Manual de Políticas Institucionales

SGE-MA-02-V1

Sistema de Gestión

UNIDAD NACIONAL DE PROTECCIÓN

09-03-2020

El futuro es de todos

Mininterior

Tabla de Contenido

1. OBJETIVO

Definir los lineamientos y directrices que deben seguir todas las partes interesadas de la Unidad Nacional de Protección, con el fin de desarrollar la política integrada MIPG-SIG, en relación con el Sistema de Gestión de Seguridad de la Información (SGSI).

2. ALCANCE

El presente manual es de obligatorio cumplimiento para todos los procesos de la entidad a nivel nacional; procesos misionales, estratégicos, apoyo y evaluación y control, funcionarios, colaboradores y partes interesadas y todos aquellos con acceso a información de la Unidad Nacional de Protección para alcanzar un adecuado nivel de protección de la información

3. DEFINICIONES

Activo: en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

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.

Amenaza: Es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Causa: Factores internos o externos, medios, circunstancias y agentes que generan los riesgos. Se pueden clasificar en cinco categorías: personas, materiales, instalaciones y entorno.

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (ISO/IEC 27000).

Consecuencia: Producto o efecto de un evento sobre los objetivos de los procesos, expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo. (ISO/IEC 27000).

Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, privilegios de acceso, modificación y borrado.

Dato: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. (Ley 1581 de 2012, art 3).

Evento: Posible ocurrencia de Incidente o amenaza de Seguridad de la Información.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados.

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".

Información: La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la entidad y, en consecuencia, necesita una protección adecuada. La definición dada por la ley 1712 del 2014, se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Información confidencial o crítica: Es aquella información que no se debe circular más allá de las personas que están autorizadas a conocerlas en la UNP.

Información Pública Clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos

particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Información Pública Reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

MSPI: Es el Modelo de Seguridad y Privacidad de la Información definido por el Ministerio de Tecnologías de la Información – MINTIC.

Parte interesada: (Stakeholder) Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (ISO/IEC 27000).

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Probabilidad: Hace referencia a la oportunidad de que algo suceda, esté o no definido, medido o determinado objetiva o subjetivamente, cualitativa o cuantitativamente, y descrito utilizando términos o matemáticos.

Propietario de la información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos

asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

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.

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

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

Sistema de Gestión de Seguridad de la Información SGSI: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Software: Se conoce como al equipo lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware. Los componentes lógicos incluyen, entre muchos otros, las aplicaciones informáticas, tales como el procesador de texto, que permite al usuario realizar todas las tareas concernientes a la edición de textos; el llamado software de sistema, tal como el sistema operativo, que básicamente permite al resto de los programas funcionar adecuadamente, facilitando también

la interacción entre los componentes físicos y el resto de las aplicaciones, y proporcionando una interfaz con el usuario.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

4. RESPONSABILIDADES

La Alta Dirección de la UNP es responsable de garantizar que la seguridad y privacidad de la información se comunique y gestione adecuadamente en la entidad.

La Resolución 0198 del 02 de marzo de 2020[1] establece los roles específicos relacionados con el SGSI.

Los funcionarios, contratistas, terceros y partes interesadas de la entidad tienen la responsabilidad de mantener la seguridad y privacidad de la información de acuerdo con los niveles de clasificación establecidos por la UNP.

Para mayor ilustración, en el numeral 9.1 Anexo Roles y Responsabilidades del SGSI del presente manual se detallan las responsabilidades adicionales que contribuyen a la gestión de la seguridad y privacidad de la UNP.

[1] " Por medio de la cual se adopta el Modelo Integrado de Planeación y Gestión de la UNP (MIPG-SIG), se designan responsabilidades, y se crean la COMISIÓN TRANSVERSAL y la SUBCOMISIÓN DE ENLACES como instancias de apoyo para el diseño, implementación y mantenimiento de MIPG-SIG"

5. MARCO LEGAL

ID	Número	Año	Descripción
N-1	Ley 39	1981	Sobre microfilmación y certificación de archivos.
N-2	Decreto 2620	1993	Por medio del cual se reglamenta el procedimiento para la utilización de medios tecnológicos para conservar los archivos de los comerciantes.
N-3	Acuerdo 11	1996	Por el cual se establecen criterios de conservación y organización de documentos.
N-4	Ley 527	1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.
N-5	Acuerdo 047 de 2000	2000	Por el cual se desarrolla el artículo 43 del capítulo V Acceso a los documentos de archivo", del Reglamento general de archivos sobre "Restricciones por razones de conservación".
N-6	Acuerdo 50 de 2000	2000	Por el cual se desarrolla el artículo 64 del título VII conservación de documento", del Reglamento general de archivos sobre "Prevención de deterioro de los documentos de archivo y situaciones de riesgo".
N-7	Ley 594 de 2000	2000	Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.
N- 8	Acuerdo 037	2002	Por el cual se establecen las especificaciones técnicas y los requisitos para la contratación de los servicios de depósitos, custodia, organización, reprografía y conservación de documentos de archivo en desarrollo de los artículos 13 y 14 y sus Parágrafos 1 y 3 de la Ley General de Archivo 594 de 2000.
N-10	Ley 1266	2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en base de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
N-11	Ley 1341	2009	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
N-12	Ley 1273 de 2009	2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".

ID	Número	Año	Descripción
N-13	Decreto 235	2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas (Ley 2550 de 1995).
N-14	CONPES 3670	2010	Lineamientos de Política para la continuidad de los programas de acceso y servicio universal a las Tecnologías de la Información y las Comunicaciones.
N-15	Conpes 3701	2011	Lineamientos de Política para Ciberseguridad y Ciber defensa.
N-16	Ley 1474	2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
N-17	Decreto 2693	2012	Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.
N-18	Ley 1581	2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
N-19	Decreto 2578	2012	Por el cual se reglamenta el Sistema Nacional de Archivos, se establece la Red Nacional de Archivos, se deroga el Decreto 4124 de 2004 y se dictan otras disposiciones relativas a la administración de los Archivos del Estado.
N-20	Decreto 2609	2012	Por la cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.
N-21	Decreto 0032	2013	Por la cual se crea la Comisión Nacional Digital y de Información Estatal.
N-22	Decreto 2573	2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
N-23	Ley 1712 de 2014	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.
N-24	Decreto 1066	2015	"Por medio del cual se expide el Decreto Único Reglamentario del Sector Administrativo del Interior"
N- 25	Decreto 415	2016	Definición y establecimiento del CIO en el sector publico
N- 26	CONPES 3854	2017	Política nacional de seguridad digital
N- 27	Resolución 2710	2017	Por la cual se establecen lineamientos para la adopción del protocolo IPV6
N- 28	Decreto 1413	2017	Establece lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

ID	Número	Año	Descripción
N-29	Decreto 1499	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
N-30	Decreto 1008	2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital en reemplazo de la Política de Gobierno en Línea
N- 31	Decreto 704	218	Creación de la Comisión Intersectorial para el Desarrollo de la Economía Digital
N- 32	CONPES 3920	2018	"Política nacional de explotación de datos (BIG DATA)".
N- 33	CONPES 3975	2019	"Política nacional para la transformación digital e inteligencia artificial"

6. CONDICIONES GENERALES

La seguridad de la información busca preservar la confidencialidad, integridad y disponibilidad de la información a través de la definición de un conjunto de procesos, normas y herramientas para la gestión eficaz de acceso a la información, y la implementación de mecanismos y medidas de seguridad tanto físicas como lógicas, orientadas a la prevención y detección de amenazas internas y externas que puedan afectar la seguridad de la organización y la continuidad del negocio.

La finalidad de la seguridad de la información es su protección independiente del medio en que se encuentre, ya sea impresa, medio digital, sistemas de información, almacenado en dispositivos de almacenamiento externo, oral u otros, contra las amenazas y eventos que atenten contra el acceso, uso, divulgación, interrupción y destrucción de forma no autorizada y que puedan afectar la confidencialidad, integridad y disponibilidad de la información.

Para el logro de estos objetivos, es fundamental contar con el compromiso de todos los involucrados, el respaldo del nivel directivo dentro de la entidad, siendo conscientes de los beneficios que se pueden obtener, con una cultura enfocada a la seguridad y privacidad de la información.

La Unidad Nacional de Protección, por medio su Política de seguridad y privacidad de la Información apoya la gestión de riesgos de los activos de información, la implementación consecuente de controles, el establecimiento de una cultura de seguridad de la información en todos los ámbitos y la estructuración de estrategias complementarias.

El presente manual hace parte de los documentos del Sistema de Gestión Integral que desarrollan la Política de Seguridad y Privacidad de la Información.

7. CONTENIDO

1.1. POLITICAS ESPECIFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1.1.1. Modelo de Seguridad y Privacidad de la Información - MSPI.

Adoptar el MSPI establecido por MinTIC al interior de la Unidad Nacional de Protección; el cual se fundamenta en las normas ISO22301:2012, ISO 27001:2013 e ISO 27002:2013; y establecer la Política de Seguridad y Privacidad de la Información de la entidad.

El Modelo de Seguridad y Privacidad de la Información de la Unidad Nacional de Protección, es extensible y aplicable a todos los procesos de la entidad, tanto a nivel central como regional; por lo tanto, todos los funcionarios, contratistas y partes interesadas de la entidad, deberán realizar los esfuerzos suficientes para su cumplimiento.

1.1.2.Principios de seguridad y privacidad de la información.

A partir de la confidencialidad, integridad y disponibilidad de la información, la Unidad Nacional de Protección define (19) principios de seguridad para soportar el Modelo de Seguridad y Privacidad de la Información, así:

1. La responsabilidad frente a la seguridad de la información será definida, compartida, publicada y aceptada por cada uno de los funcionarios, colaboradores y partes interesadas de la UNP que tengan acceso o hagan uso de información o servicios institucionales.
2. Mantener actualizado el inventario de activos de información, identificando su ubicación, características, importancia estratégica, normas, procesos informáticos, interrelación y la forma como apoyan la operación de la UNP.
3. Se deberán etiquetar los activos de información de acuerdo con el nivel de importancia con respecto a su confidencialidad.
4. Los propietarios de información catalogada como publica clasificada y/o pública reservada, serán los responsables de definir las medidas de protección, su confidencialidad, integridad y disponibilidad, durante y después del transporte o transmisión y realizarán verificaciones periódicas para asegurar el cumplimiento de estas.
5. Los líderes de cada proceso conocerán y evaluarán de forma permanente los riesgos existentes sobre los activos de información, así como los controles que se han implementado para mitigar los riesgos.
6. Se firmarán acuerdos de confidencialidad con los funcionarios, colaboradores y partes interesadas que por diferentes razones requieran conocer o intercambiar información clasificada y reservada. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para

cada una de las partes y se deberán firmar antes del acceso o uso de dicha información.

7. Los propietarios de la información son responsables de implementar controles de acuerdo con los niveles de autorización para el acceso, modificación, lectura, escritura, control total entre otros garantizando el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad definidos.
8. Proteger la información generada, procesada, transmitida o resguardada por todos los procesos de la UNP.
9. Resguardar la infraestructura tecnológica y demás activos, del riesgo generado por los accesos otorgados a terceros; proveedores, visitantes o usuarios de sus grupos de interés.
10. Proteger la información generada, procesada, transmitida o resguardada por todos los procesos de la UNP, con el fin de minimizar impactos financieros, operativos o legales debido al uso incorrecto o no autorizado. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
11. Proteger la información de la UNP de las amenazas originadas por parte del personal.
12. Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta los servicios esenciales y sus procesos críticos.
13. Controlar la operación de los procesos de la UNP garantizando la seguridad de los recursos físicos, tecnológicos y la red de datos.
14. Implementar controles de acceso a la información, los sistemas y los recursos de la red de datos institucional.
15. Garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

16. Garantizar el mantenimiento y la evolución del modelo de seguridad y privacidad a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información.
17. Garantizar la disponibilidad de los procesos de la UNP y la continuidad de su operación basados en el impacto que pueden generar los incidentes o eventos de seguridad.
18. Toda violación de estas políticas se deberá notificar inmediatamente al Grupo de Gestión de Tecnologías de la Información y al jefe inmediato del empleado o colaborador que notifica la violación, de modo que se pueda gestionar el incidente.
19. Se consideran Incidentes de Seguridad de Información cualquier hecho o evento que afecte la confidencialidad, integridad o disponibilidad de la Información, así como la violación a las Políticas de Seguridad de Información, incluyendo:
    - Accesos no autorizados
    - Alteración o Eliminación no autorizada de Información
    - Cambios o modificaciones en registros de bases de datos sin previa autorización.
    - Divulgación no autorizada de Información
    - Fuga, Robo o Pérdida de Información
    - Indisponibilidad de los Servicios
    - Información o actividades que atenten contra la propiedad intelectual o derechos de autor
    - Ingeniería Social
    - Ingreso de medios de almacenamiento no autorizados
    - Instalación de software ilegal o no licenciado
    - Presencia de virus, cadenas o correos maliciosos

- Préstamo de cuentas de usuario y contraseña
- Robo de información sensible.
- Robo y perdida de equipos de cómputo con información sensible.
- Uso indebido de los tipos de activos de información y los recursos informáticos de la entidad.
- Violación de cualquier ley o regulación nacional respecto al uso de sistemas de información.

20. Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

1.1.3.Sanciones por incumplimiento de la política de seguridad y privacidad de la información.

El incumplimiento, se refleja en toda conducta que no cumpla las políticas. Entre los ejemplos de incumplimiento se incluyen, sin limitarse a ellos los siguientes:

a) Los funcionarios, colaboradores y partes interesadas que sean negligentes en la aplicación de medidas de seguridad y control dentro de la organización.

b) Una acción u omisión por parte de un funcionario, contratista o parte interesada que contribuya a la violación de las normas orientadas al buen uso de la información.

c) Un funcionario, contratista o parte interesada que no reporte inmediatamente los eventos, incidentes o riesgos de seguridad de la información que sean detectados.

d) El funcionario, contratista o parte interesada que no tome las medidas correspondientes ante una queja o un incidente de seguridad.

e) El funcionario, contratista o parte interesada que realice, apoye o facilite divulgación y/o uso de información interna, clasificada o reservada de manera no autorizada.

Todos los funcionarios, contratistas o partes interesadas, serán responsables de la implementación de las políticas y procedimientos de seguridad de la información que se contemplan o son referenciados en este documento y sus complementarios.

Cualquier incumplimiento de las Políticas, procedimientos y documentos afines es considerado como falta disciplinaria por incumplimiento de las obligaciones contractuales y deberes del funcionario, que será sancionado en conformidad con lo previsto en la Ley y en el Reglamento interno de trabajo.

La Unida Nacional de Protección, podrá imponer a funcionarios, colaboradores y partes interesadas que se encuentran dentro del alcance de la presente política las sanciones previstas por reglamentaciones internas, decretos y leyes del orden nacional que apliquen respecto a los incumplimientos y el grado de estos en cuanto a seguridad y privacidad de la información se refiere.

8. DOCUMENTOS RELACIONADOS

- GTE-PL-04- Plan estratégico de tecnologías de la información – PETI
- GTE-PL-03-Plan de tratamiento de riesgos de seguridad y privacidad de la información
- GTE-PL-02-V Plan de seguridad y privacidad de la información

- Resolución 0198 del 02 de Marzo de 2020 “Por medio de la cual se adopta el Modelo Integrado de Planeación y Gestión de la UNP (MIPG-SIG), se designan responsabilidades, y se crean la COMISIÓN TRANSVERSAL y la SUBCOMISIÓN DE ENLACES como instancias de apoyo para el diseño, implementación y mantenimiento de MIPG-SIG”.
- Resolución 0199 del 02 de Marzo de 2020 “Por medio de la cual se actualiza la Plataforma Estratégica MIPG-SIG y se derogan las resoluciones 1295 del 5 de septiembre de 2018 y la Resolución 0085 del 30 de enero de 2019”.

9. ANEXOS

9.1 Anexo: SGE-FT-33 Formato Matriz de Responsabilidades Y Autoridades Roles del SGS

	FORMATO MATRIZ DE RESPONSABILIDADES Y AUTORIDADES				
	SISTEMA DE GESTIÓN				
	UNIDAD NACIONAL DE PROTECCIÓN				
Alcance	Sistema de Gestión Seguridad de la Información		**RENDICIÓN DE CUENTAS**		
Rol	**Resonsabilidad**	**Autoridad**	**¿Qué cuentas rinde?**	**¿A quién rinde cuentas?**	**¿Cada cuánto rinde cuentas?**
1. Director	Aprobar el uso de metodologías y procesos específicos para la seguridad de la información. Asignar los recursos y designar de responsabilidades para la gestión de la seguridad y privacidad de la información al interior de la Unidad Nacional de Protección.	Requerir informes de gestión y evaluación a cada componente para hacer seguimiento de la gestión del Sistema de Gestión	Información acerca del SGSI	Entes de control interno y externo	Mensualmente o la periodicidad de los comités o cuando exista el requerimiento
2. Representante de la Alta Dirección para el SGSI	Impulsar y gestionar el desarrollo de proyectos de seguridad de la información alineados a las directrices del MINTIC Dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Unidad Nacional de protección. Recomendar a la Alta Dirección (CIGD) el uso de metodologías y procesos específicos para la seguridad y privacidad de la información. Realizar la promoción y sensibilización de la seguridad y privacidad de la información en la UNP. Divulgar en la Entidad, los documentos generados al interior de la Subcomisión de gestión y seguridad de TI.	Suspender actividades que afecten el desempeño y seguridad de la entidad frente a seguridad de la información. Definir modificaciones en el presupuesto para dar respuesta a los temas críticos o prioritarios.	Desempeño del Sistema de Gestión Seguridad de la Información	Director	Cuando exista el requerimiento o mensualmente de acuerdo a los comités
3. Comité Institucional de Gestión y Desempeño:	Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información. Invitar al CIO – Oficial Líder de Tecnología, al Coordinador del Grupo de Tecnología, al CSO – Oficial de Seguridad, y al CISO – Oficial de Seguridad de la Información, a las sesiones de Comité en las cuales se traten temas seguridad y privacidad de la información. Realizar seguimiento a las estrategias y acciones para la operación de las políticas de Gobierno Digital y Seguridad Digital. Establecer la conformación de la Subcomisión de Gestión y Seguridad de TI interdisciplinaria, conformado por delegados de los diferentes procesos, el cual tendrá como objeto, asegurar que exista una dirección y apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad y privacidad de la información. Designar al CIO – Oficial Líder de Tecnología de acuerdo con lo establecido por el MINTIC o quién lo regule. Designar al CSO – Oficial de Seguridad de acuerdo con lo establecido por el MINTIC o quién lo regule. Designar al Líder de las políticas de Gobierno Digital y Seguridad Digital ; antes Líder GEL. Designar al CDO Oficial de Protección de Datos Personales establecido por la SIC. Velar por el cumplimiento de las políticas de seguridad y privacidad de la información Asignar las responsabilidades asociadas a la seguridad y privacidad de la Información.	Hacer seguimiento al avance de la implementación del Sistema de Gestión de Seguridad de la Información - SGSI.	Desempeño del Sistema de Gestión Seguridad de la Información	Director	Cuando exista el requerimiento o mensualmente de acuerdo a los comités

	FORMATO MATRIZ DE RESPONSABILIDADES Y AUTORIDADES				
	SISTEMA DE GESTIÓN				
	UNIDAD NACIONAL DE PROTECCIÓN				
Alcance	Sistema de Gestión Seguridad de la Información		**RENDICIÓN DE CUENTAS**		
Rol	**Resonsabilidad**	**Autoridad**	**¿Qué cuentas rinde?**	**¿A quién rinde cuentas?**	**¿Cada cuánto rinde cuentas?**
4.CIO Chief Información Officer Gerente de Sistemas o Director de Tecnologías de la Información	Alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, y establecer mejoras e innovaciones de soluciones y productos de tecnologías de la Información y las comunicaciones, como también de la seguridad Informática y Privacidad de la Información. Elaborar la Metodología del Plan de Recuperación de Desastres "DRP". Asesorar a los Procesos de la Entidad en el desarrollo de la Metodología del Plan de Continuidad del Negocio "BCP". Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. Promover la Gestión de los riesgos de seguridad de información.	Supervisar y hacer seguimiento a las actividades concernientes a la adecuada administración del PHVA del SGSI	Avances y oportunidades de mejora del Sistema de Gestión Seguridad de la Información	Director Representante de la Alta Dirección para el SGSI Jefe Oficina Asesora de Planeación e Información	Cuando exista el requerimiento o mensualmente de acuerdo a los comités
5. CTO Chief Technology Officer Coordinador del Grupo TIC	Proponer, formular y ejecutar planes, programas y proyectos de tecnologías de información y las comunicaciones de la UNP de acuerdo con los lineamientos y objetivos para el fortalecimiento institucional establecidos por el MINTIC. Alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, y establecer mejoras e innovaciones de soluciones y productos de tecnologías de la Información y las comunicaciones, como también de la seguridad Informática y Privacidad de la Información. Garantizar y designar los recursos y equipos de trabajo necesarios para ejecutar los planes, programas y proyectos de T.I. teniendo en cuenta el MSPI. Diseñar e implementar soluciones tecnológicas confiables y seguras, teniendo en cuenta requerimientos, capacidades, costos entre otros, como lo indican las buenas prácticas de gestión de T.I. Elaborar la Metodología del Plan de Recuperación de Desastres "DRP". Asesorar a los Procesos de la Entidad en el desarrollo de la Metodología del Plan de Continuidad del Negocio "BCP". Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. Programar ejecuciones periódicas de análisis de vulnerabilidades sobre la Infraestrcutura tecnológica y definir y aplacar los planes de remediación.	Supervisar y hacer seguimiento a las actividades concernientes a la adecuada administración del PHVA del SGSI	Avances y oportunidades de mejora del Sistema de Gestión Seguridad de la Información	Director Representante de la Alta Dirección para el SGSI Jefe Oficina Asesora de Planeación e Información CIO	Cuando exista el requerimiento o mensualmente de acuerdo a los comités

	FORMATO MATRIZ DE RESPONSABILIDADES Y AUTORIDADES				
	SISTEMA DE GESTIÓN				
	UNIDAD NACIONAL DE PROTECCIÓN				
Alcance	Sistema de Gestión Seguridad de la Información		**RENDICIÓN DE CUENTAS**		
Rol	**Resonsabilidad**	**Autoridad**	**¿Qué cuentas rinde?**	**¿A quién rinde cuentas?**	**¿Cada cuánto rinde cuentas?**
4.CIO Chief Información Officer Gerente de Sistemas o Director de Tecnologías de la Información	Alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, y establecer mejoras e innovaciones de soluciones y productos de tecnologías de la Información y las comunicaciones, como también de la seguridad Informática y Privacidad de la Información. Elaborar la Metodología del Plan de Recuperación de Desastres "DRP". Asesorar a los Procesos de la Entidad en el desarrollo de la Metodología del Plan de Continuidad del Negocio "BCP". Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. Promover la Gestión de los riesgos de seguridad de información.	Supervisar y hacer seguimiento a las actividades concernientes a la adecuada administración del PHVA del SGSI	Avances y oportunidades de mejora del Sistema de Gestión Seguridad de la Información	Director Representante de la Alta Dirección para el SGSI Jefe Oficina Asesora de Planeación e Información	Cuando exista el requerimiento o mensualmente de acuerdo a los comités
5. CTO Chief Technology Officer Coordinador del Grupo TIC	Proponer, formular y ejecutar planes, programas y proyectos de tecnologías de información y las comunicaciones de la UNP de acuerdo con los lineamientos y objetivos para el fortalecimiento institucional establecidos por el MINTIC. Alinear el gobierno de tecnologías de la información a los requerimientos tecnológicos, y establecer mejoras e innovaciones de soluciones y productos de tecnologías de la Información y las comunicaciones, como también de la seguridad Informática y Privacidad de la Información. Garantizar y designar los recursos y equipos de trabajo necesarios para ejecutar los planes, programas y proyectos de T.I. teniendo en cuenta el MSPI. Diseñar e implementar soluciones tecnológicas confiables y seguras, teniendo en cuenta requerimientos, capacidades, costos entre otros, como lo indican las buenas prácticas de gestión de T.I. Elaborar la Metodología del Plan de Recuperación de Desastres "DRP". Asesorar a los Procesos de la Entidad en el desarrollo de la Metodología del Plan de Continuidad del Negocio "BCP". Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. Programar ejecuciones periódicas de análisis de vulnerabilidades sobre la Infraestrcutura tecnológica y definir y aplacar los planes de remediación.	Supervisar y hacer seguimiento a las actividades concernientes a la adecuada administración del PHVA del SGSI	Avances y oportunidades de mejora del Sistema de Gestión Seguridad de la Información	Director Representante de la Alta Dirección para el SGSI Jefe Oficina Asesora de Planeación e Información CIO	Cuando exista el requerimiento o mensualmente de acuerdo a los comités

	FORMATO MATRIZ DE RESPONSABILIDADES Y AUTORIDADES				
	SISTEMA DE GESTIÓN				
	UNIDAD NACIONAL DE PROTECCIÓN				
Alcance	Sistema de Gestión Seguridad de la Información		**RENDICIÓN DE CUENTAS**		
Rol	**Resonsabilidad**	**Autoridad**	**¿Qué cuentas rinde?**	**¿A quién rinde cuentas?**	**¿Cada cuánto rinde cuentas?**
6. CISO (Chief Information Security Officer) Ofical de seguridad de la información	Velar por el mantenimiento de la documentación del SGSI, su custodia y protección. Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el MSPI en cuanto a la documentación de las lecciones aprendidas. Trabajar de manera integrada con el grupo o áreas asignadas. Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. Gestionar el desarrollo e implementación de políticas, normas, directrices, controles y procedimientos de seguridad de gestión de TI e información. Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. Liderar el proceso de gestión de incidentes de seguridad así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados. Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora.	Supervisar y hacer seguimiento a las actividades concernientes a la adecuada administración del PHVA del SGSI	Avances y oportunidades de mejora del Sistema de Gestión Seguridad de la Información	Director Representante de la Alta Dirección para el SGSI Jefe Oficina Asesora de Planeación e Información CIO CTO	Cuando exista el requerimiento o mensualmente de acuerdo a los comités

	FORMATO MATRIZ DE RESPONSABILIDADES Y AUTORIDADES				
	SISTEMA DE GESTIÓN				
	UNIDAD NACIONAL DE PROTECCIÓN				
Alcance	Sistema de Gestión Seguridad de la Información		**RENDICIÓN DE CUENTAS**		
Rol	**Resonsabilidad**	**Autoridad**	**¿Qué cuentas rinde?**	**¿A quién rinde cuentas?**	**¿Cada cuánto rinde cuentas?**
6. CISO (Chief Information Security Officer) Ofical de seguridad de la información	Aplicar conocimientos, habilidades, herramientas, y técnicas a las actividades propias del MSPI, de manera que cumpla las necesidades y expectativas de los interesados en el mismo. Identificar la brecha entre el estado actual de seguridad de la información y la implementación del MSPI. Generar el cronograma de la implementación del MSPI. (Planear, implementar y hacer seguimiento a las tareas, fechas, costos y plan de trabajo de los objetivos específicos del cronograma definido). Generar e implementar políticas de seguridad y privacidad de la información. Dirigir el cumplimiento transversal y normativo de la implementación del MSPI. Realizar seguimiento permanente a la ejecución de los planes de trabajo, monitoreando los riesgos de seguridad y privacidad de la información para brindar solución oportuna y escalar a la subcomisión de seguridad de la información de ser necesario. Valorar en términos de seguridad de la información los activos de información de la Entidad. Velar por el mantenimiento de la documentación del SGSI, su custodia y protección. Contribuir al enriquecimiento del esquema de gestión del conocimiento sobre el MSPI en cuanto a la documentación de las lecciones aprendidas. Trabajar de manera integrada con el grupo o áreas asignadas. Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. Gestionar el desarrollo e implementación de políticas, normas, directrices, controles y procedimientos de seguridad de gestión de TI e información. Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. Liderar el proceso de gestión de incidentes de seguridad así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.	Supervisar y hacer seguimiento a las actividades concernientes a la adecuada administración del PHVA del SGSI	Avances y oportunidades de mejora del Sistema de Gestión Seguridad de la Información	Director Representante de la Alta Dirección para el SGSI Jefe Oficina Asesora de Planeación e Información CIO CTO	Cuando exista el requerimiento o mensualmente de acuerdo a los comités

	FORMATO MATRIZ DE RESPONSABILIDADES Y AUTORIDADES				
	SISTEMA DE GESTIÓN				
	UNIDAD NACIONAL DE PROTECCIÓN				
Alcance	Sistema de Gestión Seguridad de la Información		**RENDICIÓN DE CUENTAS**		
Rol	**Resonsabilidad**	**Autoridad**	**¿Qué cuentas rinde?**	**¿A quién rinde cuentas?**	**¿Cada cuánto rinde cuentas?**
6. CISO (Chief Information Security Officer) Ofical de seguridad de la información	Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. Vigilar el seguimiento a las no conformidades, el estado de las acciones correctivas, además de las quejas reclamos y sugerencias sobre el seguridad digital. Presentar los informes de seguridad digital, incluyendo las principales novedades, iniciativas e incidentes de seguridad de la información, así como las lecciones aprendidas. Elaborar las campañas de sensibilización, capacitación y socialización del seguridad digital. Planificar, diseñar e implementar el SGSI de la entidad, sus Políticas, lineamientos y controles, los requerimientos legales y buenas prácticas. Planificar y diseñar el Modelo de Seguridad y Privacidad de la Información acorde con la Estrategia de Gobierno Digital. Planear las actividades correspondientes a la estrategia de Ciberseguridad definida por el Ministerio de Defensa Nacional. Desarrollar las actividades de coordinación de la Seguridad de la Información y seguridad Informática de la entidad. Establecer directrices y hacer seguimiento a los controles definidos en los procedimientos, estándares, guías, instructivos y buenas practicas relacionadas con la Seguridad de la Información y la Seguridad Informática. Revisar y actualizar la documentación definida para el Sistema de Gestión de Seguridad de la Información SGSI. Evaluar la efectividad del control definido en el Plan de Tratamiento de Riesgos referente a la Seguridad de la Información de la Entidad. Reportar los Incidentes de alto Impacto a la Gerencia de la entidad. Reportar al Jefe de la Oficina Asesora de Planeación e información, al CIO y al el incumplimiento de las actividades del Sistema de Gestión de Seguridad de la Información de la entidad. Fomentar la mejora continua del Sistema de Gestión de Seguridad de la Información de la entidad.	Supervisar y hacer seguimiento a las actividades concernientes a la adecuada administración del PHVA del SGSI	Avances y oportunidades de mejora del Sistema de Gestión Seguridad de la Información	Director Representante de la Alta Dirección para el SGSI Jefe Oficina Asesora de Planeación e Información CIO	Cuando exista el requerimiento o mensualmente de acuerdo a los comités

	FORMATO MATRIZ DE RESPONSABILIDADES Y AUTORIDADES				
	SISTEMA DE GESTIÓN				
	UNIDAD NACIONAL DE PROTECCIÓN				
Alcance	Sistema de Gestión Seguridad de la Información		**RENDICIÓN DE CUENTAS**		
Rol	**Resonsabilidad**	**Autoridad**	**¿Qué cuentas rinde?**	**¿A quién rinde cuentas?**	**¿Cada cuánto rinde cuentas?**
7. CSO Oficial de seguridad Corporativa (Fisica - Tecnológica)	Apoyar el diseño de la implementación del Modelo de Seguridad y Privacidad de la Información en toda la Entidad. Apoyar al comité institucional de gestión y desempeño en la implementación de la política de Seguridad y Privacidad de la información. Ejecutar las acciones específicas sobre seguridad y privacidad de la información definidas en el Marco de Referencia de Arquitectura Empresarial del Estado y las demás normas que lo regulen. Apoyar fundamentalmente al CIO, CTO y CISO de la entidad, en la identificación y mitigación de los riesgos asociados a la arquitectura TI. de la Entidad. Gestionar las herramientas de seguridad perimetral de la entidad. Implementar los controles definidos en los procedimientos, estándares, guías, instructivos y buenas practicas relacionadas con la Seguridad de la Información y la Seguridad Informática. Actualizar la documentación correspondiente, e implementar los cambios en el Servicio que lidera. Participar en la adopción de Planes de sensibilización frente a la Cultura de Seguridad de la Información de la entidad. Implementar y evaluar periódicamente los controles definidos en el Plan de Tratamiento de Riesgos referente a la Seguridad de la Información de la Entidad. Implementar los requerimientos de Seguridad Informática. Emitir y Evaluar, los concepto técnicos de requerimientos de Seguridad Informática. Apoyra la elaboración e implementación del Plan de Recuperación de Desastres "DRP" y continuidad del negocio - PCN Brindar lineamientos para controlar el acceso a los sistemas de información y la modificación de los privilegios. Realizar y documentar las acciones necesarias para mitigar los Incidentes de Seguridad de la Información de la entidad. Realizar las actividades para el análisis de vulnerabilidades y remediación a la Infraestructura Tecnológica de la entidad.	Supervisar y hacer seguimiento a las actividades concernientes a la adecuada administración del PHVA del SGSI (en lo referente a seguridad informatica).	Avances y oportunidades de mejora del Sistema de Gestión Seguridad de la Información	Director Representante de la Alta Dirección para el SGSI Jefe Oficina Asesora de Planeación e Información CIO CTO CISO	Cuando exista el requerimiento o mensualmente de acuerdo a los comités
8. Subcomité de Gestión y Seguridad de TI.	Revisar los diagnósticos del estado de la seguridad de la información en Nombre de la entidad. Acompañar e impulsar el desarrollo de proyectos de gestión y seguridad de TI. Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de Nombre de la entidad. Participar en la aprobación del uso de metodologías y procesos específicos para la seguridad de la información. Participar en la formulación y evaluación de planes de acción para mitigar los riesgos. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes. Promover la difusión y sensibilización de la seguridad de la información dentro de la entidad. Poner en conocimiento de la entidad, los documentos generados al interior del comité de seguridad de la información que impacten de manera transversal a la misma Las demás funciones inherentes a la naturaleza del Subcomité	Supervisar y hacer seguimiento a las actividades concernientes a la adecuada administración del PHVA del SGSI (en lo referente a seguridad informatica).	Avances y oportunidades de mejora del Sistema de Gestión Seguridad de la Información	Representante de la Alta Dirección para el SGSI Jefe Oficina Asesora de Planeación e Información	Cuando exista el requerimiento o mensualmente de acuerdo a los comités

	FORMATO MATRIZ DE RESPONSABILIDADES Y AUTORIDADES				
	SISTEMA DE GESTIÓN				
	UNIDAD NACIONAL DE PROTECCIÓN				
Alcance	Sistema de Gestión Seguridad de la Información		**RENDICIÓN DE CUENTAS**		
Rol	**Resonsabilidad**	**Autoridad**	**¿Qué cuentas rinde?**	**¿A quién rinde cuentas?**	**¿Cada cuánto rinde cuentas?**
9. Equipo Técnico SGSI	Apoyar al CISO, y CTO en la implementación de políticas, planes, programas y proyectos de seguridad y privacidad de la información Realizar diagnósticos e emitir conceptos de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo de la implementación del mspi Articular con el CTO y el CISO , en la gestión de proveedores de tecnología e infraestructura en materis de seguridad y privacidad de la información. Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el CISO .	Informar y reportar a los niveles superiores acerca del grado de cumplimiento en los distintos procesos acerca de la implementación y eficacia de las acciones en el marco del desarrollo del PHVA del SGSI.	Cambios normativos, avances del SGSI	Representante de la Alta Dirección para el SGSI Jefe Oficina Asesora de Planeación e Información	Cuando exista el requerimiento
10. CDO (Chief Data Officer) Oficial de protección de datos personales	Estructurar e implementar las políticas de protección de datos personales, manuales, procedimientos y demás documentos del SGI Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales. Tramitar las consultas, solicitudes y reclamos, en especial de la ciudadanía y titulares de los datos. Garantizar que los procesos utilicen únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran, y sean en el marco de la finalidad de la recolección y el tratmiento. Propender que los procesos estén alineados al cumplimiento de las condiciones de seguridad y privacidad de información del titular. Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.	Informar y reportar a los niveles superiores acerca del grado de cumplimiento del principio de responsabilidad demostrada segú lo dispuesto por la SIC.	Información acerca de incumplimientos, cambios, mejoras o necesidades frente al tratamiento de datos personales	Responsable de Seguridad de la Información - CISO	Cuando exista el requerimiento

	FORMATO MATRIZ DE RESPONSABILIDADES Y AUTORIDADES				
	SISTEMA DE GESTIÓN				
	UNIDAD NACIONAL DE PROTECCIÓN				
Alcance	Sistema de Gestión Seguridad de la Información		**RENDICIÓN DE CUENTAS**		
Rol	**Resonsabilidad**	**Autoridad**	**¿Qué cuentas rinde?**	**¿A quién rinde cuentas?**	**¿Cada cuánto rinde cuentas?**
11. Responsables de procesos	Asegurar la implementación de la política de seguridad y privacidad de la información al interior de los procesos. Identificar los riesgos de seguridad de la información a los cuales se encuentran expuestos los procesos. Identificar e inventariar los nuevos activos digitales de información y los riesgos cibernéticos asociados. Verificar los informes de auditorías realizadas a la seguridad digital y velar porque se apliquen las acciones correctivas identificadas, así Realizar el análisis de riesgos de seguridad de sus procesos y coordinar el plan de tratamiento con el líder o responsable de Mantener actualiazdo el inventario de activos de información, generando una correcta identificación, clasificación y etiquetado	No aplica	Información acerca de incumplimientos, cambios, mejoras o necesidades frente al tratamiento de datos oportuno	Representante de la Alta Dirección para el SGSI	Cuando exista el requerimiento
	Clasificar los activos de información de acuerdo con los criterios establecidos, dar las directrices de uso del activo al interior de sus procesos, procedimientos y actividades Informar al Oficial de Seguridad de la información, cuando detecte cualquier incidente de seguridad de la información, para que sea tratado y corregido mediante la aplicación de controles. Implementar los controles, y las medidas de seguridad de la información necesarias en su área para evitar fraudes, robos, explotación de vulnerabilidades o interrupción en los servicios o activos de información. Asegurarse de que el personal: servidores públicos, contratistas y/o proveedores apliquen los controles y cláusulas de confidencialidad y que conozcan de sus responsabilidades del tratamiento del activo.	No aplica	Información acerca de incumplimientos, cambios, mejoras o necesidades frente al tratamiento de datos oportuno	CISO	Cuando exista el requerimiento
12. Oficina de control interno:	Evaluar periódicamente las prácticas de confiabilidad, disponibilidad e integridad de la información de la entidad en el marco del modelo de seguridad y privacidad de la información Informar sobre la confiabilidad y la integridad de la información y las exposiciones a riesgos asociados y las violaciones a estas.	Informar y reportar a los niveles superiores acerca del grado de cumplimiento en los distintos procesos acerca de la implementación y eficacia de las acciones en el marco del desarrollo del PHVA del SGSI.	Información acerca de incumplimientos, cambios, mejoras o necesidades frente al tratamiento de datos oportuno	Director	Cuando exista el requerimiento o mensualmente de acuerdo a los comités
13. Funcionarios, contratistas y colaboradores de la Entidad:	Dar cumplimiento con la Política de Seguridad y Privacidad de la Información y tratamiento de datos personales Cumplir con las políticas de seguridad de la información. Reportar incidentes de seguridad que atenten contra laconfidencialidad, intgeridad o disponibilidad de la información o evidencie un incumplimiento de las políticas de seguridad de la UNP. Participar activamente de las campañas de sensibilixación del SGSI. Participar en las actividades de identificación de activos y los riesgos de seguridad de la información asociados a éstos. Apoyar el desarrollo de las auditorias internas y externas al SGSI.	No aplica	Información acerca de incumplimientos, cambios, mejoras o necesidades frente al tratamiento de datos oportuno	CISO	Cuando exista el requerimiento
Archivese en:	Carpeta digital en INTRANET				
SGE-FT-33/ V1	Oficialización: 02/12/2019			**Página** 1 de 1	

10. CONTROL DE CAMBIOS

VERSIÓN INICIAL	DESCRIPCIÓN DE LA CREACIÓN O CAMBIO DEL DOCUMENTO	FECHA	VERSIÓN FINAL
00	Creación del documento con el propósito de establecer criterios generales respecto a seguridad y privacidad de la información de la UNP	09/03/2020	01

11. BIBLIOGRAFÍA

- ICONTEC. Norma Técnica Colombiana NTC-ISO 9000. Colombia. 2015. Segunda actualización.
- ICONTEC. Norma Técnica Colombiana NTC-ISO 27001. Colombia. 2013. Segunda edición.
- ICONTEC, NTC-ISO-IEC 27001, 2013.Anexo A. En: Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C: ICONTEC, 2013, 13-24 p. (NTCISO/IEC 27001).

- ISO. Términos y Definiciones. En: Gestión de la seguridad de la información (Fundamentos y vocabulario). 2006. (NORMA ISO/IEC 27000).

- MINISTERIO DE LAS TECNOLGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 2573. Título II – Componentes, instrumentos y responsables. [En Línea] Bogotá, D.C.: [Citado el 13 julio de 2017]. Disponible en Internet: <URL: http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf>

- _____. Guía para la Gestión y Clasificación de Activos de Información. Seguridad y Privacidad de la Información. [En Línea] Bogotá, D.C. [Citado el 13 julio de 2017]. Disponible en Internet: <URL: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf>

- _____. Modelo de Seguridad y Privacidad de la Información. Seguridad y Privacidad de la Información. [En Línea] Bogotá, D.C. [Citado el 13 julio de 2017]. Disponible en internet: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf>

- NORMA TÉCNICA COLOMBIANA MTC-ISO 31000, página 9. [En Línea] Bogotá, D.C.: [Citado el 9 de Abril del 2018]. Disponible en Internet: <URL: https://sitios.ces.edu.co/Documentos/NTC-ISO31000_Gestion_del_riesgo.pdf>
- NTC-ISO 27005:2008. Tecnologías de la Información. Técnicas de seguridad. Gestión del riesgo en la seguridad de la información. Términos y definiciones. P. 2