

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

PLAN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI

**AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA
AUNAP**

2024

	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

TABLA DE CONTENIDO

1. OBJETIVO.....	0
Establecer la política, los procedimientos y controles direccionados al manejo y protección de la información y de los activos de LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP, con la incorporación de las buenas prácticas y normas de calidad, aplicables a la gestión segura de cualquier activo de información.	0
2. ALCANCE DEL MANUAL.....	0
3. DEFINICIONES	0
4. DESCRIPCIÓN.....	3
5. POLÍTICAS	6
POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS	6
POLÍTICAS DE GESTIÓN DE ACTIVOS.....	6
POLÍTICAS DE CONTROL DE ACCESO LÓGICO	6
POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO	7
POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES	7
POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES	7
POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	7
POLÍTICAS DE RELACIONES CON LOS PROVEEDORES	7
SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO	8
POLÍTICAS DE GESTIÓN DE INCIDENTES.....	8
POLÍTICAS DE CUMPLIMIENTO.....	8
USO ADECUADO DE INTERNET	8
USO ADECUADO DE CORREO ELECTRÓNICO:	9
USO DE USUARIOS Y CONTRASEÑAS:	9
6. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS	9
7. SANCIONES.....	9
8. NATURALEZA DEL CAMBIO	10

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

1. OBJETIVO

Establecer la política, los procedimientos y controles direccionados al manejo y protección de la información y de los activos de **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP**, con la incorporación de las buenas prácticas y normas de calidad, aplicables a la gestión segura de cualquier activo de información.

OBJETIVOS ESPECÍFICOS

- Proteger, almacenar y respaldar la información de la entidad, con el fin de garantizar la protección de la misma.
- Preservar y administrar objetivamente la información de **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP**, asegurando el cumplimiento de las características de confidencialidad, integridad y disponibilidad.
- Transmitir las normas y políticas de seguridad informática a todo el equipo de trabajo de **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP**.

2. ALCANCE DEL MANUAL

El presente manual de las políticas del Sistema de Gestión de Seguridad de la Información aplica a funcionarios, contratistas, terceros, usuarios y de más actores y visitantes de **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP** que por alguna razón tengan cualquier tipo de interacción con los activos de información de la entidad

3. DEFINICIONES

- **Activo de Información:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, software, información física o digital y recurso humano, entre otros, que utiliza y dispone la entidad.
- **Amenaza:** Violación potencial de la seguridad. (Rec. UIT-T X.800, 3.3.55)
- **Amenaza Informática:** Se refiere a la explotación de una vulnerabilidades o fallos que se utilizan para afectar la operatividad de un sistema, con la intención de sacar algún provecho o lograr algún beneficio contra la población, el territorio y la organización política del Estado.
- **Ataque:** Intento de destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo.

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

- **Ataque Cibernético.:** Acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).
- **Ciberespacio:** Es el espacio virtual donde las personas, utilizando software, consumen los servicios de internet como correo electrónico, sitios web, APIs y muchos otros.
- **Ciberdelito / Delito Cibernético:** Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, utilizando herramientas tecnológicas.
- **Causas:** Son los factores, medios, las circunstancias y agentes generadores de riesgo; se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.
- **Confidencialidad:** Es uno de los tres pilares fundamentales de la seguridad de la información, según la norma ISO 27001, y tiene como objetivo garantizar que la información sea accesible solo para personas autorizadas, protegiéndola contra la divulgación no autorizada y el uso indebido.
- **Consecuencia:** Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso a la entidad, **en el contexto de la seguridad de la información, suele ser negativa, Las consecuencias iniciales pueden incrementarse a través de los efectos secundarios.**
- **Control:** Es la medida adoptada por la entidad, consistente en cerciorarse o verificar el cumplimiento de los planes, manuales, normas o políticas establecidas para el manejo y/o disminución de los riesgos configurados, para la protección de los activos de información.
- **Disponibilidad:** Es otro de los tres pilares fundamentales de la seguridad de la información, según la norma ISO 27001, y refiere a que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.
- **Evaluación del Riesgo:** **Es una actividad que permite identificar las vulnerabilidades presentes en los sistemas empresariales. Esto implica realizar un análisis detallado de la infraestructura informática, los activos de datos, los procesos de seguridad y los posibles puntos débiles en el sistema.**
- **Gestión del Riesgo:** La gestión de riesgos es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, con unas actividades que incluyen la identificación, el análisis y la evaluación de riesgo, para establecer los controles y con ello evitar, disminuir y/o mitigar el riesgo.
- **Impacto:** Se entiende como el nivel de afectación que puede ocasionar a la entidad la materialización de un riesgo.
- **Incertidumbre:** Es una expresión que manifiesta el grado de desconocimiento acerca de una condición futura.

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

- **Información:** La Norma ISO/IEC 27000 Esta define un enfoque sistemático y estructurado para identificar, gestionar y mitigar los riesgos relacionados con la seguridad de la información, tiene valor para la organización y, por tanto, ha de ser protegido adecuadamente.
- **Integridad:** Es propiedad de salvaguardar la exactitud y estado completo de los activos, según la norma ISO 27001.
- **ISO:** Es la organización internacional de normalización o estándares cuya actividad es la elaboración de normas técnicas internacionales. (ISO 27001).
- **ISO 27001:** Es la norma que se encargó de establecer un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de seguridad de la información.
- **Mapa De Riesgos:** Documento con la información resultante de la gestión del riesgo.
- **Seguridad Informática:** Proceso de prevenir y detectar el uso no autorizado de un sistema informático, implica el proceso de proteger contra intrusos el uso de los recursos informáticos, con intenciones maliciosa para obtener ganancia o incluso la posibilidad de acceder a ellos por accidente.
- **Monitoreo:** Es el proceso sistemático de recolectar, analizar y utilizar información para hacer seguimiento en este caso al Mapa de Riesgos.
- **Nivel De Riesgo:** Es la magnitud de un riesgo resultante del producto del nivel de probabilidad por el nivel de consecuencia.
- **Objetivo del Proceso:** Algo perseguido o pretendido, se basa en las políticas de la entidad. Se debe transcribir el objetivo que se ha definido para el proceso al cual se le están identificando los riesgos.
- **Probabilidad:** Se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.
- **Proceso:** Conjunto de actividades mutuamente relacionadas o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados. Se debe tener claro el proceso al cual se pertenece, sus actividades, procedimientos y tareas del mismo.
- **Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Evento de Seguridad de La Información:** Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

- **Riesgo:** Representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos.
- **Riesgo de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Controles:** Medida que permite reducir o mitigar un riesgo.

4. DESCRIPCIÓN

4.1 RESPONSABLES

Es responsabilidad del Comité del Sistema de Gestión de Seguridad de la Información – SGSI, será verificar la aplicabilidad de las políticas, los procedimientos, controles, divulgación y mantenimiento de todo lo establecido en el **manual** del SGSI.

4.2 NORMATIVIDAD

Las normas que rigen la protección, aplicación y mantenimiento de la seguridad de la información son:

Resolución 746 del 11 de marzo de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021", en la cual se crea una nueva normativa que adiciona lineamientos y estándares relacionados con los proveedores de productos y servicios de seguridad digital y con la Protección de los Datos Personales.
Resolución 500 del 10 de marzo de 2021	La presente resolución tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.
Ley 527 de 1999 – Comercio electrónico	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones”.
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública, SECOP.

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

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
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 del Espectro y se dictan otras disposiciones.
Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009	Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información.
Circular 052 de 2007 (Superintendencia Financiera de Colombia)	Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.
Ley 1581 de 2012 Reglamentada por ley 1377 de 2013	Por la cual se dictan disposiciones generales para la protección de datos personales
Constitución de 1991	Artículo 15: El derecho fundamental de intimidad personal y familiar.
Ley 1266 de 2008	Establece principios para el tratamiento de datos, e impone una serie de deberes para los operadores, fuentes y usuarios, así mismo un catálogo de derechos para los titulares de la información.
Decreto 2952 de 2010	El incumplimiento de obligaciones de tratamiento de información en casos de fuerza mayor.
Decreto 1727 de 2009	Reglamenta forma de presentación del contenido de la información del titular de la información.
Ley de habeas Data (Estatutaria) 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley (Estatutaria) 1266 de 2008	Por la cual se dictan disposiciones generales para habeas data financiero.

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

4.3 CONTEXTO AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA - AUNAP

La Autoridad Nacional de Acuicultura y Pesca –AUNAP, creada mediante el Decreto 4181 de 2011, entidad de carácter técnico y especializado adscrita al Ministerio de Agricultura y Desarrollo Rural - MADR tiene como objeto ejercer la autoridad pesquera y acuícola en Colombia, para lo cual debe planificar las investigaciones, el ordenamiento y el fomento, y entre sus funciones como ejecutor de la política pesquera y acuícola, le corresponde realizar el ordenamiento, la administración y control para el aprovechamiento y desarrollo sostenible de los recursos pesqueros en el territorio nacional; bajo un esquema de aprovechamiento adecuado y sostenible, en los términos de la Constitución política, Ley 13 de 1990, Decreto 2256 de 1991, Decreto 4181 de 2011 y demás normas concordantes con la materia.

El objeto de la AUNAP es Ejercer la autoridad pesquera y acuícola de Colombia, para lo cual la AUNAP adelantará los procesos de planificación, investigación, ordenamiento, fomento, regulación, registro, información, inspección, vigilancia y control de las actividades de pesca y acuicultura, aplicando las sanciones a que haya lugar, dentro de una política de fomento y desarrollo sostenible de los recursos pesqueros.

Dentro su estructura orgánica cuenta con Dirección General, 2 Direcciones Técnicas (Dirección Técnica y Administración y Fomento – Dirección Técnica de Inspección y Vigilancia) dos Oficinas (Oficina de Generación del Conocimiento y la Información – Oficina Asesora Jurídica) y Secretaría General, que lidera todos los procesos de apoyo de la entidad. A nivel territorial, cuenta con 7 regionales que llevan al territorio toda la gestión misional de la entidad.

Actualmente cuenta con 15 procesos de los cuales 2 son de carácter estratégico (Direccionamiento Estratégico, y Comunicación Estratégica) 3 misionales (Gestión de la Administración y Fomento - Gestión de la Información y Generación del Conocimiento – Gestión de la Inspección y Vigilancia), 8 procesos de apoyo (Atención al Ciudadano, Gestión del Talento Humano, Gestión de Contratación, Gestión Financiera, Gestión Documental, Gestión Jurídica, Gestión Administrativa, Gestión de Servicios TICS –Tecnologías de la Información y la Comunicación-) y 2 procesos de Evaluación (Evaluación seguimiento y control, y Control Disciplinario)

La AUNAP, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión 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.

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

5. POLÍTICAS

LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP establece a continuación, los siguientes lineamientos de seguridad de la información, los cuales deberán ser cumplidos por todos los funcionarios, contratistas, terceros, usuarios y visitantes. Los lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

POLÍTICAS DE SEGURIDAD DE LOS RECURSOS HUMANOS

- Durante el proceso de selección de personal de planta o contratistas, se realizará verificación de antecedentes disciplinarios de los candidatos sin importar el cargo o posición al cual se postulen.
- Todo el personal que labore en la entidad o preste servicios a la misma deberá firmar un acuerdo de confidencialidad y un documento de conocimiento y aceptación de las políticas definidas para el sistema de seguridad de la información y buen uso de los activos de información. Mediante el cual se compromete a realizar un adecuado uso de estos.

POLÍTICAS DE GESTIÓN DE ACTIVOS

- Toda información sea física o digital generada, almacenada o transformada por los funcionarios, contratistas o proveedores de la entidad, utilizando los recursos dispuestos por la entidad para tal fin o en desempeño de sus labores o servicio contratado, son activos de información propiedad de **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP**.
- Los activos dispuestos por **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP** para el apoyo de las labores desempeñada por los funcionarios, contratistas o proveedores, únicamente se permitirá su utilización para ejecución de tareas establecidas en el ámbito laboral de **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP**.
- **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP** identificara, clasificara y gestionara su inventario de activos conforme a los manuales y procedimientos de Gestión de Activos formalizados.

POLÍTICAS DE CONTROL DE ACCESO LÓGICO

- Para la protección de los activos de información, se establecerán procedimientos y políticas para el control de acceso a la red, sistemas de información e infraestructura física (Instalaciones). Con el fin de mitigar los riesgos asociados al acceso no autorizado a la información.
- Todos los usuarios deberán asumir la responsabilidad sobre la información física o digital que accedan y procesan dando un uso adecuado con el fin de salvaguardar la confidencialidad, integridad y disponibilidad de la información.

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

POLÍTICAS DE SEGURIDAD FÍSICA Y DEL ENTORNO

- **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP** adoptará medidas para el control de acceso físico a las instalaciones y áreas seguras con el fin de mitigar los riesgos asociados a la afectación de la confidencialidad, disponibilidad e integridad de la información.
- **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP** definirá áreas seguras y los controles de acceso físico correspondientes para la protección de la información que allí se resguarda.
- Todas las personas que ingresen a las instalaciones de **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP** deben cumplir con los lineamientos establecidos para el control de acceso físico sin excepción.

POLÍTICAS DE SEGURIDAD EN LAS OPERACIONES

- Con el fin de asegurar las operaciones realizadas en los recursos tecnológicos que soportan la operación del negocio. **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP** planea, gestiona, respalda y monitorea la infraestructura tecnológica siguiendo los lineamientos establecidos en los procedimientos establecidos para el SGSI.

POLÍTICAS DE SEGURIDAD DE LAS COMUNICACIONES

- La oficina de sistemas OGCI, establecerá los controles para acceso lógico y protección de las redes de la **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP**, con el fin de asegurar y cumplir con los acuerdos de niveles de servicios que sean establecidos para los servicios de red y que deberán ser acordados con la alta dirección.
- **LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP** definirá procedimientos y lineamientos para la transferencia segura de información interna o externamente, de tal forma que se garantice la integridad y confidencialidad de la información.

POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

- La oficina de sistemas OGCI, velará que los sistemas de información que sean implementados en la entidad cumplan con los requerimientos de seguridad y buenas prácticas.
- Todos los procesos de la entidad que realicen desarrollos deberán cumplir con los procedimiento y metodologías de desarrollo establecidos y formalizados para poder liberar sus aplicaciones.
- Todos los procesos de la entidad deberán informar al área de tecnología sobre sus proyectos de adquisición de sistemas de información, con el fin de brindar las observaciones correspondientes y revisar los aspectos técnicos necesario para su desarrollo e implementación.

POLÍTICAS DE RELACIONES CON LOS PROVEEDORES

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

- LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP establecerá políticas y requisitos de seguridad de la información para mitigar los riesgos asociados a cada proceso de contratación.
- Antes de Iniciar la ejecución de contratos con terceras partes, deberán suscribirse los respectivos acuerdos de confidencialidad que incluyan las cláusulas de confidencialidad y los aspectos de seguridad de la información necesario durante y después del contrato.

SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

- LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP establecerá un plan de 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 oficina de sistemas OGCI generará dicho plan de continuidad tecnológica con base a Planes de Recuperación de Desastres (DRP) y Análisis de Impacto al Negocio (BIA).

POLÍTICAS DE GESTIÓN DE INCIDENTES

- Cada vez que se detecta un evento, incidente o debilidad relacionados con seguridad de la información por parte de un funcionario, contratista o terceras partes, se deberá reportar a La oficina de sistemas OGCI por cualquiera de los medios dispuestos para tal fin.
- Sera responsabilidad de La oficina de sistemas OGCI seguir los procedimientos establecidos para la gestión de los incidentes que puedan presentarse.

POLÍTICAS DE CUMPLIMIENTO

LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP velara por el cumplimiento de la legislación vigente respecto a los requisitos establecidos en la seguridad y privacidad de la información, derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública.

USO ADECUADO DE INTERNET

El internet es un recurso valioso para el desempeño de las labores de todos los funcionarios y, por lo tanto, se definen los siguientes lineamientos para su uso adecuado.

- Estará 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.
- Estará limitado el acceso a redes sociales en general.
- Se restringirá el acceso a portales de nube e intercambio de información masiva (exceptuando a la nube corporativa o institucional).
- La oficina de sistemas OGCI podrá verificar los logs o registros de navegación cuando así se solicite o se requiera para las investigaciones o requerimientos que puedan generarse.

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

USO ADECUADO DE CORREO ELECTRÓNICO:

- Los buzones de correo asignados a los funcionarios, contratistas o terceros pertenecen a LA AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP, por lo tanto, su contenido también es propiedad de la Entidad.
- El correo electrónico solo deberá emplearse para uso institucional y el desempeño de las funciones correspondientes a cada cargo.
- La oficina de sistemas OGCI, 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.

USO DE USUARIOS Y CONTRASEÑAS:

- Cada funcionario o contratista cuyas funciones requieran de acceso a sistemas de información o correo electrónico, deberá asignársele un usuario y contraseña.
- Las credenciales son personales e intransferibles.
- Deben utilizarse esquemas de seguridad para la creación de contraseñas (uso de Mayúsculas, Minúsculas, Caracteres, Números).

6. APROBACIÓN Y REVISIÓN DE LAS POLÍTICAS

Las políticas aquí definidas se harán efectivas a partir de su aprobación por el correspondiente y serán revisadas por lo menos anualmente, cuando existan incidentes de seguridad de la información o cuando se produzcan cambios estructurales considerables, esto con el fin de asegurar su vigencia y aplicabilidad dentro de **AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP**.

7. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de **AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA – AUNAP** de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos de TIC o por el incumplimiento de los lineamientos aquí descritos.

- a. Se aplicarán sanciones de acuerdo con el Código Único Disciplinario.
- b. Pueden aplicarse sanciones de tipo penal según sea el caso y la gravedad de este, si así lo consideran los entes investigativos y judiciales correspondientes.
- c. La oficina de sistemas OGCI será el encargado de recopilar y entregar a la Oficina de Control Interno Disciplinario las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para formalmente manejar la investigación inicialmente a nivel interno, así mismo, la oficina de sistemas OGCI será el encargado de registrar y gestionar el incidente de seguridad derivado con el incumplimiento de las políticas.

 AUNAP AUTORIDAD NACIONAL DE ACUICULTURA Y PESCA	NOMBRE DEL PROCESO	CÓDIGO: IN-XX-XXX
	SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI	VERSIÓN: X
		FECHA: DD/MMM/AAAA

8. NATURALEZA DEL CAMBIO

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
4	XX/0X/2024	- Se actualizo la plantilla del documento de acuerdo al formato de MinTIC - Ajuste y ampliación de las definiciones - Inclusión de normativa MinTIC- Resolución 746 de 2022 y Resolución 500 del 10 de marzo de 2021 - Ajuste, ampliación e inclusión de nuevas políticas - Ajuste a los principios de seguridad que soportan el SGSI de la AUNAP

ELABORÓ	REVISÓ	APROBÓ
Martha Lucia Sanabria Ariza Cargo: Ingeniera Contratista Fecha: XX-08-2024	Nombre: Cargo: Fecha: XX-XX-2021	Nombre: Cargo: Fecha: XX-XX-2021