Manual

DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GTE-MA-02-V1

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
10-12-2020

Tabla de Contenido

1. OBJETIVO

Definir los lineamientos y directrices que deben seguir todas las partes interesadas de la Unidad Nacional de Protección - UNP, 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 que tengan acceso a información de la Unidad Nacional de Protección, el cual debe ser cumplido para alcanzar un adecuado nivel de protección de la información.

Este manual inicia con la definición de las políticas en materia de seguridad y privacidad de la información y finaliza con la revisión del cumplimiento de los requisitos legales una vez terminada la vinculación laboral.

3. DEFINICIONES

Activo: En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, elementos de infraestructura física y computacional; 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, impresos u otros medios, entre los cuales se encuentran los públicos, y los 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).
Cadena de suministros:
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 o 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.
On Premise: El término se refiere al tipo de instalación de una solución de software. Esta instalación se lleva a cabo dentro del servidor y la infraestructura (TIC) de la empresa. Es el modelo tradicional de aplicaciones empresariales. Con este modelo la empresa es la responsable de la seguridad, disponibilidad y gestión del software
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.
Programa Fuente: Conjunto de líneas de texto (líneas de código) que forman parte esencial de un programa informático, siendo entonces las instrucciones que debe seguir el computador para poder realizar la ejecución de una orden determinada.
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).
Servicios esenciales:
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.

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.

[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"

ID	Número	Año	Descripción
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 Archivos 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".
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.

ID	Número	Año	Descripción
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.
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”
N- 34	Resolución 0198	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
N- 35	Resolución 0199	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”.

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

7.1. POLITICAS ESPECIFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Estas políticas se desarrollan teniendo como referencia las buenas prácticas definidas en el Modelo de Seguridad y Privacidad de la Información - MSPI establecidas por el Ministerio de las Tecnologías de la Información y las Comunicaciones - MinTic, los principios de la seguridad de la información y los requisitos de seguridad definidos en la declaración de aplicabilidad del Anexo A de norma ISO 27001:2013 aceptados por la UNP.

7.1.1 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 27002:2015; 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, colaboradores, contratistas y partes interesadas de la Entidad deben realizar los esfuerzos suficientes para su cumplimiento.

7.1.2 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 veinte (20) 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. Se debe 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 de su tratamiento, almacenamiento, transporte o transmisión y realizarán verificaciones periódicas para asegurar el cumplimiento de estas.
5. Los líderes de cada proceso conocerán, gestionarán y evaluarán de forma permanente los riesgos existentes sobre los activos de información, así como los controles que se han implementado para mitigarlos.
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 uso e intercambio de la información para cada una de las partes y se deberán firmar antes de otorgar el 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 y de los datos.
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 pérdida 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.

7.1.3 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.

b) 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) 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, transmisión 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 (gravísimas, graves, moderadas y/o leves) 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.

7.1.4 Políticas de seguridad y privacidad de la información por dominio

7.1.4.1 A.5.1 Orientación de la dirección para la Gestión de la seguridad de la información.

Dominio/Control: A.5.1 Políticas para la Seguridad de la Información.
Objetivo: Brindar orientación y soporte por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
Alcance: Se debe definir un conjunto de Políticas para la Seguridad de la Información, aprobada por la dirección, publicadas y comunicada a los funcionarios, colaboradores y partes interesadas.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.1.1 A.5.1.1 Políticas para la seguridad de la información

Las Políticas de Seguridad y Privacidad de la Información de la UNP están relacionadas con la información o datos que se encuentran en los recursos tecnológicos, humanos, físicos, que manejan administran y custodian los funcionarios, colaboradores, proveedores y terceros.

Las Políticas definidas a continuación se encuentran estructuradas y orientadas con base en cada dominio o control del Anexo A de la NTC ISO 27001:2013, y están alineadas con las prácticas de gestión de la NTC ISO 27002:2015.

7.1.4.1.2 A.5.1.2 Revisión de las políticas para la seguridad de la información.

a. La definición, actualización y mantenimiento del documento de Políticas de Seguridad y Privacidad de la Información de la UNP, es responsabilidad del Líder u Oficial de Seguridad de Información quien debe revisar las Políticas al menos una vez al año o cuando ocurran cambios significativos para asegurar su conveniencia, adecuación, y eficacia continua; con la debida aprobación de la alta dirección y deberá seguir los lineamientos definidos en el procedimiento de control de documentos.

b. En las revisiones periódicas se debe tener en cuenta factores como:
   - Prioridades de la Entidad.
   - Costos e impacto de los controles a implementar por la Entidad.
   - Incidentes de Seguridad de Información reportados.
   - Nuevas vulnerabilidades detectadas.
   - Cambios en los requerimientos regulatorios y/o legales.
   - Cambios en la infraestructura tecnológica de la Entidad.

- Cambios en los objetivos del Sistema de Gestión de Seguridad de la Información “SGSI”.
- Cambios en los objetivos de la Entidad entre otros.

7.1.4.2 A.6.1 Organización interna

Dominio/ Control: A.6.1 Organización Interna.
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la Seguridad de la Información dentro de la organización.
Alcance: La presente Política se alinea con el alcance de la implementación del Sistema de Gestión de Seguridad de la Información “SGSI” de la UNP.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

a. La oficina asesora de planeación e información, a través del oficial de seguridad de la información o quien haga sus veces, liderará la implementación del Sistema de Gestión de Seguridad de la Información “SGSI” en todos los Procesos:
   - Estratégicos.
   - Misionales.
   - Apoyo.
   - Evaluación.

b. La oficina asesora de planeación e información define en el Manual de Gestión Estratégica Integrada MIPG-SIG los roles y responsabilidades en seguridad de la información.

c. La Entidad deberá mantener contacto con las autoridades pertinentes y los grupos de interés especiales tales como: Comando Conjunto Cibernético, Colcert, Policía Nacional, Profesionales especializados en Seguridad de la información, entre otros.

d. Todos los nuevos proyectos que se planteen ejecutar en la Entidad, independientemente de su naturaleza deberán contemplar los requisitos de Seguridad de la Información.

7.1.4.2.1 A.6.2.1 Política para dispositivos móviles

Dominio/ Control: A.6.2.1 Política para Dispositivos Móviles
Objetivo: Garantizar la seguridad en el uso de los dispositivos móviles.
Alcance: La presente Política aplica a todos los funcionarios, colaboradores y partes interesadas o que, por su rol, hagan uso de dispositivos móviles en la entidad.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

a. La asignación de dispositivos móviles institucionales está a cargo de los grupos internos de trabajo que implementan medidas de protección de la subdirección de protección y la subdirección especializada de seguridad y protección, previa autorización del jefe de área correspondiente y la secretaria general.
b. La autorización del uso de dispositivos móviles será realizada por un funcionario o colaborador de la entidad, previa justificación de la necesidad funcional del servicio.
c. Los funcionarios y colaboradores que accedan a los sistemas de información y/o servicios tecnológicos a través de dispositivos móviles, deben hacer el registro de ingreso del dispositivo (computador portátil, tabletas o celulares) en la recepción, esto alineado con el procedimiento de seguridad de instalaciones de la entidad.
d. Para los visitantes que accedan a los sistemas de información y/o servicios tecnológicos a través de dispositivos móviles, deben hacer el registro de ingreso del dispositivo (computador portátil, tableta o celular) en la recepción, esto alineado con el procedimiento de seguridad de instalaciones de la entidad.
e. El grupo de Gestión de Tecnologías de la información efectuará labores de control de acceso a los sistemas de información y servicios tecnológicos de la entidad desde dispositivos móviles propios, personales o de terceros autorizados para conectarse a la red de la UNP, con el objeto de adoptar los mecanismos de protección de la información según las capacidades institucionales y aplicar las medidas correctivas cuando se requieran.
f. El grupo de Gestión de Tecnologías de la información debe definir los criterios para el acceso a los sistemas de información y servicios tecnológicos desde los dispositivos móviles de la entidad, personales o de terceros y se encuentren conectados en la red de la UNP, precisando mediante información documentada el uso aceptable de activos.
g. Todos los usuarios que tengan autorizado el uso de dispositivos móviles corporativos y/o personales deben cumplir con las reglas generales establecidas en la información documentada relacionada con el uso aceptable de activos.
h. Para agregar un dispositivo móvil personal a la red de la UNP, debe contar con:

- El Sistema Operativo Licenciado y actualizado (parchado).
- El antivirus licenciado y actualizado.
- La ofimática o aplicaciones necesarias para su gestión licenciadas.
- Durante el uso del dispositivo móvil se debe aplicar el bloqueo de pantalla
- Cumplir los requerimientos técnicos para habilitar su conexión a los servicios de red de la UNP.

NOTA: Si no cumple con lo anteriormente descrito y los criterios de seguridad que establece la entidad para el acceso a los sistemas de información y servicios tecnológicos, no se autoriza su acceso.

Para los colaboradores que utilicen sus equipos personales y no cumplan con todos los requisitos de seguridad, y que a pesar de ello tengan que hacer uso de su equipo, éstos se hacen responsables por los incidentes que este riesgo genere a la entidad.

i. Aquellos equipos móviles personales o de terceros que se encuentren conectados a la red de la entidad y estos no sean avalados y autorizados por el grupo de Gestión de Tecnologías de la información serán catalogados como: **"Equipos NO autorizados**" y se podrá considerar como un incumplimiento a las Políticas de Seguridad y Privacidad de la Información definidas por la entidad.
j. Los equipos personales, no tienen soporte de la Mesa de Servicios por fallas que en ellos se presenten y que no sean asociadas a los servicios de la entidad.
k. Los dispositivos móviles personales, deben estar protegidos por un sistema de control de acceso fuerte.

7.1.4.2.2 A.6.2.2 Política de Teletrabajo

Dominio/ Control: A.6.2.2 Teletrabajo.
Objetivo: Establecer los lineamientos para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza Teletrabajo.

Alcance: La presente Política aplica para todos los funcionarios que laboren bajo la modalidad de Teletrabajo.

Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

La UNP establece los siguientes lineamientos, en el marco de la Ley 1221 de 2008 "Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones":

En lo que respecta al Teletrabajo la subdirección de talento humano define los alcances de acuerdo con las modalidades definidas en la Ley 1221 de 2008 y el Decreto reglamentario 0884 del 2012.

Para los equipos de cómputo y dispositivos móviles corporativos que son utilizados en la modalidad de teletrabajo, se debe cumplir con:

La UNP, como Empleador debe:

a. Suministrar a los teletrabajadores, los equipos de trabajo para la ejecución de sus obligaciones y/o funciones (cuando a ello haya lugar) o autorizar la utilización de equipos personales para el Teletrabajo, siempre y cuando se cumpla y acepten los mecanismos y medidas de Seguridad y privacidad de la Información y en la política de trae tu propio dispositivo.

b. Será responsable del licenciamiento del Software de los equipos suministrados a los Teletrabajadores para su uso.
c. Dar a conocer a los Teletrabajadores los lineamientos impartidos a través de la presente Política y con ello los riesgos de su proceso que se derivan por el uso de los equipos tecnológicos para la Seguridad de la información de la Entidad.
d. Definir los tipos de usuarios que dispondrán de modalidad de Teletrabajo y los permisos de acceso remoto pertinentes.
e. Establecer procedimientos para la solicitud y autorización del Teletrabajo.
f. Establecer un procedimiento de conexión remota para atender problemas e incidencias puntuales relacionados con Teletrabajo.
g. Establecer un compromiso por parte del Teletrabajador frente al cumplimiento de los lineamientos adoptados a través de la presente política, así como en lo relacionado al uso exclusivo del equipo asignado por la Entidad, que se destine para la ejecución de sus obligaciones y/o funciones (según sea el caso), aceptando y cumpliendo para tales efectos con las medidas de seguridad de la información y en la política de trae tu propio dispositivo.
h. Identificar los derechos y obligaciones de cada una de las partes que intervienen en el Teletrabajo.
i. El Grupo de gestión de tecnologías e información llevara el seguimiento de las conexiones remotas a los servicios relacionados con el Teletrabajo. Especialmente se debe prestar atención a los intentos de conexión sospechosos.

Responsabilidades del Teletrabajador de la UNP:

a. Deben cumplir con las Políticas de Seguridad y Privacidad de Información definidas y establecidas por la Entidad.
b. Deben cumplir con las reglas generales establecidas en la Guía para el uso aceptable de activos.
c. La información de carácter confidencial (clasificada) y altamente confidencial (reservada) debe ser almacenada en los repositorios dispuestos por la entidad a través de los servicios tecnológicos. En concordancia con lo anterior, la información no debe ser almacenada en medios de almacenamiento removible como memorias USB, discos duros externos o discos duros de los equipos, así como en servicios de nubes no institucionales.
d. En los equipos que contengan información confidencial (clasificada) y altamente confidencial (reservada), se debe contar con la autorización previa del dueño del proceso e implementar mecanismos de cifrado del disco.
e. No podrá instalar software que no esté autorizado.
f. Los equipos asignados por la entidad no deben dejarse desatendidos, y evitar transportar el equipo si no es necesario.

g. En los casos en que se deban dejar desatendidos los equipos de cómputo, es necesario que se aseguren con la guaya o que sean guardados en un sitio bajo llave.
h. Para el transporte de equipos portátiles fuera de la oficina en que se ejecuten las funciones de Teletrabajo, es necesario disponer de un maletín que ofrezca buena resistencia a caídas, golpes, aplastamiento, derrame de líquidos u otro riesgo al que se encuentre expuesto el equipo.
i. No conectar los equipos portátiles asignados por la entidad a redes públicas como: (Wi-Fi abiertas, redes Públicas de hoteles, bibliotecas, aeropuertos, entre otros) sin algún tipo de conexión segura VPN.
j. Cuando se requiera, para acceder a los sistemas de información y/o servicios tecnológicos de la entidad desde sitios remotos, se debe hacer a través de la conexión segura VPN provista por la entidad.
k. Utilizar contraseñas seguras siguiendo los lineamientos de la Política de control de acceso de la UNP.
l. Borrar el histórico de navegación, las cookies y otros datos del navegador web en el equipo asignado por la Entidad o personal.
m. No habilitar la función de guardado automático de usuario y contraseña para acceder a los servicios tecnológicos provistos por la entidad.
n. Finalice la sesión de manera correcta (hacer click en cerrar sesión) para que al ingresar no acceda de manera automática con las credenciales de usuario.
o. Debe cerrar las conexiones con servidores y páginas web mediante la opción “desconectar” o “cerrar sesión” al finalizar su labor en el equipo asignado por la Entidad o personal.
p. Debe eliminar la información temporal alojada en carpeta de descargas, papelera de reciclaje, escritorio virtual u otras que se encuentren en diferentes carpetas del equipo asignado por la Entidad o personal.
q. En lo que respecta a la información que se encuentre contenida en medios físicos, los Teletrabajadores están en la obligación de dar estricto cumplimiento a los lineamientos de Seguridad y privacidad de la Información establecidos por la Entidad y que a continuación se relacionan:
    - Almacenar los documentos bajo llave mientras no se estén utilizando.
    - Dar cumplimiento a las medidas de seguridad adoptadas por la UNP y los lineamientos definidos por Gestión Documental que apliquen en el uso y traslado de los documentos fuera de la entidad.
    - No dejar los documentos en tránsito desentendidos en el lugar o lugares en los que se ejecutan las funciones de Teletrabajo.
    - Utilizar según las instrucciones definidas por el proceso en coordinación con el grupo de gestión de tecnologías de la información las etiquetas de protección de confidencialidad a documentos y comunicaciones electrónicos

En lo que respecta al trabajo virtual en casa, esta opción de trabajo es excepcional y transitoria, que le permite a la entidad continuar con la operación y la prestación de sus servicios a los ciudadanos, sin embargo, los riesgos de seguridad de la información son los mismos del teletrabajo, razón por la cual se deben aplicar y cumplir los controles necesarios para garantizar una comunicación segura desde los puntos de conexión individual hacia la infraestructura y servicios tecnológicos de la entidad.
Las condiciones de uso de los activos de información a través de los servicios tecnológicos están definidos de manera general en la guía de uso aceptable de activos y en la política de dispositivos móviles que hacen parte integral de los documentos del sistema de gestión de seguridad de la información.
Es de anotar, que estos documentos se actualizarán conforme se vayan presentando novedades de tipo normativo, tecnológico, ambiental entre otros que puedan afectar la seguridad de la información.

7.1.4.3 A.7. Seguridad de los recursos humanos

Dominio/Control: A.7. Seguridad del Recurso Humano.
Objetivo: Asegurar que los funcionarios y colaboradores comprendan sus responsabilidades y sean idóneos en los roles para los que se consideran.
Alcance: La presente política establece que todos los funcionarios, colaboradores y partes interesadas, deben dar cumplimiento a las Políticas de Seguridad y Privacidad de la información de la UNP.

Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

La UNP, reconoce la importancia que tiene el factor humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con personal calificado, deberá garantizar que la vinculación de los candidatos, aspirantes, contratistas, proveedores y terceros cumplan con los procesos de verificación necesarios, el cual estará orientado al perfil, a las funciones y/u obligaciones que deben desempeñar para desarrollar su labor.

7.1.4.3.1 A.7.1 Antes de asumir en empleo

Asegurar que los candidatos, aspirantes, contratistas y proveedores comprendan sus responsabilidades y sean idóneos en los roles para los que se consideran:

a. El Grupo de Selección y evaluación del proceso de Gestión de Talento Humano de acuerdo con su competencia, deben realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por los candidatos o aspirantes a ocupar un cargo en la UNP, antes de su vinculación definitiva.
b. El Grupo de Capacitación del proceso de Gestión de Talento Humano debe convocar a los funcionarios y colaboradores de la Entidad, para que asistan a las charlas de

inducción y reinducción donde se darán a conocer las Políticas de Seguridad y privacidad de la Información

c. Se debe incorporar dentro de las minutas contractuales, clausulas referentes a:
    - Estricto cumplimiento del Manual de Políticas Específicas de Seguridad y Privacidad de la Información definida por la Entidad.
    - Confidencialidad de la Información.
    - Cláusulas de Tratamiento de Datos Personales.
d. El Grupo de Selección y Evaluación del proceso de Gestión de Talento Humano de acuerdo con su competencia, debe realizar verificaciones de los antecedentes de todos los candidatos o aspirantes, se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes y deben ser proporcionales a los requisitos de la Entidad, a la clasificación de la información a que va a tener acceso, y a los riesgos percibidos.
e. El personal provisto por terceros debe garantizar el cumplimiento de los acuerdos y/o Cláusulas de Confidencialidad y de aceptación de las Políticas de Seguridad y Privacidad de la Información de la Entidad antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica de la misma.
f. En el código de integridad de la Entidad, se deberá incluir un capítulo del estricto cumplimiento a las Políticas de Seguridad y Privacidad de la Información de la Entidad por parte de los funcionarios y contratistas.

7.1.4.3.2 A.7.2 Durante la ejecución del empleo

Asegurar que todos los funcionarios, colaboradores y partes interesadas, tomen conciencia de sus responsabilidades frente a la Seguridad y Privacidad de la información, considerando el cumplimiento de los siguientes lineamientos:

a. El grupo de registro y control de la Subdirección de Talento Humano, deberá notificar cualquier novedad de funcionarios que se encuentren en situaciones administrativas tales como: (licencias, vacaciones, traslado, retiro, entre otros); para que las áreas que administran aplicativos, herramientas y procesos de la entidad, procedan para que sean bloqueados sus privilegios de acceso y/o hagan entrega de los elementos asignados según disponga su jefe inmediato o supervisor de contrato.
b. El grupo de selección de la Subdirección de Talento Humano, deberá notificar el retiro del practicante; para que las áreas que administran aplicativos, herramientas y procesos de la entidad, procedan para que sean bloqueados sus privilegios de acceso y/o hagan entrega de los elementos asignados según disponga su supervisor de la práctica.
c. El supervisor del contrato, deberá notificar cualquier novedad, de los colaboradores, proveedores y terceros tales como: (suspender, ceder, terminar contratos, entre otros),

referente a su vinculación o relación comercial con la Entidad para que las áreas que administran aplicativos, herramientas y procesos de la entidad, procedan para que sean bloqueados sus privilegios de acceso y/o hagan entrega de los elementos asignados según disponga su jefe inmediato o supervisor de contrato.

d. La Oficina Asesora de Planeación e Información, a través del Oficial de Seguridad de la información o quien haga sus veces, deberá diseñar y ejecutar de manera periódica (mínimo una vez al año) un Plan de Cultura y Sensibilización de la Información a todos los funcionarios, colaboradores, proveedores y terceros, con el objetivo de apoyar la protección adecuada de la información y de los recursos de procesamiento la misma.
e. Se debe contar con un proceso formal y comunicado para emprender acciones contra funcionarios, colaboradores y partes interesadas, que hayan cometido una violación a la política de Seguridad y Privacidad de la Información de la Entidad.
f. Se debe sensibilizar y divulgar a través de los medios establecidos por la entidad sobre la Seguridad y privacidad de la Información, a los funcionarios, colaboradores y partes interesadas, éstos deben participar activamente en los Programas o Planes de Cultura y Sensibilización en Seguridad de la Información desarrollados por el oficial de seguridad de la información y el coordinador del Grupo de Gestión de Tecnologías de la información, y de acuerdo al contenido debe ser interiorizado y aplicado según corresponda su rol y responsabilidad dentro de la Entidad.
g. El contenido de los Programas o Planes de Cultura y Sensibilización de Seguridad de la Información deben enmarcarse en tres (3) fases:
    - Diseño. Deben ser diseñados teniendo en cuenta la misión de la entidad, identificación de las necesidades y prioridades (verificación de Incidentes de Seguridad), elaboración de indicadores o métricas de desempeño que permitan generar resultados.
    - Preparación. Elaborar material de entrenamiento en el que se pueda emplear una buena pedagogía para la difusión de los temas de Seguridad y este debe ser sometido aprobación por la Alta Dirección, antes de la puesta en marcha.
    - Implementación. Socializar el programa o Plan de Cultura Sensibilización de Seguridad de la Información de la Entidad que fue diseñado y desarrollado al igual que emplear los indicadores o métricas para evaluar el desempeño del Programa o Plan.

7.1.4.3.3 A.7.3 Terminación y cambio de empleo

a. Los funcionarios, colaboradores y partes interesadas, deberán mantener la confidencialidad de la información por un periodo no inferior a cinco (5) años, contados a partir de la finalización de su vínculo laboral o relación comercial con la entidad, o por el término máximo conforme lo indica la normatividad legal vigente

b. El grupo de gestión de tecnologías de la información, las áreas que administren aplicaciones y los procesos que manejen información, deberán suspender los Servicios de TI y el acceso a cualquier tipo de información interna, clasificada o reservada a los funcionarios, colaboradores y partes interesadas que hayan finalizado su vinculación con la Entidad, siempre y cuando este sea informado por el Grupo de registro y control, selección y el supervisor del contrato.
c. Los funcionarios, colaboradores y partes interesadas, deberán entregar los elementos tales como: (computador, discos duros, tabletas, GPS, archivo físico y digital, entre otros) para que la entidad le genere el paz y salvo.

7.1.4.4 A.8 Gestión de Activos

Dominio/Control: A.8.1. Responsabilidad por los activos.
Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
Alcance: La presente política aplica para todos los funcionarios, colaboradores y partes interesadas o que, por su rol, tengan bajo su propiedad o custodia, activos de información.

Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.4.1 A.8.1.1 Inventario de Activos

El grupo de Gestión documental con el apoyo del Oficial de Seguridad de la Información o quien haga sus veces y la oficina asesora jurídica, deberán llevar a cabo funciones de orientación y apoyo en cada uno de los Procesos Institucionales a través de las actividades para la identificación, valoración y clasificación de activos de información, con el objeto de validar que los activos de cada una de las dependencias de la UNP, estén identificados en las Tablas de Retención Documental de acuerdo con los criterios establecidos en el procedimiento de Identificación, Valoración y Clasificación de Activos de Información, asegurando que:

a. Todo activo de información deberá ser clasificado por:

   - Su nivel criticidad.
   - Impacto en el compromiso de confidencialidad, integridad y disponibilidad.
   - Disposiciones legales.

b. La Matriz de identificación y clasificación de activos de información debe permanecer en un repositorio seguro con acceso restringido.
c. La Matriz de identificación y clasificación de activos de información se debe actualizar por lo menos una vez al año y/o cuando se presenten:
   - Cambios en la tabla de retención documental.
   - Retiro de activos de información

d. Mantener actualizado el inventario de los activos de información tecnológicos de la entidad tales como (redes, servidores, aplicaciones, dispositivos de red, estaciones de trabajo, portátiles y licencias de software entre otros), así como aires acondicionados, generadores de energía, unidades de potencia (UPS).
e. Los activos de información deberán estar publicados de acuerdo con la legislación actual vigente.
f. Los activos de información tanto físico como digitales deberán estar rotulados conforme lo indique la información documentada de la entidad respecto a la Clasificación y rotulado.

7.1.4.4.2 A.8.1.2 Propiedad de los activos

Quien ejerza las funciones de propietario de activos de información en la UNP deberá:

a. Asegurar que todos los activos de información bajo su propiedad se encuentren debidamente inventariados.
b. La Entidad, deberá identificar cuáles son los propietarios de la información y asignar responsabilidades para:
    - Definición de controles para la protección de los activos de Información.
    - Mantenimiento de los controles definidos para la protección de los activos de Información.
    - Seguimiento y/o monitoreo de los custodios de los activos de Información para la verificación de la aplicación de los controles definidos.
c. Verificar que los activos de información sean clasificados y protegidos de acuerdo con:
    - Su nivel criticidad.
    - Impacto en el compromiso de confidencialidad, integridad y disponibilidad.
    - Disposiciones legales.
d. Revisar al menos una vez al año o cuando ocurra un cambio significativo, las restricciones y clasificaciones de acceso a los activos de información.
e. Verificar que los procesos de eliminación o destrucción no permitan la exposición de los activos de información a terceros.

7.1.4.4.3 A.8.1.3 Uso aceptable de los activos

a. Todos funcionarios, colaboradores y partes interesadas que tengan acceso o custodia de activos de información de la Entidad, deben acatar y dar estricto cumplimiento a la información documentada y relacionada con el Uso Aceptable de los Activos de Información, y lo definido en los procedimientos que deba ejecutar según su rol.

7.1.4.4.4 A.8.1.4 Devolución de activos

a. Todos los funcionarios, colaboradores y partes interesadas, deben hacer devolución del activo de información bajo su responsabilidad, una vez finalizado el vínculo con la Entidad.
b. Una vez finalizado el vínculo con la Entidad, el Jefe de Área o Supervisor del Contrato (según sea el caso) deberá solicitar a la Mesa de servicios, la aplicación de las herramientas de borrado seguro sobre la información institucional alojada en los equipos asignados para la ejecución de sus funciones u obligaciones contractuales, previo a la generación del backup de la Información que allí se aloje.
c. El Jefe de Área o Supervisor del Contrato (según sea el caso), debe asegurarse que los activos de información que se encuentren bajo su custodia sea:

    - Reasignado a un funcionario, colaborador o parte interesada de la Entidad.
    - Devueltos al líder de proceso, archivo, bodega o almacén de la Entidad según corresponda.
    - Traspasados a otra Área, Dependencia o regionales.
    - Destruidos, dados de baja o donados a terceros según sea el caso y el proceso definido por Secretaria General.

7.1.4.5 A. 8.2 Clasificación de la información

Dominio/Control: A.8.2. Clasificación de la información
Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización
Alcance: La presente política aplica para todos los funcionarios, colaboradores y partes interesadas o que, por su rol, tengan bajo su propiedad o custodia, activos de información.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.5.1 A.8.2.1 Clasificación de la información

a. Los únicos niveles de clasificación de información establecidos en la UNP son: Publica, Uso Interno, Clasificada (Confidencial) y Reservada (Altamente confidencial), por tanto, el dueño del proceso está obligado a clasificar y dar el tratamiento adecuado a la información de acuerdo a estos niveles y siguiendo los lineamientos definidos por la información documentada de la entidad respecto a la Clasificación y Rotulado
b. Los propietarios de los activos de Información están obligados a clasificar y dar tratamiento adecuado a la misma, de acuerdo a los niveles definidos por la información documentada en la entidad respecto a la Clasificación y Rotulación.

7.1.4.5.2 A.8.2.2 Etiquetado de la información

a. Cada activo debe poseer un etiquetado en donde se identifique el nivel de clasificación asignado. El etiquetado debe ser utilizado para aquella información que se encuentre contenida tanto en medio físico, electrónico y digital, como lo indica la información documentada relacionada con la Clasificación y Rotulación de la información.

7.1.4.5.3 A.8.2.3 Manejo de activos

Para el uso, tratamiento, procesamiento, almacenamiento y comunicación de la información se deben considerar los niveles de clasificación definidos en la información documentada relacionada con la Clasificación y Rotulación de la información.

La eliminación y destrucción de la información debe realizarse de acuerdo a su nivel de clasificación y siguiendo los lineamientos definidos en la información documentada relacionada con la Clasificación y Rotulación de la información.

Teniendo en cuenta que la Integridad es un principio fundamental de la seguridad de la información, se deben cumplir con:

- En lo que respecta a todas las aplicaciones de la Entidad, se deben implementar mecanismos cuyo objeto sea el de propender por la Integridad del Activo de información con base en el nivel de clasificación y el nivel de evaluación de Riesgo identificado.
- El grupo de gestión de tecnologías de la información de la Entidad, será la única dependencia autorizada para realizar copia de Seguridad del Software Original.
- El software proporcionado por la Entidad, no puede ser copiado o suministrado a terceros.

7.1.4.6 A. 8.3 Manejo de medios

Dominio/Control: A.8.3. Manejo de Medios
Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.
Alcance: La presente política aplica para todos los funcionarios, colaboradores y partes interesadas o que, por su rol, tengan bajo su propiedad o custodia, activos de información.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos

7.1.4.6.1 A.8.3.1 Gestión de medios removibles

a. Cualquier dispositivo de almacenamiento de información de propiedad de la Entidad, se constituye en un activo de información, por tanto, el ingreso, uso, movilización y salida, debe ser previamente autorizado por la (s) dependencia (s) competente (s).
b. Se debe mantener un inventario actualizado de los dispositivos de almacenamiento de información removible de la entidad como (Cintas de Backup, Discos Duros Externos, USB, GPS, entre otros) y de sus responsables y/o propietarios.
c. Los propietarios y custodios de los medios removibles deben asegurarse que éstos no queden desatendidos debido a que pueden ser susceptibles a pérdida o robo.
d. La protección a los medios debe hacerse de acuerdo al nivel de clasificación definidos por la entidad para la información contenida en los mismos.
e. El uso de dispositivos de almacenamiento personales o de la Entidad como (usb, Micro SD, discos duros externos, entre otros) están restringidos, solamente podrán ser utilizados con la debida autorización del formato de creación o modificación de usuarios.
f. Todos los medios de almacenamiento removibles, deben ser almacenados en un ambiente seguro de acuerdo a las especificaciones de los fabricantes.
g. Si ya no se requiere de la información contenida en los medios removibles de la Entidad, se deberá aplicar técnicas de borrado Seguro definido para que estos puedan ser reutilizados.

7.1.4.6.2 A.8.3.2 Disposición de los medios

a. Una vez terminado el ciclo de vida útil de un determinado medio de almacenamiento, la información allí contenida, debe ser eliminada de manera segura, previo a la generación de backup de la información que allí se contenga.
b. Se debe tener en cuenta el procedimiento para la disposición de dispositivos tecnológicos RAES para los equipos y medios de almacenamiento que se den de baja.
c. La Entidad debe asegurarse que se implemente los controles establecidos para la Disposición Segura de Medios cuando se vayan a:

    - Destruidos o dar de baja.
    - Donados a Terceros.

d. Para la eliminación de medios de almacenamiento se debe generar un registro mediante acta con el fin de mantener registros para efectos de auditorías.

7.1.4.6.3 A.8.3.3 Transferencia de medios físicos

a. El transporte de los medios de almacenamiento de la Entidad debe darse de acuerdo a la clasificación de la información contenida en éstos, para ello se deben:
    - Utilizar servicios de mensajería confiables.
    - Verificar los tipos de monitoreo para la transferencia de medios físicos.

- Verificar si se realizan técnicas de embalaje.
- Llevar un registro correspondiente de los medios físicos que son transportados.

7.1.4.7 A.9. Control de Acceso

7.1.4.7.1 A.9.1 Requisitos del negocio para el control de acceso

Dominio/Control: A.9.1 Política de control de Acceso
Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
Alcance: La presente Política aplica para todos los funcionarios, colaboradores y partes interesadas o que, por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información de la UNP.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

a. Los Sistemas de Información de la Entidad, deben contar con mecanismos para el control de acceso lógico. Estos mecanismos se deberán revisar con una periodicidad mínimo de una (1) vez al año.
b. Establecer medidas de control de acceso físico y lógico para los funcionarios, colaboradores y partes interesadas a través de mecanismos de identificación, autenticación y autorización de acceso, a nivel de Red, Sistemas de Información, Bases de Datos y Servicios de TI de acuerdo con los perfiles y cargos establecidos en la Entidad.
c. La Entidad, proporcionará a los funcionarios, colaboradores, partes interesadas y terceros, los recursos tecnológicos necesarios para que puedan desempeñar las funciones de una manera eficaz.
d. No se permite conectar o instalar, de manera cableada o inalámbrica a la red LAN de la Entidad, cualquier dispositivo fijo o móvil como: (computadores de escritorio, portátiles, Tablet, enrutadores, switches, agendas electrónicas, Smartphone, Access point, amplificadores de señal, entre otros) que no sean autorizados por el grupo de gestión de tecnologías de la información y el oficial de seguridad de la Información si se requiere.
e. El acceso a la red interna por parte de un proveedor debe estar autorizada por el grupo de gestión de tecnologías de la información y el Oficial de Seguridad de la Información si se requiere, mediante los mecanismos definidos por la Entidad.
f. El parámetro de tiempo de inactividad de una sesión de usuario debe definirse en el comité de cambios y aplicarse a través de la herramienta de gestión de usuarios.
g. Todas las contraseñas de usuarios privilegiados o super usuarios (Administrador), se deben cambiar de acuerdo al análisis previo realizado por el grupo de gestión de

tecnologías de la información y el Oficial de Seguridad de la Información; y para ello se debe convocar a Comité de Cambios donde se aprobará y se programará el cambio.

h. Todas las contraseñas de usuarios privilegiados o super usuarios (Administrador) de los servicios tecnológicos, se deben proteger y almacenar bajo la custodia del coordinador del grupo de gestión de Tecnologías de la Información.
i. El Grupo de Gestión de Talento Humano y Gestión Contractual, deberán informar a los Administradores de los Sistemas de Información y/o Aplicaciones de la Entidad, lo referente a novedades que surjan para los funcionarios, colaboradores y partes interesadas, con el objeto de que dichos usuarios sean deshabilitados o suspendidos oportunamente, según fuere el caso.

7.1.4.7.2 A.9.2 Gestión de Acceso a usuarios

Dominio/ Control: A.9.2. Gestión de acceso de usuarios
Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
Alcance: La presente Política aplica para todos los funcionarios, colaboradores y partes interesadas o que, por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información de la UNP.

Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

a. La UNP establece los privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a los recursos y servicios tecnológicos y los sistemas de información. Así mismo, velará porque los funcionarios, colaboradores y partes interesadas tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada con procedimientos establecidos para tal fin.
b. Quien(es) ejecute (n) el rol de Coordinador de Tecnologías de la Información o quien haga de sus veces, debe (n):
   - Dar cumplimiento a la aprobación o rechazo de los permisos de conexión remota o VPN, previamente otorgado por el grupo de gestión de tecnologías de la información de la Entidad o quien haga sus veces, En lo que respecta a la solicitud de acceso lógico que efectúen los funcionarios, colaboradores y partes interesadas, esta debe ir respaldada, soportada y avalada por el Jefe inmediato o Supervisor del contrato según sea el caso.
   - Asegurar que las redes inalámbricas cuenten con métodos de autenticación que eviten accesos no autorizados.
   - Velar por el cumplimiento del procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red.

- Realizar al menos una vez al año la verificación de los controles de acceso de los funcionarios, colaboradores y partes interesadas a fin de cerciorarse que dichos usuarios acceden solamente a los recursos autorizados para la realización de sus tareas, funciones u obligaciones; así mismo debe realizar la deshabilitación o suspensión de aquellos usuarios que contando con acceso activo, presenten cualquier tipo de novedad que así lo amerite.
- Asignar los privilegios a los usuarios de acuerdo con los roles y responsabilidades, según lo establecido en el formato asignación o modificación de usuarios. La vigencia de estos privilegios podrá ser modificada solo cuando sea necesario y deben contar con autorización del Jefe o Supervisor del Contrato, visto bueno del coordinador del grupo de tecnologías de la información y el Oficial de Seguridad de Información.
- Cancelar los derechos de acceso a la información a todos los funcionarios, colaboradores y partes interesadas que no tengan vinculación con la Entidad.

c. El acceso a los recursos de red, serán controlados por medio de la creación de usuarios y las credenciales correspondientes, con el fin de prevenir el acceso no autorizado.
d. Los funcionarios, colaboradores y partes interesadas de la Entidad, tendrán solamente acceso a los servicios de red y Sistemas de Información para los cuales fueron autorizados y que son necesarios para realizar sus funciones.
e. Los funcionarios, colaboradores y partes interesadas, deben reportar cualquier sospecha de que una persona esté utilizando una contraseña o un usuario que no le pertenece en la herramienta de la Mesa de servicios como incidente de Seguridad de Información.

7.1.4.7.3 A.9.3 Responsabilidad de los usuarios

Dominio/ Control: A.9.3 Responsabilidad de los usuarios
Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
Alcance: La presente Política aplica para todos los funcionarios, colaboradores y partes interesadas o que, por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información de la UNP.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

a. Todos los funcionarios, colaboradores y partes interesadas deben bloquear el equipo en caso de ausentarse del puesto de trabajo, con el fin evitar el acceso no autorizado a cualquier aplicación de la Entidad.
b. Todos los funcionarios, colaboradores y partes interesadas, deben apagar el equipo una vez termine la jornada laboral, con el fin evitar el acceso no autorizado a cualquier aplicación de la Entidad.

c. Todos los funcionarios, colaboradores y partes interesadas bajo ningún motivo deberán prestar su usuario y contraseña para acceder al equipo y/o aplicaciones de la Entidad.
d. Es responsabilidad de los funcionarios, colaboradores y partes interesadas, el buen manejo y uso de los recursos de la Entidad, así como de las claves que le han sido asignadas.
e. Todos los funcionarios, colaboradores y partes interesadas, que, con ocasión a sus tareas u obligaciones con la Entidad, tengan acceso a los Sistemas de Información, deben acceder con las credenciales del usuario de dominio de la UNP, asignándole para ello una contraseña que cumpla con las políticas de seguridad adoptadas por la entidad, la cual deberá ser personal e intransferible.
f. Para la creación de contraseñas seguras, los funcionarios, colaboradores y partes interesadas, deben:
    - Utilizar contraseñas fáciles de recordar y difíciles de descifrar, y que no contengan información relacionada con su trabajo o vida personal, por lo cual no se debe utilizar la siguiente información: Números de identificación personal, números de teléfono, nombres de los conyugues, direcciones postales, nombres propios, lugares conocidos o términos técnicos entre otros.
    - Combinar palabras (Mayúsculas o minúsculas), puntuación y números, de tal modo que arroje como resultado una contraseña alfanumérica con símbolos especiales.
    - Transformar una palabra común utilizando un método específico.
    - Crear acrónimos (siglas que forman una palabra).
    - Crear contraseñas que contengan como mínimo 12 dígitos y cambiarla a intervalos de 3 meses.
    - Los Intentos no exitosos de ingreso de la contraseña, después de un número veces determinadas y previamente establecidas por la entidad, traerá consigo el bloqueo del usuario de manera inmediata para lo cual se deberá solicitar el desbloqueo a quien ejecute el rol de Administrador de control de acceso lógico.

g. Las contraseñas que sean suministradas a través de correo electrónico por quien ejecute el rol de administrador de un determinado Sistema, deben ser cambiadas de manera inmediata tan pronto como la misma sea recibida por parte de la persona a quien se le han asignado los permisos, siguiendo para ello con los protocolos de seguridad de la información y las buenas prácticas de uso de contraseñas.
h. Las contraseñas no deben ser almacenadas en formato legible, papeles, agendas de trabajo, computadores sin sistemas de control de acceso o cualquier otro lugar donde las personas no autorizadas puedan encontrarlas.
i. Si algún funcionario, colaborador y parte interesada, sospecha (n) de la pérdida de confidencialidad de alguna de sus claves, debe (n) notificar el evento o incidente de

seguridad de la información (según sea el caso) a través del centro de servicios, a fin de tomar las medidas pertinentes de cuidado de la información y supervisar la generación de nuevas credenciales siguiendo los lineamientos establecidos por la entidad a través de la información documentada y relacionada con la Gestión de Incidentes de Seguridad de la Información de la Entidad.

7.1.4.7.4 A.9.4 Control de Acceso a sistemas y aplicaciones

La UNP deberá asegurar, preservar y garantizar el control de acceso a los Sistemas y/o Aplicaciones Institucionales, para lo cual deberá dar cumplimiento a los siguientes parámetros de Seguridad:

a. El acceso a los Sistemas de Información y Servicios Tecnológicos de la Entidad, a través del uso de usuario de dominio, debe estar restringido y delimitado a las tareas, funciones, responsabilidades u obligaciones que ejecuten los funcionarios, colaboradores y partes interesadas de la Entidad.
b. El propietario de la aplicación y de la información (dueño del proceso que hace uso del sistema de información), deberá identificar y documentar explícitamente el grado de importancia de la información en términos de su confidencialidad de acuerdo con la clasificación de los activos de información definidos por la entidad.
c. Los propietarios de los activos de Información deben autorizar los accesos a sus Sistemas de Información y/o Aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la Clasificación de la Información
d. No está permitido para ningún funcionario, colaborador y parte interesada, acceda a los Sistemas de Información y/o Aplicaciones para el cual no haya sido autorizado.
e. Quien(es) ejecute (n) el rol de coordinador del grupo de tecnologías de la información o quien haga de sus veces, debe (n):
    - Asegurar que los grupos de servicios de información, usuarios y Sistemas de Información sean segmentados en redes.
    - Establecer los controles de acceso a los ambientes de producción de los Sistemas de Información.
    - Asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción de la Entidad.
    - Restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.
    - Asegurar que en lo que respecta a los Sistemas Operativos, Sistemas de Información y/o Aplicaciones de la Entidad, se bloquee la sesión automáticamente, después de determinados minutos de inactividad, previamente establecidos.

- Garantizar que los Sistemas de Información y/o Aplicaciones de la Entidad, tenga establecidos “Time Out” después de determinados minutos de inactividad previamente establecidos. Esto debe estar tanto para las Aplicaciones locales y web.
- En lo que respecta a la autorización y continuidad en el uso de los usuarios de los aplicativos, deberá ser responsabilidad de cada una de las Áreas, Dependencias y/o Procesos de la Entidad.

7.1.4.8 A.10. Criptografía

7.1.4.8.1 A.10.1 Controles Criptográficos

Dominio/Control: A.10.1 Controles Criptográficos.
Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
Alcance: La presente política aplica para todos los funcionarios, colaboradores y partes interesadas de la UNP que hagan uso de controles criptográficos, cuando se requiera.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

a. Quien(es) ejecute (n) el rol de coordinador del grupo de tecnologías de la información o quien haga de sus veces, debe (n):
   - Con la participación de los dueños de los activos de información, identificar los Sistemas de Información y/o Aplicaciones en los que se considere necesario hacer uso de controles criptográficos para proteger la información. El uso de controles criptográficos quedará determinado por el análisis de riesgos de los Sistemas de Información, así como el nivel o fortaleza de los mecanismos de cifrado a utilizar (algoritmos, longitudes de clave mínimas, etc.).
   - Documentar los pasos necesarios para el registro, generación, distribución, almacenamiento, recuperación, renovación, revocación y destrucción de las claves criptográficas y debe mantener un registro de actividad que evidencie su cumplimiento y permita su posterior revisión o auditoría.

b. Los aspectos importantes que se deben tener en cuenta para el uso de los controles criptográficos son:
   - Para la Información clasificada (confidencial) y/o Reservada (altamente confidencial) de la Entidad.
   - Para las líneas de comunicación por donde se almacena, procesa y transmite la información Clasificada y/o reservada.
   - Las herramientas y mecanismos de cifrado definidas por la Entidad.
   - Para cumplimiento de los Requisitos legales.

c. Se debe realizar una gestión segura de todas las claves criptográficas, por parte de quienes requieran su uso, con el objeto de garantizar la eficacia de los controles criptográficos.
d. Cuando se utilicen mecanismos de cifrado simétrico o de clave privada (compartida), se debe garantizar la confidencialidad en el intercambio de las claves (por un canal seguro o cifradas mediante mecanismos de cifrado asimétrico).
e. Cuando se utilicen mecanismos de cifrado asimétricos o de clave pública/privada, se debe:
   - En el intercambio de claves públicas, la autenticidad e integridad de estas, deben quedar avaladas por una autoridad de certificación de confianza, bien sea interna (PKI interna) o externa.
   - En el caso de uso de servicios criptográficos de terceros, los acuerdos de prestación de servicios deben cubrir aspectos de responsabilidad civil, fiabilidad y seguridad del servicio y tiempos de provisión.
f. Para los tokens de Seguridad suministrados a los funcionarios y/o colaboradores, para realizar consulta, modificación, trasmisión de información, pagos, entre otros fines:

   - Se debe guardar en un lugar seguro bajo llave, libre de acceso al mismo por personal no autorizado.
   - No se debe dejar desatendido cuando el usuario se encuentre ausente del puesto de trabajo.
   - No se puede prestar el token ni suministrar la clave bajo ninguna circunstancia.
   - No se debe utilizar fuera de las instalaciones de la Entidad.
   - No se debe utilizar en horario no laboral sin previa autorización escrita del Jefe o Supervisor de Contrato.
   - Si el token se bloquea por intentos fallidos por el uso del mismo se debe solicitar el desbloqueo a la Entidad “Administradora” del mismo, previo a solicitud en el centro de servicios del grupo de gestión de tecnologías de la información, para autorizar el servicio remoto mediante aprobación del oficial de Seguridad de la Información.

7.1.4.9 A.11. Seguridad física y del entorno

Dominio/ Control: A.11.1 Áreas Seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la UNP.

Alcance: La presente política aplica para todos los funcionarios, colaboradores y partes interesadas que por su rol tengan acceso físico a las instalaciones y áreas seguras de la UNP.

Lineamientos:

Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.9.1 A.11.1 Áreas seguras

7.1.4.9.1.1 A.11.1.1 Perímetros de seguridad física

Las áreas y dependencias de la UNP deben encontrarse protegidas por barreras y controles físicos para lo cual deben estar monitoreadas y supervisadas con circuito cerrado de cámaras**.** Para la Entidad se definen las siguientes áreas seguras:

a. **Datacenter:** corresponde al centro de procesamiento de datos en donde se albergan los sistemas de información (aplicaciones, bases de datos), los componentes de telecomunicaciones y los sistemas de almacenamiento (servidores físicos y virtuales).

b. **Centros de Cableado:** áreas de unión central que se usan para conectar los dispositivos de la red del área local (LAN) el cual alberga paneles de conexión, Hubs de cableado, Switches, Router, Puentes, entre otros.

c. **Cuartos de Suministro:** áreas en donde se ubican los servicios de suministro como: las UPS y la planta eléctrica.

d. **Archivo Físico Central:** áreas en donde se administran, custodian y conservan los documentos físicos con valor administrativo, legal, permanente, histórico entre otros, para la UNP que son transferidos por las diferentes oficinas.

e. **Archivo Físico de Gestión:** Hace referencia a aquella documentación todavía en trámite que conservan las oficinas, así como a aquella que aun después de finalizado el procedimiento administrativo, está sometida a uso continuo y consulta administrativa por las mismas oficinas, o los que aún no han podido ser trasladado a archivo central, aplicando para ello lo dispuesto en las tablas de retención documental.

f. **Oficinas:** todas aquellas dependencias y áreas de la Entidad, que por sus competencias funcionales manejan información Clasificada (confidencial) y/o Reservada (altamente confidencial), serán consideradas “Áreas Seguras”, para lo cual deben adoptarse los mecanismos tendientes para asegurar dicha información. Por todo lo expuesto, se deben adoptar por lo menos los controles definidos en el “*Numeral 11.1.2. Controles de Acceso Físico*”, según su nivel de riesgo y capacidades institucionales.

7.1.4.9.1.2 A.11.1.2 Controles de acceso físico

a. La UNP deberá contar con una herramienta que permita el registro de ingreso a las instalaciones y áreas seguras para funcionarios, colaboradores y partes interesadas; ya sea por medio de biométrico, tarjeta de acceso o registro físico.
b. Los visitantes deberán estar registrados en una bitácora manual o sistematizada proporcionada por el personal de seguridad.
c. El personal de seguridad de instalaciones deberá contar con un procedimiento que permita a las áreas informar y autorizar a los visitantes, indicando la persona que se hace responsable del visitante, la necesidad de acompañamiento, y el asunto de la visita, fecha y hora de ingreso de salida.
d. Definir elementos que permitan identificar plenamente a los visitantes desde su ingreso a la entidad.
e. Verificación periódica de accesos a áreas seguras.
f. Los sistemas de biométricos, y tarjetas de acceso deben ser verificados y depurados por lo menos una vez al año por parte del área que los administra.
g. Las áreas seguras, según su nivel de criticidad; deberán contar con barreras, puertas o elementos que restrinjan el acceso a personal no autorizado, implementando mecanismos de autenticación; incluso implementar un segundo factor según sea necesario.
h. Para el acceso a los Centros de Cableado, se debe diligenciar la bitácora de ingreso y salida. Esto debe aplicarse para los funcionarios, colaboradores y partes interesadas de la Entidad.

i. Los privilegios de acceso a las áreas seguras de la UNP, deben ser definidos y otorgados por el profesional u oficina encargada del área segura, para ello debe tener en cuenta los siguientes tipos de usuario:

- Profesionales que trabajan regularmente en las áreas seguras.
- Profesional de soporte que requiere acceso periódico.
- Visitantes (funcionarios, colaboradores y partes interesadas) que requieren acceder muy rara vez.

j. Teniendo en cuenta lo anterior, los únicos que deben tener privilegios de acceso permanente a las áreas seguras son los profesionales que trabajan regularmente en ellas. Los demás usuarios deben solicitar autorización para el acceso y portar un documento que demuestre y en todo caso acredite la calidad en la que actúa para efectuar dicho ingreso. En este tipo de casos, se debe asignar por parte del área responsable del área segura un profesional que acompañe y supervise la labor de dicho visitante, hasta su salida.

- El acceso al Datacenter está restringido y su ingreso es a través de tarjeta de proximidad y donde aplique por medios biométricos. Estos accesos solamente lo tienen las personas autorizadas.
- Las actualizaciones a los derechos de acceso, pueden ser efectuadas cuando ello así se requiera por parte de cada profesional u oficina encargada del área segura,

para lo cual si es del caso, se revocarán aquellos permisos que ya no sean necesarios.

7.1.4.9.1.3 A.11.1.3 Seguridad de oficinas, recintos e instalaciones

Con el propósito de mantener la Confidencialidad, Integridad y Disponibilidad de la Información en las Oficinas, recintos e instalaciones, es necesario establecer y dar cumplimiento a las siguientes directrices de Seguridad:

a. Impedir que aquellas áreas cuyas ventanas den al exterior por su ubicación, permitan de alguna manera (al menos mínima) la visibilidad hacia el interior de la Entidad, es necesario que cuenten con películas de vinilo, de esmeril o Sandblasting que garanticen la privacidad del área segura.
b. Implementar el uso de chapas de seguridad en las puertas de las áreas seguras con el objeto de que permanezcan cerradas.
c. Todos los funcionarios, colaboradores y partes interesadas deben presentar su carné o documento de identificación, según sea el caso, para el ingreso a las instalaciones de la Entidad.
d. Todos los funcionarios, colaboradores y partes interesadas deben portar visiblemente la escarapela, carné o documento que los acredite como tal, mientras se encuentren en las instalaciones de la Entidad.
e. Todas las oficinas de la UNP que procesen, almacenen y/o gestionen información clasificada y/o reservada deben implementar y adoptar las medidas tendientes a asegurar dicha información.
f. Para aquellas oficinas cuyo acceso físico, se de a través de puertas, es deber del Jefe de Oficina correspondiente, salvaguardar las llaves de esta y asegurar una copia en un lugar diferente y seguro.
g. Los materiales o combustibles deben ser almacenados de manera segura a una distancia prudente de las áreas de procesamiento y almacenamiento de Información.
h. Los suministros de papelería no deben almacenarse en Áreas Seguras como: (Datacenter, Centros de Cableado, Cuarto de Suministro, Archivo Físico Central y Archivo Físico de Gestión).
i. En las Áreas Seguras como: (Datacenter, Centros de Cableado, Cuarto de Suministro, Archivo Físico Central y Archivo Físico de Gestión), no se debe utilizar como bodega.
j. Las salidas de emergencia deben estar identificadas, señalizadas y socializadas conforme lo indica en plan de emergencia.

7.1.4.9.1.4 A.11.1.4 Protección contra amenazas externas y ambientales

La UNP, debe proveer las condiciones físicas y medio ambientales necesarias para brindar la protección de las personas y a la Seguridad de la Información de la Entidad, ante posibles eventos como incendios, inundaciones, terremotos, explosiones, ataques maliciosos, entre otros. Por lo anterior se debe dar cumplimiento a los siguientes lineamientos:

a. El grupo de seguridad de instalaciones y de seguridad y salud en el trabajo deben hacer una revisión periódica de las condiciones físicas de las áreas seguras; de procesamiento de información, generando las recomendaciones para el cumplimiento normativo correspondiente.
b. El grupo de gestión de tecnologías de la Información, debe propender por la Seguridad del (Datacenter y Centros de Cableado) que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
c. En el Datacenter, Centros de Cableado y Archivos documentales deben existir sistemas de control ambiental de temperatura, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
d. El propietario del activo de información debe propender porque la Información se almacene en un ambiente protegido y seguro.

7.1.4.9.1.5 A.11.1.5 Trabajo en Áreas seguras

Para el trabajo en áreas seguras, éstas deben propender por que:

a. Las actividades ejecutadas en las áreas seguras solamente deben ser conocidas por los funcionarios, colaboradores y partes interesadas autorizadas que las ejecutan o supervisan de acuerdo con su rol.
b. Todas las actividades ejecutadas al interior de un área segura, deberá ser supervisada por el responsable del área segura o quien él asigne.
c. Las áreas seguras vacías deberían estar cerradas con llave y se deberían revisar periódicamente;
d. No se debería permitir equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.
e. Asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.
f. Tener control de: (cualquier cambio, modificación, actualización, ajuste o soporte) que se realice sobre los procesos, Áreas Seguras y Sistemas de Procesamiento de Información, que puedan afectar uno o más de los “Pilares de Seguridad de Información (Confidencialidad, Integridad y Disponibilidad)”; para ello deben pasar por la aprobación del Comité de Cambios antes de su ejecución.

7.1.4.9.1.6 A.11.1.6 Áreas de despacho y carga

La UNP define controles para restringir el acceso a personal no autorizado en áreas de carga y despacho:

- El área de carga y despacho debe estar claramente definida.

- Si la puerta de acceso al área despacho y carga está al interior de la Entidad, ésta debe mantenerse cerrada y con control de acceso restringido.
- Las puertas externas deben permanecen cerradas mientras se efectúa el cargue o despacho.
- El material que llega o sale, se debe registrar, revisar e inspeccionar que sea el que corresponde con la lista de verificación, y que no contenga materiales o líquidos extraños que pueda ocasionar daños o afectar la seguridad de la información.
- Se debe restringir los accesos al área de carga y descarga desde fuera de las instalaciones y solamente al personal autorizado y debidamente identificado.
- Las áreas de entrega de reciclaje deben ser monitoreadas y custodiadas por personal de vigilancia mientras se realiza la entrega.

7.1.4.9.2 A.11.2 Equipos

Dominio/ Control: A.11.2 Equipos
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
Alcance: La presente Política aplica para todos los funcionarios, colaboradores, y partes interesadas que tengan acceso a la información, en medio digital o físico, de la UNP.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.9.2.1 A.11.2.1 Ubicación y protección de equipos

a. Los computadores portátiles y de escritorio tipo “todo en uno” asignados a los funcionarios y colaboradores de la entidad, deben ser entregados con guaya de seguridad (según disponibilidad), para permitir su anclaje en el puesto de trabajo con el fin de mitigar el riesgo de pérdida o robo del mismo.
b. Los equipos que tienen o manejan información clasificada (confidencial) o reservada (altamente confidencial), deben estar ubicados en áreas donde el acceso es restringido.
c. Los sistemas de información y los equipos de comunicaciones que requieren protección especial deben estar aislados para reducir el nivel del riesgo al que puedan estar expuestos.
d. Las condiciones ambientales en las instalaciones donde se encuentran los servidores y equipos activos (switches, enrutadores, entre otros), deben ser adecuados, deben contar aire acondicionado, detector de humo, alarma contra incendio.
e. Está prohibido el consumo de bebidas y comidas en las instalaciones de procesamiento de información.
f. Está prohibido fumar dentro de las instalaciones de la UNP.
g. Las impresoras, fotocopiadoras, scánners y/o multifuncionales que procesan información interna, confidencial (clasificada) y/o altamente confidencial (reservada) deben ser ubicadas en áreas seguras para prevenir el acceso, transmisión no autorizada o duplicación de documentos.

h. Para prevenir y minimizar riesgos, el grupo de tecnologías de tecnologías de la información debe establecer medidas de protección lógica que limitan el acceso de los usuarios a cada impresora o periférico compartido a través de la red de la UNP.
i. Para la impresión de documentos que no sea públicos, se deben implementar mecanismos de seguridad que garanticen que el documento sea impreso por quien tenga los privilegios autorizados.

7.1.4.9.2.2 A.11.2.2 Servicios de suministro

a. La infraestructura tecnológica de la entidad, debe estar protegido contra problemas eléctricos que puedan causar una falla o mal funcionamiento de los mismos.
b. Los servicios de suministro como, electricidad, agua, alcantarillado, aire acondicionado, ventilación/calefacción se deben inspeccionar regularmente para garantizar su buen funcionamiento.
c. Frente a posibles fallas en el suministro de energía para los equipos en la Entidad especialmente todos aquellos que sustentan las operaciones críticas para la continuidad de las actividades, se deben proveer sistemas de suministro eléctrico apoyado de fuentes de energía interrumpible como UPS.
d. Los equipos (computadores) deben estar conectados a las tomas de corriente regulada.
e. Se debe monitorear periódicamente el funcionamiento de los equipos de soporte, verificando que cumplan con requisitos de configuración y capacidad recomendados por el fabricante (por ejemplo: U.P.S., aire acondicionado, planta eléctrica, entre otros).
f. Para los dispositivos que lo permitan, se deben implementar herramientas de monitoreo que habiliten alertas acerca de su funcionamiento relacionado con la capacidad, memorias, desempeño, disponibilidad, entre otras.

7.1.4.9.2.3 A.11.2.3 Seguridad del cableado

a. El grupo de Gestión Administrativa y el Grupo de gestión de tecnologías de la información, deben garantizar que dentro de la infraestructura física de la UNP, el cableado de energía eléctrica y de telecomunicaciones que transporta los datos o soporta los Servicios de Información de la entidad estén protegidos para evitar daño o mala manipulación.
b. Las áreas de distribución de redes (eléctricas y comunicaciones) deben estar físicamente aseguradas para prevenir la modificación o el acceso no autorizado a las mismas.

7.1.4.9.2.4 A.11.2.4 Mantenimiento de equipos

Se debe generar anualmente el plan de mantenimiento de servicios tecnológicos, el cual incluye el mantenimiento a equipos de cómputo. Dicho plan debe contener al menos los siguientes elementos:

a. La instalación de cualquier tipo de software en los equipos de la entidad, es responsabilidad del grupo de gestión de tecnologías de la Información y por tanto son los únicos autorizados para realizar y/o autorizar esta labor, que se realizará con usuario administrador del equipo local.
b. El mantenimiento de los equipos, se deben realizar a intervalos planificados teniendo en cuenta las especificaciones y recomendaciones de los fabricantes; por lo que es necesario llevar un registro de las fallas presentadas.
c. El centro de servicios de la Entidad, no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración) a equipos personales.
d. Los usuarios no deben realizar cambios en los equipos de la Entidad; referente a: la configuración del equipo, conexiones de red, papel tapiz y protector de pantalla definido por la UNP, plantilla del correo institucional. Estos cambios pueden ser realizados únicamente por el personal del centro de servicios designado para tal labor por parte del grupo de gestión de tecnologías de la información, a través de una solicitud de ticket previamente autorizada.

7.1.4.9.2.5 A.11.2.5 Retiro de activos

a. Para funcionarios y contratistas se debe diligenciar el registro de entrada y/o salida del equipo, de acuerdo a los procedimientos establecido por la entidad. (el grupo de seguridad física en instalaciones.
b. Para los terceros se requiere autorización de salida del equipo aprobado por el jefe de área donde está ubicado el equipo y/o la persona a quien está asignado el equipo, y visto bueno del coordinador del grupo de gestión de tecnologías de la información y el Oficial de Seguridad de Información si se requiere, el cual deberá ser registrado de acuerdo a los establecido por el grupo de seguridad física en instalaciones.
c. Los tiempos de retiro se definen de acuerdo con la actividad a realizar.
d. El recibo y entrega de los equipos se debe formalizar a través de los formatos GAA-FT-10 Formato de transferencia de bienes y/o GTE-FT-14 Formato de Asignación de Activos de Información-. En caso del cese de labores del usuario en la Entidad, se debe gestionar adicionalmente los formatos GAA-FT-88 Formato Paz y salvo Contratistas y/o GTH-FT-02 Formato Paz y Salvo Funcionarios.

7.1.4.9.2.6 A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones

a. Los activos de información independiente de su medio de conservación (Físicos y/o digitales) que sean retirados de las instalaciones no se deben dejar desatendidos en lugares públicos o en lugares que pongan en riesgo su protección y/o conservación.
b. Las personas que son autorizadas para retirar cualquier equipo de las instalaciones de la UNP, son los responsables directos de su protección.

a. Para el uso de los equipos fuera de las instalaciones se debe tener en cuenta las consideraciones definidas en la información documentada relacionada con la Clasificación y rotulado de la información y el Uso aceptable de los activos.
b. En caso de presentarse alguna situación que comprometa la confidencialidad, integridad y disponibilidad de la información como robo, daño, acceso no autorizado entre otros, se deberá reportar la situación como un incidente de seguridad de la información, el cual será tratado de acuerdo al procedimiento respectivo.

7.1.4.9.2.7 A.11.2.7 Disposición segura o reutilización de equipos

a. Para los equipos que contengan información de carácter confidencial (clasificada) y/o altamente confidencial (Reservada), antes de su disposición o reutilización, se deberán aplicar mecanismos de borrado seguro para prevenir el riesgo de acceso no autorizado a la información confidencial de la entidad, previa elaboración del backup.
b. Antes de cualquier venta o donación, todos los medios de almacenamiento deben ser borrados de acuerdo con los mecanismos de eliminación o borrado seguro de información que adopte la entidad, previa generación de backup de la información allí almacenada.
c. En caso de reasignación del equipo y que vaya a ser utilizado para procesar información de carácter confidencial (clasificada) y/o altamente confidencial (reservada) se deben implementar mecanismos de cifrado de discos de acuerdo a las capacidades de la entidad

7.1.4.9.2.8 A.11.2.8 Equipos de usuario desatendidos

Los usuarios deben asegurar que el equipo desatendido tiene una adecuada protección y están obligados a:

a. No dejar la sesión abierta, cuando se ausente del puesto de trabajo.
b. En el momento de dejar desatendido el computador o portátil en el puesto de trabajo, el usuario debe bloquear su equipo usando las teclas: “Botón de windows + la tecla L” o “Ctrl + ALT+ SUPR + ENTER”.
c. Bloquee la sesión y/o cierre la sesión de usuario, cuando finalice la tarea (no es correcto apagar la pantalla o el equipo sin salir de la sesión de usuario).
d. Los equipos que se encuentren bloqueados deberán contar con protector de pantalla definido por la entidad, de acuerdo al tiempo límite de inactividad definida por el Administrador.
e. Los equipos portátiles y los equipos de escritorios tipo “todo en uno“, deberán contar con el uso de guaya como mecanismo de Seguridad Física.
f. Los dispositivos móviles corporativos y/o personales, a través de los cuales se accede a información corporativa de tipo confidencial o interna, deben tener implementados los

controles de bloqueo o acceso para evitar el riesgo de fuga de información por personas no autorizadas.

7.1.4.9.2.9 A.11.2.9 Políticas de escritorio limpio y pantalla limpia

a. Escritorio limpio

La política de escritorio limpio y pantalla limpia reduce los riesgos de acceso no autorizado, pérdida y daño de información durante y fuera de las horas laborales normales; aplica para todos los puestos de trabajo, es responsabilidad de toda su custodia y se debe dar cumplimiento con los siguientes lineamientos:

- Proteja la información siempre que abandone su puesto de trabajo.
- Durante la jornada laboral o al finalizarla, no se deben dejar documentos con información clasificada o reservada, al alcance de personal no autorizado, en caso de tener este tipo de información en físico, ésta debe ser guardada bajo llave y la llave en un sitio seguro con un responsable asignado.
- No se debe dejar documentos que se encuentre en tránsito al alcance de personal no autorizado, independiente de su clasificación que contiene información institucional.
- La impresión de documentos con información interna, confidencial (clasificada) y/o altamente confidencial (reservada) de la entidad debe realizarse a través del mecanismo de control establecido para ello (código o pin). La información debe ser retirada de las impresoras de manera inmediata por el dueño o la persona autorizada.
- No se debe consumir comidas o bebidas en el puesto de trabajo.

b. Pantalla Limpia

- El escritorio virtual del equipo de cómputo debe permanecer libre de documentos digitales, independiente de su clasificación de información.
- Cada vez que el personal se ausente de su lugar de trabajo debe bloquear la pantalla del computador con el fin de evitar el acceso no autorizado a la información de la Entidad.
- Bloqueo automático de la sesión en el equipo de cómputo tras inactividad superior al tiempo establecido por el área de T.I. (5 minutos)
- Los usuarios apagan los equipos de cómputo al finalizar la jornada laboral.

- Los computadores de escritorio y equipos portátiles deben tener aplicado el estándar relativo al protector de pantalla definido por el grupo de gestión de tecnologías de la información.

7.1.4.10 A.12. Seguridad de las operaciones

Dominio/ Control: A.12 Seguridad en las Operaciones.
Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
Alcance: La presente Política aplica para todas las operaciones que se desarrollen en la Entidad, a través de funcionarios, colaboradores y partes interesadas, con los que interactúa la UNP.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.10.1 A.12.1 Procedimientos operacionales y responsabilidades

7.1.4.10.1.1 A.12.1.1 Procedimientos de operación documentado

a. Los procedimientos operativos se deben documentar y poner a disposición de los funcionarios, colaboradores y partes interesadas que los necesitan para la ejecución de sus funciones, teniendo en cuenta el nivel de clasificación (público, interno, confidencial y/o altamente confidencial).

b. Los procedimientos operativos específicos de la Entidad, deben ser tratados como documentos formales y los cambios que se generen deben ser autorizados.

c. El grupo de gestión de tecnologías de la información debe incluir en la documentación de los procedimientos operacionales, entre otras las siguientes características:

- la instalación, configuración, actualización y renovación de la plataforma y sistemas de información.;
- el procesamiento y manejo de información, de todos los servicios tecnológicos que se prestan a través de la infraestructura tecnológica.
- las copias de respaldo;
- los requisitos de programación, incluidas las interdependencias con otros sistemas,
- los tiempos de finalización del primer y último trabajos;
- las instrucciones para manejo de errores u otras condiciones excepcionales que podrían surgir durante la ejecución del trabajo, incluidas las restricciones sobre el uso de utilidades del sistema
- contactos de apoyo y de una instancia superior (escalamiento), incluidos los contactos de soporte externo, en el caso de dificultades operacionales o técnicas inesperadas;

- instrucciones sobre manejo de medios y elementos de salida especiales, tales como el uso de papelería especial o la gestión de elementos de salida confidenciales, incluidos procedimientos para la disposición segura de elementos de salida de trabajos fallidos
- Reinicio y recuperación del sistema para uso en el caso de falla del sistema;
- Gestión de rastros de auditoría (Audit Trail) y de la información de registro del sistema (System Log).
- procedimientos de seguimiento.

7.1.4.10.1.2 A.12.1.2 Gestión de cambios

a. El grupo de gestión de tecnologías de la información, debe implementar un procedimiento documentado para la Gestión de Cambios, que aplique para todos los procesos relacionados con la gestión de TI en cuanto a las instalaciones, los sistemas de información e infraestructura, donde se pueda ver comprometida la seguridad de la información.

   a. El procedimiento de gestión de cambios debe contemplar entre otras las siguientes características:

      - la identificación y registro de cambios significativos;
      - la planificación y puesta a prueba de los cambios;
      - la valoración de los impactos potenciales, incluidos los impactos de estos cambios en la seguridad de la información;
      - el procedimiento de aprobación formal para los cambios propuestos;
      - la verificación de que se han cumplido los requisitos de seguridad de la información;
      - la comunicación de todos los detalles de los cambios a todas las personas pertinentes;
      - los procedimientos de apoyo, incluidos procedimientos y responsabilidades para abortar cambios no exitosos y recuperarse de ellos, y eventos no previstos;
      - el suministro de un proceso de cambio de emergencia que permita la implementación rápida y controlada de los cambios necesarios para resolver un incidente.

7.1.4.10.1.3 A.12.1.3 Gestión de la capacidad

a. El grupo de gestión de tecnologías de la información debe adelantar actividades relacionadas con la gestión de la capacidad, que incluya análisis y proyecciones para el procesamiento y almacenamiento de la información. Se deben tener en cuenta entre otros los siguientes aspectos:

- Los nuevos requerimientos de Servicios tecnológicos.
- Cambios Tecnológicos.
- El crecimiento de los Sistemas actuales de Procesamiento de la Información.
- Crecimiento o proyección institucional.
- Se deberían aplicar controles de detección que indiquen los problemas oportunamente.

7.1.4.10.1.4 A.12.1.4 Separación de los ambientes de Desarrollo, Pruebas y Operación

a. El grupo de gestión de tecnologías de la información debe separar los ambientes de Desarrollo, Pruebas y Producción para reducir los Riesgos de accesos o cambios no autorizados a los Sistemas en Producción, así como posibles inconvenientes en la operación de los mismos.

b. Los usuarios que por su rol tiene acceso a los ambientes desarrollo, pruebas o producción, deben aplicar los controles definidos en la gestión de cambios que permitan asegurar la continuidad de la operación sin afectar la disponibilidad de los servicios tecnológicos asociados al cambio.

7.1.4.10.2 A.12.2 Protección contra códigos maliciosos

Dominio: A.12.2. Protección contra códigos maliciosos.
Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.

Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.10.2.1 A.12.2.1 Controles contra código malicioso

a. El grupo de gestión de tecnologías de la información, debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la UNP y los servicios que se ejecutan en la misma.
b. El grupo de gestión de tecnologías de la información debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y derechos de actualizaciones, para mitigar las vulnerabilidades de la plataforma tecnológica
c. El grupo de gestión de tecnologías de la información debe garantizar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus.

d. El grupo de gestión de tecnologías de la información, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware, únicamente podrán realizar tareas de escaneo de virus en diferentes medios.
e. Para los usuarios que tienen el permiso de acceder a medios de almacenamiento extraíble, el grupo de gestión de tecnologías de la información debe asegurar que, al momento de conectarse un dispositivo de almacenamiento externo, se ejecute el software de antivirus de manera automática.
f. Los usuarios deben asegurarse de que los archivos adjuntos de los correos electrónicos, descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas para evitar el contagio de virus informáticos, ejecución o instalación de programas con software malicioso en los recursos tecnológicos.
g. Los usuarios que sospechen o detecten alguna infección por software malicioso deben notificar a la Centro de servicios para que se tomen las medidas de control correspondientes.

7.1.4.10.3 A.12.3 Copias de respaldo

7.1.4.10.3.1 A.12.3.1 Respaldo de la información

a. El grupo de gestión de tecnologías de la información, debe definir un procedimiento para las actividades de backup de la Información de la Entidad, teniendo en cuenta la criticidad y las necesidades de disponibilidad de los datos. Este procedimiento debe estar debidamente documentado para seguimiento y control.
b. Los dueños de proceso son las personas autorizadas para solicitar o consultar copias de respaldo de los sistemas de información de sus procesos.
c. Es responsabilidad de quien (es) ejecute (n) el rol de administrador de cada Sistema de información, realizar la solicitud de copia a quien (es) ejecute (n) el rol de administrador de backup, validar y asegurar que su Sistema de Información se encuentre contemplado en el cronograma de copias de seguridad, además de hacer seguimientos regulares a su ejecución.
d. Quien (es) ejecute (n) el rol de Administrador de backup debe validar el resultado de la ejecución de las copias de Seguridad y registrar las novedades en la bitácora establecida para ello como lo debe indicar el procedimiento.
e. Es responsabilidad de quien (es) ejecute (n) el rol de Administrador de backup realizar pruebas de restauración de copias de seguridad de manera trimestral siguiendo los lineamientos del Procedimiento Backup y Recuperación de la Información.
f. Cada copia de seguridad debe quedar registrada en la máquina donde son realizados (logs de servidor) o en un archivo externo (texto, planilla, etc.) que permita mantenerla disponible para controles o auditoría.
g. Los medios de respaldo removibles deben ser almacenado en un lugar que garantice la fiabilidad, Seguridad y disponibilidad de estos.

h. El grupo de tecnologías de la información pone a disposición de todos los usuarios, servicios de almacenamiento como One Drive, Sharepoint, (Pandora) y los definidos por los procesos, donde éstos deben almacenar la información generada y gestionada de su proceso, es responsabilidad de cada usuario utilizar estos servicios para garantizar la disponibilidad de su información.

7.1.4.10.4 A.12.4 Registro y seguimiento

7.1.4.10.4.1 A.12.4.1 Registro de eventos

a. Se deben generar, mantener y revisar regularmente (2 veces al año), los registros de auditoría sobre las actividades de los usuarios, excepciones y eventos de seguridad de información para soportar futuras investigaciones y revisión regular del control de acceso.
b. Los registros de eventos se deben generar procurando no afectar el desempeño y la disponibilidad de los servicios tecnológicos en la nube y on premise y de acuerdo con sus capacidades institucionales sobre, para lo cual se deben considerar los siguientes aspectos:

- identificación de usuarios;
- actividades del sistema;
- fechas, horas y detalles de los eventos clave, por ejemplo, entrada y salida;
- identidad del dispositivo o ubicación, si es posible, e identificador del sistema;
- registros de intentos de acceso al sistema exitosos y rechazados;
- registros de datos exitosos y rechazados y otros intentos de acceso a recursos;
- cambios a la configuración del sistema;
- uso de privilegios;
- uso de utilidades y aplicaciones del sistema;
- archivos a los que se tuvo acceso, y el tipo de acceso;
- direcciones y protocolos de red;
- alarmas accionadas por el sistema de control de acceso;
- activación y desactivación de los sistemas de protección, tales como sistemas antivirus y sistemas de detección de intrusión;
- registros de las transacciones ejecutadas por los usuarios en las aplicaciones.

7.1.4.10.4.2 A.12.4.2 Protección de la información de registro

a. Los registros de información se deben proteger contra intentos de alteración y acceso no autorizado, de acuerdo con las capacidades de la Entidad.

7.1.4.10.4.3 A.12.4.3 Registros del administrador y del operador

a. Todas las evidencias que se recolecten como resultado de las auditorías practicadas, deben contar con un lugar para el almacenamiento de los registros y monitoreo de los eventos de seguridad.

b. Todo acceso administrativo a sistemas críticos o servicios esenciales de la Entidad que no sea por consola debe ser accedido de forma segura (protocolos SSH, HTTPS).

7.1.4.10.4.4 A.12.4.3 Sincronización de relojes

a. Se debe tener como referencia la hora legal colombiana y no está permitida la desactivación del sistema de sincronización o la manipulación manual de la hora. Los relojes de todos los servicios tecnológicos On Premise de la UNP deben estar sincronizados con la fuente oficial.
b. Para los servicios tecnológicos que consume la UNP y que son gestionado por un proveedor de servicios externo, se debe garantizar que la hora se encuentre sincronizada con la hora oficial colombiana.
c. El ajuste correcto de los relojes de computador es importante para asegurar la exactitud de los registros de auditoría (Logs), que pueden ser necesarios para investigaciones o como evidencia legal o en casos disciplinarios.

7.1.4.10.5 A.12.5 Control de Software operacional

7.1.4.10.5.1 A.12.5.1 Instalación de software en sistemas operativos

a. El grupo de gestión de tecnologías de la información, debe establecer responsabilidades y procedimientos para controlar la instalación y gestión del software operativo, de acuerdo con los procedimientos establecidos para ello.
b. El grupo de gestión de tecnologías de la información, debe asegurarse que el software operativo instalado en la plataforma tecnológica cuente con soporte de los proveedores.
c. El grupo de gestión de tecnologías de la información, debe conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
d. El grupo de gestión de tecnologías de la información debe validar los riesgos que genera la migración hacia nuevas versiones del software operativo. Se debe asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.
e. El grupo de gestión de tecnologías de la información debe establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la entidad.
f. Los controles definidos para instalación y gestión de software operativo, aplican de igual manera al cualquier otro tipo de software utilizado por la UNP.

7.1.4.10.6 A.12.6 Gestión Control de la vulnerabilidad técnica

a. El grupo de gestión de tecnologías de la información, debe implementar procedimientos para la gestión de vulnerabilidades técnicas y remediación de las mismas.
b. La ejecución del análisis de vulnerabilidades tiene como fin, identificar las brechas de seguridad con las que cuenta un sistema de información y la infraestructura tecnológica, por lo tanto, la Entidad debe ejecutar análisis de vulnerabilidades periódico a los activos de información, y se deben :

    - Documentar los resultados.
    - Priorizar las vulnerabilidades.
    - Documentar el plan de remediación para corregir o mitigar (según sea el caso) las brechas identificadas.
    - Entregar los resultados de las pruebas realizadas a cada uno de los responsables de los sistemas de información e infraestructura tecnológica, quienes son los encargados de definir y aplicar el plan de remediación.

c. El grupo de gestión de tecnologías de la información, debe revisar periódicamente la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica con el fin de prevenir la exposición al riesgo de estos.
d. El grupo de gestión de tecnologías de la información a través de sus funcionarios, colaboradores y partes interesadas, debe generar, ejecutar y hacer seguimiento a los planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica.
e. Dependiendo de la prioridad con la que se necesite tratar una vulnerabilidad técnica, la acción tomada se debe a llevar a cabo de acuerdo con los procedimientos de finidos por la entidad, relacionados con la Gestión de cambios y/o la gestión de incidentes.
f. El grupo de gestión de tecnologías de la información debe implementar los controles necesarios para evitar la instalación de software no autorizado por parte de los funcionarios, colaboradores y partes interesadas, para mitigar posibles vulnerabilidades técnicas derivadas de estas instalaciones.

7.1.4.10.7 A.12.7 Consideraciones sobre auditorias de sistemas de información

7.1.4.10.7.1 A.12.7.1 Controles de auditorías de sistemas de información

a. Las auditorías que involucren accesos a los sistemas de información deben ser planificadas y acordadas, para minimizar las interrupciones en los procesos de la entidad.
b. Durante el desarrollo de las auditorias, se deben tener en cuenta los siguientes aspectos:

    - los requisitos de auditoría para acceso a sistemas y a datos se deberían acordar con el área Auditada.

- el alcance de las pruebas técnicas de auditoría se debería acordar y controlar;
- las pruebas de auditoría se deberían limitar a acceso a software y datos únicamente para lectura;
- el acceso diferente al de solo lectura solamente se debería prever para copias aisladas de los archivos del sistema (System Files), que se deberían borrar una vez que la auditoría haya finalizado, o se debería proporcionar protección apropiada si hay obligación de mantener estos archivos bajo los requisitos de documentación de auditoría;
- los requisitos para procesos especiales o adicionales se deberían identificar y acordar;
- las pruebas de auditoría que puedan afectar la disponibilidad del sistema se deberían realizar fuera de horas laborales;
- se debería hacer seguimiento de todos los accesos y regístralos (Logged) para producir un rastro de referencia (Reference Trail).
- Las pruebas de auditoría deben desarrollarse en ambientes que no afecten la operación del negocio.

7.1.4.11 A.13. Seguridad en las comunicaciones

Dominio/ Control: A.13 Seguridad de las Comunicaciones
Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
Alcance: La presente Política aplica para todos los funcionarios, colaboradores y partes interesadas o que por su rol, requieran acceder a la información y a las instalaciones de procesamiento de información de la UNP.

Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.11.1 A.13.1 Gestión de la seguridad de las redes

7.1.4.11.1.1 A.13.1.1 Controles de redes

a. Se deben controlar los accesos a servicios internos y externos conectados en red.
b. Funcionarios, colaboradores y partes interesadas, antes de contar con acceso lógico por primera vez a la red de datos de la UNP, deben contar con la autorización previa por parte de su Jefe inmediato y/o supervisor del Contrato, para proceder a la creación, activación de las cuentas de usuario, está solicitud se debe hacer al grupo de gestión de tecnologías de la información por el canal definido por la Entidad.
c. El acceso a los sistemas de la red se debe hacer a través de usuarios autorizados, de acuerdo con los roles definidos en el manual del sistema de gestión de seguridad de la información y aplicar los privilegios de manera puntual para cada servicio tecnológico según las condiciones definidas por el dueño del proceso y el grupo de gestión de tecnologías de la información.

d. Los sistemas deben permitir llevar un registro y seguimiento para detectar acciones que puedan afectar la seguridad de la información, los privilegios pueden ser revocados si se evidencia un uso inadecuado de los mismos, situación que podría generar un incidente de seguridad de la información, derivando en sanciones disciplinarias o contractuales.

7.1.4.11.1.2 A.13.1.2 Seguridad de los servicios de red

a. El grupo de gestión de tecnologías de la información de la Entidad, como responsable de las redes de datos y los recursos de red de la UNP (internos y externos), debe propender porque dichas redes estén debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.
b. En los acuerdos con proveedores se deben identificar e incluir acuerdos de niveles de Servicio ANS) como mecanismos de seguridad, al igual que el derecho de poder hacer seguimiento con regularidad y acordar el derecho de auditoría.

7.1.4.11.1.3 A.13.1.3 Separación en las redes

a. El grupo de gestión de tecnologías de la información, debe implementar mecanismos de control de acceso a través de la segmentación de las redes en función de los grupos de servicios, usuarios, sistemas de información y físicas).
b. El grupo de gestión de tecnologías de la información, debe proveer los mecanismos, controles y recursos necesarios para tener niveles adecuados de separación física y lógica con el fin de reducir el acceso no autorizado y evitar usos y cambios inadecuados sobre los servicios de T.I. (servicios de red, acceso a sistemas de información, servicios de internet).
c. El grupo de gestión de tecnologías de la información, debe asegurar que las redes inalámbricas de la UNP, cuenten con procedimientos de autenticación para evitar accesos no autorizados a funcionarios, colaboradores y partes interesadas.
d. No deben realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción de la Entidad.

7.1.4.11.2 A.13.2 Transferencia de información

Dominio/Control: A13.2 Transferencia de Información.
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
Alcance: La presente política aplica para funcionarios, colaboradores y partes interesadas, transfieran información dentro de la entidad y con cualquier entidad externa.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.11.2.1 A.13.2.1 Políticas y procedimientos de transferencia de información

a. La entidad establece los mecanismos de control formales para proteger la transferencia de información, teniendo en cuenta la clasificación de la información y los medios de difusión dispuestos por la entidad.
b. Los usuarios deben hacer uso únicamente de los canales establecidos por la entidad para la transferencia de información y cualquier otro medio no especificado se considera no autorizado.
c. La entidad debe definir los mecanismos de control para transferencia de información según su clasificación, que contemple entre otras las siguientes consideraciones según aplique:

    - No se deben usar servicios personales o libres para el intercambio de información diferentes a los adoptados por la entidad.
    - No se debe enviar información institucional a través de servicios diferentes a los adoptados por la entidad.
    - Proteger la información transferida contra interceptación, copiado, modificación, enrutado y/o destrucción;
    - Detección de software malicioso y protección contra éste, que puede ser transmitido mediante el uso de comunicaciones electrónicas;
    - Proteger la información electrónica que se transmite como archivos adjuntos;
    - El uso mal uso, almacenamiento, transmisión o difusión de la información es responsabilidad del funcionario, contratista y parte interesada que lo realiza.
    - Técnicas criptográficas, (proteger la confidencialidad, la integridad y la autenticidad de la información).
    - Directrices sobre retención y disposición para toda la correspondencia de la Entidad, incluidos mensajes, de acuerdo con la legislación y reglamentaciones locales y nacionales;
    - Controles y restricciones asociadas con las instalaciones de comunicación, (el reenvío automático de correo electrónico a direcciones de correo externas);
    - Brindar asesoría al personal para que tome las precauciones apropiadas acerca de no revelar información confidencial;
    - j) no dejar expuesta la información (impresa en los multifuncionales, fax, mensajes de voz, contestadoras, entre otras

7.1.4.11.2.2 A.13.2.2 Acuerdos sobre transferencia de información

a. Cuando se trate de intercambios periódicos, se debe privilegiar la transmisión de datos a través de vías seguras, con los cuales se establecen convenios o nexos de diferente naturaleza, y que involucran de alguna forma el intercambio de información.

b. La entidad debe definir los protocolos para transferencia de información según su clasificación, que contemple entre otras las siguientes consideraciones según aplique:

    • las responsabilidades de la dirección para controlar y notificar la transmisión, despacho y recibo;

- los controles para asegurar trazabilidad y no repudio;
- los estándares técnicos mínimos para empaquetado y transmisión;
- certificados de depósito de títulos en garantía;
- estándares de identificación de mensajería;
- las responsabilidades y obligaciones en el caso de incidentes de seguridad de la información, tales como pérdidas de datos;
- el uso de un sistema de etiquetado acordado para información sensible o crítica, que asegure que el significado de la etiqueta se entiende de inmediato, y que la información está protegida apropiadamente.
- las normas técnicas para registro y lectura de información y software;
- cualquier control especial que se requiera para proteger elementos sensibles, tales como criptografía;
- mantener una cadena de custodia para la información mientras está en tránsito;
- los niveles aceptables de control de acceso.

7.1.4.11.2.3 A.13.2.3 Mensajería electrónica

a. Todos los mensajes enviados desde la cuenta Institucional de la entidad, deben respetar el estándar de formato e imagen Corporativa de la UNP.
b. Archivos que contengan extensiones como .mp3, wav, .exe, .com, .dll, .bat. o cualquier otro archivo ejecutable; en caso de que sea necesario hacer un envío de este tipo de archivos deberá ser autorizado por el grupo de gestión de tecnologías de la información.
c. El uso del correo electrónico en cadenas o mensajes enviados a un número de destinatarios y estos a su vez son reenviados a otros, sin un propósito relacionado con la misión de la UNP, degradan el desempeño del Servicio de Correo y consumen recursos de TI valiosos. El usuario debe abstenerse de reenviarlos a otras personas.
d. No enviar o recibir cadenas de correo, mensajes con contenido religioso, juegos, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos. Si un usuario encuentra este tipo de material deberá reportarlo a la Mesa de servicios como un incidente de seguridad de la información.
e. La Entidad, debe asignar una cuenta de correo electrónico como herramienta de trabajo para cada uno de los funcionarios, colaboradores o quien por su rol, lo requieran para el desempeño de sus Funciones y/o Obligaciones y en algunos casos a terceros previa autorización; su uso se encuentra sujeto a lo establecido en la presente Política.
f. Los mensajes y la información contenida en los buzones de correo son de propiedad de la UNP, y cada usuario es responsable de su buzón, por lo que debe mantener solamente los mensajes relacionados con el desarrollo de sus Funciones y/o Obligaciones.

g. Para los servicios de mensajería electrónica autorizados por la Entidad, como el correo electrónico se debe implementar un mensaje de advertencia que indique el tipo de información al que podría estar teniendo acceso, por ejemplo el siguiente texto:

Aviso Legal: Este mensaje puede contener ser información interna, confidencial (clasificada) y/o Altamente confidencial (Reservada) de la UNP. Si usted ha recibido este correo por error, equivocación u omisión, por favor informe de ello a quien lo envía y destrúyalo en forma inmediata. Está prohibida su retención, grabación, reimpresión, utilización o divulgación con cualquier propósito. Este mensaje ha sido verificado con software antivirus; sin embargo, la UNP no se hace responsable por la presencia en él o en sus anexos de algún virus que pueda generar daños en los equipos o programas del destinatario. Recuerde que la interceptación y substracción de esta comunicación está sujeto a sanciones penales correspondientes (ley 1273 del 2009). Recordemos que todos debemos aportar al cumplimiento de la ley 1581 del 2012.

7.1.4.11.2.4 A.13.2.4 Acuerdos de confidencialidad o de no divulgación

a. La presente política de confidencialidad, tiene por objeto informarles a todos los funcionarios, colaboradores y partes interesadas o quien por su rol estén vinculados con la UNP, sobre el compromiso frente a la no divulgación de la información relacionada con las funciones y/o obligaciones contractuales que desempeña en la Entidad, a personal interno o externo de la misma.
b. Todos los funcionarios, colaboradores y partes interesadas o quien por su rol estén vinculados con la UNP, deben firmar la cláusula y/o acuerdos de confidencialidad definidos, y este deberá ser parte integral de cada uno de los contratos. Este requerimiento también se aplicará para los casos de contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la Entidad a personas o entidades externas.
c. La UNP, firmará acuerdos de Confidencialidad con los funcionarios, colaboradores y partes interesadas, que por sus funciones accedan a información interna, confidencial (clasificada) y/o altamente confidencial (reservada) de la entidad. En estos los acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.
d. Todos los funcionarios, colaboradores, proveedores y terceros de la UNP, deben guardar absoluta reserva en relación con la información a la que tenga acceso con ocasión de la ejecución de las Funciones y/o Obligaciones, aun después de finalizada su ejecución, por el tiempo establecido por la normatividad legal vigente y aplicable para cada caso en particular.

7.1.4.12 A.14. Adquisición, desarrollo y mantenimiento de sistemas

Dominio/ Control: A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas.

Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.
Alcance: Para todas las Aplicaciones de la Entidad.

Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos.

7.1.4.12.1 A.14.1 Requisitos de seguridad en los sistemas de información

7.1.4.12.1.1 A.14.1.1 Análisis y especificaciones de requerimientos de seguridad de la información

a. Se deben incluir en todos los proyectos de desarrollo y adquisición de sistemas de información propios o de terceros, requisitos de seguridad de la información desde la etapa de diseño aplicables en todo el ciclo de vida del sistema.
b. El propietario de cada Sistema de Información en la Entidad deberá identificar y documentar que tipo de clasificación de la información se encuentra contenida en los mismos.
c. Los propietarios de los Activos de Información deben autorizar los accesos a sus Sistemas de Información o Aplicativos, de acuerdo con los perfiles establecidos, las necesidades de uso y la clasificación de la información definida por la Entidad.
d. Todo proyecto relacionado con implementación de sistemas información, debe ser coordinado con el grupo de tecnologías de la información, con la debida anticipación para preparar y garantizar los recursos necesarios.
e. Para la adquisición y actualización de software, es necesario efectuar la solicitud al grupo de gestión de tecnologías de la Información con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.

7.1.4.12.1.2 A.14.1.2 Seguridad de servicios de las aplicaciones en Redes Públicas

a. En lo posible no se deben utilizar redes públicas (aeropuertos, hoteles, centros comerciales, café internet entre otros) para acceder a los servicios y/o sistemas de información de la UNP.
b. Para las redes domésticas que pueden ser identificadas y accedidas, se deben aplicar entre otras las siguientes recomendaciones.
    - Cambio de la contraseña periódicamente, utilice contraseñas seguras y mínimo con 12 caracteres de longitud.
    - El nombre de la red no debe suministrar datos que permitan asociar al propietario de la red o la contraseña.
    - Utilice el mejor protocolo de seguridad que le proporcione le dispositivo.

c. Tanto para públicas como domésticas se deben aplicar las siguientes recomendaciones_

- Tener licenciados y actualizados el Sistemas Operativo y Antivirus
- El navegador (Google Chrome, Mozilla Firefox, Microsoft Edge, Zafari, Opera entre otros) debe estar con la última versión liberada
- No habilitar o autorizar el guardado automático de contraseñas.
- Cerrar la sesión de manera segura una vez las utilice.
- Utilizar sistemas de múltiple factor de autenticación
- Utiliza conexiones seguras como red privada virtual (VPN)
- Utiliza conexiones SSL
- Desactiva la función de uso compartido de recursos del equipo
- No habilitar la función de visibilidad del equipo en la red
- Desactiva la conexión Wi-Fi cuando no la necesites

7.1.4.12.1.3 A.14.1.3 Protección de transacciones de los servicios de aplicaciones

a. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurar que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.
b. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) establecer los controles de acceso a los ambientes de producción de los sistemas de información.
c. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
d. Quien (es) ejecute (n) el rol de Administrador del control de acceso lógico debe (n) asegurar que en lo que respecta a los sistemas operativos de la entidad, se bloquee la sesión automáticamente, después de determinados minutos de inactividad, previamente establecidos.
e. Quien (es) ejecute (n) el rol de desarrollador de sistemas de información debe (n) garantizar que se cierre la sesión en las aplicaciones, después de determinados minutos de inactividad (Timeout) previamente establecidos.
f. Se debe asignar el rol del Administrador de programas fuentes, quien tendrá la responsabilidad de custodiar dichos programas y por virtud de su función no debería pertenecer al equipo de desarrollo.
g. La actualización de las bibliotecas de fuentes del programa, así como la emisión de las fuentes para los programadores sólo se deben realizar después de haber recibido la autorización del Arquitecto de Soluciones.
h. Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe (n) mantener un registro de auditoría de todos los accesos a las bibliotecas de fuentes del programa.
i. Los desarrolladores Internos y Externos deben aplicar un procedimiento que garantice que toda vez que se migre a producción el módulo fuente, se cree el código ejecutable correspondiente en forma automática.
j. Quien (es) ejecute (n) el rol de Administrador de programas fuentes debe(n) asegurarse de que los programas fuentes cuenten con una copia de respaldo actualizada, conforme a lo estipulado en el procedimiento de backup.

k. No está permitido facilitar el usuario o la contraseña a otra persona para adelantar cualquier labor en los Sistemas de Información y/o Aplicaciones.

7.1.4.12.2 A.14.2 Seguridad en los procesos de desarrollo y de soporte

Dominio/ Control: A.14.2 Seguridad de los Procesos de Desarrollo Seguro.

Objetivo: Propender porque se diseñe e implemente dentro del ciclo de vida de Desarrollo de los Sistemas de Información buenas prácticas de Seguridad de Información.

Alcance: La presente política aplica para los Sistemas de Información, tanto desarrollos propios como de terceros, que integren cualquiera de los ambientes administrados por la Entidad en: (desarrollo, producción y/o pruebas).

Lineamientos:
La protección de la Confidencialidad de los Activos de Información de la Entidad, se delimita el acceso a los mismos, de acuerdo a los niveles de clasificación y riesgos identificados y definidos por el propietario de los mismos, para lo cual se debe considerar la separación de los ambientes tecnológicos como son: desarrollo, pruebas y producción. Por lo anterior se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.12.2.1 A.14.2.1 Política de desarrollo seguro

La UNP velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por el la Entidad.

a. Normas dirigidas a: PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN

- Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.
- Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

b. Normas dirigidas a: GRUPO DE GESTION DE TECNOLOGIAS DE LA INFORMACION

- El grupo de Gestión de Tecnologías de la Información debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
- El grupo de Gestión de Tecnologías de la Información debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la UNP.
- El grupo de Gestión de Tecnologías de la Información debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
- El grupo de Gestión de Tecnologías de la Información debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
- El grupo de Gestión de Tecnologías de la Información, a través de sus funcionarios, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
- El grupo de Gestión de Tecnologías de la Información debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la UNP.

c. Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Los desarrolladores de los sistemas de información deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los mismos, pasando desde el diseño hasta la puesta en marcha.
- Los compiladores, editores y otras herramientas de desarrollo o utilitarios del sistema no deben ser accesibles desde los ambientes de producción cuando no se requiera.
- Los desarrolladores deben proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el software aplicativo de la UNP; dicho soporte debe contemplar tiempos de respuesta aceptables.
- Los desarrolladores deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
- Los desarrolladores deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de

caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

- Los desarrolladores deben suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
- Los desarrolladores deben asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como tokens o el ingreso de parámetros adicionales de verificación.
- Los desarrolladores deben asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.
- Los desarrolladores deben garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
- Los desarrolladores deben remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
- Los desarrolladores deben prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
- Los desarrolladores deben remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
- Los desarrolladores deben certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
- Los desarrolladores deben desarrollar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos solo tengan privilegios de lectura.
- Los desarrolladores deben proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
- Los desarrolladores deben asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

7.1.4.12.2.2 A.14.2.2 Procedimientos de control de cambios en sistemas

a. La entidad debe documentar e implementar un procedimiento para la gestión de Cambios, cuando se realicen cambios a los Sistemas de Información; estos cambios pueden ser:

- Modificación a Sistemas de Información en Producción (campos, tablas, parámetros, entre otros).
- Nuevos Requerimientos a Sistemas de Información en Producción (módulos, tablas, campos, entre otros).
- Nuevos Sistemas de Información (desarrollo interno o externo).
- Cambios reglamentarios.
- Y demás que afecten los Sistemas de Información por necesidades puntuales de la Entidad.

b. En el ambiente de producción se ubicarán todos los servidores y aplicativos que prestarán los servicios a los usuarios finales internos y/o externos a la entidad. Luego que la etapa de pruebas llegue a su fin y se tenga un aplicativo estable en ambiente de pruebas donde se haya probado la instalación y la funcionalidad, el responsable de la aplicación desarrollada, debe hacer una solicitud de cambio al Comité de cambios para migrar de manera controlada dicho aplicativo hacia producción. Para poder recibir un software en el ambiente de Producción se debe tener en cuenta las siguientes condiciones:

- Tipo y clasificación de la información que maneja.
- Características del respaldo y restauración (cantidad de información, periodicidad, crecimiento esperado, tiempo de retención, tiempo aceptable de recuperación, desde cuándo se debe recuperar).
- Plan de contingencia (preferiblemente alineado con el plan de continuidad de la entidad).
- Documento de control de cambios o documentación de implementación.
- Resultado del plan de pruebas detallado y exhaustivo (con pruebas de desempeño y funcionales).
- Pruebas de seguridad y controles aplicados a la mitigación o respuesta al riesgo.

7.1.4.12.2.3 A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.

a. Los cambios en los sistemas operativos y aplicaciones se deben poner a prueba en un entorno de pruebas antes de aplicarlos a los ambientes de producción.

7.1.4.12.2.4 A.14.2.4 Restricciones en los cambios a los paquetes de software

a. Se deben definir y documentar las reglas para la transferencia de software del ambiente de pruebas al ambiente de producción.

7.1.4.12.2.5 A.14.2.5 Principios de construcción de los sistemas seguros

a. La Entidad, debe garantizar que los criterios de Seguridad de la Información se cumplan en todas las etapas de desarrollo y durante todo el ciclo de vida de un determinado software, con el objeto de incluir los requisitos de Seguridad de la Información en la metodología utilizada para tal fin en el que se establezcan las directrices de codificación seguras para cada lenguaje de programación usado y se apliquen los siguientes pasos:

    - Análisis de requerimientos.
    - Análisis arquitectónico.
    - Tipo de desarrollo (propio o a terceros).
    - Pruebas (funcionales, no funcionales y de Seguridad).
    - Producción.
    - Mantenimiento.

b. La UNP, asegurará que el software adquirido y/o desarrollado al interior de la Entidad, cumplirá con los requisitos de Seguridad con Calidad.
c. El grupo de gestión de tecnologías de información, incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.
d. En caso de desarrollos propios la Entidad, debe verificar que estén:

    - Que estén completamente documentados.
    - Que las diferentes versiones se preservan adecuadamente en varios medios.
    - Que se guarda copia de respaldo externa a la Entidad.
    - Que sean registrados ante la “Dirección General de Derechos de Autor”.

7.1.4.12.2.6 A.14.2.6 Ambiente de desarrollo seguro

a. Los usuarios deben usar diferentes perfiles de usuario para los ambientes de producción y los ambientes de pruebas, y los menús deben desplegar mensajes de identificación apropiados para reducir el riesgo de error.

7.1.4.12.2.7 A.14.2.7 Desarrollo contratado externamente

a. El software que se adquiera a través de los proyectos o programas debe quedar a nombre de la Unidad Nacional de Protección – UNP.
b. El grupo de gestión de tecnologías de información corroborara que cumpla con los requerimientos del sistema incluyendo los de seguridad y validando que éstos hayan sido implementados en todo el ciclo de vida del sistema.

7.1.4.12.2.8 A.14.2.8 Pruebas de seguridad de sistemas

a. Las pruebas no se deben llevar a cabo en el ambiente de producción.

7.1.4.12.2.9 A.14.2.9 Pruebas de aceptación de sistemas

a. El grupo de gestión de tecnologías de información debe aplicar los documentos relacionas con el Ciclo de vida de Desarrollo, definidos en el Numeral: 14.2.5 de esta Política

12.1.4.12.3 A.14.3 Datos de prueba

12.1.4.12.3.1 A.14.3.1 Protección de datos de prueba

a. Los datos de carácter clasificados y/o reservados no se deben copiar en el ambiente de pruebas, salvo que se suministren controles equivalentes al ambiente de producción.

7.1.4.13 A.15. Relaciones con proveedores

Dominio/ Control: A.15 Relación con los Proveedores.
Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores
Alcance: La presente Política aplica para todos los Proveedores o Terceros, que requieran acceso a los Activos de Información de la Entidad.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.13.1 A.15.1 Seguridad de la información en las relaciones con los proveedores

7.1.4.13.1.1 A.15.1.1 Política de seguridad de la información para las relaciones con proveedores

a. La Entidad, durante la Etapa Precontractual, desde la construcción de los estudios previos, el área solicitante de la contratación, debe identificar los Riesgos de Seguridad de la Información con el apoyo del Oficial de Seguridad de la Información, los cuales deben ser parte de la estimación y cobertura de los riesgos del proceso de contratación. De acuerdo con lo anterior, el análisis de riesgos de seguridad de la información debe incluir la identificación de los mismos en la respectiva contratación, su clasificación, probabilidad de ocurrencia estimada, su impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.
b. La Entidad, en cabezada del Comité evaluador debe identificar sí el objeto de la propuesta u oferta evaluada, requiere del acceso de los proveedores a:
   - A la información confidencial (clasificada) y/o altamente confidencial (reservada).
   - A los Sistemas de Información.
   - A las Áreas Seguras.

c. Los responsables de la estructuración técnica deben garantizar que se determine e incluyan los requisitos de seguridad y los controles necesarios por parte del proveedor a lo largo de la vigencia de este.
d. En medio de la Etapa Contractual, se debe asegurar la inclusión de las cláusulas, indicando responsables y tratamiento:

- De Confidencialidad.
- De Protección de Datos.
- Derechos de Autor.
- Las Políticas de Seguridad y Privacidad de la Información definida por la Entidad.

e. Los documentos relacionados con la seguridad y privacidad de la información definidos por la Entidad, deben ser conocidos y aceptados por los proveedores para el perfeccionamiento del contrato.

7.1.4.13.1.2 A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

a. Se debe identificar para cada contrato, a qué tipo de información tendrá acceso el proveedor de acuerdo con el objeto del contrato, y es responsabilidad del supervisor del contrato verificar el cumplimiento de las obligaciones respecto a la seguridad y privacidad de la información.
b. Se deben definir acuerdos con los proveedores, en los cuales se incluyan los siguientes criterios:

- Identificación de la información que se va a suministrar o a la que se va a tener acceso, y los métodos para suministrar la información o para acceder a ella;
- El tipo información a que va a tener acceso interno, confidencial (clasificada) y/o altamente confidencial (reservada).
- Los requisitos legales y de reglamentación, incluida la protección de datos, los derechos de propiedad intelectual y derechos de autor, y una descripción de cómo se asegurará que se cumplan;
- La obligación de cada parte contractual de implementar y acordar un grupo de controles que incluyan controles de acceso, revisión del desempeño, seguimiento, reporte y auditoría;
- Las reglas de uso aceptable de la información, incluido el uso inaceptable, si es necesario;
- Una lista explícita de personal del proveedor autorizado para tener acceso a la información de la organización o recibirla de ella, o los procedimientos o

condiciones para la autorización, y el retiro de la autorización para el acceso o recibo de información de la organización por parte del personal del proveedor;

- Las políticas de seguridad y privacidad de la información pertinentes al contrato específico;
- Los requisitos y procedimientos de gestión de incidentes (especialmente notificación y colaboración durante la remediación de incidentes);
- Los requisitos de formación y toma de conciencia para procedimientos específicos, y los requisitos de seguridad de la información, por ejemplo, para respuesta a incidentes,
- Procedimientos de autorización;
- Identificar las partes interesadas en el contrato y los datos de contacto para los asuntos relacionados con el servicio y la seguridad de la información;
- Requisitos de selección, si los hay, para el personal del proveedor, incluidas las responsabilidades para la realización de la selección, y los procedimientos de notificación, si la selección no se ha finalizado, o si los resultados son motivo de duda o inquietud;
- El derecho de auditar los procesos y controles de los proveedores, relacionados con el acuerdo;
- Los procesos de solución de defectos y resolución de conflictos;
- La obligación de los proveedores de entregar periódicamente un informe independiente sobre la eficacia de los controles y un acuerdo sobre la corrección oportuna de los asuntos pertinentes presentados en el informe;
- Las obligaciones de los proveedores relativas al cumplimiento de los requisitos de seguridad de la organización.

7.1.4.13.1.3 A.15.1.3 Cadena de suministro de información y comunicaciones

a. Para los Servicios contratados externamente, se debe exigir que los Proveedores conozcan, adopten y comuniquen los requisitos y prácticas de Seguridad y privacidad de la información de la UNP a lo largo de la cadena de suministros.
b. Para los Servicios de Tecnología y de Comunicaciones contratados externamente, se debe exigir que los Proveedores conozcan, adopten y comuniquen los requisitos y prácticas de Seguridad y privacidad de la información de la UNP a lo largo de la cadena de suministro, los cuales incluyan como mínimo los siguientes.

- Requisitos de seguridad de la información para aplicar a la adquisición de productos o servicios de tecnología y de las relaciones con los proveedores;
- Exigir que los proveedores conozcan, adopten y comuniquen los requisitos de seguridad de la Entidad a lo largo de la cadena de suministro.

- Implementar y hacer seguimiento al cumplimiento de los controles establecidos en los requisitos de seguridad y privacidad de la información para los proveedores.
- Prestar especial atención y vigilancia a los controles de la cadena de suministros que soportan los servicios esenciales de la Entidad
- Definir los protocolos para compartir información de manera segura con la cadena de suministro, y de solución de eventos o incidente de seguridad de la información.
- Identificar los riesgos en la cadena de suministros, relacionado con la obsolescencia tecnológica y la desaparición del proveedor y los productos del mercado.

c. Para la contratación de servicios o componentes de la Infraestructura de TI y/o Áreas Seguras, se debe exigir a los Proveedores la presentación de los Planes de Contingencia que aseguren la Disponibilidad de la Información, suministrada y procesada entre las partes.

7.1.4.13.2 A.15.2 Gestión de la prestación de servicios de proveedores

7.1.4.13.2.1 A.15.2.1 Seguimiento y revisión de los servicios de los proveedores

a. Como parte de la supervisión a la ejecución del contrato, se debe contemplar procesos de auditoria a proveedores cuyo objetivo sea validar el cumplimiento de los requisitos de Seguridad de la Información estipulados en la etapa contractual, dichos resultados deben quedar consignados también en los informes presentados por el supervisor del contrato.
b. Los procesos de auditoria a los proveedores, se realizaran de acuerdo con las capacidades institucionales y serán apoyados por el grupo de auditores internos de la entidad, los cuales conforman la segunda línea de defensa de los sistemas de gestión.
c. La entidad definirá los instrumentos para validar la existencia de los controles mínimos de seguridad y privacidad, que deberán cumplir los proveedores de acuerdo al nivel de protección asociado al, tipo de información al cual accederá a través del servicio prestado.
d. Durante la ejecución del contrato, es función de la UNP, monitorear y hacer seguimiento a los controles establecidos para asegurar la confidencialidad, integridad y disponibilidad de la información, frente a los riesgos previamente identificados.
e. Se deben definir acuerdos de niveles de servicios con todos los proveedores que tengan acceso o no a información confidencial o altamente confidencial, estos acuerdos deben estar monitoreados permanentemente por el supervisor del contrato.
f. La Entidad debe fortalecer los lineamientos de seguridad y privacidad de la información con los proveedores, manteniendo actualizados el Manual de contratación, guía de gestión de proveedores, guía operativa de supervisión e interventoría, teniendo en cuenta entre otros los siguientes requisitos cuando apliquen:

- Hacer seguimiento de los niveles de desempeño de servicio para verificar el cumplimiento de los acuerdos
- Revisar los reportes de cumplimiento y calidad del servicio elaborados por el proveedor.

- Auditar y hacer seguimiento a los hallazgos y recomendaciones cuando sea requerido.
- Reportar de manera inmediata cualquier incidente que comprometa la seguridad y privacidad de la información por parte de un proveedor.
- Resolver y gestionar cualquier problema identificado;
- Asegurar que el proveedor mantenga la capacidad de servicio suficiente para mantener los niveles de continuidad del servicio acordados, después de fallas considerables en el servicio, o después de un desastre.

7.1.4.13.2.2 A.15.2.2 Gestión de cambios en los servicios de los proveedores

a. Toda gestión del proveedor que represente una modificación, mantenimiento, revisión al Servicio de Tecnología de la Información, Comunicaciones o Equipos de Suministros, debe cumplir con los lineamientos de gestión de cambios definidos por la entidad, donde se contemplen entre otros:

   - Cambios en los acuerdos con los proveedores;
   - Cambios hechos por la Entidad para implementar las mejoras a los servicios ofrecidos en la actualidad, desarrollo de nuevas aplicaciones y sistemas, modificaciones o actualizaciones a las políticas y procedimientos de la Entidad, controles nuevos o modificados para resolver incidentes de seguridad de la información y mejorar la seguridad;
   - Los cambios en los servicios de los proveedores para implementar cambios y mejoras en las redes, el uso de nuevas tecnologías, la adopción de nuevos productos o versiones/ediciones más recientes, nuevas herramientas y ambientes de desarrollo, cambios en las ubicaciones físicas de las instalaciones de servicio, cambio de proveedores y/o contratación externa de otros proveedores.

7.1.4.14 A.16. Gestión de incidentes de seguridad de la información

Dominio/ Control: A.16 Gestión de Incidentes de Seguridad de la Información.
Objetivo: Asegurar un enfoque coherente y eficaz para la Gestión de Incidentes de Seguridad de la Información, incluida la comunicación sobre eventos de seguridad y debilidades.
Alcance: La presente Política aplica para todos los funcionarios, colaboradores y partes interesadas, los cuales deben reportar todo Evento o Incidente de Seguridad de la Información a la Mesa de servicios, a través de los canales oficiales establecidos por la Entidad, y estos a su vez, deben ser gestionados por los responsables de acuerdo con el procedimiento establecido para tal fin.

Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.14.1 A.16.1 Gestión de incidentes y mejoras en la seguridad de la información

7.1.4.14.1.1 A.16.1.1 Responsabilidad y procedimientos

a. La UNP promoverá entre los servidores, funcionarios, colaboradores y partes interesadas, el deber de reportar los incidentes relacionados con la seguridad de la información.
b. Los propietarios de los Activos de Información, deben informar al grupo de gestión tecnologías de la información, a través de la Mesa de servicios los Eventos e Incidentes de Seguridad de la información que identifiquen o que reconozcan ante su posibilidad de materialización.
c. La UNP en cabeza del Oficial de Seguridad gestionará el incidente de seguridad y se apoyará con las áreas afectadas para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigarlo y solucionarlo, tomando las medidas necesarias para evitar su reincidencia.
d. La entidad debe aplicar y mantener actualizado el procedimiento de Gestión de incidentes de seguridad de la información, el cual debe contemplar entre otros los siguientes aspectos:

Preparación, reporte y registro de eventos e incidentes

Establecer las características de la actividad normal de la operación de la entidad, de este modo, se pueden detectar cambios que puedan ser indicadores o advertencias de incidentes.
Verificar que el incidente de seguridad sea válido.
Activar el tratamiento de incidentes de seguridad.
Clasificar y calificar los incidentes.
Actualizar la documentación del incidente.

Detección y análisis.

Determinar la criticidad del incidente y describir los detalles del incidente.
Determinar grado de daño causado a los recursos o información y documentar hallazgos y daños detectados.
Determinar posibles causas del incidente.
Determinar las posibles consecuencias o impacto.

Contención, erradicación, recuperación, en la (infraestructura).

Las estrategias para evitar que el incidente siga sucediendo (contención), varían dependiendo del tipo de incidente e impacto.
En las actividades para la eliminación de la causa del incidente o eliminación de todo rastro de los daños (erradicación), se realiza la eliminación de aquellos componentes asociados al incidente para resolverlo o prevenir futuras ocurrencias.
Las siguientes actividades son una de las maneras de hacerlo:
Aislar los servicios, servidores y en general los recursos. informáticos afectados.

Bloquear el acceso al sistema cuando sea necesario.
Instalar los parches de seguridad, cambios de reglas del firewall o de listas de acceso en dispositivos de red.
Analizar información resultante del incidente.
Definir plan de acción para la implantación de acciones correctivas para evitar reincidencias.
Identificar amenazas a partir del incidente presentado.
Notificar sobre disponibilidad de los sistemas.
Ejecutar las acciones adicionales que se consideren pertinentes.

Investigación

Se deben recoger evidencias de los incidentes para su utilización con fines de análisis y como posibles pruebas en caso de ser requerido el inicio de acciones legales. Las evidencias pueden ser de sistemas de información (archivos, imágenes de discos, equipos) o cualquier otra que se considere relevante para el análisis del incidente o para inicio de procedimientos legales. Hay que tener en cuenta los siguientes aspectos en el momento de recolectar evidencias:
AUTENTICIDAD: Quien haya recolectado la evidencia debe poder probar que es auténtica.
CADENA DE CUSTODIA: Debe existir un registro detallado del tratamiento de la evidencia, incluyendo quiénes, cómo, dónde y cuándo la transportaron, almacenaron y analizaron, a fin de evitar alteraciones o modificaciones que comprometan la misma.
Actividades Post-Incidentes.
Notificar al Líder de seguridad de la información acerca de las acciones realizadas.
Documentar el incidente.

Cerrar incidente.

7.1.4.14.1.2 A.16.1.2 Reporte de eventos de seguridad de la información

- Todos los funcionarios, colaboradores y partes interesadas, que tengan acceso a información interna, confidencial (clasificada) y/o altamente confidencial (reservada), independiente de su medio de conservación física o digital, deben:

a. Reportar de manera oportuna y a través de los medios establecidos por la entidad, los eventos o incidentes de seguridad de la información técnicos y no técnicos, donde se puedan ver comprometidos la confidencialidad, integridad y disponibilidad de los activos de información. Lo anterior siguiendo los lineamientos del procedimiento de Gestión de Incidentes de seguridad de la información.
b. Para el reporte de eventos o incidentes de seguridad de la información se deberá tener en cuenta entre otras las siguientes situaciones:

- ✓ un control de seguridad ineficaz;
- ✓ violación de la integridad, confidencialidad o expectativas de disponibilidad de a
- ✓ información;
- ✓ errores humanos;
- ✓ no conformidades con políticas o directrices;
- ✓ violaciones de acuerdos de seguridad física;
- ✓ cambios no controlados en el sistema;
- ✓ mal funcionamiento en el software o hardware;
- ✓ violaciones de acceso.

7.1.4.14.1.3 A.16.1.3 Reporte de debilidades de seguridad de la información

a. Los funcionarios, colaboradores y partes interesadas de la UNP, que hagan uso de la infraestructura tecnológica de la entidad, deben informar a través de los canales oficiales establecidos por la Entidad y de acuerdo con el procedimiento de Gestión de incidentes de seguridad de la información, aquellas debilidades que puedan comprometer los activos de información.
b. El incumplimiento al uso adecuado de los activos de información de la UNP por los funcionarios, colaboradores y partes interesadas podría ser interpretado como un mal uso potencial derivando en la respectiva investigación y sanciones según el caso.

7.1.4.14.1.4 A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos

a. El centro de servicios debe analizar el caso reportado y de acuerdo con los criterios de verificación se determinará si es un evento o un incidente, para realizar la gestión respectiva.
b. La UNP deberá consolidar una base de datos de conocimiento que podrá ser utilizada como apoyo para gestionar incidencias de seguridad relacionados.

7.1.4.14.1.5 A.16.1.5 Respuesta a incidentes de seguridad de la información

a. La UNP, debe designar personal calificado, para gestionar adecuadamente los incidentes de seguridad de la información reportados, siguiendo los lineamientos del procedimiento Gestión de incidentes de seguridad de la información, para garantizar la seguridad y la continuidad de los servicios comprometidos.
b. La respuesta a incidentes de seguridad de la información debe contemplar entre otras las siguientes condiciones:

- Recolectar la evidencia lo más pronto posible después de que ocurra el incidente;
- Llevar a cabo análisis forense de seguridad de la información, según se requiera;

- Llevar el asunto a una instancia superior (escalar), según se requiera;
- Asegurarse de que todas las actividades de respuesta involucradas se registren (Logged) adecuadamente para análisis posterior;
- Comunicar la existencia del incidente de seguridad de la información o de cualquier detalle pertinente a él, al personal interno o externo a las organizaciones que necesitan saberlo;
- Tratar las debilidades de seguridad de información que se encontraron que causan o contribuyen al incidente;
- Una vez que el incidente se haya tratado exitosamente, cerrarlo formalmente y hacer un registro de esto.

7.1.4.14.1.6 A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información

a. Las lecciones aprendidas a través de los incidentes de seguridad de la información deben ser socializadas con todos los funcionarios, colaboradores y partes interesadas según corresponda, como ejemplos de lo que podría ocurrir, cómo responder a estos incidentes y cómo evitarlos en el futuro.

7.1.4.14.1.7 A.16.1.7 Recolección de evidencia

a. La UNP incluye en el procedimiento Gestión de incidentes de seguridad de la información actividades para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia con propósitos de acciones legales y/o disciplinarias.

    - La identificación, es el proceso que involucra la búsqueda, reconocimiento y documentación de evidencia potencial.
    - Recolección, es el proceso de reunir elementos físicos que pueden contener evidencia potencial.
    - Adquisición, es el proceso de crear una copia de los datos dentro de un grupo definido.
    - Preservación, es el proceso de mantener y salvaguardar la integridad y la condición original de la evidencia potencial.

b. La UNP se asegura que la identificación, recolección, adquisición y preservación de evidencias, sea realizado por personal idóneo donde se cumpla con las siguientes características:

- La cadena de custodia;
- La seguridad de la evidencia;
- La seguridad del personal;
- Los roles y responsabilidades del personal involucrado;
- La competencia del personal;
- La documentación;
- Las sesiones informativas

Si no se cuenta con las capacidades (conocimiento, herramientas y demás), esta actividad deberá ser contratada externamente o apoyada con las autoridades competentes.

7.1.4.15 A.17. Aspectos de seguridad de la información de la gestión de continuidad de negocio

Dominio/ Control: A.17 Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio.
Objetivo: La Continuidad de Seguridad de la Información se debería incluir en los Sistemas de Gestión de la Continuidad de Negocio de la organización.
Alcance: La presente Política establece que la UNP, debe determinar sus requisitos para la Continuidad del Negocio, basados en la planificación, implementación y verificación de los mismos, para todos los procesos de la Entidad.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.15.1 A.17.1 Continuidad de la seguridad de la información

7.1.4.15.1.1 A.17.1.1 Planificación de la continuidad de la seguridad de la información

La entidad debe realizar el diagnóstico del estado de la continuidad de la seguridad de la información, definir el plan (costo-beneficio) para cerrar las brechas identificadas y proveer los recursos suficientes para proporcionar una respuesta efectiva de sus funcionarios, colaboradores y procesos en caso de contingencia o eventos catastróficos que afecten la continuidad de la operación de la entidad. Este plan debe contener al menos los siguientes elementos:

a. Análisis de impacto del negocio identificando los procesos claves y los tiempos de recuperación. Especificaciones de TI, comunicaciones, sistemas, personal interno y contactos de emergencia.

b. Diseñar una estrategia de continuidad que salvaguarde la información esencial (indispensable para la operación de la entidad) donde incluyan contención, backup y recuperación, sitio alterno, cubrimiento de seguros entre otros.
c. Actividades de recuperación del negocio, fase de pruebas, simulacros y entrenamiento.
d. La UNP a través de la oficina de planeación e información; debe liderar el Plan de Continuidad del Negocio y el grupo de mejoramiento continuo debe promover que los procesos documenten procedimientos alternos que sean usados en caso de contingencias (falta de acceso a uno o varios recursos que regularmente estarían accesibles) para asegurar el nivel de Continuidad requerido para la Seguridad de la Información durante una situación adversa.

7.1.4.15.1.2 A.17.1.2 Implementación de la continuidad de la seguridad de la información

a. El grupo de gestión de tecnologías de la información, debe elaborar el Plan de Recuperación Ante Desastres (DRP) y retorno a la normalidad, para cada uno de los Servicios y Sistemas de Información que tengan un impacto alto en los Procesos de la UNP.
b. La UNP debe establecer, documentar, aprobar, implementar y mantener planes, procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
c. La UNP, debe contar con una estructura de gestión adecuada para prepararse, mitigar y responder ante un evento perturbador usando personal con la autoridad, experiencia y competencias.
d. Todos los procesos son responsables de la identificación, establecimiento y documentación de protocolos alternos y en la ejecución del plan.

7.1.4.15.1.3 A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

a. La UNP, debe asegurar la realización de pruebas periódicas del Plan de Recuperación Ante Desastres (DRP) y/o Continuidad de Negocio, verificando la Seguridad de la Información durante su realización y la documentación de dichas pruebas
b. La UNP, debe verificar a intervalos regulares los controles de Continuidad de la Seguridad de la Información, implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
c. Para dar cumplimiento a los requisitos de la continuidad de la seguridad de la información, la UNP debe elabora y mantener actualizado su Plan de continuidad del negocio.

7.1.4.15.2 A.17.2 Redundancias

7.1.4.15.2.1 A.17.2.1 Disponibilidad de instalaciones de procesamiento de información

a. El grupo de gestión de tecnologías de la información, debe asegurar la disponibilidad de instalaciones de Procesamiento de Información de la UNP y propender por la existencia de una Plataforma Tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables, de acuerdo con los niveles de servicio establecidos por la Entidad.
b. El grupo de gestión de tecnologías de la información, debe analizar y establecer los requerimientos de redundancia para los Sistemas de Información esenciales para la Entidad y la Plataforma Tecnológica que los apoya.
c. El grupo de gestión de tecnologías de la información, debe evaluar y probar soluciones de redundancia Tecnológica y seleccionar la solución que mejor cumple los requerimientos de la Entidad.
d. El grupo de gestión de tecnologías de la información, a través de sus funcionarios, colaboradores y partes interesadas, deben administrar las soluciones de redundancia tecnológica y realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad de la Entidad.

7.1.4.16 A.18. Cumplimiento

Dominio/ Control: A.18 Cumplimiento.
Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con Seguridad de la Información y de cualquier requisito de Seguridad.
Alcance: La presente Política establece que se debe dar cumplimiento a los requisitos estatutarios, reglamentarios y contractuales pertinentes, establecidos por la Entidad a través de las Políticas de Seguridad y Privacidad de la Información.
Lineamientos:
Se debe dar cumplimiento a los siguientes lineamientos:

7.1.4.16.1 A.18.1 Cumplimiento de requisitos legales y contractuales

7.1.4.16.1.1 A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales

a. La Entidad, identifica los requisitos estatutarios, reglamentarios y contractuales relacionados con la seguridad de la información, formalizados a través del normograma institucional en lo que respecta al modelo de seguridad y privacidad de la información y del SGSI.

7.1.4.16.1.2 A.18.1.2 Derechos de propiedad intelectual

a. La entidad implementará las medidas a que haya lugar para asegurar el cumplimiento de ley y requerimientos regulatorios y contractuales acerca de la propiedad intelectual (derechos de autor, patentes, entre otros) y el uso de productos de software.

- Adquirir software solo a través de fuentes conocidas y confiables, para asegurar que no se violen los derechos de autor.
- Crear conciencia sobre los derechos de propiedad intelectual.
- El grupo de gestión de tecnologías de la información, debe garantizar que solo haya instalado software autorizado y productos con licencia.
- Está prohibido reproducir total o parcialmente libros, artículos, reportajes, música, software u otros documentos diferentes de los permitidos por la ley de derechos de autor.
- El grupo de gestión de tecnologías de la información, debe establecer la línea base de software autorizado para ser instalado en las estaciones de trabajo.

7.1.4.16.1.3 A.18.1.3 Protección de registros

La protección de los registros de los activos de información es responsabilidad de la Entidad, de los funcionarios, contratistas y partes interesadas, quienes deben propender por :

a. Proteger los registros contra perdida, destrucción, falsificación y acceso no autorizado; para dar cumplimiento a los Requisitos Legales.
b. Garantizar la confidencialidad, integridad y disponibilidad de la información, teniendo en cuenta su clasificación de acuerdo con el nivel de importancia.
c. Definir los periodos de retención y conservación de la información. Los registros correspondientes a información confidencial (clasificada) o altamente confidencial (Reservada) deben ser protegidos independiente de los medios de conservación, ya sea física o digital.
d. Los registros se deben clasificar por tipos de registros, por ejemplo, registros contables, registros de bases de datos, registros de transacciones (Logs), registros de auditoría (Audit Logs) y procedimientos operacionales, cada uno con detalles de los períodos de retención y tipo de medio de almacenamiento permisible, por ejemplo, papel, microfichas, medios magnéticos, medios ópticos.
e. Cuando se escogen medios de almacenamiento electrónico, se deben establecer procedimientos para acceder a los datos (legibilidad de medios y de formatos) durante todo el período de retención, para proteger contra pérdida debido a cambios futuros en la tecnología.

f. Se debe emitir directrices acerca de la retención, almacenamiento, manejo y disposición de registros e información, de acuerdo con los lineamientos del procedimiento establecido para ello.

7.1.4.16.1.4 A.18.1.4 Privacidad y protección de información de datos personales

La UNP en cumplimiento de lo establecido en la normatividad legal vigente aplicable a la privacidad y protección de datos personales en Colombia, actúa como Responsable de los datos personales que por virtud de sus funciones y competencias legalmente establecidas, le han sido suministradas y se encuentran en sus bases de datos siendo cada de una de las dependencias de la Entidad él o la Encargada del tratamiento.

a. Por tanto, la UNP podrá dar tratamiento a los datos personales de TITULARES con los cuales tiene, ha tenido o espera tener algún tipo de relación, cualquiera sea su naturaleza (civil, comercial y/o laboral, etc.) y entre los cuales se incluyen, pero sin limitarse, los grupos de interés (usuarios directos, usuarios indirectos, terceros relacionados y entidades externas), sin detrimento de lo estipulado en las normas aplicables tanto externas como internas para tales efectos.
b. Salvo en los casos exceptuados por la ley, la UNP solicitará a más tardar en la recolección de la información, autorización del TITULAR para capturar, almacenar, procesar, usar, circular, suprimir y en todo caso tratar los datos personales que hayan sido suministrados a la entidad por cualquier medio, bien sea digital, físico, verbal, telefónico o cualquier otro formato que sea susceptible de ser consultado y en desarrollo de su objeto social o con ocasión de cualquier tipo de relación civil o comercial que llegue a surgir en virtud de sus actividades conexas o propias de su naturaleza; dicha autorización deberá estar contenida en un documento físico o electrónico o en cualquier medio que pueda ser posteriormente constatado o verificado.
c. Para todos los efectos, se entiende que la autorización por parte de los TITULARES a favor de la UNP para el suministro y/o tratamiento de sus datos personales, realizada a través de los canales físicos o electrónicos, o por escrito o mediante conductas inequívocas, es:
    - Expresa y voluntaria, lo que implica que EL TITULAR y/o sus representantes, según sea el caso, acepta todo el contenido de la presente y le concede(n) a la UNP su autorización para que utilice dicha información personal conforme a las estipulaciones de la presente política, la cual también está publicada en la página web www.unp.gov.co obligándose a leerla, conocerla y consultarla en desarrollo del derecho que le asiste como TITULAR de datos personales.

- En el evento en que desee manifestar su negativa frente a la mentada autorización o solicitar la supresión de la información, podrá ejercer su derecho a través de los canales dispuestos por la entidad o en cualquiera de los puntos de atención al ciudadano, dentro de los 15 días hábiles siguientes a la implementación y publicación de la Política de Privacidad y Protección de Datos Personales de la UNP.
- Una vez vencido el periodo señalado anteriormente, la UNP podrá mantener un tratamiento sobre los datos suministrados con anterioridad a esta legislación, en atención a lo consagrado en el numeral cuarto del artículo 10° del Decreto 1377 de 2013, sin perjuicio de la facultad que el TITULAR de la Información de ejercer en cualquier momento su derecho a pedir la eliminación del dato.
- No obstante, se hace la salvedad que de conformidad al artículo 9 del decreto 1377 del año 2013, la solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el TITULAR de esta, tenga un deber legal o contractual de permanecer en la base de datos de la entidad.

d. Por su parte, la UNP asegura un manejo adecuado de los datos personales recolectados en sus bases de datos, registros de Ingreso a las instalaciones, registro fotográfico, firmas de asistencia, y de más medios de recolección, con el fin de proteger la privacidad de la misma y conservarla bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, así como el respeto de los derechos del TITULAR, según lo estipulado en la ley. De esta manera la entidad manifiesta que garantiza los derechos de privacidad e intimidad en el tratamiento de los datos personales, en consecuencia todas sus actuaciones se regirán por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.
e. Todas las personas que en desarrollo de diferentes actividades, contractuales, laborales, entre otras, sean permanentes u ocasionales, llegaran a suministrar a la UNP cualquier tipo de información o dato personal, podrá conocerla, actualizarla y rectificarla
f. En efecto, la UNP:

- Garantiza al TITULAR, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Conserva la información bajo las condiciones de Seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Realiza oportunamente la actualización, rectificación o supresión de los datos en los términos que estipula la ley.
- Actualiza la información reportada por los Encargados del Tratamiento en los términos que estipula ley.

- Tramita las consultas y los reclamos formulados por los TITULARES en los términos señalados en la ley.
- Se abstiene de circular información que esté siendo controvertida por el TITULAR y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permite el acceso a la información únicamente a las personas que pueden tener acceso a ello.
- Informa a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los TITULARES.
- Cumple las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

g. Cualquier consulta, reclamo o requisito debe ser dirigido a través de los diferentes sitios y canales de atención dispuestos por la UNP para tal fin, los cuales se pueden consultar en la página web www.unp.gov.co

7.1.4.16.1.5 A.18.1.5 Reglamentación de controles criptográficos

Se deben implementar controles criptográficos, en cumplimiento de la normatividad, acuerdos y reglamentación pertinentes.

7.1.4.16.2 A.18. 2 Revisiones de seguridad de la información

7.1.4.16.2.1 A.18.2.1 Revisión independiente de la seguridad de la información

La Entidad, deberá realizar auditorias al Sistema de Gestión de Seguridad de la Información, con el fin de llevar a cabo la mejora continua.
Estas auditorias deberán ser programadas previamente con ciclos preestablecidos y ser ejecutadas por un grupo de Auditores externos al sistema con independencia del mismo, y deberá ser coordinadas por la segunda Línea de defensa del sistema.
La oficina de control interno es parte interesada en el proceso de auditoría y en el proceso operación del sistema.

7.1.4.16.2.2 A.18.2.2 Cumplimiento con las políticas y normas de seguridad

a. Las políticas, procedimientos, y demás normatividad relacionada con seguridad de la información, implementada por la UNP, es de obligatorio cumplimiento para los funcionarios, colaboradores y partes interesadas y que por su naturaleza en su relación con la entidad tengan acceso a cualquier tipo de información.

b. Se debe asegurar por los directivos en cada área, la aplicación por parte de los funcionarios, colaboradores y partes interesadas, de las políticas, los procedimientos y demás controles de seguridad de la información definidos por la Entidad.
c. El incumplimiento a la Política de Seguridad y Privacidad de la información de la Entidad, traerá consigo, las consecuencias legales que aplique a la normatividad vigente.

7.1.4.16.2.3 A.18.2.3 Revisión del cumplimiento

a. El grupo de gestión de tecnologías de la información debe asegurar que se realicen revisiones periódicas a la implementación de las políticas y de los controles de seguridad de la información en los sistemas de información y los servicios tecnológicos.
b. La valoración de vulnerabilidades y las pruebas de penetración (Penetration Test) deben ser realizadas por personal idóneo para:

    - Identificar fallos en las actualizaciones de los sistemas.
    - Examinar la eficacia de los controles.
    - Establecer medidas correctivas antes de que estos fallos puedan suponer una amenaza real para los sistemas y servicios tecnológicos.

c. De acuerdo con el resultado de la valoración de vulnerabilidades y las pruebas de penetración se debe tener en cuenta:

    - Informar al responsable del activo, al grupo de gestión de tecnologías de la información y al Oficial de Seguridad de la Información.
    - Priorizar el tratamiento soportado en un análisis de riesgos.
    - Documentar las acciones tomadas.
    - Aplicar gestión del cambio.

7.1.4.16.2.4 Vigencia de las políticas

Las políticas descritas en este documento regirán a partir de la fecha de aprobación y publicación de la misma.

8. DOCUMENTOS RELACIONADOS

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

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.	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
	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.				
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.	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
	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.				

	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. 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. Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la institución. Establecer directrices y hacer seguimiento a los controles definidos en los procedimientos, estándares, guías, instructivos y buenas prácticas 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. 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. 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.	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	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. 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. Desarrollar las actividades de coordinación de la Seguridad de la Información y seguridad Informática de la entidad. 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. Reportar los Incidentes de alto Impacto a la Gerencia 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
	Fomentar la mejora continua del Sistema de Gestión de Seguridad de la Información de la entidad.				

	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.	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
	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				
	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	No aplica	Información acerca de incumplimientos, cambios, mejoras o necesidades frente al tratamiento de datos oportuno	CISO	Cuando exista el requerimiento
	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.				
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 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
	Informar sobre la confiabilidad y la integridad de la información y las exposiciones a riesgos asociados y las violaciones a estas.				
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	No aplica	Información acerca de incumplimientos, cambios, mejoras o necesidades frente al tratamiento de datos oportuno	CISO	Cuando exista el requerimiento
	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.				
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 específicos de operación respecto a la seguridad y privacidad de la información de la UNP.	10/12/2020	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