CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	21/12/2020	Primera versión del documento
2	18/11/2021	Segunda versión del documento

Elabora	Revisa	Aprueba
Freddy Orlando Mora Granados Contratista Oficina de Generación del Conocimiento y la Información. **Martha Lucia Sanabria Ariza** Contratista Oficina de Generación del Conocimiento y la Información. **José Yesid Cutiva Oyola** Contratista Oficina de Generación del Conocimiento y la Información. **Laura Vanessa Torres Cepeda** Contratista Oficina de Generación del Conocimiento y la Información. **Edilberto Gutierrez Castillo** Contratista Planeación Normalización SIG	**Juan Carlos Hoyos Murillo** Profesional Universitario – Código 2044, grado 11 **Elsa Malo Lecompte** Profesional Especializado Grado 14 con Funciones de Planeación Revisión SIG	**María Rosa Angarita Peñaranda** Jefe Oficina de Generación del Conocimiento y la Información

Tabla de contenido

1. INFORMACIÓN GENERAL DEL PLAN

1.1 OBJETIVO GENERAL DEL PLAN:

Definir el plan estratégico de seguridad de la información en adelante PESI, para responder a la necesidad de preservar la confidencialidad, integridad y disponibilidad de los activos de información y disminuyendo el nivel de riesgos asociado a los activos.

1.1.1 OBJETIVOS ESPECÍFICOS

- Definir las responsabilidades relacionadas con el manejo de la Seguridad en la AUNAP.
- Establecer una metodología de gestión de la seguridad clara y estructurada.
- Reducir el riesgo de pérdida, robo o corrupción de información.
- Garantizar que los usuarios tengan acceso a la información a través de medidas de seguridad con la garantía de calidad y confidencialidad.
- Implementar monitoreo interno para identificar las debilidades del sistema y las áreas a mejorar.
- Garantizar la continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Cumplir con la legislación vigente sobre información personal y propiedad intelectual.
- Optimizar la gestión de la seguridad de la información con base en la gestión de procesos.

2. ALCANCE DEL PLAN:

El PESI tiene como finalidad el diagnóstico, análisis, definición y planeación del manejo de la seguridad de los procesos relacionados con los activos de información que se ejecutan en la AUNAP y será verificado y/o actualizado anualmente o conforme a la necesidad; este plan estratégico apoyará el cumplimiento de los procesos y objetivos propuestos por las diferentes dependencias de la Entidad y está articulado de manera global con la seguridad de la información, abarcando todos los elementos informáticos con que cuenta la entidad y el 100% de la información que se genera a través de los diferentes canales de comunicación de la AUNAP como lo son las radicaciones internas y externas, los documentos o comunicaciones generadas al interior o exterior de la entidad que tengan relación con las actividades donde participe la AUNAP.

3. FINALIDAD DEL PESI

La Autoridad Nacional de Acuicultura y Pesca a través del plan estratégico de seguridad de la información apoyará las siguientes actividades:

- Facilitar la integración de la seguridad de la información entre las unidades de negocio y con los clientes del portafolio ofrecido por AUNAP.
- Fortalecer las competencias de seguridad de la información, soportada en una infraestructura que permita su accesibilidad.
- Proponer alternativas que aseguren la información, estando a la vanguardia de la tecnología, que sean flexibles, adaptables y escalables para las necesidades que tenga la entidad.

4. DEFINICIONES

ACCESIBILIDAD: Se refiere a los medios y técnicas que posibilitan el acceso a la información de toda la entidad, usuarios y personas con limitaciones.

ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

AMENAZA: Causa potencial de un incidente no deseado, que pueda provocar daños a un sistema o a la organización.

AUTENTICACIÓN: Provisión de una garantía de que una característica afirmada por una entidad es correcta.

CONFIDENCIALIDAD: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

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 también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

CLASIFICACIÓN DE DATOS: El proceso de determinar la sensibilidad y criticidad de la información.

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

IMPACTO: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

INTEGRIDAD: La propiedad de salvaguardar la exactitud y complejidad de la información.

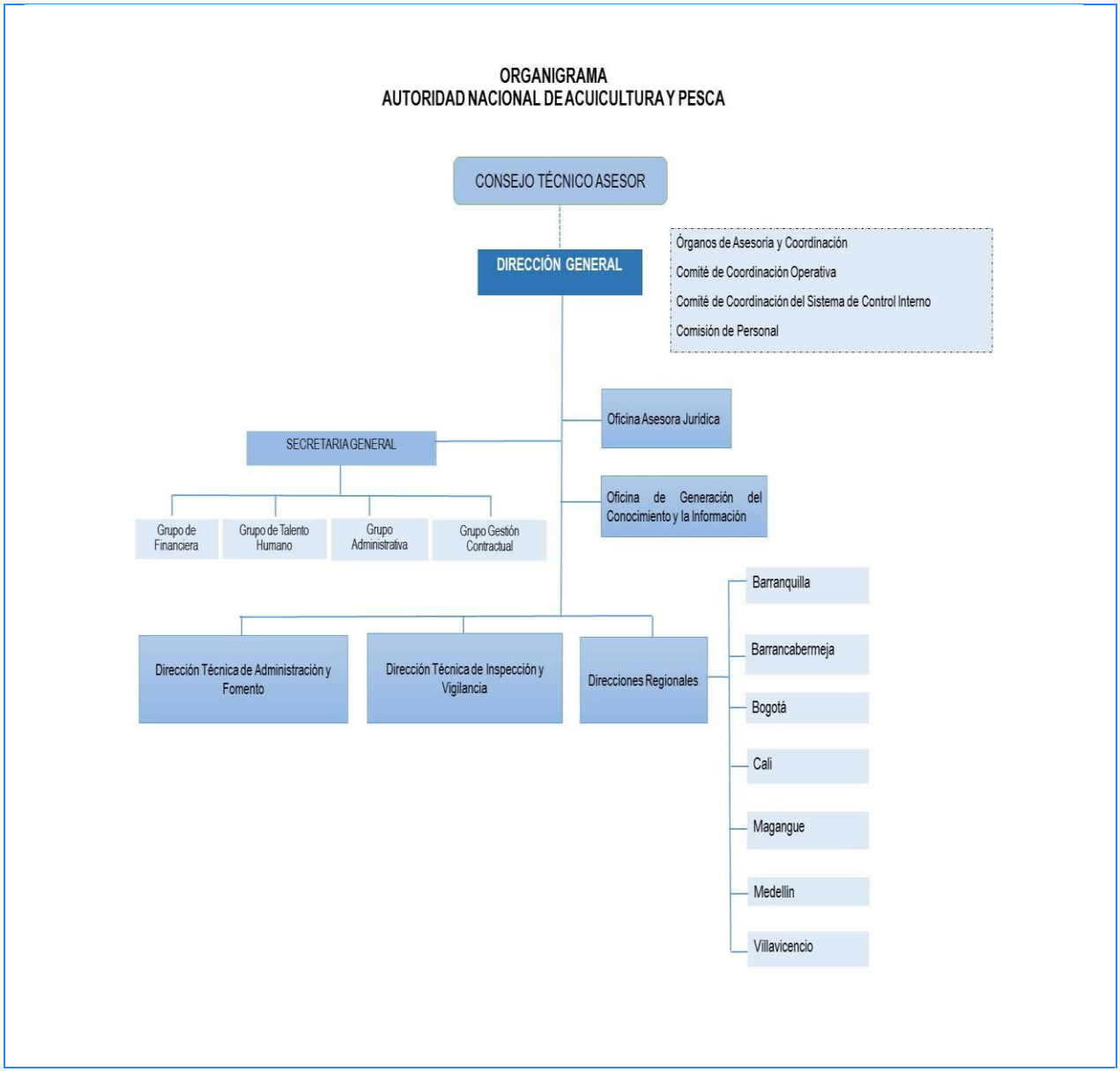
NORMA: Establecer los límites permisibles de acciones y procesos para cumplir con las políticas.

POLÍTICA: Declaración de alto nivel sobre la intención y la dirección de la gerencia.

RIESGO: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

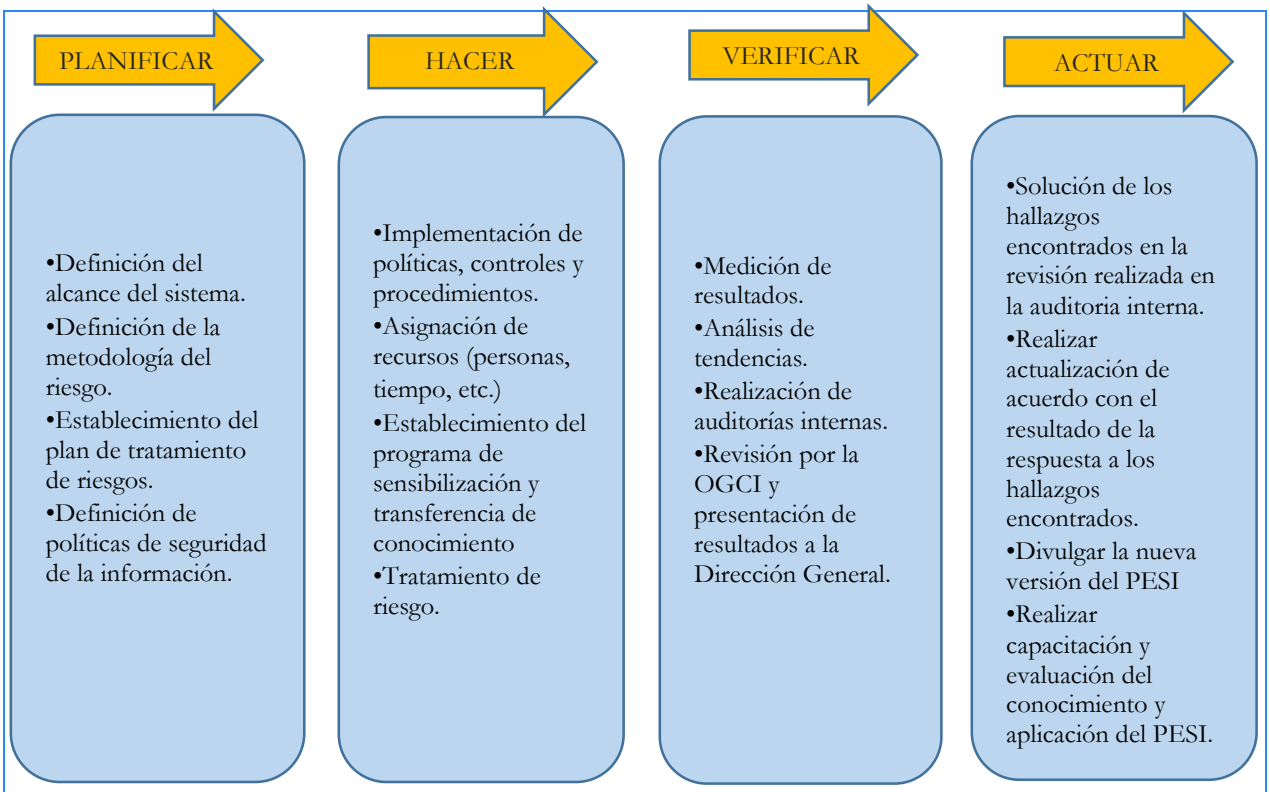
SEGURIDAD DE LA INFORMACIÓN: Preservación de la confidencialidad, integridad y disponibilidad de la información.

5. ESTRUCTURA ORGANIZACIONAL



6. PLANEACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La AUNAP trabaja permanentemente en pro de implementar el Sistema de Gestión de Seguridad dela Información - SGSI siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la Información - MSPI de la Política de Gobierno Digital con el fin de preservar la integridad, confidencialidad, disponibilidad de la información se cuenta, entonces, con un ciclo que permite establecer, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI.



7. ANÁLISIS DEL RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN

POLÍTICA MSPI	RIESGO	NIVEL DE RIESGO	IMPACTO	ZONA DE RIESGO	MITIGACIÓN
CONTROL DE ACCESO A LA INFORMACIÓN	-Tener el acceso por parte de personas no autorizadas a la información de la AUNAP -Presentar pérdida o daño de la información	Improbable	Moderado	Moderada	-Realizar controles para regular el acceso a las redes. -Hacer copias de respaldo de la información de los servidores. -Establecer un identificador único de usuaria (ID).

SERVICIOS DE COMPUTACIÓN EN LA NUBE	- presentar pérdida de información -Generar fuga de información	Probable	Menor	Alta	-Contar con antivirus en cada estación de trabajo. -Contar con firewall para proteger la salida y entrada de datos desde internet. -Copia de seguridad o backup de la información de los servidores.
TRANSFERENCIA O INTERCAMBIO DE INFORMACIÓN	- Generar fuga de información -Afectar la integridad del documento	Improbable	Insuficiente	Baja	-Acuerdos de confidencialidad -Copia de seguridad o backup de la información.
USO DE DISPOSITIVOS MÓVILES	-Ingresar un dispositivo móvil no autorizado a la red de la AUNAP -Afectar la disponibilidad de los servicios de red.	Rara vez	Moderado	Moderada	-Revisión periódica de los dispositivos móviles conectados a la red de la AUNAP. -Solicitud de acceso a la red de la AUNAP mediante corre electrónico a sistemas@aunap.gov.co -El área de Tics establecerá usuario y contraseña para el acceso del dispositivo móvil
RELACIONES CON PROVEEDORES	- Generar fuga de información -Afectar los servicios de red -Afectar la integridad de la información	Improbable	Insuficiente	Baja	-Acuerdos de confidencialidad -Autorizar el acceso solo al equipo o software requerido

ESCRITORIO Y PANTALLA LIMPIOS	-Presentar pérdida o daño de la información - Generar fuga de información	Rara vez	Insuficiente	Baja	-Controles de ingreso seguros a las estaciones de trabajo -Bloqueo de la sesión por inactividad -Solicitud de cambio de contraseña cada 2 meses
RESPALDOS DE INFORMACIÓN	- Presentar pérdida de información	Rara vez	Mayor	Alta	-Copia de seguridad o backup de la información. -Restablecimiento de las copias de seguridad o backup de la información
DESARROLLO DE SOFTWARE	-Incumplir los estándares para el desarrollo de software	Improbable	Insuficiente	Baja	-Establecer una metodología para el desarrollo a realizar
PROTECCIÓN DE DATOS PERSONALES (HABEAS DATA)	- Generar fuga de información de datos personales -Afectar el derecho a la intimidad de las personas, de quien se tengan los datos.	Improbable	Mayor	Alta	-Acceso a las bases de datos solo a personal autorizado mediante usuario y contraseña -Verificación periódica de la existencia de autorización por parte del titular del uso de los datos personales -Verificación de la destrucción de la información de datos personales, cuando así se requiera -Paz y Salvo de entrega de los equipos de cómputo

Una vez realizado el análisis, se determina el nivel de riesgo inherente aplicando el mapa de calor

Probabilidad de ocurrencia						
	CASI SEGURO (5)	A	A	E	E	E
	PROBABLE (4)	M	A	A	E	E
	POSIBLE (3)	B	M	A	E	E
	IMPROBABLE (2)	B	B	M	A	E
	RARA VEZ (1)	B	B	M	A	E
		INSIGNIFICANTE (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATASTROFICO (5)
	Impacto					

B: Zona de riesgo Baja: Asumir el riesgo, Reducir el riesgo
M: Zona de riesgo Moderada: Reducir el riesgo, Eliminar
A: Zona de riesgo Alta: Reducir el riesgo, Eliminar, Evitar, Compartir o Transferir
E: Zona de riesgo Extrema: Reducir el riesgo, Eliminar, Evitar, Compartir o Transferir[1]

8. PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

A continuación, se presentan los procedimientos de seguridad de la información para el Modelo de Seguridad y privacidad de la Información.

8.1. SEGURIDAD DEL RECURSO HUMANO: Con los funcionarios y contratista de la entidad se plantean los siguientes procedimientos.

- CAPACITACIÓN Y SENSIBILIZACIÓN DEL PERSONAL: Realizar la capacitación y sensibilización del personal en temas de seguridad de la información teniendo en cuenta los diferentes roles y responsabilidades.

- INGRESO Y DESVINCULACIÓN DEL PERSONAL: Esto indica la manera como la AUNAP gestionará de manera segura del ingreso y desvinculación, incluyendo temas como verificación de antecedentes, firma de acuerdos de confidencialidad del tratamiento de la información para contratistas y recepción de entregables

[1] Tomado del Manual Integral de Gestión del Riesgo - AUNAP – MN-DE-001 V2

requeridos para generar paz y salvos al finalizar el contrato o acta de entrega para funcionarios.

8.2. GESTIÓN DE ACTIVOS: En la entidad se pueden encontrar los siguientes activos los cuales se clasifican de acuerdo a su criticidad y nivel de confidencialidad.

· IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS:

En atención a la misionalidad y las funciones de la AUNAP se establecen como activos de información los siguientes, con su respectiva clasificación de acuerdo a su nivel de confidencialidad o criticidad:

ACTIVO	CLASIFICACIÓN
SEPEC	Pública
RGPA	Pública
AZ DIGITAL	Clasificada
PÁGINA WEB	Pública
INTRANET	Reservada
RED LAN	Clasificada
RED WIFI	Clasificada
EQUIPOS DE COMPUTO	Clasificada
EQUIPOS DE IMPRESIÓN	Clasificada
SERVIDORES	Reservada
SISTEMA DE ALMACENAMIENTO Y BACKUP	Reservada
CORREO ELECTRÓNICO	Clasificada
EXPEDIENTES JURÍDICOS	Clasificada
EXPEDIENTES CONTRACTUALES	Pública
FILE SERVER	Clasificada
RECURSO HUMANO	Clasificada
SOFTWARE DE NOMINA	Reservada
SOFTWARE DE ALMACÉN	Clasificada
ALMACÉN DE LA ENTIDAD	Clasificada
SIRECI	Clasificada
SIIF	Clasificada

8.3. CONTROL DE ACCESO: La AUNAP para acceder a la información y a sus instalaciones estableció ciertas medidas de acceso que se explican a continuación:

- INGRESO SEGURO A LOS RECURSOS DE LA ENTIDAD:

Conforme a la clasificación de los activos de información por el nivel de criticidad o confidencialidad se establecen las siguientes medidas de acceso:

ACTIVO	INGRESO
SEPEC	Autenticación
RGPA	Autenticación
AZ DIGITAL	Autenticación
RED LAN	Autenticación
RED WIFI	Autenticación
EQUIPOS DE COMPUTO	Autenticación
EQUIPOS DE IMPRESIÓN	A través de equipo de cómputo y autenticación
SERVIDORES	Autenticación
SISTEMA DE ALMACENAMIENTO Y BACKUP	Autenticación
CORREO ELECTRÓNICO	Autenticación
EXPEDIENTES JURÍDICOS	Autorización del responsable de la información y/o por orden judicial
FILE SERVER	Autenticación
RECURSO HUMANO	Autorización del responsable de la información y/o por orden judicial
SOFTWARE DE NOMINA	Autorización del responsable de la información, autenticación y/o por orden judicial
SOFTWARE DE ALMACÉN	Autorización del responsable de la información y autenticación
ALMACÉN DE LA ENTIDAD	Autorización del responsable de la información y cerradura de seguridad
SIRECI	Autenticación
SIIF	Autenticación

- AUTENTICACIÓN: las contraseñas establecidas deberán tener un nivel de seguridad aceptable, prohibiendo hasta una tercera reutilización posterior, solicitando automáticamente el cambio cada dos meses, incluyendo mayúsculas, números y caracteres especiales o permitiendo a los usuarios cambiarla regularmente.

- SEGURIDAD FÍSICA Y DEL ENTORNO: El acceso a áreas no autorizadas de la AUNAP, se llevará a cabo, mediante lector de huellas y/o llave de seguridad y/o tarjeta de proximidad.

  En caso de requerir acceso a un área restringida, deberá solicitarse por escrito al responsable de esta área a su cargo.

- CONTROL DE ACCESO FÍSICO: El acceso seguro a las instalaciones de la AUNAP por parte del personal autorizado se hará mediante lector de huellas y/o tarjeta de proximidad.

- PROTECCIÓN DE ACTIVOS:

Conforme al tipo de activo de información la AUNAP establece su ubicación en atención al servicio prestado y pertinencia del mismo y consigo las medidas de protección ante cualquier necesidad o suceso inesperados de la siguiente forma:

ACTIVO	UBICACIÓN (lugar de almacenamiento)	MEDIDA DE PROTECCIÓN
SEPEC	Data center	Lector de huella y registro de ingreso al Data center. Detector humedad. Detector de humo. Contar con polo a tierra.
RGPA	Data center	Lector de huella y registro de ingreso al Data center. Detector humedad. Detector de humo. Contar con polo a tierra.
PÁGINA WEB	Hosting	Protección con firewall. Medidas de protección propias del Hosting.
INTRANET	Hosting	Protección con firewall. Medidas de protección propias del Hosting.
RED LAN	Infraestructura entidad	Protección con firewall. Protección propia de los switches. Cableado estructurado. Autenticación por dominio. Autenticación por equipo de cómputo.
RED WIFI	Infraestructura entidad	Protección con firewall. Protección propia de los access point.

		Autenticación por SSID
EQUIPOS DE COMPUTO	Estación de trabajo	Protección con firewall. Protección propia de las estaciones de trabajo. Autenticación por dominio. Autenticación por equipo de cómputo. Protección con antivirus.
EQUIPOS DE IMPRESIÓN	Infraestructura entidad	Autenticación por dominio. Autenticación por equipo de impresión.
SERVIDORES	Infraestructura entidad	Protección con firewall. Protección propia de los servidores. Autenticación por dominio. Protección con antivirus. Lector de huella y registro de ingreso al Data center. Detector humedad. Detector de humo. Contar con polo a tierra.
SISTEMA DE ALMACENAMIENTO Y BACKUP	Infraestructura entidad	Protección con firewall. Protección propia del sistema de almacenamiento. Autenticación por dominio y propio del sistema de backup. Protección con antivirus. Lector de huella y registro de ingreso al Data center. Detector humedad. Detector de humo. Contar con polo a tierra.
CORREO ELECTRÓNICO	Servicio en la nube	Protección con firewall. Medidas de protección propias del servicio de correo electrónico en la nube. Autenticación propia del servicio.
EXPEDIENTES JURÍDICOS	Estantería y almacenamiento en la entidad	Acceso restringido. Chapa o control de acceso de seguridad. Bitácora de ingresos. Bitácora de préstamo de expedientes.

		Backup digital de los expedientes.
EXPEDIENTES CONTRACTUALES	Estantería y almacenamiento en la entidad	Bitácora de préstamo de expedientes. Backup digital de los expedientes.
FILE SERVER	Infraestructura entidad	Protección con firewall. Protección propia del file server. Autenticación por dominio. Protección con antivirus. Lector de huella y registro de ingreso al Data center. Detector humedad. Detector de humo. Contar con polo a tierra.
RECURSO HUMANO	Colaboradores	Acuerdo de confidencialidad para contratistas. Salidas de emergencia y/o rutas de evacuación. Control de ingreso. Capacitaciones. Seguridad en el trabajo y salud ocupacional. Bienestar humano.
SOFTWARE DE NOMINA	Data center	Protección con firewall. Protección propia de la aplicación. Autenticación por dominio. Protección con antivirus. Lector de huella y registro de ingreso al Data center. Detector humedad. Detector de humo. Contar con polo a tierra.
SOFTWARE DE ALMACÉN	Data center	Protección con firewall. Protección propia de la aplicación. Autenticación por dominio. Protección con antivirus. Lector de huella y registro de ingreso al Data center. Detector de humo. Contar con polo a tierra.

ALMACÉN DE LA ENTIDAD	Estantería y almacenamiento en la entidad	Acceso restringido. Chapa o control de acceso de seguridad. Bitácora de ingresos. Bitácora de préstamo o asignación de elementos. Video vigilancia

9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

9.1. DESARROLLO DE SOFTWARE

- En caso de desarrollos propios la OGCI mediante los profesionales de apoyo en sistemas asignaran recursos tecnológicos independientes para los ambientes de desarrollo, prueba y producción.

- La OGCI mediante los profesionales de apoyo en sistemas deberá realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la operatividad de estos.

- La OGCI mediante los profesionales de apoyo en sistemas desarrollará y/o adquirirá el software requerido por la AUNAP; de manera coordinada con el Área que manifieste la necesidad del software.

- La OGCI mediante los profesionales de apoyo en sistemas será la única dependencia autorizada para realizar copia de seguridad del software original y la instalación de este en y los equipos informáticos de la AUNAP.

- La OGCI mediante los profesionales de apoyo en sistemas implementará reglas y herramientas que restrinjan la instalación de software no autorizado en los equipos de información que hacen parte de la AUNAP.

9.2. MANTENIMIENTO DE EQUIPOS:

- El mantenimiento preventivo de cada equipo tecnológico de la entidad deberá ser realizado por lo menos una vez al año, el cual implique el mantenimiento y limpieza de la parte física y las actualizaciones disponibles de software y las aplicaciones.

- El mantenimiento correctivo de cada equipo tecnológico de la entidad deberá ser registrado bajo solicitud a los profesionales de apoyo de sistemas, el cual va a ser atendido con base en los acuerdos de nivel de servicio ANS.

- El mantenimiento mejorativo de cada equipo tecnológico de la entidad deberá ser registrado bajo solicitud a los profesionales de apoyo de sistemas, el cual va a ser atendido con base en la disponibilidad de repuestos o presupuesto.

9.3. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS

- En la AUNAP cada uno de los equipos deberá contar con la licencia de software del antivirus y sus respectivas actualizaciones de definiciones de virus, que permitan controlar la protección contra códigos maliciosos

9.4. TRANSFERENCIA DE INFORMACIÓN

- La transferencia de la información se debe realizar previa autorización del custodio de la información, la cual se realizará de manera segura dentro de la entidad o con entidades externas, de acuerdo con la herramientas disponibles y autorizadas por la AUNAP.

9.5. CONTROL SOFTWARE:

- La AUNAP realizara el control de software, mediante la restricción para la instalación del software del usuario asignado a cada equipo de cómputo, es decir, solo el área de sistemas de la entidad a través del usuario administrador podrá realizar la instalación del software en cada equipo.

- El control de inventario de software se realizará mediante una herramienta o una bitácora que registre la cantidad de software instalado en los quipos de computo de la AUNAP.

10. ROLES Y RESPONSABILIDADES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Todos los funcionarios de la AUNAP serán responsables de identificar, evaluar y controlar los riesgos de seguridad de información que generen sus actividades y/o funciones.

Los jefes o Directores de las diferentes dependencias de la AUNAP designarán un responsable para garantizar el cumplimiento de las políticas de la seguridad de la información y Seguridad Digital, quién será el garante de la información que se genere en dicha área y almacenarla en un medio asignado por el Tics, con su respectiva copia de seguridad.

La responsabilidad de la persona delegada de la seguridad de la información de cada área, deberá realizar los siguientes controles:

- Identificar, registrar y actualizar los activos de información de su dependencia o proceso de responsabilidad.
- Realizar la clasificación y valorización de los activos de información y adelantar una revisión anualmente.
- Revisar y gestionar que los controles de seguridad sean implementados de acuerdo al nivel de clasificación de la información de su proceso.
- Determinar los privilegios de acceso y criterios de respaldo para los activos de información bajo su responsabilidad.

- Revisar y asegurar que los privilegios de acceso a los activos de información de los cuales es responsable sean los adecuados.
- Comunicar violaciones de seguridad, actividades sospechosas o incidentes sobre los activos de información de su proceso.
- Garantizar que la información que le ha sido confiada sea protegida durante todo su ciclo de vida (creación, almacenamiento, distribución, transporte y destrucción segura) de modificaciones y usos no autorizados.

11. PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN

El plan estratégico corresponde a la ejecución de los proyectos propuestos concernientes al tema de seguridad de la información que aportan al cumplimiento de los objetivos de seguridad de la información y al plan estratégico TIC (PETI).

- Desarrollar el programa de capacitación y sensibilización en seguridad de la información para empleados, contratistas, proveedores y Terceros.
- Operación y mantenimiento del Sistema de Gestión de Seguridad de la Información.
- Gestión de Riesgos de Seguridad de la Información.
- Realizará análisis de vulnerabilidades.

12. GESTIÓN DE LOS PROYECTOS

La AUNAP actualmente tiene en ejecución y en elaboración los siguientes proyectos que contribuyen a la seguridad de la información de la Entidad alineados con el Plan de Seguridad y Privacidad de la Información, y la Implementación de la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, Decreto 1008 de 2018.

Descripción del Proyecto que apoya la seguridad de la información en la AUNAP	Estado del proyecto
1. Contrato de consultoría 296 de 2020, para la transición al protocolo IPV6	Ejecutado, se debe actualizar cada año
2. Contrato 286 de 2021 el desarrollo de software de Guías de Movilización o Salvoconductos	En ejecución
3. Compra de computadores, impresoras y escáner	Ejecutado 2021
4. Renovar el aire acondicionado y UPS para el datacenter	En ejecución
5. Contratar software de Mesa de Ayuda	En elaboración de estudios previos

	para contratación 2022
6. Asegurar el funcionamiento y la operación de la infraestructura adquirida en el 2021, a nivel de centro de datos y red de comunicaciones (Para 2022)	Se realizará en el año 2022
7. Realizar el aseguramiento y corrección de las vulnerabilidades mediante los escaneos periódicos y en los informes de hacking ético interno (Para 2022)	Pendiente de elaboración del proyecto
8. Actualización y depuración de inventario físico de computadores y elementos TICs, en el sistema QUICK DATA (Para 2022)	Se realizará en el año 2022
9. Implementar procedimientos que permitan la realización de las copias de seguridad y contraseñas seguras (Socializar con los funcionarios de AUNAP el plan de seguridad y procedimientos). (Para 2022)	Se realizará en el año 2022
10. Contratar la implementación del software para control de impresión	Se realizará en el año 2022
11. Contratar un segundo canal de internet para tener mayor disponibilidad del servicio	Se realizará en el año 2022
12. Contratar servicio de hosting para la página WEB y la Intranet	Se realiza cada año

Esta gestión de proyectos podrá ser actualizada o modificada de acuerdo a las Políticas de Gobierno Digital de MINTICS.

13. INFORMACIÓN DOCUMENTADA RELACIONADA

13.1 DOCUMENTOS INTERNOS

DOCUMENTO	CÓDIGO	RESPONSABLE DEL DOCUMENTO	TIEMPO TRD
N/A	N/A	N/A	N/A

13.2 DOCUMENTOS EXTERNOS

DOCUMENTO	FECHA DE PUBLICACIÓN	ENTIDAD QUE EMITE EL DOCUMENTO	MEDIO DE CONSULTA
N/A	N/A	N/A	N/A

13.3 NORMATIVIDAD VIGENTE

NORMA	AÑO	EPÍGRAFE	ARTÍCULO(S)
N/A	N/A	N/A	N/A