CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	21/12/2020	Primera versión del documento
2	29/10/2021	Segunda versión del documento

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

Tabla de contenido

1. INFORMACIÓN GENERAL DEL PLAN

1.1 OBJETO:

Definir el plan estratégico de tratamiento de riesgos y privacidad de la información, para salvaguardar la información recolectada y generada por la AUNAP, estableciendo lineamientos de protección para los activos de información de la entidad.

1.1.1 OBJETIVOS ESPECÍFICOS

- Definir las responsabilidades relacionadas con el manejo de la Seguridad y privacidad de la información en la AUNAP.
- Establecer una metodología de gestión de la seguridad y privacidad de la información clara y estructurada.
- Informar la metodología establecida para mantener la seguridad y privacidad de la información.
- Garantizar que los usuarios tengan acceso a la información a través de medidas de seguridad con la garantía de calidad y confidencialidad.

1.2 ALCANCE DEL PLAN:

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y que permita integrar en los procesos de la entidad, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos, la gestión de riesgos de seguridad de la información y su tratamiento, podrá ser aplicada sobre cualquier proceso de la AUNAP, a cualquier sistema de información o aspecto particular de la entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información.

2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En el marco del Modelo de Seguridad y Privacidad de la Información y el Sistema de Gestión de Seguridad de la Información –SGSI, la AUNAP busca prevenir las consecuencias no deseadas que se puedan presentar relacionados con la seguridad y privacidad de la información afectando su integridad, confidencialidad y disponibilidad; por lo cual, es importante establecer y controlar los riesgos a nivel de seguridad que puedan afectar la información de la entidad.

Los lineamientos del Modelo de seguridad y privacidad de la información (MSPI) serán aplicados a los procesos estratégicos, misionales, apoyo, evaluación y control de la AUNAP, los cuales son la base fundamental para el desarrollo de las actividades de la entidad y a través de cuales se recolecta y/o genera información que requiere ser protegida y reguardada bajo los criterios de seguridad y privacidad.

La AUNAP se compromete a mantener una cultura de gestión del riesgo asociada con la responsabilidad de diseñar programas y proyectos que sean adoptados y promovidos dentro de la entidad, al igual que los programas y proyectos del sector TIC, regulando los riesgos que se generen entorno a la seguridad y privacidad de la información, mediante mecanismos y controles enfocados a la prevención y detección de hechos asociados, fortaleciendo la eficiencia y eficacia de las medidas para optimizar de manera continua y oportuna la respuesta a los riesgos de manera Integral.

La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesaria a todos los colaboradores relacionados directa o indirectamente con la AUNAP

Se deben tener en cuenta alguna de las siguientes opciones.

Evitar: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad, fuente de riesgo o la exposición a este. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área restringida.

Prevenir: corresponde a planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones, el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos.

Reducir o mitigar: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de contingencia, equipos de protección personal, ambiental y mantener copias de respaldo.

Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad.

3. CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

La Autoridad de Acuicultura y Pesca, buscando dar cumplimiento a la ley y mejorar prácticas ha realizado una identificación de activos de la siguiente manera.

Clasificación de acuerdo con la confidencialidad

INFORMACIÓN PÚBLICA RESERVADA: Corresponde a Información disponible sólo para un proceso que maneje la Entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo de índole legal, operativa, o de pérdida de imagen.

INFORMACIÓN PUBLICADA CLASIFICADA: Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de esta.

Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del responsable.

INFORMACION PÚBLICA: Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

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

Clasificación de acuerdo con la integridad y disponibilidad

Bajo: La no disponibilidad del activo o pérdida de este no conlleva a un impacto negativo en los procesos, pero puede causar demoras en otros procesos.

Medio: La no disponibilidad o integridad de la información puede generar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdida de credibilidad.

Alto o crítico: La no disponibilidad de la información puede conllevar un impacto critico de índole legal o económico, retrasando o perdiendo por completo procesos, o generar pérdidas severas al punto del cierre de la entidad o empresa y a la destitución de sus funcionarios responsables.

Clasificación de acuerdo con la integridad y disponibilidad

Bajo: La no disponibilidad del activo o pérdida de este no conlleva a un impacto negativo en los procesos, pero puede causar demoras en otros procesos.

Medio: La no disponibilidad o integridad de la información puede generar un impacto negativo de índole legal o económico, retrasar sus funciones, o generar pérdida de credibilidad.

Alto o crítico: La no disponibilidad de la información puede conllevar un impacto critico de índole legal o económico, retrasando o perdiendo por completo procesos, o generar pérdidas severas al punto del cierre de la entidad o empresa y a la destitución de sus funcionarios responsables.

ACTIVO	CLASIFICACIÓN
SEPEC	Medio
RGPA	Medio
AZDIGITAL	Medio
PÁGINA WEB	Medio
RED LAN	Bajo
RED WIFI	Bajo
EQUIPOS DE COMPUTO	Bajo
EQUIPOS DE IMPRESIÓN	Bajo
SERVIDORES	Medio

4. SEGUIMIENTO DEL PLAN

4.1 TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

La entidad realiza la clasificación del riesgo, de acuerdo con el nivel de evaluación de los mismos, tomando como base el nivel de evaluación de los riesgos que se describen a continuación:

Evitar: El riesgo, su propósito es proceder con la actividad o la acción que da origen al riesgo, para evitar que se materialice (ejemplo, realizar actividades de seguimiento, tomar alternativas de solución, etc.).

Transferir o compartir el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).

Reducir o Mitigar el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto (ejemplo, la implementación de buenas prácticas para acceder a los sistemas de información)

Retener o aceptar el riesgo, se tomará la decisión de implementar medidas de control adicionales. Monitoreo para confirmar que no se incrementa. (ejemplo, aceptar que el riesgo se materializó y tomar las medidas de control y seguimiento para que no se vuelvan a presentar)

La entidad debe realizar periódicamente una revisión del valor de los activos, impactos, amenazas, vulnerabilidades y probabilidades en busca de posibles cambios, que exijan la valoración de los riesgos de seguridad de la información.

4.2 ROLES Y RESPONSABILIDADES

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

Los jefes o Directores de las diferentes dependencias de la AUNAP designaran un responsable para la Seguridad de la Información en la entidad, el cual debe ser responsable de la información que se genere en dicha área y almacenarla en un medio con su respectiva copia de seguridad y bajo estándares de seguridad.

Las principales responsabilidades de la persona delegada de la seguridad de la información de su área deberán realizar los siguientes controles:

- Identificar, registrar y actualizar los activos de información de su dependencia o proceso de responsabilidad.
- Realizar la clasificación y valorización de los activos de información y revisarla como mínimo anualmente.
- Revisar y gestionar para que los controles de seguridad sean implementados de acuerdo al nivel de clasificación de la información de su proceso.
- Determinar los privilegios de acceso y criterios de respaldo para los activos de información bajo su responsabilidad.
- Revisar y asegurar que los privilegios de acceso a los activos de información de los cuales es responsable son los adecuados.
- Comunicar violaciones de seguridad o incidentes sobre los activos de información de su proceso.
- Garantizar que la información que le ha sido confiada sea protegida durante todo su ciclo de vida (creación, almacenamiento, distribución, transporte y destrucción segura) de modificaciones y usos no autorizados.

5. OPORTUNIDAD DE MEJORA

Realizar un seguimiento continuo para detectar oportunidades de mejora con el fin de Implementar con los funcionarios y contratistas de la entidad un seguimiento y control de seguridad de la información para que pueda ser empleado por cada una de sus áreas y continuar con el seguimiento a lo que ya están definidos.

Adicionalmente la finalidad de este plan es realizar un trabajo en equipo, para socializar las medidas de protección y seguridad de la información que se han establecido en estos planes y así mismo plantear nuevas medidas o acciones conforme al conocimiento de funcionarios y contratistas, en las actividades propias de cada área, dirección o jefatura.

6. INFORMACIÓN DOCUMENTADA RELACIONADA

6.1 Documentos Internos

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

6.2 Documentos externos

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

7. NORMATIVIDAD VIGENTE

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