CONTROL DE CAMBIOS		
VERSION	**FECHA**	**DESCRIPCION DE LA MODIFICACION**
1	06/10/2020	Primera versión del documento

Elabora	Revisa	Aprueba
Heidelberg Eleycer Cossio Mena Contratista Oficina de Generación del Conocimiento y la Información **Larry Javier Robles Cubillos** Contratista Oficina de Generación del Conocimiento	**Ulver María Triviño Hermida** Revisión Sistema Integrado de Gestión	**María Rosa Angarita Peñaranda** Jefe Oficina de Generación del Conocimiento y la Información

Contenido

1 INFORMACIÓN GENERAL

La Política de Seguridad y Privacidad de la Información de la Autoridad Nacional de Acuicultura y Pesca (AUNAP en adelante) tienen como fin determinar los requisitos para preservar la confidencialidad, integridad y disponibilidad de la información, mediante la aplicación de procedimientos y controles debidamente alineados a las necesidades y objetivos estratégicos de la AUNAP. En lo esencial, las políticas aquí descritas brindan las herramientas necesarias para que los funcionarios, contratistas y terceros involucrados dentro de la gestión de la seguridad de la información AUNAP puedan ajustar los controles exigidos para asegurar la información, gestionar adecuadamente los riesgos de seguridad, hacer usos de los controles establecidos y procurar la mejora continua, buscando la implementación escalonada de un sistemas articulado de gestión de seguridad y privacidad de la información

El cumplimiento de las políticas de seguridad de la información y la posterior implementación del Sistema de seguridad y privacidad de la información comprende la integración de procesos, sistemas de información y controles orientados hacia un objetivo común: lograr una adecuada y eficiente gestión de los riesgos que genere un nivel de confianza óptimo a las partes interesadas. Entre otros fines, las políticas estarán orientadas a: generar controles para proteger los activos de información; generar conciencia en los usuarios frente al uso responsable de las tecnologías de la información y comunicaciones y realizar una gestión de riesgos adecuada que permita minimizar su impacto.

Las políticas deberán ser conocidas y cumplidas plenamente por todos los funcionarios, contratistas y terceras partes de la Autoridad Nacional de Acuicultura y Pesca - AUNAP que tienen acceso a los activos de la información y a los sistemas de procesamiento de información.

1.1. Objetivo de la política

Generar lineamientos para conservar y salvaguardar los activos de la información, y proteger los datos producidos por los procesos de la AUNAP, evitando su posible pérdida mediante exposición a amenazas latentes en el entorno, como acceso no autorizado, manipulación o deterioro de la información.

1.2. Alcance

Esta política aplica a todos los funcionarios, contratistas, terceros y partes interesadas de la entidad que en el ejercicio de sus funciones utilicen información y servicios TI de la AUNAP.

2.0. Glosario

Las siguientes definiciones fueron tomadas de la Guía de mi TIC, de la norma ISO y otros documentos que se relacionan:

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.

Amenaza informática: la aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado (Ministerio de Defensa de Colombia).

Análisis de riesgos: proceso para comprender la naturaleza del riesgo y determinar su nivel de riesgo.
Anonimización del dato: eliminar o sustituir algunos nombres de personas (físicas o jurídicas). Direcciones y demás información de contacto. Números identificativos. Apodos o cargo.

Autenticación: provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad: Propiedad de que una entidad es lo que afirma ser. (ISO 27000.es, 2012).

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

Ciberespacio: ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701).

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.

Custodio de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de administrar y hacer efectivo los controles que el- propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

Datos abiertos: son datos primarios o sin procesar. Los cuales son puestos a disposición de cualquier ciudadano. Con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos biométricos: parámetros físicos únicos de cada persona que comprueban su identidad y se evidencian cuando la persona o una parte de ella interacciona con el sistema (ej. huella digital o voz).

Datos personales sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Dato privado: es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

Dato público: es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.

Dato semiprivado: es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

Disco duro: disco de metal cubierto con una superficie de grabación ferro magnético. Haciendo una analogía con los discos musicales, los lados planos de la placa son la superficie de grabación, el brazo acústico es el brazo de acceso y la púa (aguja) es la cabeza lectora/grabadora. Los discos magnéticos pueden ser grabados, borrados y regrabados como una cinta de audio.

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

DVD: Disco Versátil (video) Digital. En la actualidad constituye el natural sucesor del CD para la reproducción de sonido e imagen de calidad.

Evento de seguridad de la información: ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

Gestión de claves: son controles que realizan mediante la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información: procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: actividades coordinadas para dirigir controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Habeas data: derecho a acceder a la información personal que se encuentre en archivos o bases de datos; implica la posibilidad de ser informado acerca de los datos registrados sobre sí mismo y la facultad de corregirlos.

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.

Incidente de seguridad de la información: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
Integridad: la propiedad de salvaguardar la exactitud y complejidad de la información.

Inventario de activos: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos. (ISO 27000.es, 2012)

No repudio: servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido). (ISO-7498-2).

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.

Plan de continuidad del negocio: plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

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.

Proceso: conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas. (ISO 27000.es, 2012)

Propietario de activo de información: identifica a un individuo, un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

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).

Responsable del tratamiento: persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros. Decida sobre la base de datos y/o el Tratamiento de los datos.

Segregación de tareas: reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información.

Subsistema 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, basando en un enfoque de gestión y de mejora a un individuo o entidad.

Titular de la información: es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

Teletrabajo: actividad laboral que se desarrolla afuera de las instalaciones de la entidad, las cuales emplean tecnologías de la información y de la comunicación para su desarrollo.

Trazabilidad: cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas. (ISO 27000.es, 2012).

Siglas

(**CPD)** Centro de procesamiento de datos Data Center Princ

(TICs) Tecnologías de la Información y la Comunicación

3. Normatividad vigente

Ley 1221 de 2008, Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
Ley 527/99 Por medio de la cual se define y se reglamenta el acceso y el uso de los mensajes de datos. El mensaje de datos es "La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos, Internet, el correo electrónico, el telegrama, el té/ex o el telefax.
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.
Ley 1273/09 Por medio de la cual 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. "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos".
Resolución 2886 de 2012- Por la cual se definen las entidades que harán parte de la Red Nacional de Fomento al Teletrabajo y se dictan otras disposiciones.
Ley 1581/12 Por medio de la cual se dictan disposiciones generales para la Protección de Datos Personales. Hace referencia, principalmente, al artículo 15 de la Constitución Nacional en el cual se establece que "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 bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución". La ley tiene por objeto "desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma"
Decreto 884 de 2012 Por medio del cual se reglamenta la Ley 1221 de 2008 y dictan otras disposiciones. El propósito de la Ley 1221 de 2008 es promover y regular el teletrabajo como un instrumento de generación de empleo y autoempleo mediante la utilización de tecnologías de la información y las telecomunicaciones.

Decreto 886 de 2014 Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, en lo relativo al Registro Nacional de bases de datos. Serán objeto de inscripción en el Registro Nacional de Bases de Datos, "las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual se realice por personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él, en este último caso, siempre que al responsable del Tratamiento o al Encargado del Tratamiento Je sea aplicable la legislación colombiana en virtud de normas y tratados internacionales. Lo anterior sin perjuicio de las excepciones previstas en el artículo 2º de la Ley 1581 de 2012".

Decreto Nacional 2573 de 2014 Estrategia de Gobierno en Línea ahora Gobierno Digital de la Republica de Colombia**, e**l Decreto establece los lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Decreto 1008 de 2018 Por medio del cual se establecen los lineamientos generales de la política de Gobierno Digital

Ley 1712 DE 2014 Ley de Transparencia y de Derecho de Acceso a la Información Pública
Hace referencia, principalmente, al artículo 74 de la Constitución Nacional en el cual se establece que "Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la ley".
El objeto de la ley es "regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información".

4. Políticas de Seguridad y Privacidad de la Información

La Autoridad Nacional de Acuicultura y Pesca - AUNAP, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de la política de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para La Autoridad Nacional de Acuicultura y Pesca - AUNAP, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la Entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de La Autoridad Nacional de Acuicultura y Pesca – AUNAP.
- Garantizar la continuidad del negocio frente a incidentes.

5. Descripción de las políticas

5.1. Política No.1. Control de acceso a la información

5.1.1. Objetivo:
Definir los lineamientos generales para controlar el acceso a la información, los activos y sistemas informáticos de la AUNAP.

5.1.2 Alcance

La política aplica a todos los funcionarios, contratistas y terceros que tengan acceso a la información, activos y sistemas informáticos de la Autoridad Nacional de Acuicultura y Pesca - AUNAP.

5.1.3. Detalle

La AUNAP, como se ha mencionado, tiene como fin preservar la confidencialidad, integridad y disponibilidad de los activos de información que son accedidos o se encuentran a cargo de los funcionarios o contratistas debido a su cargo y/o responsabilidades. Por tal motivo, ha establecido controles que permitan regular el acceso a las redes, datos e información, así como la implementación de perímetros de seguridad para la protección de las instalaciones, especialmente, aquellas clasificadas como áreas restringidas, como los centros de procesamiento de información, áreas de almacenamiento de información física, cuartos de suministro de energía eléctrica, aire acondicionado, entre otras.

Todos los funcionarios públicos y contratistas que laboran para la AUNAP deben tener acceso sólo a la información necesaria para el desarrollo de sus funciones y/o actividades. En el caso de personas ajenas a la AUNAP, la Dirección General, Secretaria General, Dirección Técnica de Inspección y Vigilancia y la Dirección Técnica de Administración y Fomento, La Oficina de Generación del Conocimiento y la Información, las Direcciones Regionales y la Oficina Asesora Jurídica deben autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación. Para que un funcionario público o contratista tenga acceso a los servicios y recursos informáticos dispuestos por la AUNAP, se requiere que el jefe inmediato, coordinador, Secretario General o el Director General solicite a la oficina de Gestión de Servicios Tics, mediante un oficio escrito, la activación de dichos servicios con el perfil requerido y las restricciones de algunos servicios. Cada vez que se recibe una computadora de escritorio o portátil para darle acceso a los servicios tecnológicos que brinda la institución a los usuarios, es necesario, requerido y obligatorio, por parte de la Oficina de Mantenimiento de equipos de cómputo, entregar el equipo con todos los servicios instalados, configurados y en operación. Esto es, instalación, y configuración de un antivirus, actualización al último programa y versión de la base de datos de vacunas del antivirus, instalación y configuración del servicio de red inalámbrica, verificación e instalación de herramienta para comprimir, verificación e instalación de herramienta para gestionar archivos PDF, verificación e instalación de herramientas para la trasferencia de información. El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin. Todos los privilegios para el uso de los sistemas de información de la institución deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la AUNAP. Proveedores o terceros las personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas. Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la institución, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal. Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la institución, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones tendientes a su solución.

La AUNAP llevará a cabo un control de acceso a la información que tendrá en cuenta tanto los aspectos lógicos como físicos que permitan garantizar la trazabilidad de las acciones realizadas, identificando, entre otros datos relevantes, quién realiza el acceso, las operaciones ejecutadas, hora, lugar, fecha y cantidad de intentos de accesos denegados, etc.

Una vez se apruebe el acceso a la información, los funcionarios y contratistas no deben realizar modificaciones sobre la información sin la debida autorización, guardar confidencialidad de la información a la cual tiene acceso, no vulnerar los controles de seguridad establecidos por la AUNAP, informar al Oficial de Seguridad de la Información sobre las debilidades o eventos de seguridad.

5.1.4. Responsabilidades

La información de naturaleza pública de la AUNAP debe de estar disponible al ciudadano siempre y cuando no esté sometida a reserva legal o existan restricciones para su acceso.

El acceso a la información será controlado conforme a los roles y responsabilidades de los funcionarios y contratistas de la AUNAP. La autorización será otorgada por los responsables de los activos de información. Los registros de acceso y actividades desarrolladas podrán ser auditadas para propósitos de control e investigación a los que haya lugar dentro de la naturaleza de la AUNAP, y así mismo para minimizar el riesgo de la pérdida de integridad o confidencialidad de la información.

Como responsables de la información, los funcionarios, contratistas y terceros de la Autoridad Nacional de Acuicultura y Pesca deberán administrar y hacer cumplir los lineamientos establecidos, con el fin de evitar accesos no autorizados, pérdidas o utilización indebida de los activos de información.

Los funcionarios, contratistas y terceros de la Autoridad Nacional de Acuicultura y Pesca, tienen como responsabilidad velar por la integridad, confidencialidad y disponibilidad de la información, los activos y los sistemas informáticos para los cuales han sido designados y autorizados, asegurándose que estos solo sean utilizados para el desarrollo de las labores encomendadas dentro de la AUNAP.

Los accesos tanto físicos como lógicos, asignados a los funcionarios, contratistas y terceros deberán ser desactivados o modificados una vez terminados los vínculos contractuales con la AUNAP.

Todos los usuarios tendrán un identificador único (ID del usuario) para su uso personal que les permita validar los accesos y verificar su buen uso.

AUNAP establecerá controles para restringir accesos a áreas seguras, entre otros, deberá registrar los sistemas, datos de identificación de la persona que accede a la información, el motivo de ingreso, el tiempo empleado para el desarrollo de la actividad, y asimismo, cuidará que un responsable del activo de información acompañe a la persona durante su instancia en el área.

El responsable o Encargado del activo de información será el responsable de realizar revisiones periódicas de los derechos de acceso de los usuarios a intervalos regulares.

5.2. Política No.2. Servicios de computación en la nube

5.2.1 Objetivo

Mantener la seguridad de la información y de los servicios de procesamiento de información en plataformas de computación en la nube que son utilizados por la AUNAP, garantizando su continuidad, cumpliendo los niveles de servicio requeridos por los procesos de la Entidad y reduciendo los riesgos legales y técnicos a niveles aceptables.

5.2.2 Alcance

Esta política se aplica a los servicios de computación en nube que sean utilizados o contratados por la Entidad, así como a los procesos que hagan uso de dichos servicios.

5.2.3 Detalles

En los procesos de contratación y uso de servicios de computación en la nube se deben identificar, valorar y gestionar los riesgos de seguridad asociados al tratamiento de información institucional, acceso a información personal, protección de secretos comerciales, riesgos legales, riesgos técnicos, riesgos de continuidad y riesgos asociados a la transmisión transfronteriza de la información institucional o personal. El análisis y gestión de los riesgos se debe realizar de acuerdo con el procedimiento Gestión de riesgo del Sistema Integrado de gestión de la AUNAP. Los resultados del análisis y gestión de riesgos se deben documentar de acuerdo con el procedimiento de gestión de riesgo de la AUNAP. No se deben utilizar servicios de computación en la nube cuyo análisis de riesgos indique niveles no tolerables para la protección de información institucional o personal. Los resultados del análisis y gestión riesgos deben ser determinantes para aceptar o rechazar para la utilización de servicios de computación en la nube de pago o gratuitos.

En los contratos celebrados con proveedores de servicios de computación en la nube se debe incluir la necesidad de cumplir las políticas de seguridad de la información de la Entidad, el cumplimiento de los acuerdos de niveles de

servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, leyes y regulaciones sobre la protección de la información de la Entidad e información de carácter personal.

En los casos que se requiera el almacenamiento de información en la nube clasificada como reservada, pública clasificada e información de carácter personal esta debe permanecer cifrada para evitar su divulgación o acceso no autorizados. El cifrado se debe realizar de acuerdo con las políticas de seguridad de la información definidas por el sistema de gestión de seguridad de la información de la AUNAP.

5.2.4 Responsabilidades

Las personas encargadas de procesos de la AUNAP son responsables de coordinar la ejecución de las actividades de análisis y gestión de riesgos para el uso de servicios de computación en la nube

TICs es responsable de asistir a los diferentes procesos de la Entidad en la identificación, gestión y tratamiento de los riesgos asociados al uso de servicios de computación en la nube.

Todos los usuarios de servicios TICs de la AUNAP, deben tramitar sus solicitudes de uso de servicios de computación o almacenamiento en la nube a través de la mesa de servicios de TICs.

5.3. Política No.3. Controles criptográficos

5.3.1 Objetivo

Proteger la confidencialidad, autenticidad o integridad de la información de la Autoridad Nacional de Acuicultura y Pesca a través de medios criptográficos.

5.3.2 Alcance

La presente política será aplicada para garantizar la confidencialidad, integridad y autenticidad en el tratamiento de la información de la AUNAP, de acuerdo con los niveles de clasificación determinados y los sistemas electrónicos o de almacenamiento utilizados.

5.3.3 Detalles

La Oficina de las TICs, serán los encargados de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de la AUNAP, con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no repudio en las comunicaciones o en el tratamiento de la información. El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los funcionarios y contratistas de la AUNAP.

Para establecer el sistema de cifrado, los responsables tendrán en cuenta la normatividad colombiana vigente frente a la protección de los datos, estándares aplicables y la tecnología existente. Así mismo, serán los encargados de realizar la respectiva creación, activación, distribución y revocación de las llaves criptográficas a los usuarios autorizados y velarán porque la llave se encuentre activa en el período de tiempo previsto.

5.3.4 Responsabilidad

La solicitud de acceso o actualización al sistema o llaves de cifrado se debe efectuar de manera formal la Mesa de Servicios, en la medida en que las actividades laborales así lo demanden. Aquellas personas autorizadas deberán velar por la conservación de la disponibilidad, integridad y confidencialidad de las llaves, así como de la información a la cual se le haya aplicado algún proceso de cifrado. De igual modo, la información cifrada o descifrada deberá ser tratada conforme a su nivel de clasificación y su eliminación deberá realizarse a través de borrado seguro.

Los responsables del sistema de cifrado y de las llaves criptográficas serán los encargados de establecer los controles para asegurar el sistema y las llaves, así como gestionar el acceso sólo a los funcionarios, contratistas y terceros autorizados.

La AUNAP deberá establecer mecanismos de control y gestión para la creación, activación, distribución, recuperación y revocación de las llaves criptográficas.

Las actividades relacionadas con la administración y eliminación de las llaves criptográficas deberán ser registradas por la persona encargada. Las llaves serán deshabilitadas cuando estas tengan riesgo de divulgación o cuando los funcionarios, contratistas y terceros autorizados culminen la relación laboral o contractual con la AUNAP.

Los funcionarios, contratistas y terceros tendrán la responsabilidad de reportar, mediante los canales autorizados, las fallas reales o potenciales y los posibles riesgos del sistema de cifrado.

5.4 Política No. 4. Transferencia o intercambio de información

5.4.1 Objetivo

Definir las pautas generales para la protección de la información durante el intercambio de la información entre los funcionarios, contratistas y terceros de la AUNAP, y de la entidad con partes externas, preservando las características de disponibilidad, integridad y confidencialidad.

5.4.2 Alcance

La presente política debe de ser adoptada por todos los funcionarios, contratistas y terceros de la AUNAP que en cumplimiento de sus funciones realicen intercambio de información.

5.4.3 Detalle

La transmisión de la información perteneciente a la AUNAP se deberá controlar según los niveles de clasificación de la información establecidos y las políticas de seguridad de la AUNAP. En caso de que se requiera intercambiar información sensible o confidencial, se deberán adoptar controles de cifrado de información de acuerdo con lo establecido en la política descrita en el presente documento.

Los intercambios de información con otras entidades o partes interesadas externas deberán ser soportados por medio de contratos o acuerdos formalizados, determinando en ellos los medios y controles en el tratamiento de la información. Así mismo, se firmarán acuerdos de confidencialidad que garanticen la protección de la información durante y posterior al tiempo de ejecución de las labores encomendadas.

El uso de la información transmitida o intercambiada deberá realizarse conforme a las características del contrato o acuerdo suscrito con el tercero.

La transmisión de la información se desarrollará teniendo en cuenta la normatividad colombiana vigente, especialmente la relativa a la Ley de Habeas Data (Ley 1266 de 2008), la Ley de Protección de Datos Personales (Ley 1581 de 2012 y sus decretos reglamentarios) y Ley de Transparencia (Ley 1712 de 2014) que se pueden observar más detalladamente en el numeral 3 del presente documento.

5.4.4 Responsabilidad

La información deberá protegerse de divulgación no autorizada conforme a los Procedimientos de Clasificación y Etiquetado de la Información definidos en el SGSI de la AUNAP, así como a los mecanismos y controles establecidos para el tratamiento de la información. La información sólo podrá ser usada para las actividades autorizadas dentro de los acuerdos suscritos entre la AUNAP y las partes interesadas.

El intercambio de información se efectuará según los acuerdos establecidos, que describirán: las responsabilidades y procedimientos para la transferencia segura de la información, el responsable y proceso a seguir en caso de presentarse un incidente de seguridad, los niveles de clasificación de la información a ser intercambiada.

Para la transferencia de información se tendrán presentes los riesgos asociados y los canales a utilizar que permitan brindar los niveles de seguridad apropiados. En cualquier medio que se lleve a cabo la transferencia de información (física o electrónica), esta se realizará a través de canales que preserven los niveles de confidencialidad e integridad de la información, conforme a su nivel de clasificación.

Se deben firmar acuerdos de confidencialidad con las partes interesadas que accedan e intercambien información perteneciente la Autoridad Nacional de Acuicultura y Pesca, en donde reposen las responsabilidades y se garantice la reserva de la información y el alcance frente al tratamiento de esta.

5.5 Política No. 5. Uso de dispositivos móviles

5.5.1 Objetivo

Garantizar la seguridad de la información en los dispositivos móviles cuando se administre, transmita o almacene información de la AUNAP, y cuando estos se utilicen dentro de AUNAP.

5.5.2 Alcance

La presente política aplica a todos los dispositivos y equipos móviles de los funcionarios, contratistas y terceros de la AUNAP que le autorice acceso a la red, a la información o a cualquier servicio de tecnologías de la información y las comunicaciones de la AUNAP.

5.5.3 Detalle

AUNAP implementará las directrices necesarias para la autorización de acceso a los recursos y activos de información a través de los dispositivos de tecnología móviles (computadores portátiles, Smartphone, tabletas, o cualquier equipo de dispositivos electrónicos con capacidad de acceso a las redes), conforme a los riesgos asociados. Así mismo, establecerá mecanismos de control de seguridad de la información de estricto cumplimiento por parte de los funcionarios, contratistas y terceros para el acceso a la información, tecnologías de la información y comunicaciones o servicios y recursos de la Autoridad Nacional de Nacional de Acuicultura y Pesca - AUNAP desde dichos dispositivos.

5.5.4 Condiciones obligatorias

Los dispositivos móviles tendrán acceso a la información autorizada a través de redes diferentes a las redes de producción de los sistemas de información de la AUNAP.

Se deberán proteger física y lógicamente los dispositivos móviles propiedad de la AUNAP para evitar el hurto, acceso o la divulgación no autorizada de la información.

De acuerdo con los niveles de clasificación de la información almacenada en el dispositivo móvil, se determinará la necesidad de su cifrado, así como la ejecución de copias de respaldo.

El área de TICS, con la información suministrada del Área de Talento Humano o Grupo de Contratación, brindará o denegará el acceso a los funcionarios, contratistas y terceros a la información o sistemas de información que son accedidos a través de dispositivos móviles.

En caso de extravió o hurto de un dispositivo móvil asignado por la AUNAP, el funcionario, contratista o tercero será el responsable de informar de manera inmediata a la Entidad a través de la mesa de servicio, con el propósito de establecer las medidas de seguridad adecuadas para la protección de la información contenida o acceso a los sistemas de información desde el dispositivo.

Los funcionarios, contratistas y terceros de la AUNAP que han sido dotados con dispositivos móviles de la entidad, no podrán instalar software sin previa autorización y coordinación por el área de las TICS, así mismo, no se deberá realizar conexiones externas a redes públicas que no cuenten con protecciones de seguridad equivalentes a las definidas por el SGSI de la AUNAP.

Los dispositivos móviles de propiedad de la AUNAP preferiblemente deberán tener la capacidad de determinar perfiles de usuario y negocio, para separar el uso personal del institucional para la protección de los datos de la entidad.

El área de las TIC deberá tener la potestad de realizar la desactivación, borrado y retiro de los accesos a los sistemas de la AUNAP, cuando el dispositivo móvil haya sido extraviado o robado al funcionario o contratista responsable.

5.5.5 Responsabilidades

El área de TIC adaptará los mecanismos de seguridad adecuados para proteger la información contenida y transmitida desde los dispositivos móviles de los funcionarios, contratistas y terceros de la AUNAP.

El área de TIC junto con el Área de Talento Humano realizará campañas de sensibilización periódicas a los funcionarios, contratistas y terceros de AUNAP encaminadas al uso responsable de dispositivos móviles.

5.6 Política No. 6. Relaciones con proveedores

5.6.1 Objetivo

Preservar los niveles de seguridad y privacidad de los activos de información de la Autoridad Nacional de Acuicultura y Pesca – AUNAP, que sean accedidos o administrados por proveedores, a través de la implementación de controles que minimicen los riesgos asociados.

5.6.2 Alcance

La presente política aplica a todos los funcionarios, contratistas y proveedores que accedan y operen activos de información de la AUNAP.

5.6.3 Detalle

Cuando se requiera otorgar acceso a los activos de información a los proveedores de la AUNAP, el responsable del activo, con apoyo del área de TIC, deberá realizar un análisis de riesgos con el fin de determinar los controles de seguridad que preserven la confidencialidad, disponibilidad e integridad, así como la finalidad del uso de los datos y el respectivo consentimiento en los casos que aplique conforme a los procedimientos legales y administrativos.

Antes de conceder los permisos de acceso se determinarán por parte del responsable del activo: las necesidades del acceso requerido, (físico o lógico), el nivel de clasificación de la información a acceder, la finalidad de uso, los controles mínimos a tener en cuenta frente al tratamiento de la información y el manejo de incidentes de seguridad de la información. Así mismo se validarán los antecedentes del proveedor conforme a los procedimientos establecidos por la AUNAP, con el objeto de garantizar el adecuado manejo de la información. En ningún caso se otorgará acceso a la información, sistemas de información o áreas seguras de la AUNAP a proveedores, hasta no haber realizado la adecuada gestión de los riesgos, formalizado la relación contractual y firmado el acuerdo de confidencialidad.

Dentro de los acuerdos, contratos o convenios formalmente firmados entre las partes se deberán definir claramente los requerimientos de seguridad y privacidad tales como: información a tratar; niveles de clasificación; finalidad; autorizados para el tratamiento; controles a tener en cuenta antes, durante y después del tratamiento de los datos por parte del proveedor, con el respectivo consentimiento por parte de los titulares en los casos que aplique; así como las responsabilidades de las partes conforme a los lineamientos de la AUNAP y a la legislación vigente.

Siempre que se otorgue acceso a la información de la AUNAP a terceros, se establecerán acuerdos de confidencialidad que tengan como principio el cumplimiento de las políticas de seguridad de la información de la AUNAP y cláusulas requeridas para proteger la información a acceder.

5.6.4 Responsabilidades

Todos los funcionarios, contratistas y proveedores que tengan acceso a la información deberán cumplir con las políticas de seguridad y privacidad de la información, así mismo, en caso de que identifiquen una amenaza que pueda llegar a vulnerar la información, deberán reportarla a la mesa de servicio a través de los conductos establecidos.

El responsable del activo de información no permitirá el acceso a la información hasta no tener firmados y formalizados, por medio de un contrato o acuerdo con los proveedores, los fines de uso, condiciones de tratamiento, así como la debida implementación de los controles requeridos para preservar las características de confidencialidad, integridad y disponibilidad de la información.

Antes de brindar acceso a los activos de información, los proveedores deben aceptar formalmente el cumplimiento de las políticas de seguridad y privacidad de la información de la Autoridad Nacional de Acuicultura y Pesca – AUNAP.

5.7 Política No.7. Política de teletrabajo

5.7.1 Objetivo

Definir las pautas generales para asegurar la información de la AUNAP frente a riesgos asociados al teletrabajo.

5.7.2 Alcance

La política aquí descrita aplica a todos los funcionarios, contratistas y terceros de la Autoridad Nacional de Acuicultura y Pesca que se encuentren autorizados para realizar actividades de teletrabajo.

5.7.3 Detalle

La autoridad Nacional de Acuicultura y Pesca autorizará actividades de teletrabajo conforme a las condiciones del trabajo, los roles y perfiles de los funcionarios, contratistas y terceros de la Entidad. Las actividades de teletrabajo sólo se podrán llevar a cabo siempre y cuando se establezcan controles de seguridad alineados con las políticas de seguridad y privacidad de la información de la AUNAP y frente al respectivo análisis del riesgo.

La AUNAP dispondrá de los recursos tecnológicos, organizacionales y del personal del área de TI para la adopción de un modelo de teletrabajo, que permita cumplir con los intereses y necesidades de la entidad, considerando los riesgos y su respectiva gestión.

La AUNAP preverá mecanismos de seguridad física y lógica a los equipos y documentos requeridos para el desarrollo de las actividades de teletrabajo, con el fin de conservar las características de integridad, disponibilidad y confidencialidad de la información.

La AUNAP definirá las condiciones del teletrabajo, los roles y perfiles de los funcionarios, contratistas y terceros de la Entidad que manejen información sensible, a una revisión por parte del área de TI de los equipos personales para realizar una valoración de los riesgos que pueden estar expuestos, esto debe ser solicitado por el jefe del área al que pertenece con previa autorización de la persona propietaria del equipo.

El área de TI que hace parte de la OGCI no se hace responsable de equipos personales con el cual se desarrolle labores de teletrabajo en todo lo relacionado con soporte técnico, única y exclusivamente realizaran una valoración de los riesgos que estos equipos puedan presentar al realizar labores que involucren información sensible para la AUNAP.

Para el desarrollo de las actividades de teletrabajo se deberá realizar un análisis de riesgos, a partir del cual se adopten los mecanismos de control para la protección de la información y los sistemas de información de la AUNAP accedidos durante las actividades.

Antes de llevar a cabo cualquier actividad de teletrabajo, se definirán entre la AUNAP y el funcionario, contratista o tercero, el alcance de las actividades a desarrollar y se determinarán como mínimo: la información a acceder, el horario de las actividades y los sistemas y servicios requeridos conforme la necesidad de la AUNAP y la legislación colombiana vigente.

Se realizará el monitoreo y evaluación de los logros en relación con las metas propuestas por parte de la AUNAP, determinando la productividad y rendimiento de los funcionarios y contratistas en el cumplimiento de las metas, nivel de satisfacción laboral, entre otros factores previstos.

En caso de pérdida o hurto de un equipo en el cual se lleven actividades de teletrabajo, será responsabilidad del funcionario, contratista o tercero informar de forma inmediata a través de la mesa de servicios de la AUNAP el evento, con el fin de establecer las medidas de seguridad adecuadas para la protección de la información contenida.

5.7.4 Responsabilidades

El Área Jurídica con el apoyo del Área de Talento Humano y el área de TICS, determinará las condiciones de los contratos o acuerdos con los funcionarios, contratistas y terceros, determinando las condiciones, responsabilidades conforme las necesidades de la AUNAP y la normatividad colombiana vigente.

El área de TIC, con la información remitida por el Área de Talento Humano o Grupo de Contratación, brindará o denegará el acceso a la información o sistemas de información que puedan ser accedidos a través de los equipos usados para las actividades de teletrabajo.

El área de TIC será la responsable de implementar los controles de seguridad necesarios para llevar a cabo las actividades de teletrabajo.

Los funcionarios, contratistas y terceros que se encuentren autorizados para el desarrollo de actividades de teletrabajo, deberán cumplir con las responsabilidades y condiciones acordadas, así mismo reportar cualquier situación que pueda afectar el desarrollo de las actividades o ponga en peligro la información de la AUNAP.

El área de TIC junto con el Área de Talento Humano realizará campañas de sensibilización para las buenas prácticas de las actividades de teletrabajo.

El área de TIC determinará los canales de comunicación y métodos de autenticación apropiados para controlar el acceso de usuarios remotos a la información y sistemas de información de la AUNAP.

El área de TIC, generarán protocolos que den respuesta a situaciones de alerta como una avería del ordenador causada por un virus, una configuración incorrecta o un fallo de hardware. Estableciendo controles de seguridad tales como copias de respaldo o equipos o dispositivos de reserva en caso de daño o pérdida de los equipos.

5.8 Política No. 8. Escritorio y pantalla limpios

5.8.1 Objetivo

Establecer los lineamientos generales para reducir los riesgos de acceso no autorizado, pérdida o daño de información en escritorios y estaciones de trabajo durante o por fuera de las horas laborales.

5.8.2 Alcance

La política aquí descrita concierne a todos los funcionarios, contratistas y terceros de la AUNAP que tengan acceso a la información tanto en formato físico como digital.

5.8.3 Detalle

Para lograr un adecuado aseguramiento de la información los funcionarios, contratistas y terceros de la Autoridad Nacional de Acuicultura y Pesca AUNAP deberán adoptar buenas prácticas para el manejo y administración de la información física y electrónica que se encuentra a su cargo, conforme a su clasificación, con el fin de evitar que personas no autorizadas accedan a dicha información. Para ello, los funcionarios, contratistas y terceros deberán tener presente:

Almacenar de forma segura documentos y elementos de almacenamiento externos (CD, DVD, USB, etc.) conforme los niveles de clasificación de la información, para evitar accesos no autorizados, pérdida o daño de la información en la jornada laboral o fuera de ella.

Durante los lapsos de tiempo en los que se deja desatendidas las estaciones de trabajo, se tendrá cuidado con bloquear la sesión del equipo para evitar que terceros no autorizados accedan a la información contenida en el

computador. Así mismo, se generarán los controles adecuados con la información que reposa sobre el lugar de trabajo.
Al imprimir información reservada o pública clasificada, los documentos deberán ser retirados de forma inmediata para evitar divulgación no autorizada de la información.
Los archivos que contengan información sensible o confidencial deberán ser almacenados en rutas que impidan el fácil acceso por terceros, evitando, por ejemplo, guardarlos en el área de escritorio de la pantalla del computador.

5.8.4 Responsabilidades

El área de TICS será la encargada de establecer controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee en un lapso de tiempo determinado. Los funcionarios, contratistas y terceros que tenga dentro de sus funciones la atención al público, deberán almacenar los documentos y dispositivos de almacenamiento bajo llave y ubicar el equipo de cómputo de tal forma que se evite el acceso o revisión de la información por parte de los visitantes no autorizados.

5.9 Política No.9. Respaldo de información

5.9.1 Objetivo

Definir los lineamientos generales para la generación, administración, retención y custodia de las copias de respaldo, con el fin de preservar la disponibilidad e integridad de la información.

5.9.2 Alcance

Esta política deberá ser cumplida por los funcionarios, contratistas y terceros que tengan a su cargo realizar, administrar y custodiar las copias de respaldo definidas por la AUNAP, con el propósito de reducir el impacto frente a la pérdida de información o a incidentes que comprometan la continuidad del negocio.

5.9.3 Detalle

La información requerida para el cumplimiento de las actividades misionales y los objetivos estratégicos de la Autoridad Nacional de Acuicultura y Pesca deberá ser respaldada conforme a los lineamientos legales, técnicos, requisitos de las tablas de retención documental, la gestión de riesgos, así como a los niveles de clasificación de la información. Los tiempos de preservación de las copias de respaldo serán definidos teniendo en cuenta los requerimientos anteriormente expuestos, así como también la tecnología requerida para la restauración de la información contenida.

Para la realización de las copias de respaldo, el responsable de la información deberá solicitar a través de la mesa de servicios, determinando las necesidades, la información sujeta al respaldo, periodos, niveles de clasificación de la información y el tiempo de retención de las copias.

Las copias de respaldo se almacenarán de forma segura para garantizar no sea manipulada por personas no autorizadas. A su vez, se deberán registrar todas las actividades desarrolladas frente al tratamiento y manipulación de las copias de respaldo para asegurar la trazabilidad de estas.

El responsable de las copias de respaldo deberá realizar las respectivas pruebas de restauración conforme a los propósitos para las cuales han sido recaudadas.

Las copias de respaldo deberán ser almacenadas en lugares que tengan los debidos controles de seguridad físicos y tecnológicos, que permitan limitar el acceso sólo a las personas autorizadas y garanticen la disponibilidad de la información.

Al cumplir el ciclo de vida útil de los medios de almacenamiento de las copias de respaldo deberán ser destruidos o eliminados de forma segura, evitando la recuperación de la información contenida y acceso por personas no autorizadas.

5.9.4 Responsabilidades

Los funcionarios, contratistas y terceros responsables de la infraestructura, sistemas de información y Bases de datos requeridos para la operación de la AUNAP, deberán generar las respectivas copias de respaldo, estableciendo la periodicidad, tipo de almacenamiento y registrando la información según lo establecido dentro de la presente política.

Los encargados de las copias de respaldo deben velar porque la información sea almacenada conforme a los lineamientos establecidos, de forma controlada y conforme a las necesidades de la AUNAP. Así mismo deberán realizar una prueba periódica de las copias con el fin validar el correcto funcionamiento y la efectiva restauración.

Los responsables de la información serán los encargados de velar porque las copias de respaldo se realicen de acuerdo con lo establecido y que las estrategias utilizadas se ajusten a las necesidades y requerimientos de la AUNAP.

Los funcionarios, contratistas y terceros de la AUNAP deberán almacenar la información requerida para sus procesos operativos, en la ubicación establecida por el área de TICS dentro del servidor de almacenamiento, con el fin de garantizar la disponibilidad y copias de respaldo de cada una de las áreas. Así mismo serán responsables de depurar la información para la optimización de los recursos de la Entidad.

5.10 Política No. 10. Desarrollo de software

5.10.1 Objetivo

Definir los lineamientos generales para el desarrollo, mantenimiento y adquisición de software al interior de la Autoridad Nacional de Acuicultura y Pesca, con el fin de determinar los controles de seguridad en el desarrollo de código fuente.

5.10.2 Alcance

La presente política deberá ser cumplida por funcionarios, contratistas y terceros de la AUNAP que realicen actividades correspondientes al desarrollo, mantenimiento y adquisición de software dentro de la AUNAP.

5.10.3 Detalle

Para el desarrollo de software dentro de la Autoridad Nacional de Acuicultura y Pesca - AUNAP se deberá realizar un proceso de planeación en donde se determine la respectiva metodología a utilizar; las etapas de desarrollo; la estructura de desglose de trabajo, con sus respectivos responsables, criterios de aceptación y las pruebas de funcionalidad y seguridad teniendo en cuenta los requerimientos y el cumplimiento de los objetivos estratégicos de la AUNAP. Las etapas deberán estar debidamente documentadas, con el objeto de generar registros de trazabilidad frente a los requerimientos, desarrollo y aceptación del software.

La solicitud de desarrollo de software será realizada por los directores y/o jefes de área de las áreas de manera formal, la identificación de las necesidades y requisitos de funcionalidad, calidad y seguridad se realizará entre el área solicitante y el área de TICS, y los mismos deberán ser validados durante el proceso de aprobación del desarrollo de software.

Para el desarrollo y puesta de producción del software, se deberán tener presente tres ambientes separados de desarrollo, pruebas y producción, conformados por infraestructura y personal propios en cada uno de ellos, evitando así las alteraciones o modificaciones no autorizadas del código fuente.

Los cambios requeridos sobre el software de la AUNAP se llevarán a cabo a través del Procedimiento de Control de Cambios, el cual permite que se documenten y establezcan los requerimientos y los niveles de aceptación del cambio. Dentro de los requerimientos que se establezcan será necesario analizar los riesgos asociados a la seguridad de la información y la identificación de los controles a implementar para su aseguramiento.

Se establecerán acuerdos en procesos de desarrollo que establezcan con claridad la propiedad de las licencias y derechos intelectuales de los códigos fuentes, así como sus condiciones de usabilidad.

5.10.4 Responsabilidad

Antes de iniciar el desarrollo de software, el área de TICS y las áreas de la AUNAP implicadas deberán acordar una metodología; una estructura de trabajo, con los respectivos responsables; así como el cronograma de desarrollo, determinando el alcance, los procesos afectados y los requerimientos.

El área solicitante validará los criterios de aceptación correspondientes a la funcionalidad y calidad para dar la aceptación formal del desarrollo de software.

El área de las TICS validará los criterios de aceptación técnicos: interoperabilidad, buenas prácticas de programación y seguridad, para dar la aceptación formal del desarrollo de software. La aceptación de los criterios estará determinada por los resultados de las pruebas planteadas, las cuales tendrán dentro de sus. objetivos detectar, entre otras vulnerabilidades, los códigos maliciosos, las puertas traseras, etc.

Los datos de pruebas con los que se llevarán a cabo las pruebas del software no deben utilizar datos reales de producción.

En el desarrollo de software es necesario establecer controles que permitan conservar la seguridad y privacidad de la información; por lo tanto, es importante tener en cuenta los mecanismos de acceso a la información, autenticación, detección de intrusos, cifrado de datos, salvaguarda de confidencialidad, integridad, disponibilidad y protección de los datos personales.

La metodología de desarrollo de software debe contemplar una etapa de gestión de riesgos.

El área de TICS deberá llevar a cabo revisiones periódicas a los desarrollos realizados, con el propósito de garantizar que se estén desplegando los controles conforme a lo establecido dentro de la fase de planeación.

En el desarrollo de software se llevará a cabo un control de versiones con los respectivos documentos de soporte, ello con el objeto de verificar el buen funcionamiento del software y el respectivo control de su ciclo de vida.

5.11 Política No. 11. Protección de datos personales (habeas data)

5.11.1 Objetivo

Establecer las medidas generales para garantizar los niveles de seguridad y privacidad adecuados para la protección de datos personales, con el fin de evitar posibles adulteraciones, pérdidas, consultas, usos o accesos no autorizados.

5.11.2 Alcance

La presente política será aplicable a los datos personales registrados en cualquier base de datos de la AUNAP, cuyo titular sea una persona natural.

5.11.3 Detalle

La AUNAP implementará una política de Tratamiento de la información, en un lenguaje claro y sencillo, que deberá ser puesta en conocimiento de los Titulares y tendrá que incluir como mínimo:

Nombre o razón social, domicilio, dirección, correo electrónico y teléfono del responsable.
El Tratamiento al cual serán sometidos los datos y la finalidad de este, si este no se ha informado por medio del aviso de privacidad.
Derechos que asisten a los Titulares de la información.

El área o persona responsable de la atención de las consultas, peticiones y reclamos ante la cual el Titular de la información puede ejercer sus derechos.
Procedimiento por medio del cual los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar, suprimir información y revocar la autorización.

Los mecanismos para la autorización del tratamiento de los datos personales podrán ser determinados a través de medios técnicos, de forma oral o por medio de conductas inequívocas que permitan determinar el otorgamiento de la autorización por parte del Titular. Los responsables del tratamiento de la AUNAP deben conservar el registro de la autorización.

Así mismo, los funcionarios, contratistas o terceros sólo deberán recopilar la cantidad mínima de datos personales requerida para cumplir con los propósitos de AUNAP. Dicho recaudo sólo se realizará una vez se obtenga la respectiva autorización por parte del Titular de los datos.

Además, el responsable de las bases de datos deberá adoptar las medidas necesarias para garantizar la seguridad de los datos de carácter personal y así evitar su destrucción, alteración, pérdida o tratamiento no autorizado. Estas medidas deberán incluir los mecanismos de seguridad físicos y lógicos más adecuados, de acuerdo con el desarrollo tecnológico, de tal forma que garanticen la protección de la información almacenada y el secreto profesional.

Las bases de datos que contengan datos personales deben ser administradas de tal modo que se garantice el respeto a derechos fundamentales como la intimidad, el buen nombre, y en especial, el Habeas Data.

Ningún funcionario o contratista de la AUNAP deberá retirar o transmitir información que contenga datos personales sin la debida autorización expresa del responsable; y en caso de que se facilite información a terceros, se deberá garantizar el buen uso y contar con el debido consentimiento para el tratamiento de los datos conforme a su finalidad, firmado por el Titular de los datos. Los mecanismos de transferencia se realizarán a través de las políticas y procedimientos de seguridad y privacidad descritas en el presente documento.

Los responsables y encargados del tratamiento de los datos personales sólo podrán recolectar, almacenar, usar o circular dichos datos durante el tiempo establecido para cumplir las finalidades que justificaron el tratamiento. Por lo tanto, una vez se cumpla con los objetivos y las finalidades del tratamiento, el responsable y el Encargado deberán suprimir los datos personales que tengan en su posesión de una forma segura.

Los funcionarios, contratistas y terceros de la AUNAP no podrán realizar el tratamiento de datos personales de niños, niñas y adolescentes, excepto cuando se trate de datos públicos. En este caso, la AUNAP deberá respetar los intereses y los derechos fundamentales, conforme a una autorización previa del representante legal de cualquiera de ellos.

En el caso de que no sea posible poner a disposición del Titular de la información las políticas de tratamiento, los responsables deberán informar por medio de un Aviso de Privacidad al Titular sobre la existencia de las políticas y la forma en la cual puede acceder a las mismas, a más tardar en el momento en el que se vaya a realizar la recolección de datos personales.

5.11.4 Responsabilidad

Los funcionarios, contratistas y terceros que tengan acceso a datos personales tratados y administrados por la AUNAP, deberán cumplir con la política anteriormente descrita, haciendo uso de los controles y medidas establecidas para la protección de la información conforme a su nivel de clasificación.

El responsable de las bases de datos que contengan información personal deberá asegurar que antes de realizar cualquier tratamiento de los datos, la AUNAP cuente con las autorizaciones de los Titulares y los mecanismos de control para la protección de la información.

Los funcionarios, contratistas y terceros deberán evitar el acceso a los datos personales para los cuales no se encuentren autorizados y en caso de que observen violación o fallas de los mecanismos de control de seguridad y privacidad, estos hechos deberán ser reportados a la mesa de servicios para determinar las acciones a desarrollar.

En caso de que se requiera realizar transferencia de datos personales, se deberá efectuar de acuerdo con el Procedimiento de Recepción y/o Transferencia de Información de la AUNAP.

Se deberá realizar la actualización periódica de las listas de acceso de las personas y funcionarios autorizados para efectuar cualquier tipo de tratamiento frente a los datos personales. Así mismo, se identificarán, de acuerdo con los niveles de clasificación, los mecanismos apropiados para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Una vez culmine el lapso del tratamiento de los datos personales, el responsable de estos deberá velar porque sean eliminados de forma segura, para evitar su recuperación.