendo en cuenta las directrices de la entidad, con el apoyo de los funcionarios que se encuentran formados como auditores internos.	01/11/2019 al 30/11/2019	Control Interno Auditores Internos
	Realizar auditoria al Sistema de Gestión de Seguridad de Información.			
	Realizar el informe de auditoría al Sistema de Gestión de Seguridad de Información.			

FASE ACTUAR				
PRODUCTO	**ACTIVIDAD**	**METODOLOGÍA**	**FECHA INICIO / FECHA FIN**	**RESPONSABLE**
Plan de mejoramiento.	Definir plan de mejoramiento para el cierre de hallazgos	De acuerdo a las no conformidades cada proceso responsable definirá las acciones necesarias para eliminar la causa raíz.	01/12/2019 al 15/12/2019	Líder de cada proceso.

Elaborado:
Mayra Alexandra Agudelo Carvajal
Profesional Especializado – Oficina de Tecnología

Revisado:
Oscar Javier Suárez Ramos
Jefe Oficina de Tecnología