UNP

Manual

DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

GTE-MA-02-V4

Gestión Tecnológica
UNIDAD NACIONAL DE PROTECCIÓN
01-11-2024

Tabla de Contenido

INTRODUCCIÓN

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, políticas y herramientas para la gestión eficaz de acceso a la información y la implementación de mecanismos y controles de seguridad tanto físicos como lógicos, orientados a la prevención y detección de amenazas que puedan afectar la seguridad de la organización y la continuidad del negocio.

El presente documento se encuentra alineado con el marco de referencia de arquitectura de TI, Manual Integrado de Planeación y Gestión (MIPG) y el Manual de Seguridad y Privacidad de la Información quienes actúan como habilitadores transversales de la política de Gobierno Digital desarrolladas en las guías de orientación definidas en el interior de este documento.

Su finalidad es establecer los principios y lineamientos orientadores de la seguridad de la información en la UNP, implementar las directrices para la aplicación de mecanismos que eviten la vulneración de la seguridad y privacidad de la información, orientados en la mejora continua y el desempeño del Sistema de Gestión de Seguridad de la Información-SGSI con el objetivo de orientar 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.

1. OBJETIVO

Definir los lineamientos que deben apropiar y seguir los servidores públicos, contratistas, colaboradores y todas las partes interesadas de la Unidad Nacional de Protección con el fin de fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información, enmarcados en el Anexo A de la ISO 27001:2022, basados en la identificación, valoración, tratamiento y monitoreo de los riesgos de seguridad y privacidad de la información, la gestión de incidentes de seguridad y velar por la protección de su confidencialidad, integridad y disponibilidad, asegurando el mantenimiento y la mejora continua del SGSI.

2. ALCANCE

El presente manual inicia con la definición, cumplimiento e implementación en la Entidad, de las políticas específicas del Sistema de Seguridad y Privacidad de la Información; sigue con su apropiación y cumplimiento según los lineamientos establecidos por MinTic adaptados a la UNP, continua con la sensibilización para su apropiación y cumplimiento, y concluye con la mejora continua del MSPI

El cumplimiento del presente manual es obligatorio para todos los procesos de la Entidad, servidores públicos, contratistas, colaboradores, personal vinculado a la UNP y todas las partes interesadas con acceso a la información institucional.

3. DEFINICIONES

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. (Norma ISO 27000)

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. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

Causa: Factores internos o externos, medios, circunstancias y agentes que generan los riesgos. Se pueden clasificar en cinco categorías: personas, materiales, instalaciones y entorno. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

Ciberespacio: 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. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados. (Norma ISO 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. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

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. (Norma ISO 27000).

Dato: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (Norma ISO 27000)

Impacto. Cambio adverso en el nivel de los objetivos del negocio logrados. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

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". (Norma ISO 27000)

Información: Conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. (Ley 1712 de 2014)

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. (Norma ISO 27000), Propiedad de la información relativa a su exactitud y completitud. (Norma ISO 27000)

Metodología ágil: es un conjunto de técnicas aplicadas en ciclos de trabajo cortos, con el objetivo de que el proceso de entrega de un proyecto sea más eficiente. Así, con cada etapa completada, ya se pueden entregar avances y se deja de lado la necesidad de esperar hasta el término del proyecto**. (**fuente**:** https://www.zendesk.com.mx/blog/metodologia-agil-que-es/)

Metodología ágil Scrum: es un marco de trabajo ágil a través del cual las personas pueden abordar problemas complejos adaptativos a la vez que se entregan productos de forma eficiente y creativa con el máximo valor. Así, Scrum es una metodología que ayuda a los equipos a colaborar y realizar un trabajo de alto impacto (fuente: https://asana.com/es/resources/what-is-scrum)

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. (Norma ISO 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. (Norma ISO 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. (Norma ISO 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. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

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. (Norma ISO 29110)

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. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

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. (Guía de Administración del Riesgo y el Diseño de Controles en Entidades Públicas – DAFP)

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (Norma ISO 27000).

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

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

4. RESPONSABILIDADES

La Alta Dirección de la Unidad Nacional de Protección - UNP es responsable de garantizar que la seguridad y privacidad de la información se comunique y gestione adecuadamente en la Entidad.

Los servidores públicos, contratistas y partes interesadas de la Entidad tienen la responsabilidad de mantener la seguridad y privacidad de acuerdo con el presente documento establecido por la Unidad Nacional de Protección - UNP.

5. MARCO LEGAL

A continuación, se relaciona la normativa que aplica al Manual de Políticas Específicas de Seguridad y Privacidad de la Información.

Item	Número	Descripción - Epígrafe
1	Constitución Política 1993	Artículos 15. Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.
2	Ley 1273 de 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.
3	Ley 1474 de 2011	Por la cual se dictan Políticas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
4	Decreto Ley 4065 de 2011	Por el cual se crea la Unidad Nacional de Protección (UNP), se establecen su objetivo y estructura.
5	Ley 1581 de 2012	“Por la cual se dictan disposiciones generales para la protección de datos personales”.
6	Ley 1712 de 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”.
7	Ley 1915 de 2018	“Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos”.

Item	Número	Descripción - Epígrafe
8	Ley 1341 de 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 de Espectro y se dictan otras disposiciones".
9	Decreto 1377 de 2013	**"Por el cual se reglamenta parcialmente la Ley 1581 de 2012**, **Derogado Parcialmente por el Decreto 1081 de 2015".**
10	Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública
11	Decreto 1499 de 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".
12	Decreto 1078 de 2015 (DUR-TIC),	"Por medio del cual se expide el Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones".
13	Decreto 2106 de 2019,	"Por el cual se dictan Políticas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública".
14	Decreto 767 de 2022	"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".
15	Decreto 1263 de 2022	"Por el cual se adiciona el Título 22 a la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de definir lineamientos y estándares aplicables a la Transformación Digital Pública"
16	Decreto 1227 de 2022	Por el cual se modifican los artículos 2.2.1.5.3, 2.2.1.5.5, 2.2.1.5.8 y 2.2.1.5.9. y se adicionan los artículos 2.2.1.5.15 al 2.2.1.5.25 al Decreto 1072 de 2015, Único Reglamentario del Sector Trabajo, relacionados con el Teletrabajo.
17	Directiva Presidencial N° 4 de 2012	Eficiencia Administrativa y Lineamientos de la Política Cero Papel en la Administración Pública.
18	Directiva Presidencial N° 9 de 2018	Directrices de Austeridad
19	Resolución 0054 de 2024	"Por medio de la cual se actualiza la Plataforma Estratégica de la Unidad Nacional de Protección – UNP para el período 2023-2026 y se deroga la Resolución 0199 del 2 de marzo de 2020"

Item	Número	Descripción - Epígrafe
20	Resolución 1291 de 2023	Por medio de la cual se modifica el artículo 1 de la Resolución 0298 de 31 de febrero de 2022.
21	Resolución 1519 de 2020	"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos". - Min Tic
22	Resolución UNP 1767 de 2024	- Por la cual se organiza el modelo integrado de Planeación y Gestión y deroga Resolución 1023 de 2022 de la UNP
23	Resolución 932 de 2023	Por medio de la cual se crea el Grupo de las Tecnologías (GGT) y modifica parcialmente la Resolución número 501 de 2021.
24	Resolución 1291 de 2023	Por medio de la cual se modifica el artículo 1 de la Resolución 0298 de 31 de febrero de 2022 (Política MIPG -SIG)
25	Resolución No. 2460 de 2022	"Por medio de la cual se regula la Política de Teletrabajo en la Unidad Nacional de Protección, se derogan las Resoluciones 1228 y 1826 de 2021, y se dictan otras disposiciones"
26	Resolución 500 de 2021	Por el cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el manual de seguridad y privacidad como habilitador de la política de Gobierno Digital
27	CONPES 3854 de 2016	Política Nacional de Seguridad Digital. Busca fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia.
28	CONPES 3995 de 2020	Política Nacional de Confianza y Seguridad Digital Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de manuales con énfasis en nuevas tecnologías".
29	Norma Técnica Colombia NTC-ISO/IEC 27002	Seguridad de la información, ciberseguridad y protección de la privacidad Control de la seguridad de la información
30	Norma Técnica Colombiana NTC-ISO/IEC 27001	Sistemas de Gestión de la Seguridad de la Información. Política Técnica
31	Norma Técnica Colombiana NTC-ISO 9001	Sistemas de Gestión de la Calidad.

Item	Número	Descripción - Epígrafe
32	Norma Técnica Colombiana NTC-ISO 22301	Sistemas de Gestión de la Continuidad del Negocio

Fuente: Elaboración propia

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 controles de seguridad tanto físicos como lógicos, orientados a la prevención y detección de amenazas 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.

La Información Documentada que se mantiene en el Sistema de Gestión de Seguridad y Privacidad de la Información, se desarrolla teniendo como referencia las buenas prácticas de gestión y control establecidas por el Ministerio de las Tecnologías de la Información y las Comunicaciones - MINTIC, las directrices dadas por la Función Pública DAFP y los requisitos establecidos en la Norma Internacional ISO/IEC 27001:2022, que han sido aceptados por la Unidad Nacional de Protección – UNP y se describen de la siguiente manera:

7. CONTENIDO

Las políticas Específicas de seguridad y privacidad de la información 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 27001:2022 aceptados por la Unidad Nacional de Protección - UNP

7.1 Política General de Seguridad y Privacidad de la Información

La Entidad, en la política vigente en la materia se compromete a proteger y preservar la integridad, confidencialidad, disponibilidad y privacidad de los activos de seguridad de la información, mediante la implementación de controles organizacionales, físicos, de personas y tecnológicos; orientados a establecer un marco de confianza en el ejercicio de

la misionalidad institucional, prevenir incidentes de seguridad de la información, propender por la continuidad de la operación de los servicios, promover la mejora continua del MSPI.

En consonancia con lo anterior, las políticas que se desarrollan a continuación tienen como referencia las buenas prácticas definidas en el Manual de Seguridad y Privacidad de la Información – MSPI establecidas por el Ministerio de las Tecnologías de la Información y las Comunicaciones - MINTIC, las directrices dadas por la Función Pública DAFP y los requisitos establecidos en la Política Internacional ISO/IEC 27001:2022.

Las siguientes políticas aplican a todos las personas, servidores públicos, contratistas, y partes interesadas que, por su rol, hagan uso de dispositivos móviles en la Entidad y las cuales son de obligatorio cumplimiento. Los lineamientos de seguridad aquí definidos están clasificados en temáticas, teniendo en cuenta el contexto interno y externo de la Entidad.

7.1.1 Objetivos de la Política de Seguridad y Privacidad de la Información.

La Política de Seguridad y Privacidad de la Información de la Unidad Nacional de Protección tendrá los siguientes objetivos:

1. Contribuir a la gestión integral de los riesgos de seguridad y privacidad de la información y de seguridad digital en la Unidad Nacional de Protección.
2. Mitigar el impacto de los incidentes de seguridad de la información de la Unidad Nacional de Protección de forma efectiva, eficaz y eficiente.
3. Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información.
4. Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital, orientados a la mejora continua y al alto

El Sistema de Gestión de Seguridad y Privacidad de la Información – en adelante SG-SPI - de la Unidad Nacional de Protección tiene tres compromisos de cumplimiento que se enuncian a continuación:

- Gestionar los riesgos de seguridad y privacidad de la información, implementando los controles necesarios que permitan proteger la integridad, confidencialidad y disponibilidad de acuerdo con su clasificación.

- Impulsar una cultura en seguridad y privacidad de la información con las partes interesadas pertinentes, a través del desarrollo de programas de divulgación y toma de conciencia.

- Implementar controles dentro del proceso de Gestión Tecnológica que permita mantener los niveles de disponibilidad definidos para que los procesos cumplan sus objetos.

Estos compromisos se despliegan a su vez en los siguientes objetivos:

1. Implementar los controles del Modelo de Seguridad y Privacidad de la Información - MSPI a partir de los requisitos de seguridad con el propósito de gestionar los riesgos y preservar la confidencialidad, integridad y disponibilidad de los activos de información.

2. Promover la cultura de seguridad y privacidad de la información.

3. Definir y mantener actualizados los servicios de TI que permitan el cumplimiento de los objetivos estratégicos institucionales.

A través de la aplicación de acciones de gestión en la implementación de estos objetivos, se busca alcanzar los principios del sistema establecidos en el Modelo de Seguridad y Privacidad de la Información MS-PI, los cuales son los siguientes:

- ✓ Responsabilidad frente a la seguridad y privacidad de la Información.

- ✓ Proteger la información generada, procesada, transmitida, resguardada, entre otras.
- ✓ Aplicación de Controles de acuerdo con la Clasificación de la Información.
- ✓ Proteger la información de la UNP de las amenazas internas y externas.
- ✓ Proteger las instalaciones de procesamiento y la infraestructura tecnológica.
- ✓ Controlar la operación de los procesos de la UNP.
- ✓ Implementar controles de acceso a la información, los sistemas y los recursos de la Red de datos institucional.
- ✓ Garantizar que la Seguridad sea parte integral del Ciclo de Vida de los Sistemas de Información.
- ✓ Garantizar el mantenimiento a través de la adecuada gestión de riesgos de seguridad.
- ✓ Garantizar la Disponibilidad y Continuidad de la Operación basada en el impacto.
- ✓ Cumplimiento de las obligaciones legales, regulatorias y contractuales.
- ✓ Revisión y actualización del manual de Políticas de Seguridad y Privacidad de la Información.

7.2 Políticas Específicas

7.2.1 Política de Dispositivos Móviles

La presente Política aplica a todos los servidores públicos, contratistas, terceros y partes interesadas que, por su rol, hagan uso de dispositivos móviles en la Entidad.

CONTROL	RESPONSABILIDADES
5.15 Control de acceso 5.18 Derechos de acceso	La asignación de dispositivos móviles institucionales está a cargo de los grupos internosde trabajo que implementan medidas de protección de la Subdirección de Protección yla Subdirección Especializada de Seguridad y Protección, previa autorización del jefe de área correspondiente y la Secretaría General.
	La autorización del uso de dispositivos móviles será realizada por un servidor público o contratista de la Entidad, previa justificación de la necesidad funcional del servicio
	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
	Los equipos móviles personales o de terceros que se encuentren conectados a lared de la Entidad y estos no sean avalados y autorizados por El Grupo de Gestión de las Tecnologías serán catalogados como: “Equipos no autorizados” y se podrá considerarcomo un incumplimiento a las Políticas de Seguridad y Privacidad de la Información definidas por la Entidad. Estos dispositivos se bloquearán a través de los controles operacionales propios del proceso por medio de la controladora Wi-Fi definida en la mesa de servicios de la Entidad
	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

Fuente: Elaboración propia

7.2.2 Política de Dispositivos Removibles

CONTROL	RESPONSABILIDADES
5.15 Control de acceso 5.18 Derechos de acceso 5.11 Devolución de activos 8.1 Dispositivos de punto final 8.3 Restricción de acceso a la información	El uso de medios de almacenamiento removibles está restringido en la UNP
	La Unidad Nacional de Protección reconoce que el único medio autorizado para el tratamiento de datos personales es el dueño de la información, de acuerdo con la Ley de protección de datos personales 1581 de 2012 y el decreto 1377 o la que la adicione, modifique o derogue.
	Es responsabilidad del jefe usuario solicitar el servicio de los medios removibles de forma clara con justificación al Coordinador de GGT o quien haga sus veces, quien estudia, evalúa y autoriza la solicitud y proporcionará las soluciones tecnológicas, y comunicará a la mesa de servicios para que se realice la tarea y se pueda monitorear y verificar la actividad para actuar, en caso de que se evidencie una presencia de Programa maligno (Malware) y controlar los medios de almacenamiento removibles
	Toda la información relacionada en la Unidad Nacional de Protección se encuentra en un ambiente seguro y respaldada en OneDrive, Share Point, infraestructura (servidores), por lo que no hay justificación para utilizar medios removibles.
	En los tiempos de entrega del medio removible como se indica en el Formato

CONTROL	RESPONSABILIDADES
	GTE-FT-40 Solicitud de servicios medios removibles, esta información deberá ser borrada de forma segura; si ya no es requerida para el soporte y cumplimiento de sus funciones
	Todo medio de almacenamiento que sea propiedad de la UNP y que quiera ser retirado de sus instalaciones deberá ser notificado por los responsables de proceso y usuarios que tengan a cargo los elementos para proceder con la respectiva autorización por las áreas responsables de este proceso
	La información que se encuentre almacenada en los medios removibles deberá tener las condiciones adecuadas de seguridad de acuerdo con la clasificación definida. Es responsabilidad del jefes, servidor público y contratista a quien se autorizó el servicio del medio removible tome las medidas adecuadas para su almacenamiento y resguardo, así como evitar accesos no autorizados, daños pérdida de información o extravío del medio. Si se llegara a presentar alguno de estos casos. Esto se considera como incidente de seguridad de la información y deberán ser reportado inmediatamente a la mesa de servicios (plataforma tecnológica)
	Mesa de Servicios no debe exponer los medios de almacenamiento removibles a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.)
	Todo traslado o reasignación de equipos debe ser autorizado, ejecutado y debidamente registrado en el formato Transferencia de Bienes GABS-FT-10 por el actual y el nuevo responsable
	Cualquier dispositivo removible usado para actividades del negocio que contenga información sensible, no se deberá prestar a nadie y será responsabilidad exclusiva del servidor público que lo tenga asignado
	Los medios removibles no pueden ser empleados para la extracción de copias de respaldo y/o seguridad con miras a recuperación ante desastres, solo pueden ser utilizados como herramientas de apoyo frente al transporte de los datos e información requerida para el desarrollo Política de las funciones de la UNP
	El manejo de la información institucional en Medios Removibles está expuesta a riesgos, como pérdida, fuga o modificación, que compromete no solamente la información sino también la infraestructura tecnológica de la Entidad, por lo tanto, el Servidor público y/o contratista que los use será quien asuma las sanciones de ley aplicables en esta materia, siendo responsable de la seguridad

Fuente: Elaboración propia

7.2.3 Política de Teletrabajo

La Unidad Nacional de Protección – en cabeza de la Subdirección de Talento Humano establece los lineamientos del Teletrabajo en el marco de la Ley 1221 de 2008, Decreto reglamentario 0884 del 2012, Decreto 1227 de 2022 y la Resolución Interna 2460 de 2022:
Para dar cumplimiento a esta política se asignan las siguientes responsabilidades:

CONTROL	RESPONSABILIDADES
5.10 Uso aceptable de la información y otros activos asociados **5.15 Control de acceso** **5.16 Gestión de identidad** **5.18 Derechos de acceso** **6.2 Términos y condiciones de empleo** **6.6 Acuerdo de Confidencialidad o no Divulgación** **6.7 trabajo Remoto** **7.7 Escritorio y pantalla despejados** **7.9 Seguridad de los activos fuera de las Oficinas**	Los servidores públicos y/o contratistas deben tener en cuenta los lineamientos y directrices relacionados en el procedimiento GTH-PR-32 Procedimiento para la implementación del teletrabajo definido por la Subdirección de Talento Humano.
	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 establecidos por El Grupo de Gestión de las Tecnologías
	Será responsable del licenciamiento del Software de los equipos suministrados a los Teletrabajadores para su uso.
	Definir los tipos de usuarios que dispondrán de modalidad de Teletrabajo y los permisosde acceso remoto pertinentes
	Realizar la solicitud formal y autorización del Teletrabajo de acuerdo con los lineamientos definidos en el procedimiento oficializado en el SIG.
	Determinar las herramientas de conexión remota para atender requerimientos y problemas relacionados con Teletrabajo
	El Grupo de Gestión de las Tecnologías realizará seguimiento de las conexiones remotas a los servicios relacionados con el Teletrabajo.
	El Grupo de Gestión de las Tecnologías tendrá la responsabilidad de ejecutar cifrado de losDiscos Duros de los equipos asignados por la Entidad para las funciones de Teletrabajo

Fuente: Elaboración propia

7.2.3.1 Responsabilidades del Teletrabajadores

1. Cumplir con las Políticas de Seguridad y Privacidad de Información definidas y establecidas por la Entidad

2. Cuando se requiera, para acceder a los sistemas de información y/o servicios tecnológicos de la Entidad desde sitios remotos, se debe hacer uso de los mecanismos de conexión segura establecidos por la Entidad.
3. La solicitud de medios removibles solamente será justificado y autorizado a los Servidores Públicos contratistas con el aval del Supervisor del Contrato o jefe inmediato y cuya actividad la realizará mesa de servicios.

7.2.4 Política de Control de Acceso

CONTROL	RESPONSABILIDADES
5.10 Uso aceptable de la información y otros activos asociados **5.15 Control de acceso** **5.16 Gestión de Identidad** **5.17 Información de autenticación** **5.18 Derechos de acceso** **6.6 Acuerdo de Confidencialidad o no Divulgación** **6.7 trabajo Remoto** **8.3 Restricción de acceso a la información** **8.5 Autenticación segura**	La conexión remota a la red de área local para el acceso a la Unidad Nacional de Protección a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por El Grupo de Gestión de las Tecnologías, y mesa de servicios y esta debe ser solicitada por medio de la plataforma de mesa de servicio Ivanti.
	La conexión remota a la red de área local para el acceso a la Unidad Nacional de Protección a través de una conexión VPN, la cual debe ser aprobada, registrada y monitoreada por El Grupo de Gestión de las Tecnologías, y mesa de servicios y esta debe ser solicitada por medio de la plataforma de mesa de servicio Ivanti.
	El Grupo de Gestión de las Tecnologías, debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servidores y servicios publicados.
	El Grupo de Gestión de las Tecnologías, debe establecer una segregación de las redes, separando los entornos de red de usuarios de los entornos de red de servidores y servicios públicos
	El Grupo de Gestión de las Tecnologías, debe asegurar que las redes inalámbricas de la Entidad cuenten con métodos de autenticación que evite accesos no autorizados.
	El Grupo de Gestión de las Tecnologías para los eventos que se realicen en el Ministerio debe generar usuario y clave de red Wifi, el cual debe expirar una vez finalizado el evento
	El uso de recursos personales de procesamiento de información puede ocasionar riesgos de seguridad, por tal razón los servidores públicos, contratistas o terceros deben solicitar al proceso de Gestión Tecnológica previa autorización de uso y posteriormente se debe revisar que los recursos personales que se conecten a las redes de datos de la Unidad Nacional de Protección cumplan con todos los requisitos o controles para autenticarse y únicamente podrán realizar las tareas para las que fueron autorizados.

CONTROL	RESPONSABILIDADES
	Se deberá realizar el doble factor de autenticación para acceso, permisos y privilegios de los recursos otorgados por la Unidad Nacional de Protección UNP.

Fuente: Elaboración propia

7.2.5 Política de Gestión de Acceso, Administración de Usuarios y Cuentas Genéricas.

CONTROL	RESPONSABILIDADES
5.15 Control de acceso **5.16 Gestión de la identidad** **5.17 Información de autenticación** **5.18 Derechos de acceso** **6.6 Acuerdo de Confidencialidad o no Divulgación** **6.7 trabajo Remoto** **8.3 Restricción de acceso a la información** **8.5 Autenticación segura**	El Grupo de Gestión de las Tecnologías, debe controlar que los servidores públicos, colaboradores, proveedores o partes interesadas no puedan utilizar ninguna estructura o característica de contraseña que pueda dar como resultado una contraseña que sea predecible o deducible con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical que permita sea vulnerada.
	Se debe seguir los lineamientos y directrices enmarcados en el GTE-PR-40 Procedimiento de Administración y Creación de Cuentas de Usuario y Cuentas Genéricas definido en el SIG.
	Los Servidores Públicos, colaboradores, proveedores o partes interesadas no podrán compartir, prestar su usuario y/o contraseña es de uso personal e intransferible.
	El usuario de correo electrónico debe ser igual al usuario de red, y contar con single con (mismo usuario, misma contraseña) en los dos (2) servicios
	Después de (10) diez intentos fallidos al ingresar los datos de acceso, la cuenta debe quedar bloqueada, y sólo podrá ser desbloqueada por los responsables de mesa de servicios GGT
	El Grupo de Gestión de las Tecnologías sólo otorgará a los usuarios, los accesos solicitados y autorizados por el jefe inmediato, supervisor del contrato o un jefe de mayor jerarquía.
	Por defecto los usuarios creados no tienen permisos de administrador.
	El usuario y la contraseña asignados para el acceso a los diferentes servicios tecnológicos, es personal e intransferible. Cualquier actividad que se realice con el usuario y clave será responsabilidad del servidor público y contratista al cual le fue asignado.
	Una vez finalizada la gestión de servicios prestados por terceras partes para la Entidad, el supervisor de contrato debe garantizar que los accesos queden cerrados al finalizar el proceso o contrato.

CONTROL	RESPONSABILIDADES
	Todos los accesos de servicios de red deben estar conectados a la cuenta del directorio activo, si esta caduca, todos los accesos también, como son (VPN, cuentas de usuario, Sistemas de información, plataforma de servicios Ivanti, servicio de impresión, intranet y telefonía, etc.)
	El Grupo de Gestión de las Tecnologías, debe deshabilitar los servicios o funcionalidades no utilizadas de los sistemas operativos, el firmware, bases de datos y demás recursos tecnológicos.
	El Grupo de Gestión de las Tecnologías, debe mantener un listado actualizado con las cuentas que administren todos los recursos tecnológicos.
	Al usuario se le entrega una contraseña temporal cuando se le crea el usuario y es responsabilidad de él que cuando cree su propia contraseña tenga en cuenta los lineamientos y recomendaciones para tener una contraseña segura
	El Grupo de Gestión de las Tecnologías, debe establecer controles para que los usuarios finales de los servicios tecnológicos no tengan instalado en sus equipos de cómputo software o herramientas que permitan la obtención de privilegios no autorizados.

Fuente: Elaboración propia

7.2.5.1 Responsabilidades de los usuarios

CONTROL	RESPONSABILIDADES
5.15 Control de acceso **5.16 Gestión de la identidad** **5.17 Información de autenticación** **5.18 Derechos de acceso** **6.6 Acuerdo de Confidencialidad o no Divulgación** **6.7 trabajo Remoto** **8.3 Restricción de acceso a la información** **8.5 Autenticación segura**	Las contraseñas deben contener como mínimo ocho (8) caracteres (dígitos) Incluir caracteres de tres de las siguientes categorías: ✓Mayúsculas (de la A la Z) ✓Minúsculas (de la A la z) ✓Dígitos de base 10 (del 0 al 9) ✓Caracteres no alfanuméricos (¡por ejemplo, !, $, #, %) Estos requisitos de complejidad se exigen al cambiar o crear contraseñas.
	El Grupo de Gestión de las Tecnologías por medio del sistema de gestión de contraseñas tiene como directiva que los Servidores Publicos y colaboradores deben cambiar la contraseña cada 42 días, según su perfil y rol, las credenciales de acceso son de uso personal e intransferible
	Servidores de la Unidad Nacional de Protección UNP son responsables por el uso apropiado de las credenciales de acceso asignadas.
	Los Servidores Publicos, colaboradores, proveedores o partes interesadas no podrán compartir, prestar su usuario y/o contraseña es de uso personal e intransferible.
	Es responsabilidad del funcionario y contratista dar buen uso a los recursos, plataformas tecnológicas y de sistemas, además, es exclusivo para fines Institucionales. No está permitido disponer, compartir o utilizarlos con fines personales (fotos, videos, correos electrónicos e

	Información personal).
	No deben compartir sus credenciales o contraseñas con ninguna persona o hacerla pública por cualquier medio.
	Las acciones que se realicen con una cuenta usuario en los sistemas de información serán total responsabilidad del usuario.
	Se deberá realizar el doble factor de autenticación para acceso, permisos y privilegios de los recursos otorgados por la Unidad Nacional de Protección UNP.
	Es responsabilidad del servidor público y contratista dar buen uso a los recursos, plataformas tecnológicas y de sistemas, además, es exclusivo para fines Institucionales. No está permitido disponer, compartir o utilizarlos con fines personales (fotos, videos, correos electrónicos e Información personal).

Fuente: Elaboración propia

7.2.5.2 Gestión de acceso de usuarios con los sistemas de Información o aplicativos Inhouse o de terceros

Control: Los dueños de los activos deberá revisar la gestión de acceso de los usuarios, a intervalos regulares como se ajuste en el procedimiento.

CONTROL	RESPONSABILIDADES
5.15 Control de acceso **5.18 Derechos de acceso**	El jefe o supervisor de área o dependencia será responsable por el otorgamiento de los permisos y perfiles de acceso a los sistemas de información Inhouse o de terceros que cuente la Unidad Nacional de Protección.
6.6 Acuerdo de Confidencialidad o no Divulgación **6.7 trabajo Remoto**	El jefe o supervisor de área o dependencia será responsable por el otorgamiento de los permisos que se autoricen o se justifiquen para los accesos a los recursos de la plataforma tecnológica, servicios de red, los y áreas seguras.
8.3 Restricción de acceso a la información **8.5 Autenticación segura**	El Grupo de Gestión de las Tecnologías, deben velar por que los servicios tecnológicos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, teniendo en cuenta la matriz de roles y perfiles para cada sistema de información.
8.25 Ciclo de vida de desarrollo seguro	El Grupo de Gestión de las Tecnologías se debe acoger a las buenas prácticas de desarrollo seguro en los productos entregados, controlando el acceso lógico cuando estos estén en producción.

CONTROL	RESPONSABILIDADES
	El Grupo de Gestión de las Tecnologías, debe establecer ambientes separados a nivel físico y lógico para el desarrollo-pruebas y producción; contando con su plataforma, servidores, aplicativos, dispositivos y versiones independientes de los otros ambientes, para evitar así que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad, confidencialidad y disponibilidad de la información de los servicios en producción.
	Los desarrolladores deben asegurar que no se desplieguen en pantalla las contraseñas ingresadas.
	Los desarrolladores deben, a nivel de los aplicativos, restringir el acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y Políticas utilizadas para los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.
	Se deberán establecer controles de acceso a los ambientes de desarrollo, pruebas y producción de los sistemas de información y garantizar que se cumplan con las autorizaciones que le fueron otorgadas.
	Para acceder a los códigos fuente de programas se debe contar con la autorización del coordinador de GGT y/ líder de desarrollo, lo anterior con el fin de evitar la introducción de funcionalidades no autorizadas, evitar cambios involuntarios y mantener la confidencialidad de propiedad intelectual.
	Para cada proyecto de Desarrollo Inhouse o de terceros se contará con un líder dispuesto por el Coordinador de GGT, quien solo tendrá los permisos para realizar acciones en el mismo.

Fuente: Elaboración propia

7.2.5.3 Gestión de habilitación o des habilitación del usuario y sus accesos

Control: Los derechos de acceso de todos los Servidores Públicos y contratistas, proveedores o partes interesadas que tienen un usuario con permisos a los recursos tecnológicos, información se deberían retirar al terminar su vacante, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios (traslados).

CONTROL	RESPONSABILIDADES
5.10 Uso aceptable de la información y otros activos asociados **5.15 Control de acceso**	La asignación y utilización de los derechos de accesos privilegiados se debe restringir y controlar, tales como: “root”, “adm” “administrador” y “system”, entre otros, debe ser controlado por El Grupo de Gestión de las Tecnologías dejando registro de la trazabilidad de uso de estos accesos.

CONTROL	RESPONSABILIDADES
5.18 Derechos de acceso **6.5 Responsabilidades después de terminar el empleo** **6.6 Acuerdo de Confidencialidad o no Divulgación** **6.7 trabajo Remoto** **8.3 Restricción de acceso a la información** **8.5 Autenticación segura**	La administración los usuarios y sus accesos se deben revisar y reasignar, ya sea por los reportes que deben enviar las áreas de la Subdirección de Talento Humano y por el Grupo de Contratación reportando las novedades.
	La Subdirección de Talento Humano reportará al Grupo de Gestión de las Tecnologías la solicitud para habilitar o deshabilitar según novedad; Permisos de 3 días, Licencias remuneradas o no remuneradas, Incapacidades, Vacaciones, Cambio de cargo o traslado de área, Retiro de la Entidad.
	El Grupo de Contratación reportará la solicitud para habilitar o deshabilitar según la novedad como: Suspensión del contrato, Terminación de contrato, Cambio de área
	Estas Novedades deben ser reportadas los primeros 10 días de cada mes y en caso de cambios que ocurran en el transcurso de este.

Fuente: Elaboración propia

7.2.6 Política Uso Adecuado de Internet

CONTROLES	RESPONSABILIDADES
5.15 Control de acceso **5.18 Derechos de acceso** **8.20 Seguridad de redes** **8.23 Filtrado web**	El Grupo de Gestión de las Tecnologías administra los accesos y restricciones que se realizan en consulta en la navegación de internet y tiene limitado el acceso a portales de: Juegos, pornografía, drogas, terrorismo, segregación racial, hacking, malware, software gratuito o ilegal y/o cualquier otra página que vaya en contra de las leyes vigentes.
	El Grupo de Gestión de las Tecnologías limitará el acceso a redes sociales en general. En concordancia con la necesidad de la operación solo se habilitarán a las áreas que justifiquen su usabilidad la cual estará utilizada solo para temas institucionales.
	El Grupo de Gestión de las Tecnologías, restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).
	El Grupo de Gestión de las Tecnologías, podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

Fuente: Elaboración propia

7.2.7 Política de Uso Adecuado de Correo Electrónico:

CONTROL	RESPONSABILIDADES
	Los buzones de correo asignados a los Servidores Públicos, contratistas o terceros pertenecen a la Unidad Nacional de Protección, por lo tanto, su contenido también es propiedad de la Entidad.

CONTROL	RESPONSABILIDADES
5.10 Uso aceptable de la información y otros activos asociados **8.5 Autenticación segura** **8.7Protección contra malware**	El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
	El Grupo de Gestión de las Tecnologías, podrá verificar el contenido de los buzones de los correos telefónicos en los casos que se requiera acudir a información para continuar con la prestación del servicio o para investigaciones específicas con la autorización de los jefes de dependencias y por solicitudes de estos
	el Grupo de Gestión de las Tecnologías realizará revisión de las cuentas de usuario y genéricas y las deshabilitara si no tiene continuidad
	El Grupo de Gestión de las Tecnologías, no eliminará ninguna cuenta de correo electrónico y se salvaguardará para cualquier requisito que se solicite de consulta, o entrega con algún ente externo quien lo solicite con un documento formal y autorizado por la alta dirección o el jefe de la OAPI.

Fuente: Elaboración propia

7.2.8 Política Control De Software Operacional

7.2.8.1 Uso de programas utilitarios privilegiados

Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.

CONTROL	RESPONSABILIDADES
8.9 Gestión de configuración **8.18 Uso de programas de utilidad privilegiados** **8.19 Instalación de software**	El Grupo de Gestión de las Tecnologías debe establecer responsabilidades y controlar la instalación del software operativo que interactúa con el procedimiento de cambios existente en la Unidad Nacional de Protección.
	El Grupo de Gestión Tecnológica, debe conceder accesos temporales y controlados a los fabricantes y terceros autorizados para realizar actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.
	El Grupo de Gestión de las Tecnologías, estableció una política desde el servidor del Directorio Activo en el cual tiene las restricciones y limitaciones para la instalación del software operativo en los equipos de cómputo en la Unidad nacional de Protección.
	El Grupo de Gestión de las Tecnologías, debe generar un plan de actualizaciones para el software, aplicaciones y librerías de programas que deberán llevar a cabo los administradores, bajo la autorización CIO.
	Está estrictamente prohibido el uso de programas utilitarios, software o aplicaciones no autorizadas por parte de Servidores públicos y contratistas o proveedores sin la debida autorización por el Grupo de Gestión de las Tecnologías.

CONTROL	RESPONSABILIDADES
	El uso de herramientas o utilitarios propios de los sistemas operativos debe ser limitado a personal autorizado y su uso está restringido en casos específicos y debe disponerse de la trazabilidad de las operaciones realizadas en los casos que son autorizados. Y solo deben ser por plataforma de mesa de servicios.
	El uso de los recursos, plataformas tecnológicas y de sistemas es exclusivo para fines Institucionales. No está permitido disponer, compartir o utilizarlos con fines personales (fotos, videos, correos electrónicos e Información personal)
	El Grupo de Gestión de las Tecnologías, debe manejar un sistema de control de configuración para mantener el control de todo el software implementado, al igual que se debe mantener la documentación del sistema.

Fuente: Elaboración propia

7.2.9 Política de Gestión de Contraseñas

CONTROL	RESPONSABILIDADES
5.15 Control de acceso **5.16 Gestión de la identidad** **5.17 Información de autenticación** **5.18 Derechos de acceso** **8.5 Autenticación segura**	NO, Utilizar contraseñas que contengan información personal relacionada, por lo cual no se debe utilizar información como números de identificación personal, números de teléfono, nombres de los conyugues y/o familiares, dirección de residencia, nombres propios, lugares conocidos, entre otros.
	Las contraseñas deben contener como mínimo ocho (8) caracteres (dígitos) Incluir caracteres de tres de las siguientes categorías: - Mayúsculas (de la A a la Z) - Minúsculas (de la a a la z) - Dígitos de base 10 (del 0 al 9) - Caracteres no alfanuméricos (¡por ejemplo, !, $, #, %) Estos requisitos de complejidad se exigen al cambiar o crear contraseñas.
	El Grupo de Gestión de las Tecnologías por medio del sistema de gestión de contraseñas tiene como directiva que los Servidores públicos y colaboradores deben cambiar la contraseña cada 42 días, según su perfil y rol, las credenciales de acceso son de uso personal e intransferible
	El sistema de gestión de contraseñas bloqueará el acceso del usuario una vez se identifiquen diez (10) intentos de inicio de sesión fallido consecutivo.
	Los administradores del Sistema de Gestión de contraseñas deberán obligar por medio del Sistema al cambio de contraseña de los usuarios de acuerdo con la periodicidad establecida en la presente Política.
	El sistema de gestión de contraseñas administrado por el Grupo de Gestión de las Tecnologías deberá restringir el uso de las últimas doce (12) contraseñas usadas por los usuarios de los Sistemas de Información y Aplicaciones de la Unidad Nacional de Protección – UNP.

	Por medio de la Mesa de Servicios el Grupo de Gestión de las Tecnologías, se debe gestionar el cambio de la primera contraseña para los usuarios que ingresan por primera vez a los sistemas de información y aplicaciones de la Unidad Nacional de Protección – UNP

Fuente: Elaboración propia

7.2.10 Política de Controles Criptográficos y Gestión de Llaves

CONTROL	RECOMENDACIONES
5.15 Control de acceso **5.16 Gestión de la identidad** **5.17 Información de autenticación** **5.18 Derechos de acceso** **8.24 Uso de la Criptografía**	El Grupo de Gestión de las Tecnologías, debe usar herramientas de controles criptográficos para llevar a cabo el cifrado de los equipos de los servidores públicos que se encuentran en la modalidad de teletrabajo en la Unidad Nacional de Protección, conel fin de salvaguardar la seguridad de la información de la Entidad en los equipos que se encuentran fuera de las instalaciones.
	Para la conexión externa hacia la Infraestructura Tecnológica de la Unidad Nacional deProtección, El Grupo de Gestión de las Tecnologías, deberá garantizar que dichas conexiones cuenten con mecanismos de conexión segura y cifrada entre las partes
	El Grupo de Gestión de las Tecnologías y el responsable de la Infraestructura Tecnológica, serán los que deben administrar las contraseñas utilizadas para llevar a cabo el cifrado de la información de la Unidad Nacional de Protección – UNP.
	Para la gestión de llaves de firma electrónica (tokens), el Grupo de Gestión de las Tecnologías asignará una única llave por cada usuario que lo requiera de acuerdo con sus funciones y obligaciones contractuales.
	Una vez asignadas las llaves de firma electrónica por parte del El Grupo de Gestión de las Tecnologías el usuario deberá ser el responsable de la custodia y administración de esta, así como del entendimiento de que la llave entregada deberá ser personal e intransferible.
	La Unidad Nacional de Protección deberá garantizar que las llaves de firma electrónica usadas por la Entidad sean entregadas de forma segura por un Ente acreditado dentrodel país para dicha gestión.

Fuente: Elaboración propia

7.2.11 Política de Gestión de Redes

CONTROL	RESPONSABILIDADES
8.2 Seguridad de Redes	El Grupo de Gestión de las Tecnologías, será responsable de controlar los accesos aservicios internos y externos conectados en red.

CONTROL	RESPONSABILIDADES
8.21 Seguridad de los servicios de red **8.22 Segregación de redes**	El Grupo de Gestión de las Tecnologías, 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.
	El Grupo de Gestión de las Tecnologías, debe proveer los mecanismos, controles y recursos necesarios para llevar a cabo la separación física y lógica con el fin de reducir el acceso no autorizado y evitar usos y cambios inadecuados sobre los servicios y redes de la Unidad Nacional de Protección – UNP.
	El Grupo de Gestión de las Tecnologías, debe asegurar que las redes inalámbricas de la UNP cuenten con controles de autenticación para evitar accesos no autorizados a servidores públicos, contratistas, terceros y partes interesadas.
	Los usuarios de la red interna de la Unidad Nacional de Protección – UNP, no están autorizados para ejecutar acciones y cambios exclusivos por el Grupo de Gestión de las Tecnologías.
	La Unidad Nacional de Protección – UNP, deberá contar con separación de redes de acuerdo con los niveles y necesidades de los servidores públicos, contratistas y terceros autorizados.
	Con el fin de garantizar la correcta conexión Wi-Fi a la red de la Unidad Nacional de Protección, se deberá disponer de las siguientes segmentaciones: **1.Red Wi-Fi de Servidores Públicos**: servidores públicos, contratistas y terceros autorizados que tienen cuenta institucional. **2.Red Wi-Fi Grupo VIP:** Niveles Directivos, Grupo de Comunicaciones Estratégicas, y asistenciales de los niveles directivos que por sus funciones requieren navegar por la red VIP de la Entidad. **3.Red Wi-Fi de Invitados**: Externos a la Unidad Nacional de Protección – UNP. **4.Red Wi-Fi Dependencias**: De acuerdo con regulación vigente dada por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC.

Fuente: Elaboración propia

7.2.11.1 Uso De Puntos De Red

CONTROL	RESPONSABILIDADES
8.16 Actividades de seguimiento	Los puntos de red de datos solo pueden ser utilizados por equipos pertenecientes al inventario de la corporación, los equipos externos a la UNP solo podrán ser conectados a la red wifi asignada para su uso dependiendo de la labor a realizar.
	Los usuarios no deben manipular los puntos de red, ni intercambiar los cables ya configurados e instalados, en caso de alguna falla en el servicio, ésta debe ser reportada al grupo de tecnologías para su posterior revisión.

	Los usuarios no deben manipular la configuración de red en los equipos de cómputo asignados, solo lo podrán realizar los Servidores públicos y/o contratistas al Grupo de Gestión de las Tecnologías

Fuente: Elaboración propia

7.2.11.2 Segregación de Redes

CONTROL	RESPONSABILIDADES
8.20 Seguridad redes **8.21 seguridad servicio de redes** **8.22 Segregación redes**	Se debe garantizar que los sitios destinados a alojar los Switches y Routers esté protegido ante cualquier intromisión no autorizada; así mismo, deben estar ubicados en un espacio con las condiciones de temperatura óptimas según la Política vigente, sin acceso al público en general y con supervisión constante de los encargados de la infraestructura de sistemas.
	Para asegurar la protección de los elementos que están en los centros de datos y cableados se deben seguir las siguientes recomendaciones: ● No consumir alimentos en los centros de datos. ● No fumar en los centros de datos. ● Mover o desconectar equipos sin autorización. ● Alterar el software instalado sin autorización. ● Extraer información.
	Los centros de datos y de cableado deben estar en óptimas condiciones físicas, aseado, y con control de incendios, humedad activos.
	Los dispositivos que proveen la señal inalámbrica y que están distribuidos en toda el área de la UNP no deben ser manipulados por personal diferente al grupo de tecnologías, adicionalmente, estos dispositivos deben estar encendidos y sin obstrucciones a la vista para que puedan funcionar de una manera óptima.

Fuente: Elaboración propia

7.2.12 Política de Gestión de Copias de Respaldo

CONTROLES	RESPONSABILIDADES
Medios de Almacenamiento **7.14 Disposición o reutilización segura de los equipos** **8.13 Copia de seguridad de la Información**	El Grupo de Gestión de las Tecnologías, debe realizar copias de respaldo sobre la configuración e información que contiene la Infraestructura Tecnológica de la Unidad Nacional de Protección.
	Es responsabilidad del El Grupo de Gestión de las Tecnologías, determinar la periodicidad y tipo de copia para la toma de copias de respaldo sobre la configuración e información que contiene la Infraestructura Tecnológica de la Unidad Nacional de Protección.
	La información contenida dentro de la nube corporativa de la Unidad Nacional de Protección – UNP será respaldada por el proveedor de esta teniendo en cuenta los respectivos acuerdos

	contractuales
	El Grupo de Gestión de las Tecnologías, debe realizar restauración de las copias de respaldo de la Infraestructura física con el fin de garantizar su correcto funcionamientoen caso de necesitarse la oportuna restauración de la información contenida.
	Los desarrolladores generan su copia de seguridad de las aplicaciones en Share Point.

Fuente: Elaboración propia

7.2.13 Política de Escritorio y Pantalla Limpia

CONTROLES	RESPONSABILIDADES
7.1 Escritorio y pantalla limpios	Los servidores públicos, contratistas y terceros autorizados no deben dejar la sesión abierta del equipo de cómputo, cuando se ausenten del puesto de trabajo.
	Los servidores públicos, contratistas y terceros autorizados deberán llevar a cabo el cierre de sesión sobre los sistemas de información y aplicaciones de la Unidad Nacionalde Protección – UNP, una vez finalicen las actividades y labores requeridas durante la jornada laboral.
	El Grupo de Gestión de las Tecnologías, será el responsable de realizar la configuración de bloqueos automáticos de las sesiones de los sistemas operativos de los equipos de cómputo de la Unidad Nacional de Protección – UNP, por medio de la herramienta conque la Entidad cuente para realizar dichas configuraciones.
	Los servidores públicos, contratistas y terceros autorizados no deben dejar documentos con información clasificada o reservada expuesta y al alcance de personal no autorizado, en caso de tener este tipo de información en físico, ésta debe ser guardadaen un lugar seguro.
	El Grupo de Gestión de las Tecnologías, determinará el tiempo de bloqueo automático de losequipos de cómputo de acuerdo con las realidades de la Unidad Nacional de Protección – UNP y a las buenas prácticas en seguridad de la información.
	El escritorio virtual (papel tapiz) del equipo de cómputo debe permanecer libre de documentos digitales, para evitar acceso no autorizado a la información contenida dentro del equipo de cómputo.
	Se generará una directiva desde el Directorio activo AD para que el papel tapiz del escritorio siempre esté libre de carpetas y documentos para poder ver las piezas, comunicaciones importantes y de interés.

Fuente: Elaboración propia

7.2.14 Política de Transferencia de la Información

CONTROLES	RESPONSABILIDADES
5.12 Clasificación de la Información **5.13 Etiquetado de la información** **5.14 transferencia de Información**	Los servidores públicos, contratistas y terceros autorizados que requieran transferir información de la Unidad Nacional de Protección – UNP no deben usar herramientas de uso personal o libre para el intercambio de esta información.
	El Grupo de Gestión de las Tecnologías, es el responsable de implementar, gestionar y mantener implementados los controles de seguridad necesarios para proteger la información que se transfiere externamente a la Entidad.
	Los servidores públicos, contratistas y terceros autorizados no deben emitir copias, realizar divulgación o emplear indebidamente datos e información contenida en las aplicaciones, bases de datos y sistemas de información a los cuales se les haya otorgado acceso, con fines diferentes al cumplimiento de sus obligaciones.
	Las herramientas y medios para la transferencia de la información externa a la Entidaddeberán contar con controles criptográficos con el fin de proteger la confidencialidad, laintegridad y la autenticidad de la información.
	Es responsabilidad de los servidores públicos, contratistas y terceros autorizados no comprometer a la Entidad por difamación, acoso, suplantación, entre otros por la transferencia de información con fines personales o no autorizados.
	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 diferentenaturaleza, y que involucran de alguna forma el intercambio de información.

Fuente: Elaboración propia

7.2.15 Política para el Desarrollo de Software, Adquisición y Mantenimiento

CONTROLES	RESPONSABILIDADES
5.1 Políticas de seguridad de la información **5.12 Clasificación de la información** **5.14 Transferencia de información** **5.15 Control de acceso** **5.23 Seguridad de la información para el uso de servicios en la nube**	El Grupo de Gestión de las Tecnologías, debe contemplar e incorporar en todos los proyectos de desarrollo y adquisición de sistemas de información propios o de terceros, requisitos de seguridad de la información las siguientes características: ✓ Arquitectura de software ✓ Análisis ✓ Diseño ✓ Cifrado de datos ✓ Especificación de requerimientos ✓ Controles de seguridad de la información ✓ Calidad de software ✓ Estandarización de los mensajes de error y eventos de seguridad ✓ Documentación técnica y de usuario
5.34 privacidad y protección de la información de identificación personal	El Grupo de Gestión de las Tecnologías, trabaja con los sistemas de información con la metodología ágil y que será una estrategia con el usuario para los proyectos que se trabajen.

CONTROLES	RESPONSABILIDADES
8.3 Restricción de acceso a la información **8.4 Acceso al código fuente** **8.8 Gestión vulnerabilidades** **8.12 Prevención fugas de datos** **8.13 Copia de seguridad de la información** **8.16 Actividades de seguimiento** **8.27 Arquitectura de sistemas seguros y principios de ingeniería** **8.31 Separación de entornos de desarrollo, evidencia y producción** **8.32 Gestión de cambios** **8.33 Información de pruebas** **8.34 Protección de los sistemas de información durante pruebas de auditoría**	Es responsabilidades de todas las áreas de la UNP en los proyectos de los sistemas d información apoyar con recursos para recurso humano e infraestructura en los casos que sean necesarios
	Los sistemas de información que se requiera interoperabilidad con otras Entidades y sus sistemas deben cumplir con el Anexo 2.1 Guía de diseño gráfico para sedes electrónicas de MinTic
	El Grupo de Gestión de las Tecnologías, debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Unidad Nacional de Protección - UNP.
	El Grupo de Gestión de las Tecnologías, 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 las Tecnologías, 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.
	Los servidores públicos, contratistas y terceros autorizados a cargo del Desarrollo de Software de la Unidad Nacional de Protección – UNP, deberán tener en cuenta las siguientes consideraciones: Asegurar el trabajo en conjunto del servidor público y contratista (dueño del producto) realizar cada una de las actividades que se generan desde el inicio del proyecto (documentación) y mediante el desarrollo evolutivo hasta la entrega. Considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, 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 nose requiera.
	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.
	Proporcionar un nivel adecuado de soporte para solucionar los problemas que sepresenten en el software desarrollado para la Unidad Nacional de Protección – UNP.
	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.

CONTROLES	RESPONSABILIDADES
	Suministrar opciones de desconexión o cierre de sesión de las aplicaciones (logout) que permitan terminar completamente con la sesión o conexión asociada.
	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.

Fuente: Elaboración propia

7.2.15.1 Responsabilidades de los usuarios de desarrollo in House como adquisición terceros.

CONDICIONES	RESPONSABILIDADES
Todo proyecto relacionado con desarrollo Inhouse o adquisición de sistemas de información debe cumplir con las siguientes características	El Grupo de Gestión de las Tecnologías, los usuarios y terceros ✓ El Grupo de Gestión de las Tecnologías, los usuarios, trabará en conjunto el desarrollo in House y adquisición de sistemas de información desde su inicio hasta su entrega al usuario.
	✓ Es responsabilidad de los usuarios con los desarrollos In house después de recibirlos asumir lo siguiente: Son responsables del soporte fase 1, la cual comprende la administración de: • Todo el sistema. • Manejar el módulo de usuarios asignándole los perfiles que le competen a cada usuario en el cumplimiento de sus actividades dentro del sistema de información. • Brindar capacitaciones para los usuarios que trabajen o utilicen el sistema. • Los soportes deben registrarse enla Plataforma de mesa de servicios en cada uno de los sistemas de información a los que se genere la solicitud.
	El Grupo de Gestión de las Tecnologías, los usuarios y terceros ✓**Gestión Tecnologías y terceros**. GGT, es responsabilidad de entregar la información de la infraestructura que se maneja en la UNP, para la realización de la adquisición de los sistemas la plataforma con que se trabaja y los lenguajes y estructura de seguridad.
	✓ **Responsabilidad del tercero** ajustarse a las Políticas y necesidades de la Entidad como también cumplir los lineamientos de seguridad de la 27001 y MinTic con relación a la estructura de sistemas de información sus ambientes y plantillas que debe estar dispuestas para ser administradas por la UNP por cabios de Política (logos de gobierno, institucionales y lineamentos de MinTic.

CONDICIONES	RESPONSABILIDADES
	✓ Las actualizaciones que se requiera en el sistema de información es responsabilidad del tercero dueño del producto. No puede ser del Ingeniero porque el Código Fuente no es de la UNP.
	✓ **Responsabilidad de GGT, Administrar:** • La infraestructura para los sistemas de información, teniendo en cuenta los ambientes para in house (desarrollo, pruebas y producción) • Ambientes para terceros (pruebas y producción). • Realización del backup del sistema • Revisar todas las herramientas (firewall) y certificados de seguridad que apoyen la protección de estos.

Fuente: Elaboración propia

7.2.15.2 Requerimientos funcionales de seguridad

CONDICIONES	RESPONSABILIDADES
Confidencialidad: Considerando la clasificación para los activos de información de la UNP cada aplicación debe proveer los mecanismos para proteger la confidencialidad con base en su nivel de criticidad. (Cifrado, Control de Acceso y Registro Logs). Los mecanismos de las aplicaciones desarrolladas para la UNP deben proveer:	**Cifrado de datos catalogados como públicos clasificados y públicos reservados**: Opción de cifrar los datos en tránsito (Ejemplo: VPN) y almacenamiento con un algoritmo criptográfico fuerte.
	Control de acceso: Mecanismos de autenticación por usuario y contraseña siguiendo la Política de control de acceso a la información de la UNP. Este control de acceso debe establecerse para cada activo de información con base en los accesos definidos por cada grupo responsable de los datos o por cada dueño de la información.
	Registro: Permitir la parametrización para generar el registro en logs de eventos que permitan registrar los accesos a la información y así poder evidenciar potenciales violaciones a la confidencialidad de la información.
Integridad: Para proteger la integridad de la información las aplicaciones deben desarrollar las siguientes utilidades, y deben ser aplicadas con base en la clasificación del activo de información:	**Control de acceso**: Equivale a la funcionalidad descrita para la protección de la Confidencialidad.
	Verificación por Hashing: Opción que permita validar la integridad de los datos almacenados y/o transmitidos utilizando un campo de hashing que se genere con el algoritmo de cifrado fuerte, para las aplicaciones o sistemas de información críticos.
	Registro: Permitir la parametrización para generar el registro en logs de eventos que permitan registrar los accesos a la información y así poder evidenciar potenciales violaciones a la integridad de la información.
Disponibilidad	Para cumplir con los requerimientos de disponibilidad de la información y del sistema, se debe garantizar la validación de entradas de datos, procesamiento y calidad de datos, autenticación entre las interfaces del sistema.

Fuente: Elaboración propia

7.2.15.3 Seguridad en los procesos de desarrollo y de soporte.

CONDICIONES	RESPONSABILIDADES
Ambiente de desarrollo	Juntamente con la evaluación de riesgos, realizada según la metodología de evaluación y tratamiento de riesgos de la UNP, se debe realizar periódicamente la evaluación de los siguientes aspectos: a. Los riesgos relacionados con el acceso no autorizado al ambiente de desarrollo. b. Los riesgos relacionados con los cambios no autorizados sobre el ambiente de desarrollo. c. Las vulnerabilidades técnicas de los sistemas de TI utilizados en la UNP. **d.** Los riesgos que puede traer una nueva tecnología para la UNP.
	Es imprescindible y fundamental aplicar la metodología de riesgos en cada etapa del ciclo de vida de desarrollo de software y, así mismo, a cada uno los proyectos e iniciativas de desarrollo y adquisición de sistemas de información.
	El uso de una metodología de análisis de riesgos permite gestionar de manera adecuada los riesgos que puedan afectar al negocio, como lo son los fraudes, afectación a los ciudadanos, fuga de información, incumplimientos regulatorios, impacto reputacional o imagen, impactos operativos, impactos financieros. Así mismo, debe aumentar el nivel de madurez de seguridad de la información y ciberseguridad de la Entidad.
	Los cambios a los sistemas de información dentro del ciclo de vida se deben controlar mediante la aplicación de los lineamientos definidos en el “Procedimiento de Gestión de Cambios Tecnológicos”, Este se debe realizar con el fin de minimizar el impacto en las operaciones de negocio.

Fuente: Elaboración propia

7.2.15.4 Principios para desarrollo de sistemas seguros

CONDICIONES	RESPONSABILIDADES
Los manuales y los lineamientos para garantizar la seguridad. Herramientas de infraestructura	Para el desarrollo de software en la UNP se definen en este manual los lineamientos que garantizan la seguridad en el ciclo de vida del desarrollo del software, igualmente se deben diseñar controles adecuados en las aplicaciones existentes en la UNP, para garantizar un correcto procesamiento de datos, validación de los datos entrada y de salida, validación de mensajes de error, conciliación de datos al cerrar las transacciones, etc.

	Las aplicaciones o sistemas que se desarrollen en la UNP deben cumplir con principios mínimos de seguridad, para minimizar las brechas de seguridad, pérdidas y modificaciones no autorizadas o usos indebidos en la información de las aplicaciones, estas medidas deben ser dadas conforme a las buenas prácticas de metodologías de desarrollo seguro y Política vigente.

Fuente: Elaboración propia

7.2.15.5 Ambientes de Desarrollo

7.2.15.5.1 Ambiente Desarrollo y Producción

CONTENIDO	RESPONSABILIDADES
En este ambiente se encuentran las aplicaciones, archivos, bases de datos y demás, que soportan las operaciones de negocio en la UNP, por tal razón se deben considerar los siguientes requisitos:	Los analistas de desarrollo de sistemas de información no deben tener acceso al ambiente de producción
	Los cambios a los sistemas de información dentro del ciclo de vida del desarrollo y de las pruebas, e implementación en producción, se deben controlar mediante la aplicación de los lineamientos definidos en el “Procedimiento de Gestión de Cambios Tecnológicos”, con el fin de minimizar el impacto en las operaciones de negocio.
	Para la atención de problemas en producción, será a través de un cambio aprobado y de conocimiento por el dueño de la información (dueño del proceso) contenida en el sistema de información y éste debe ser implementado por el administrador del sistema de información y/o base de datos.
	Los cambios de emergencia cuando ocurren problemas bien sean de programas, de operación, de grabación o por deficiencia del sistema, deben ser evaluados, estar aprobados, gestionados por el área de desarrollo, documentados y presentados posteriormente socializados en la reunión de cambios.
	Los cambios de emergencia sobre datos en producción deben ser autorizados por el dueño de la información, se deben documentar las razones del cambio, para posterior revisión y formalización del cambio desde la plataforma de gestión de cambios.
	Los datos deben ser sometidos a procesos de enmascaramiento u ofuscamiento con rutinas aprobadas.
	Los grupos de la Entidad donde se gestionen datos personales deben implementar controles de cifrado sobre los sistemas de información, carpetas o archivos que manejen información personal.

Fuente: Elaboración propia

7.2.15.5.2 Ambiente de Pruebas

CONTROLES	RESPONSABILIDADES
En este ambiente se encuentran las aplicaciones, archivos, bases de datos y demás, información para las pruebas del sistema evolutivo **A.8.33 Información de pruebas**	En la fase de pruebas de los sistemas de información desarrollados o adquiridos, no se deben utilizar datos de producción.
	En el caso de que se llegare a utilizar datos de producción, estos deben ser entregados a un funcionario responsable de los mismos, quien debe firmar acuerdo de confidencialidad sobre los datos recibidos para pruebas. Una vez terminadas las pruebas estos deben ser borrados de manera segura.
	En cumplimiento de los requisitos legales de privacidad y seguridad de la información, los datos de prueba no deben contener información que permitan la identificación de la persona natural o jurídica a la que pertenezca la información.
	No se permite el acceso desde el ambiente de pruebas al ambiente de producción
	Los analistas de desarrollo de sistemas de información, software o proveedores deben tener un ambiente de pruebas con una separación entre infraestructura, plataforma y aplicaciones; conjuntamente deben tener datos enmascarados o transformados para proteger la confidencialidad de la información esto aplica para todas las plataformas.
	Las pruebas deben dar evidencia de que los controles diseñados e implementados van a proteger la información contra acceso, divulgación, modificación, destrucción uso no autorizado de la información.
	Los datos deben ser sometidos a procesos de enmascaramiento u ofuscamiento con rutinas aprobadas. Cuando los datos deban ser usados en el ambiente de pruebas, teniendo la autorización del responsable y/o custodio de la información.
	Se deben analizar los riesgos y controles complementarios sugeridos, cuando se requieran copias de la información de los ciudadanos para la realización de pruebas contemplando controles necesarios para garantizar su destrucción, una vez concluidas las mismas.
	El set de pruebas de seguridad debe permitir el análisis y la auditoría de la aplicación en todos los componentes, así como el análisis de la aplicación basado en pruebas de penetración y pruebas de seguridad, que permitan demostrar vulnerabilidades en el sistema. Para esto es importante: • Integrar las pruebas al proceso de desarrollo de software. • Establecer procesos que optimicen las pruebas de seguridad, alineadas a los requerimientos del negocio. • Realizar pruebas de seguridad durante todo el ciclo de vida de desarrollo de software.

	Utilizar herramientas automatizadas y de confianza, así como personas con las habilidades apropiadas para la ejecución de estas

Fuente: Elaboración propia

7.2.15.5.2 La metodología de análisis de seguridad

CONDICIONES	RESPONSABILDADES
8.28 Codificación Segura **Para la detección de brechas de seguridad, deben incluir las siguientes acciones:**	Análisis de Vulnerabilidades durante y después del desarrollo del software.
	Pruebas de Intrusión o de Penetración en la puesta en producción.
	Revisión y análisis de código estático.
	El ambiente no puede ser utilizado para evadir los controles de seguridad establecidos.
	Cualquier falla de seguridad en las pruebas del sistema de información o software, detectada y que no pueda ser contralada antes del paso a producción, debe ser reportado al Oficial de Seguridad de la Información.

Fuente: Elaboración propia

7.2.15.6 Adquisición Desarrollo Contratado por un Tercero

CONDICIONES	RESPONSABILIDADES
	La UNP debe contar con un procedimiento para la selección de proveedores, en el cual se incluya los criterios para la evaluación de propuestas y para la ponderación del cumplimiento de los requerimientos.
	Los procesos que participan en la selección y evaluación de proveedores tendrán la responsabilidad de preparar y negociar un contrato con el proveedor, estableciendo los requerimientos de la adquisición, incluyendo costos y plazos del producto, sistema o servicio de software a entregar. El contrato debe tener en cuenta los derechos de marca, uso, propiedad intelectual, garantía y licenciamiento.
Por cada proyecto o servicio contratado deberá tener un líder de proyecto en la UNP la cual será:	El área que genera la necesidad encargada de velar por el cumplimiento de los acuerdos definidos.
	Por parte de tecnología la responsabilidad es acompañamiento desde el inicio hasta el fin con la entrega del producto y disponer de lo requerido por infraestructura.
Todo desarrollo a través de un tercero o de adquisición, debe contener los siguientes aspectos de seguridad de autenticidad del software:	Derechos de Autor.
	La plantilla del software del proveedor debe ajustare a la misionalidad, logos, nombres y logueo de la Entidad que adquirió el software, sin perder sus derechos de Autor.
	Requerimientos mínimos de seguridad y calidad de datos.
	Licencia para uso del software desarrollado o adquirido.

	Aviso de uso y privacidad del software.

Fuente: Elaboración propia

7.2.15.7 Pruebas de funcionalidad y aceptación de sistemas

CONDICIONES	RESPONSABILIDADES
El plan de pruebas debe describir las actividades que se efectuarán para demostrar que los sistemas cumplan con los requisitos previamente definidos	Se deben definir procedimientos de pruebas de funcionalidad de los sistemas y aceptación de estos, para los sistemas de información nuevos, actualizaciones y nuevas versiones.
	La aceptación de los sistemas debe ser basada en la estrategia y los criterios de aceptación definidos por la Oficina de Tecnologías e Información. Se debe tener en cuenta la preparación de los casos, datos, procedimientos y entorno de las pruebas, demás, si aplica se debe establecer en qué grado se debe involucrar al proveedor
	Las pruebas técnicas y de funcionalidad del producto o servicio de software solo se debe aceptar cuando el producto satisfaga todas las condiciones de aceptación definidas.
	Para la aceptación de los sistemas se debe cumplir con los criterios de evaluación definidos y validados por Seguridad de la Información definidas de la UNP.
	Una vez se haya definido la adquisición del software, la Oficina de Tecnología e Información debe asumir la responsabilidad para la gestión de la configuración del software entregado, mediante el Procedimiento de Gestión de la Configuración.

Fuente: Elaboración propia

7.2.15.8 Servicios de Back-End, Servidores de la Plataforma Móvil y las APIs

CONTROLES	RESPONSABILIDADES
Se debe contar con medidas específicas para proteger los backends de aplicaciones móviles, esto incluye el aseguramiento de los Web Services, APIs y protocolos empleados para conectarse con las plataformas de back-end, así como la infraestructura tecnológica y software utilizado por la aplicación móvil.	Se debe analizar periódicamente en busca de vulnerabilidades.
	Mantener el servidor de la plataforma móvil, completamente actualizado.
	Establecer los mecanismos necesarios para llevar a cabo un análisis forense, si de un incidente se trata. Utilizar medidas para prevenir ataques de denegación de servicio.

Fuente: Elaboración propia

7.2.15.9 Protección de la Privacidad en dispositivos Móviles

Los diseños de aplicaciones móviles deben evitar la divulgación de la información Personal o privada desde el dispositivo móvil.

CONTROL	RESPONSABILIDADES
La seguridad del software en los dispositivos móviles debe contemplar actualizaciones teniendo en cuenta los siguientes aspectos:	No distribuya las aplicaciones a través de repositorios inseguros.
	Las aplicaciones deben estar diseñadas para aceptar actualizacione de seguridad.
	Establezca canal de comunicaciones seguros, para que los usuario pueden reportar fallos de seguridad a través de éstos.
Tenga en cuenta, a la hora de desarrollar una aplicación móvil aspectos importantes que pueden ser identificados como buenas prácticas en la construcción de software para dispositivos móviles, entre éstos contemplar:	La validación de todas las entradas de información.
	Minimizar las líneas de código y su complejidad.
	Utilizar analizadores de código, para buscar fallos de seguridad.
	Utilizar funciones seguras con el fin de prevenir desbordamientos de búfer, etc.
	Ejecutar las aplicaciones con el mínimo nivel de privilegios.

Fuente: Elaboración propia

7.2.15.10 Documentación requerimientos mínimos para desarrollo

CONDICIONES	RESPONSABILIDADES
El desarrollo, adquisición y mantenimiento de sistemas de información o software es un proceso imprescindible en la Entidad, por tal motivo es necesario incorporar en la entrega de estos productos, las pruebas y la documentación que son a su vez un factor de soporte en todo el ciclo de vida del desarrollo del software. Es así como se relaciona la siguiente documentación para que se contemple en todas las entregas de estos productos:	Modelo -Entidad - relación de la base de datos. • Generación de Diagrama en la base de datos
	a. Diccionario de datos • Nombre del campo • Nombre de la tabla • Regla de Validación • Descripción de la tabla • Descripción • Tipo longitud • Dominio
	b. Inventario de versionamiento de los sistemas de información o software.
	c. Diagrama de contexto • Creación diagrama de contexto por unidades funcionales
	d. Inventario de versionamiento de los sistemas de información o software
	e. Diagrama de contexto
	f. Diagrama de despliegue • Diagrama de despliegue solución del SI
	g. Código fuente TFS o GIF • Documentación del código
	h. Manual de Técnico.
	i. Manual Usuario
	j. Historia de usuario del Diseño, Análisis y arquitectura
	k. Informe de pruebas funcionales. Bien documentadas con pantallazos
	l. Informe de pruebas de vulnerabilidades y remediadas.
	m. Informe de aseguramiento o hardening para el componente

CONDICIONES	RESPONSABILIDADES
	hardware. n. Acta de control de cambios para la puesta en producción. o. Acta por fases de módulos p. Acta de cierra de entrega del Sistema de información

Fuente: Elaboración propia

7.2.15.11 Documentación mínima de Infraestructura

CONDICIONES	RESPONSABILIDADES
Documentos que hacen parte del desarrollo que por parte de infraestructura se contemplan como apoyo a la gestión, son los siguientes:	Diagrama de despliegue
	Manual de instalación
	Manual de configuración
	Diagramas de configuración de comunicación y seguridad de la aplicación
	Plan de administración de la capacidad
	Informe instalación en ambiente de desarrollo
	Informe instalación en ambiente de producción
	Informe instalación en ambiente de pruebas
	Política de backup
	Información de certificados SSL (Vigencia)
	Pruebas de ethical hacking (Si aplica)

Fuente: Elaboración propia

7.2.15.12 Interoperabilidad

El intercambio de información y conocimiento entre ellos, la capacidad de comunicación entre distintos sistemas con distintos datos en distintos formatos de modo que la información pueda ser compartida, accesible desde distintos entornos y comprendida por cualquiera de ellos.

Mediante los lineamientos de MinTic y al interior de la UNP se debe realizar lo dispuesto para que todo quede centralizado y unificado para el mejoramiento del servicio.

En la UNP es fundamental por parte de los sistemas de información, el compartir datos y posibilitar

En la UNP es fundamental por parte de los sistemas de información, el compartir datos y posibilitar

7.2.16 Política de Seguridad de la Información en las Relaciones con los Proveedores

CONTROLES	RESPONSABILIDADES
5.19 Seguridad de la información en relación con proveedores,	Todos los servidores públicos y contratistas deben seguir los lineamientos del Grupo de gestión Contractual, sus estudios previos y demás documentos que sean parte de un proceso contractual, y el manejo de la plataforma de SECOP

CONTROLES	RESPONSABILIDADES
5.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores **6.6 Acuerdo Confidencialidad y no divulgación**	Los servidores públicos y contratistas únicamente deben proporcionar acceso a la información de la Unidad Nacional de Protección – UNP a los proveedores cuando se requiera para cumplir con su objeto contractual, aplicando el principio de mínimos privilegios.
	Se deberá identificar, mitigar y monitorear los riesgos relacionados con los proveedores de servicios, incluida la cadena de suministro de servicios de tecnología o las comunicaciones.
	Se deberá divulgar las Políticas de seguridad de la información de la Unidad Nacional de Protección – UNP a los proveedores, así como velar porque el acceso a la información por parte de los proveedores se realice con las Políticas de la Entidad.
	Se deberá establecer y monitorea las condiciones de comunicación y transmisión de información desde y hacia los proveedores de servicios.
	Todos los proveedores de servicios de la Unidad Nacional de Protección – UNP, deberán firmar los acuerdos de confidencialidad y no divulgación de la información de la Entidad, con el fin de prevenir cualquier intento de divulgación no autorizada.

Fuente: Elaboración propia

7.2.17 Política de Incidentes

CONTROLES	RESPONSABILIDADES
5.7 Inteligencia de amenazas **5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información** **5.25 Evaluación y decisión sobre eventos de seguridad de la información** **5.26 Respuesta a incidentes de seguridad de la Información** **5.27 Aprender de los incidentes de seguridad de la información** **8.7 Protección contra malware**	Un incidente será declarado como mayor cuando una o varias de las siguientes condiciones se presenten: registro de 5 y más servicios o casos por la misma causa en la herramienta de gestión en el mismo periodo de tiempo (1 día calendario).
	El incidente mayor debe ingresar a través de la mesa de servicios como detección de un evento crítico que genera un Incidente Proactivo.
	Todos los incidentes mayores deben ser registrados y gestionados única y exclusivamente en la herramienta de gestión.
	El Ingeniero a cargo del incidente mayor actualizará la herramienta de gestión cada vez que tenga un avance.
	El gestor de incidentes debe realizar seguimiento a los incidentes mayores como mínimo tres veces al día (24 horas calendario).
	El especialista al cual se le haya sido asignado el incidente mayor debe informar a la mesa de servicio N1 el momento en que la falla sea solucionada para que desde allí se valide con los usuarios el restablecimiento del servicio.
	Es de obligatorio cumplimiento que el ingeniero que haya gestionado un incidente mayor diligencie el formato “Formato Reporte de Falla Incidente Mayor UNP” y lo adjunte al caso. El formato se entrega adjunto a este documento

CONTROLES	RESPONSABILIDADES
8.16 Actividades de seguimiento	Si el Incidente mayor es atribuible a un proveedor este deberá entregar un informe (informe Causa Raíz) con la información detallada de la incidencia y este será adjuntado a la herramienta.
	Cuando se resuelva un incidente mayor sin identificar la causa raíz, el ingeniero debe resolver el caso de incidente mayor con la solución temporal y solicitar al gestor de problemas la creación de un caso de problema para identificación de la causa raíz.
	Se debe realizar notificación a los usuarios la indisponibilidad de los servicios; así mismo el restablecimiento.

Fuente: Elaboración propia

7.2.17.1 Clasificación de la Información

CONTROL	RESPONSABILIDADES
5.12 Clasificación de la información **5.13 etiquetado de la información**	La Unidad Nacional de Protección define los niveles más adecuados para clasificar su información, de acuerdo con su sensibilidad.
	El Grupo de Gestión Documental, Interno de trabajo de apoyo a la secretaria general, deben diseñar lineamientos para la administración de los archivos de acuerdo con lo establecido en la Política.
	Las Tablas de Retención Documental (TRD) deben indicar el tipo de clasificación de las series, subseries y documentos en ella contenidas.
	Los Servidores Públicos, contratistas o terceros de la Unidad Nacional de Protección deben aplicar la clasificación de la información, las TRD, el inventario de activos de información y lineamientos para la administración de los archivos.
	Cada propietario del activo de Información debe velar por el cumplimiento de su clasificación de acuerdo con lo establecido en lineamientos para la administración de los archivos y activos de Información
	Para el intercambio de información se debe tener en cuenta su clasificación para su debida protección en términos de confidencialidad.

Fuente: Elaboración propia

7.2.17.2 Etiquetado de la información

CONTROLES	RESPONSABILIDADES
5.13 etiquetado de la información	El Grupo de Gestión Documental, brindará la directriz de cómo se debe etiquetar la información manejo que se dará a los documentos.

CONTROLES	RESPONSABILIDADES
	La información no etiquetada se presume como pública. La información en el Sistema de Gestión documental SGDA, se configura de acuerdo con el Manual de la Herramienta, y por controles de acceso y uso de la aplicación se registre el ingreso a los grupos pre-configurados
	El usuario que genera la información configurará permisos de acceso de acuerdo con las directrices y tipos de comunicados de la entidad.
	Para documentos con contenido mixto y/o que contengan información relacionada a la privacidad y protección de datos se debe usar la etiqueta: “Clasificada – Contiene Información pública y confidencial

Fuente: Elaboración propia

7.2.17.3 Manejo de Nube

CONTROLES	RESPONSABILIDADES
5.23 Seguridad de la información para el uso de servicios en la nube	La Unidad Nacional de Protección cuenta con la plataforma inteligente de Microsoft y licencias 365 que ofrece un espacio de trabajo compartido con diferentes soluciones para llevar a cabo tus proyectos desde un único sitio.
	El Grupo de Gestión Tecnológica, administra los servicios que brinda las licencias de 365 para operar en la UNP.
	El Grupo de Gestión Tecnológica, cuenta con un espacio en Intranet Share Point un espacio por dependencia y grupo el cual es administrado por ellos mismos en los cuales se manejan información institucional y compartida.
	Se recomienda que la información de carácter personal o relacionada con el trabajo individual se almacene en OneDrive, mientras que la información de interés grupal o colaborativa debe ser gestionada y almacenada en SharePoint. Esta práctica facilita la organización de los datos y mejora los controles de acceso, garantizando que la información se encuentre en la plataforma más adecuada según su uso y alcance.
	Para asegurar el acceso a la información almacenada en la nube, se debe implementar el uso de métodos de autenticación multifactor (MFA). Esta medida añade una capa adicional de seguridad que protege las cuentas y la información frente a accesos no autorizados, fortaleciendo la protección contra

	posibles amenazas

Fuente: Elaboración propia

7.2.17.4 Seguridad de la Información en la Continuidad de Negocio

CONTROLES	RESPONSABILIDADES
A5.29 Sistemas de información durante la interrupción **A.5.30 Preparación de las TIC para continuidad del negocio**	La Unidad Nacional de Protección establecerá un instrumento para la continuidad tecnológica donde se debe incluir la continuidad de la seguridad de la información y restauración oportuna de los servicios en un escenario de contingencia
	La Unidad Nacional de protección define lineamientos propios para el cumplimiento de las estrategias de continuidad establecidas en el protocol de contingencia de crisis de tecnología y seguridad de la información.
	El Grupo de Gestión de las Tecnológías, será la responsable de identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la entidad en seguridad de la información, evaluará los riesgos para determinar el impacto de dichas interrupciones, identificaran los controles preventivos, y recomendarán ajustes a los planes de contingencia necesarios para garantizar la continuidad de las actividades en la UNP.

Fuente: Elaboración propia

7.2.17.5 Derechos de propiedad intelectual

CONTROLES	RESPONSABILIDADES
5.32 Derechos de propiedad intelectual	La Oficina Asesora Jurídica debe implementar los documentos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
	La Oficina Asesora Jurídica es la responsable de definir que todas las obras creadas (Referencia; Software de aplicaciones y otros documentos de carácter confidencial industrial) serán propiedad de la Unidad Nacional de Protección, en cumplimiento del artículo 91 de la ley no 23 de 1982 (28 de enero de 1982) sobre derechos de autor.”
	El Grupo de Gestión de las Tecnologías, debe realizar revisiones periódicas del uso del software instalado en las estaciones de trabajo y servidores de la Entidad, con el fin de validar el cumplimiento de la Ley 603 de Derechos de Autor, conjuntamente debe identificar los activos de información que se encuentran afectados por derechos de propiedad intelectual

CONTROLES	RESPONSABILIDADES
	El Grupo de Gestión de las Tecnologías, debe asegurarse de que todo el software que se ejecute en de la Unidad Nacional de Protección esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
	Para todos los servidores y contratistas, es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de Ley.
	La Oficina Asesora Jurídica y el Grupo de Contratación deben incluir cláusulas de propiedad intelectual y derechos de autor en los contratos, que protejan el software, documentos, derechos de diseño, marcas registradas, patentes y códigos fuente.

Fuente: Elaboración propia

7.2.18 Políticas de Cumplimiento

CONTROLES	RESPONSABLES
5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información	El incumplimiento al presente Manual de Políticas específicas de Seguridad y Privacidad de la Información trae consigo, las consecuencias legales que apliquen a la Política de la Unidad Nacional de Protección y se comunicara a las dependencias de la falta a que haya lugar. El Grupo de Gestión de las Tecnologías, debe liderar la revisión periódica o cuando se requiera actualizar o anualmente en el cumplimiento de las políticas y procedimientos de seguridad de la información.

Fuente: Elaboración propia

8 VIGENCIA

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

9 DOCUMENTOS RELACIONADOS

- GTE-PL-01 Plan de Mantenimiento de la Infraestructura Tecnológica
- GTE-PL-02 Plan de seguridad y privacidad de la información
- GTE-PL-03 Plan de tratamiento de riesgos de seguridad y privacidad de la información
- GTE-PR.39 Procedimiento de Gestión de Medios Removibles

- GTE-PR-40 Procedimiento de Administración y Creación de Cuentas de Usuario y Cuentas Genéricas.
- GTE-FT-40 Formato Solicitud de Servicios Medios Removibles.
- GABS-FT-10 Formato Transferencia de Bienes.

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
01	Actualización de total del Manual para que refleje la realidad de la Entidad y las políticas de seguridad que actualmente se encuentran implementadas dentro de la UNP. Se establece un total de 16 políticas de seguridad de la información.	22/06/2022	02
02	Actualización del documento por cambio de imagen de gobierno, cambio en normatividad en relación con transparencia e inclusión de numerales nuevos en la policita de dispositivos móviles para generar claridad en relaciona manejo de puertos de comunicación. Se eliminaron 6 políticas del documento como la política de uso aceptable de activos, clasificación y etiquetado de la información, medios removibles, seguridad de la información y gestión de proyectos, control de acceso e instalación de software en sistemas operativos, toda vez que se crearán documentos adicionales para lineamientos y directrices de estas políticas al interior del proceso.	16/11/2023	03
03	Actualización del documento de forma que se refuerza la Política de control de acceso, responsabilidades de los usuarios con los recursos tecnológicos entregados por la Entidad, la Política de dispositivos móviles en la que se deja los responsables con lo que se aplica, contraseñas seguras dejando como medios de seguridad para que los usuarios tomen la Política y se aplique, la Política de los desarrollo y adquisición de los sistemas de información aplicando los controles de la ISO/ 27001- 2022, políticas, removibles, interoperabilidad, incidentes, etiquetado Actualización de logos de acuerdo con el manual de identidad de imagen vigente	01/11/2024	04

10 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, 2022 Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. Bogotá D.C: ICONTEC.
- ISO. Términos y Definiciones. En: Gestión de la seguridad de la información (Fundamentos y vocabulario). 2006. (POLÍTICA ISO/IEC 27000).
- 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 >
- POLÍTICA 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 >

11 ANEXOS

- Anexo 1. Declaración de Aplicabilidad – agosto de 2024
- Anexo 2 GTE-FT-50-V1Análisis de Impacto de Negocios-BIA por procesos
- Anexo 3 INFORME ANALISIS DE IMPACTO DE NEGOCIOS – BIA - UNP