Plan

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
GTE-PL-02-V2

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
31-01-2020

Tabla de Contenido

1. PROPÓSITO

Definir y adoptar el Plan de Seguridad y Privacidad de la Información de la Unidad Nacional de Protección, revisado y aprobado por la Dirección General.

2. OBJETIVO

Establecer las actividades definidas en el Modelo de Seguridad y Privacidad de la Información MSPI, alineadas con la NTC/IEC ISO 27001:2013, la Política de Seguridad Digital y Continuidad del servicio, en el Mapa de Procesos de la Unidad Nacional de Protección – UNP.

3. ALCANCE

La implementación del Modelo de Seguridad y Privacidad de la Información – MPSI, implica a todos los niveles de la Unidad Nacional de Protección – UNP, incluyendo funcionarios, contratistas, proveedores, operadores y personas o terceros que en razón del cumplimiento de sus funciones y las de la UNP compartan, utilicen, recolecten, procesen, intercambien o consulten información institucional, así como a los Entes de Control, Entidades relacionadas que accedan, interna o externamente a cualquier activo de información de la Entidad, independientemente de su ubicación geográfica.

Igualmente, aplica a toda la información creada, procesada o utilizada sin importar el medio, formato o presentación o lugar en el cual se encuentre.

4. DEFINICIONES

Control: Medida que modifica y mitiga el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Riesgo de seguridad de la información: posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Activos de información: Los activos de información son datos o información propietaria en medios electrónicos, impreso o entre otros medios, considerados sensitivos o críticos para los objetivos de la entidad.

Incidente de seguridad de la información: Un incidente de seguridad de la Información está indicado por un único evento o una serie de eventos de Seguridad de la Información indeseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones de la entidad y de amenazar la seguridad de la información".

Vulnerabilidad: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

5. RESPONSABILIDADES

Las responsabilidades del Modelo de Seguridad y Privacidad de la Información – MPSI de la Unidad Nacional de Protección – UNP están definidas en la Política de Seguridad y Privacidad de la Información de la Entidad mediante la resolución 1847 de 2018 en el artículo 3º - Roles y responsabilidades del MSPI.

6. CONTENIDO

6.1 Estrategias

La Unidad Nacional de Protección – UNP, a través de la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, enmarcado en el Sistema de Gestión de Seguridad de la información - SGSI, tiene como objeto proteger, preservar y administrar la confidencialidad, integridad y disponibilidad de la información, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales reduciendo la probabilidad de ocurrencia de incidentes y dando cumplimiento a los requisitos legales y reglamentarios, orientados a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad de la Información, propendiendo así por el acceso, uso efectivo y apropiación masiva de las TIC.

Para lograr el cumplimiento del Plan se definen las siguientes estrategias:

1. Gestionar los riesgos de seguridad y privacidad de la información, de manera integral.
2. Mitigar los impactos y reducir la ocurrencia de posibles incidentes de Seguridad y Privacidad de la Información, de forma efectiva, eficaz y eficiente.
3. Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad de la información de la UNP.
4. Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
5. Generar conciencia para el cambio organizacional requerido para la apropiación eficaz de la Seguridad y Privacidad de la Información como eje transversal en la UNP.
6. Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información y protección de información personal.

6.2 Proyectos

A continuación, los proyectos propuestos para dar cumplimiento a la aplicación del MSPI, los cuales se deberán analizar de acuerdo con las directrices, capacidades, aprobaciones y apoyo directivo para su ejecución:

1. Apoyo a la gestión documental para el levantamiento de activos de información y fortalecimiento de instrumentos archivísticos.
2. Contrato para el desarrollo de pruebas de penetración (pen test) para análisis de vulnerabilidades.
3. Implementación del sistema de gestión de seguridad de la información.
4. Fortalecimiento, uso y apropiación de herramientas de control y restricción para la seguridad de la información.

   Microsoft (MFA, Encriptación de comunicaciones, encriptación de archivos, parámetros de auditoría, control de acceso, etc.)

   Symantec (Protección de correo, malware, DLP, etc.)

6.3 Acciones

Las acciones abajo listadas son la requeridas para dar cumplimiento a los objetivos propuestos del plan de seguridad y privacidad de la información de acuerdo con el estado actual de la Entidad, definiendo metas, productos, responsables y cronograma de ejecución:

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Activos de Información	Definir lineamientos para el levantamiento de activos de información.	Elaboración metodología e instrumento de levantamiento de activos de información	Gestión documental	Trimestre I 2020	
	Levantamiento Activos de Información	Socializar la guía de activos de Información.	Gestión documental	Trimestre I 2020	
		Realizar el levantamiento y actualización de los activos de información partiendo de las TRD.	Gestión Documental, Enlace MIPG-SIG.	Trimestre I 2020	
		Actualización del inventario de activos de información cuando se requiera.	Gestión Documental, Enlace MIPG-SIG	II Trimestre 2020	IV Trimestre 2020
	Publicación de información de acuerdo con la Ley 1712	Validar los activos de información por proceso.	Gestión Documental, Enlace MIPG-SIG	I Trimestre 2020	IV Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
		Consolidar los activos de información de cada proceso en el instrumento de activos de Información.	Gestión Documental, Enlace MIPG-SIG.	I Trimestre 2020	IV Trimestre 2020
		Publicar los instrumentos de activos de información consolidado en el link de transparencia.	Gestión Documental, Enlace MIPG-SIG	I Trimestre 2020	IV Trimestre 2020
	Valoración de activos de información desde la perspectiva de Seguridad de la Información -CID	Identificar y valorar los activos de información respecto a la Confidencialidad, Integridad y Disponibilidad de la información.	Responsable del proceso, OAPI, CIO, CISO	I Trimestre 2020	IV Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Reporte Datos Personales	Reportar al Oficial de Datos personales o Seguridad de la Información la información recolectada en el instrumento de activos de información, correspondiente a bases de datos.	Responsable del proceso	I Trimestre 2020	IV Trimestre 2020
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	OAPI, CIO – CISO	II Trimestre 2020	II Trimestre 2020
	Sensibilización sobre la metodología	Socialización Guía y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información, Seguridad Digital y Continuidad de la Operación	OAPI, CIO – CISO	II Trimestre 2020	II Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Ejecución de metodología de identificación de riesgos de seguridad digital	Diligenciamiento del MIR (Instrumento del Mapa Integral de Riesgos): Identificación, Análisis y Evaluación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación. Aceptación, aprobación Riesgos identificados y planes de tratamiento	OAPI, CIO – CISO, TODOS LOS PROCESOS	III Trimestre 2020	III Trimestre 2020
	Publicación	Publicación Matriz de riesgos	OAPI, CIO – CISO, TODOS LOS PROCESOS	III Trimestre 2020	III Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Seguimiento Fase de Tratamiento	Seguimiento Estado planes de tratamiento de riesgos identificados y verificación de evidencias	OAPI, CIO – CISO, TODOS LOS PROCESOS	IV Trimestre 2020	IV Trimestre 2020
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	OAPI, CIO – CISO, TODOS LOS PROCESOS	IV Trimestre 2020	IV Trimestre 2020
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	OAPI, CIO – CISO, TODOS LOS PROCESOS	IV Trimestre 2020	IV Trimestre 2020
		Actualización Guía Gestión de Riesgos Seguridad de la información, de acuerdo a los cambios solicitados.	OAPI, CIO – CISO, TODOS LOS PROCESOS	IV Trimestre 2020	IV Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Gestión de Incidentes de Seguridad de la Información	Elaboración de procedimiento de gestión de incidentes de seguridad	Elaboración del procedimiento de gestión de incidentes basados en la ISO 27035	Equipo Incidentes	I Trimestre 2020	I Trimestre 2020
	Publicar y Socializar el procedimiento actualizado de incidentes de seguridad de la información	Publicar el procedimiento de gestión de incidentes de Seguridad de la Información en el SIG	Encargado de la Gestión de Incidentes de Seguridad de la Información	I Trimestre 2020	I Trimestre 2020
		Socializar el procedimiento a los especialistas del GGTI, indicando los cambios en el procedimiento	Encargado de la Gestión de Incidentes de Seguridad de la Información	I Trimestre 2020	I Trimestre 2020
		Socializar el procedimiento a los colabores de la Entidad.	Encargado de la Gestión de Incidentes de Seguridad de la Información	I Trimestre 2020	I Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Gestionar los incidentes de Seguridad de la Información identificados	Gestionar los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento definido.	Especialistas GGTI - Gestión de la información	I Trimestre 2020	IV Trimestre 2020
	CSIRT	Socializar los boletines informativos de seguridad, Integrar con CSIRT de Gobierno	Oficial de Seguridad de la Información, Encargado de Seguridad Informática y Equipo de trabajo Interno de Seguridad de la Información de Gobierno Digital	I Trimestre 2020	IV Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Eventos/vulnerabilidades	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	Profesional de la GGTI, encargado de la Gestión de Incidentes de Seguridad de la Información.	II Trimestre 2020	IV Trimestre 2020
Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Elaborar el documento del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	I Trimestre 2020	I Trimestre 2020
	Elaborar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Ejecutar las actividades relacionadas en el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	I Trimestre 2020	IV Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Continuidad de la Operación	Ejecutar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Publicar y Socializar el Plan de Gestión de Cultura Organizacional en Apropiación del SGSI con los gestores de procesos	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	I Trimestre 2020	IV Trimestre 2020
		Implementar las estrategias del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Gestor de procesos	IV Trimestre 2020	IV Trimestre 2020
	Analizar el Plan de Cambio y Cultura de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Analizar los instrumentos de medición del Plan de Gestión de Cultura Organizacional en Apropiación del SGSI	Oficial de Seguridad de la Información, profesional del Grupo de uso y apropiación de TIC	II Trimestre 2020	II Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Matriz de verificación de Requisitos Legales de Seguridad de la Información	Creación de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Crear la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la información	I Trimestre 2020	I Trimestre 2020
	Revisión de la Matriz de verificación de Requisitos Legales de Seguridad de la Información	Evidenciar el cumplimiento de los Requisitos Legales de Seguridad de la Información	Oficina Asesora Jurídica, Oficial de Seguridad de la información	I Trimestre 2020	I Trimestre 2020
Plan de Continuidad del Negocio	Documentación del Análisis de Impacto de la Operación	Elaboración del Análisis de Impacto del Negocio	Equipo de Continuidad del Negocio (OAPI CIO – CISO - GGTI Alta Gerencia) Todos los procesos	I Trimestre 2020	I Trimestre 2020
		Aprobación y publicación del Análisis de Impacto del Negocio	Alta Gerencia	I Trimestre 2020	I Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Documentación de Valoración de Riesgos de Interrupción	Elaboración del documento Valoración de Riesgos de interrupción para el plan de continuidad de la operación	(OAPI CIO – CISO - GGTI Alta Dirección)	II Trimestre 2020	II Trimestre 2020
		Aprobación y publicación Valoración de Riesgos de interrupción	Alta Gerencia	II Trimestre 2020	II Trimestre 2020
	Documentación de Estrategias de Continuidad	Elaboración del documento Estrategias de Continuidad de la Operación	(OAPI CIO – CISO - GGTI Alta Dirección)	III Trimestre 2020	III Trimestre 2020
		Publicación Estrategias de Continuidad de la Operación	Alta Dirección	III Trimestre 2020	III Trimestre 2020
	Documentación del Plan de continuidad de la Operación	Crear Documentación del Plan de continuidad de la Operación	(OAPI CIO – CISO - GGTI Alta Dirección)	IV Trimestre 2020	IV Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
		Aprobación del Plan de continuidad de la Operación	Alta Dirección	IV Trimestre 2020	IV Trimestre 2020
Acciones correctivas y Notas de mejoras SGSI	Reporte del estado de las Acciones Correctivas y Oportunidades de Mejora	Generar acciones del estado actual de las AC y OM en SIG	Líder del SGSI	I Trimestre 2020	IV Trimestre 2020
	Generar observaciones o recomendaciones a los acompañamientos realizados a los Procesos	Hacer seguimiento a las observaciones o recomendaciones dejadas a los acompañamientos realizados a los Procesos	Líder del SGSI	I Trimestre 2020	IV Trimestre 2020
Planeación	Elaborar el Manual Políticas Específicas de Seguridad y Privacidad de la Información	Elaborar el Manual de Políticas Específicas de Seguridad y privacidad de la Información	Oficial de Seguridad de la Información	I Trimestre 2020	I Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Gobierno Digital	Adopción de estrategia de Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	CIO, Líder de Gobierno digital, GGTI, Oficial de Seguridad de la Información	I Trimestre 2020	IV Trimestre 2020
		Revisar y alinear la documentación del SGSI de la Entidad al MSPI, de acuerdo con la Normatividad vigente.	CIO, Líder de Gobierno digital, GGTI, Oficial de Seguridad de la Información	I Trimestre 2020	IV Trimestre 2020
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	CIO, Líder de Gobierno digital, GGTI, Oficial de Seguridad de la Información	I Trimestre 2020	IV Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	CIO, Líder de Gobierno digital, GGTI, Oficial de Seguridad de la Información	I Trimestre 2020	IV Trimestre 2020
	Participación en las mesas de infraestructura crítica	Cumplimiento requerimientos infraestructuras críticas del gobierno	CIO, Oficial de Seguridad de la Información	I Trimestre 2020	IV Trimestre 2020
Auditorías Internas y Externas	Participación en las auditorías internas y externas de la norma ISO 27001:2013	Participar en las auditorías internas y externas de la norma ISO 27001:2013 programadas en el SIG	Todos los procesos	III Trimestre 2020	IV Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Revisión de los controles de la norma ISO 27001:2013	Revisión de los controles de la norma ISO 27001:2013,	Aplicar la herramienta diseñada para realizar la validación del cumplimiento de la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación	Oficial de Seguridad de la Información	I Trimestre 2020	IV Trimestre 2020
Indicadores SGSI	Provisión de información a los indicadores de medición del SGSI	Formular, Implementar y actualizar los indicadores del SGSI	Líder del SG, Calidad, Oficial de Seguridad de la Información	I Trimestre 2020	II Trimestre 2020
		Reportar indicadores	Gestores de procesos	III Trimestre 2020	IV Trimestre 2020
Vulnerabilidades	Definir lineamientos para ejecutas las pruebas de vulnerabilidades y pen test	Definir los lineamientos y el alcance para la realización de pruebas de vulnerabilidades	Oficial de Seguridad, GGTI	II Trimestre 2020	II Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
	Contratar Análisis de Vulnerabilidades y Pen test	Definir estudios previos y procesos de contratación para realizar el pen test y análisis de vulnerabilidades teniendo en cuenta el alcance y mitología	Oficial De Seguridad, GGTI, Profesional de contratos	II Trimestre 2020	II Trimestre 2020
	Ejecutar las pruebas de vulnerabilidades y pen test	Ejecución de las pruebas de vulnerabilidades y pen test de acuerdo con el alcance y la metodología establecida	Pen tester	II Trimestre 2020	II Trimestre 2020
	Ejecutar plan de remediación	Ejecutar el plan de remediación sobre los sistemas y plataforma de acuerdo con los resultados del análisis de vulnerabilidades y pen test	Oficial De Seguridad, GGTI	II Trimestre 2020	IV Trimestre 2020

Actividades del Plan de Seguridad y Privacidad de la Información					
Ámbito	**Actividad**	**Tareas**	**Responsable**	**Fecha de Cumplimiento**	
Protección de datos personales	Identificación	Elaborar y emitir un memorando para la identificación y reporte de bases de datos personales de acuerdo con los estándares emitidos por la SIC	Oficial de Seguridad y Secretaría General	II Trimestre 2020	II Trimestre 2020
	Analizar las bases de datos identificadas	Revisar y realimentar la información recolectada por las áreas para el registro de las bases de datos	Oficial De seguridad y gestor de procesos	III Trimestre 2020	IV Trimestre 2020
	Registro y actualización de las bases de datos	Registrar o actualizar las bases de datos teniendo en cuenta la información suministrada por las áreas y el levantamiento de activos de información	Líder de Gobierno digital, Oficial de seguridad	IV Trimestre 2020	IV Trimestre 2020

7. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	° Creación del Plan Seguridad y Privacidad de la Información	31/01/2019	01
01	° Actualización del Plan de Seguridad y Privacidad de la Información para la vigencia 2020	31/01/2020	02

8. CRÉDITOS

FIRMAS DE ELABORACIÓN, REVISIÓN Y APROBACIÓN DEL DOCUMENTO	
Elaboró Nombre: David Yacel Espinosa Vanegas Cargo y/o Vinculación/dependencia: CISO – UNP Contratista - Grupo de Gestión de las Tecnologías de Información / Oficina Asesora de Planeación e Información	
Nombre: Mario Alexander Muriel Salamanca Cargo: Coordinador del Grupo de Gestión de las Tecnologías de Información / Oficina Asesora de Planeación e Información	
Reviso: Nombre: Samir Manuel Berrio Scaff Cargo y/o Vinculación/dependencia: Jefe de la Oficina Asesora de Planeación e Información	
Aprobó: Nombre: Pablo Elías González Monguí Director General	
FIRMA DE OFICIALIZACIÓN DEL PROCEDIMIENTO- SISTEMA DE GESTIÓN	
Oficializó: Nombre: Samir Manuel Berrio Scaff Cargo: Jefe de la Oficina Asesora de Planeación e Información	