

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Empresa de Servicios Públicos
Administración Pública
Cooperativa AAA

**EMPRESA DE
SERVICIOS
PÚBLICOS AAA
LA BELLEZANA**



Contenido

Introducción	3
Objetivos	3
Objetivo General	3
Objetivos Específicos	4
Alcance	5
Glosario	5
Marco Normativo	10
Desarrollo del Plan	11
Descripción Del Ciclo De Operación	11
Fase de Diagnostico	12
Fase de Planeación	14
Política de Seguridad y Privacidad de la Información	17
Políticas de seguridad y Privacidad de la Información	19
Procedimientos De Seguridad Y Privacidad De La Información	22
Roles Y Responsabilidades	27
Inventario De Activos De Información	27
Comité Ti	27
Cumplimiento	28
Comunicación	28
Fase Implementación	28
Divulgación De La Información	28
Actualización De Recursos Informáticos	29
Administración y control	29
Sitio Web	29
Licencias De Software	30
Gestión Documental	30
Identificación, Contraseñas Y Autorizaciones	30
Seguridad Física	31
Seguridad Informática	31
Seguimiento Y Control	31
Actividades	32
Fase De Mejora Continua	33



Introducción

La cooperativa de acueducto, aseo y alcantarillado La Bellezana, del municipio la Belleza, Santander, empresa de servicios públicos mixta, cuyo objeto social es la prestación del servicio y tratamiento de agua potable y saneamiento básico, que comprende barrido de calles, disposición final de residuos, promover el reciclaje y sus actividades complementarias; propone el siguiente plan de seguridad de la información para la vigencia 2024.

Siendo consiente que la seguridad y privacidad de la información, debe ser un componente crítico y fundamental dentro de la estrategia institucional de las entidades a nivel nacional, por ello la Administración pública Cooperativa de acueducto, aseo y alcantarillado, AAA. La Bellezana, presenta a los grupos de interés y a la ciudadanía el presente plan donde reconoce la importancia de la información como recurso valioso para el desarrollo de sus funciones.

El Plan de Seguridad y Privacidad de la Información se elaboró teniendo en cuenta los lineamientos del Manual de Política de Gobierno Digital y del Modelo de Privacidad y Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones, como lo dispone la ley 1712 de 2014, especialmente desarrollando acciones preventivas para el cumplimiento de la misma.

Objetivos

Objetivo General

Definir las acciones para incrementar el nivel de madurez de seguridad y privacidad de la información de la Cooperativa AAA. La Bellezana, de acuerdo con las estrategias de Gobierno Digital, MIPG, requerimiento de la entidad, disposiciones legales y buenas prácticas, garantizando la integridad, confidencialidad, disponibilidad, resguardo y



privacidad de la información institucional.

Objetivos Específicos

Fortalecer y optimizar la seguridad y privacidad de la información al interior de la Bellezana, apoyando el cumplimiento de los objetivos estratégicos de la entidad.

Identificar, clasificar y mantener actualizados los activos de información de la Cooperativa AAA. La Bellezana.

Gestionar los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad de la operación tecnológica, que puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información.

Gestionar los eventos e incidentes de seguridad de la información que afecten o puedan afectar la integridad confidencialidad, disponibilidad y privacidad de manera oportuna y pertinente reduciendo su impacto y propagación.

Atender los requerimientos de seguridad de la información, seguridad digital y ciberseguridad, establecidos por las diferentes entidades a nivel nacional y requerimientos regales.

Fortalecer la cultura, los conocimientos y habilidades de los contratistas y gerencia en los temas de seguridad y privacidad de la información.

Desarrollar estrategias que permitan la continuidad de los servicios tecnológicos prestados por la Cooperativa, frente a situaciones adversas que impidan el normal funcionamiento y prestación de estos.



Alcance

El presente plan de seguridad y privacidad de la información aplica a todos los procesos definidos en cada área de la entidad, funcionarios, contratistas y terceros.

Glosario

Acceso a la Información Pública:

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC27000).

Activo de Información:

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo:

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art



3).

Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización:

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales:

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC



2258 de 2009).

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos:

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales:

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos:

Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados:

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).



Datos Personales Mixtos:

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

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.(Decreto 1377 de 2013, art 3).

Declaración de aplicabilidad:

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad:

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos:

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del tratamiento. (Ley 1581 de 2012, art 3).



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. (ISO/IEC 27000).

Información Pública Clasificada:

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Información Pública Reservada:

Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6).

Ley de Habeas Data:

Se refiere a la Ley Estatutaria 1266 de 2008



Marco Normativo

Ley 594 de 2000 “Por medio de la cual se dicta la ley general de archivos y se dictan otras disposiciones.

Acuerdo 003 de 2015 “Por el cual se establecen lineamientos generales para las entidades del estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la ley 1437 de 2011, se reglamenta el artículo 21 de la ley 594 de 2000 y el capítulo IV del decreto 2609 de 2012”.

Ley 1712 de 2014 “Por medio de la cual se crea la ley de transparencia y el derecho de acceso a la información pública nacional y se dictan otras disposiciones.

Decreto 338 de 2022 “Título 21 lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de la seguridad digital.

Resolución 1519 de 2020 “Sobre transparencia en el acceso a la información, accesibilidad web, seguridad digital web y datos abiertos

Responsables

Todas las áreas y contratistas de la cooperativa son responsables del cumplimiento de los lineamientos y actividades definidas en este plan.

Desarrollo del Plan

Tomando como base el modelo de seguridad y privacidad de la información del MINTIC, se adoptan las 5 fases que comprenden el ciclo de operación, con el fin de gestionar adecuadamente la seguridad y privacidad de los activos de la información de la Cooperativa AAA. La Bellezana.

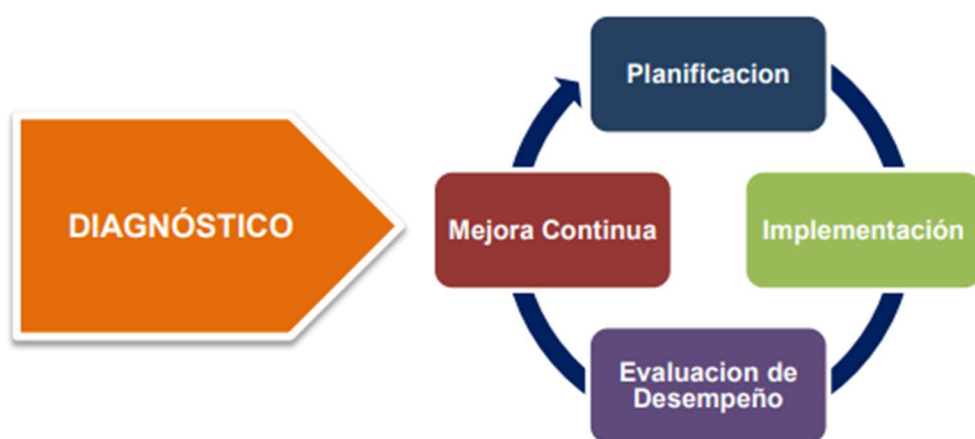


Figura1. Ciclo de Operación del modelo de seguridad y privacidad de la información – tomado del MINTIC

Descripción Del Ciclo De Operación

A continuación, se explica a manera general el ciclo del funcionamiento del modelo de operación adoptado por la entidad, el cual está comprendido por 5 fases, los cuales permiten que la seguridad y privacidad de la información, sea un sistema de gestión sostenible dentro de la Cooperativa de Acueducto, Aseo y Alcantarillado la Bellezana.

Diagnosticar	Planear	Realizar	Verificar	Implementar
Identificación del estado actual	Definición de las políticas de seguridad y privacidad de la información	Asignación Recursos de	Medición resultados de	Aplicación de las acciones correctivas y mejora
metas	Estimar Riesgos	Inventario Activos de	Análisis Tendencias de	Resultados
Identificar el uso de las buenas prácticas	Objetivos	Políticas de seguridad y privacidad de la información	Revisión y supervisión de la organización	Definición de indicadores de gestión

Tabla 1. Descripción del Ciclo de Operación 2023 de la AAA. La Bellezana.

Fase de Diagnostico

Esta fase permite por medio de herramientas de diagnóstico online de aquellas entidades que ejercen control sobre la cooperativa y demás entidades del estado colombiano, inspeccionar a manera crítica las condiciones técnicas mínimas y de seguridad digital web que actualmente se cumple para de esta manera establecer el nivel de madurez en cuando a seguridad y privacidad de la información y así poder definir las actividades en el proceso de la implementación del MSPI.

Teniendo en cuenta que actualmente el nivel de cumplimiento ITA para el periodo 2023 es de un 79 sobre 100 puntos, lo cual nos sitúa aún en un nivel básico de cumplimiento en accesibilidad, gestión de la información y seguridad digital web, por lo que se viene



ADMINISTRACIÓN PÚBLICA COOPERATIVA ACUEDUCTO, ASEO, ALCANTARILLADO
LA BELLEZA SANTANDER
NIT: 900.348.296 - 2

adelantando la actualización de los planes y políticas de seguridad y privacidad de la información, manejo de conjunto de datos directamente en la plataforma de datos abiertos, bajo el perfil AAA La Bellezana, con el fin de cumplir condiciones de publicación de los activos de información de la entidad.

A corte de diciembre de 2023, el avance general de acuerdo con la medición del instrumento de identificación de la línea base de seguridad, proporcionado por el Ministerio de Tecnologías de la Información y las comunicaciones, se encuentra con e un estado de implementación de la siguiente manera:

No.	Evaluación de Efectividad de Controles	Calificación	
	Dominio	Actual	Objetivo
A.5	Políticas de Seguridad de la Información	60	60
A.6	Organización de la Seguridad de la Información	30	60
A.7	Seguridad de los Recursos Humanos	40	60
A.8	Gestión de Activos	40	60
A.9	Control de Acceso	50	60
A.10	Criptografía	10	60
A.11	Seguridad Física y del Entorno	30	60
A.12	Seguridad de las Operaciones	60	60
A.13	Seguridad de las Comunicaciones	50	60
A.14	Adquisición, Desarrollo y Mantenimiento de Sistemas	30	60
A.15	Relaciones con los proveedores	30	60
A.16	Gestión de incidentes de seguridad de la información	0	60
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	20	60
A.18	Cumplimiento	30	60
PROMEDIO		34.28	60

Tabla 2. Estado de implementación a corte diciembre 31-2024 de la AAA. La Bellezana.



Fase de Planeación

En esta fase relacionamos el resultado dado en la fase de diagnóstico y el estado actual de la Cooperativa AAA. La Bellezana, por lo que permite la identificación de las acciones claves que van a definir y orientar las actividades para los propósitos de seguridad y privacidad.

El nivel de implementación del MSPI permitirá a la administración pública cooperativa de acueducto, aseo y alcantarillado del municipio la Belleza, Santander, establecer la estrategia a desarrollar para la vigencia 2024 y de esta manera llevar a cabo mejoras en la seguridad y privacidad de la información, para los procesos internos de gestión, control y apoyo de la entidad y toda la infraestructura que los soporte.

Planificación			
Metas	Resultados	Instrumentos MSPI	MRAE
Política de Seguridad y Privacidad de la Información	Se logra actualizar el documento con la política de seguridad de la información, debidamente aprobado por la Gerencia y socializada al interior de la Cooperativa e implementación de la misma.	Guia N° 2 _ Política General MSPI	
Políticas de seguridad y privacidad de la información	Dentro de la política general de seguridad y privacidad de la información se logran establecer y actualizar las políticas de seguridad y privacidad de la información, debidamente aprobados por la Gerencia y socializados al interior de la		



ADMINISTRACIÓN PÚBLICA COOPERATIVA ACUEDUCTO, ASEO, ALCANTARILLADO
LA BELLEZA SANTANDER
NIT: 900.348.296 - 2

	entidad		
Procedimientos de Seguridad de la Información	Procedimientos documentados dentro de las políticas de seguridad y privacidad de la información,, socializados y aprobados por el comité que TI. En proceso de mejora de la documentación para año 2024.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08 LI.ES.09 LI.ES.10 LI.GO.01 LI.GO.04
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se creará con las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la Gerencia de la Cooperativa, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad. El cual se encuentra en proceso de elaboración de la resolución para su aprobación.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	LI.GO.07 LI.GO.08 LI.GO.09 LI.GO.10 LI.INF.01 LI.INF.02 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23 LI.SIS.01 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12
Inventario de activos de información.	Documento con la metodología para identificación, clasificación y	Guía No 5 - Gestión De Activos	LI.ST.13 LI.ST.14 LI.UA.01



ADMINISTRACIÓN PÚBLICA COOPERATIVA ACUEDUCTO, ASEO, ALCANTARILLADO
LA BELLEZA SANTANDER
NIT: 900.348.296 - 2

	<p>valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la Gerencia.</p> <p>Matriz con la identificación, valoración y clasificación de activos de información.</p> <p>Documento con la caracterización de activos de información, que contengan datos personales</p>		<p>LI.UA.02</p> <p>LI.UA.03</p> <p>LI.UA.04</p> <p>LI.UA.05</p> <p>LI.UA.06</p>
Integración del MSPI con el Sistema de Gestión documental.	Se encuentra en un proceso la Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestión Documental	
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de Riesgos, análisis y evaluación de Riesgos, el plan de tratamiento de Riesgos, con la declaración de aplicabilidad. <p>Documento en proceso de revisión y aprobación por de la Gerencia.</p>	Guía No 7 - Gestion de Riesgos	Guía No 8 - Controles de Seguridad



Plan de Comunicaciones	Documento llamado Plan Estratégico de Tecnologías de la Información tiene integrado el plan de comunicación, para la entidad, en proceso de mejora y aprobación.	Guía No 14 - Plan de comunicación, sensibilización y capacitación	
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6 en proceso de implementación	Guía No 20 - Transición IPv4 a IPv6	

Tabla 3. Planificación 2024 de la AAA. La Bellezana

A continuación se explica de manera general la fase de planificación del Modelo de Seguridad y Privacidad de la Información.

Política de Seguridad y Privacidad de la Información

La política de seguridad y privacidad de la información está contenida en el documento llamado POLITICA DE SEGURIDAD DE LA INFORMACIÓN - AAA LA BELLEZANA, el cual lleva un historial de actualización desde su creación en el año 2016 al 2023, el mencionado se encuentra publicado en el sitio web dentro del footer o pie de página, en donde se encuentra un enlace de consulta o descarga del archivo, de clic [AQUÍ](#) para visualizar.

A continuación se expone la política de seguridad de la información de la Cooperativa:
En la Cooperativa de servicios públicos AAA LA BELLEZANA, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada a la administración de riesgos y la consolidación de una cultura de seguridad.



Consciente de sus necesidades actuales, la Cooperativa de servicios públicos AAA LA BELLEZANA Implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios vigentes.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de vigilancia seleccionados para obtener los niveles de protección esperados en la Cooperativa; este proceso será liderado de manera permanente por Gerencia General y los designados para tal fin.

Esta política será revisada con regularidad como parte del proceso de revisión estratégica, o cuando se identifiquen cambios en la Entidad, su estructura, sus objetivos o alguna condición que afecte la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

La Cooperativa de servicios públicos **AAA LA BELLEZANA**, para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

- 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.
- Implementar el sistema de gestión de seguridad de la información.
- 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.

- Garantizar la continuidad del negocio frente a incidentes.
- La Cooperativa AAA. La Bellezana ha decidido definir, implementar, operar y mejorar de forma continua un sistema de gestión de seguridad de la información, soportado en lineamientos claros y alineados a las necesidades del negocio, y a los requerimientos regulatorios.

Políticas de seguridad y Privacidad de la Información

La Cooperativa AAA. La Bellezana, con el propósito de salvaguardar la información de la entidad, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha optado la elaboración del plan de seguridad y privacidad de la información, con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados o duplicación de la misma sin previa autorización, a su vez ofrece una política de seguridad de la información física recibida, emitida y resguardada en instalaciones de la Cooperativa, no obstante la información digital que es tratada por funcionarios internos y externos, los cuales deben cumplir con la preservación de las políticas dispuestas en el documento publicado en el sitio web en el pie de página en el link [Políticas de Protección de datos](#), donde podrá ser direccionado para la consulta del documento.

A continuación, se establecen las 12 políticas de seguridad que soportan el SGSI de La Cooperativa de servicios públicos **AAA LA BELLEZANA**.

1. La Cooperativa de servicios públicos **AAA LA BELLEZANA** ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. La Cooperativa de servicios públicos **AAA LA BELLEZANA** indica que las responsabilidades frente a la seguridad de la información serán definidas,



ADMINISTRACIÓN PÚBLICA COOPERATIVA ACUEDUCTO, ASEO, ALCANTARILLADO
LA BELLEZA SANTANDER
NIT: 900.348.296 - 2

compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

3. La Cooperativa de servicios públicos **AAA LA BELLEZANA** protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos.
4. La Cooperativa de servicios públicos **AAA LA BELLEZANA** protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. La Cooperativa de servicios públicos **AAA LA BELLEZANA** protegerá su información de las amenazas originadas por parte del personal.
6. La Cooperativa de servicios públicos **AAA LA BELLEZANA** protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. La Cooperativa de servicios públicos **AAA LA BELLEZANA** controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. La Cooperativa de servicios públicos **AAA LA BELLEZANA** implementará control de acceso a la información, sistemas y recursos de red.
9. La Cooperativa de servicios públicos **AAA LA BELLEZANA** garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. La Cooperativa de servicios públicos **AAA LA BELLEZANA** garantizará a través



ADMINISTRACIÓN PÚBLICA COOPERATIVA ACUEDUCTO, ASEO, ALCANTARILLADO
LA BELLEZA SANTANDER
NIT: 900.348.296 - 2

de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

11. La Cooperativa de servicios públicos **AAA LA BELLEZANA** garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

12. La Cooperativa de servicios públicos **AAA LA BELLEZANA** garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.



Procedimientos De Seguridad Y Privacidad De La Información

Actualmente la Cooperativa AAA. La Bellezana cuenta con un conjunto de procedimientos de seguridad de la información para el Modelo de Seguridad y Privacidad de la Información para la entidad, teniendo en cuenta las características particulares, activos de información, procesos y servicios de información que pueda prestar.

1. Seguridad Del Recurso Humano:

En este dominio relacionado con el personal que labora dentro de la entidad, se pueden definir los siguientes procedimientos:

1.1. Procedimiento De Capacitación Y Sensibilización Del

Personal: Antes de asumir el empleo la gestión contractual debe establecer mecanismos o controles necesarios para proteger la confidencialidad y reserva de la información contenidas en las historias laborales y expedientes contractuales.

1.2. Procedimiento Durante La Ejecución Del Empleado: Los servidores públicos y contratistas deben informar de los incidentes de la seguridad de la información a trabes de los medio dispuestos por la gerencia de la triple A.

1.3. Procedimiento De Ingreso Y Desvinculación Del Personal: En el proceder del ingreso, la entidad deberá verificar antecedentes del aspirante al cargo tales como: Antecedentes disciplinarios, fiscales y judiciales, adicional la validación de título y el historial laboral presentado en su hoja de vida. Una vez validada la información suministrada por el mismo, se procede a la contratación e inmediatamente se debe hacer cargo del objeto por el cual ha sido contratado y deberá conocer sus obligaciones como contratistas para poder desempeñar la ejecución de contrato pactado, también tener claro los documentos a presentar como evidencia del cumplimiento de su labor durante el proceso contractual hasta finalizar el



contrato.

Al finalizar el periodo de labor la entidad liquida el contrato con la información pertinente, la cual deberá ser validada y aprobada por las dos partes, solo de esta manera se podrá dar por finalizada la contratación. Teniendo conocimiento de los términos de confidencialidad inicialmente expuestos.

2. Gestión De Activos

En este dominio relacionado con la identificación y clasificación de activos de acuerdo a su criticidad y nivel de confidencialidad se pueden definir los siguientes procedimientos.

- 2.1. Procedimiento De Identificación Y Clasificación De Activos De Información:** Los servidores públicos, contratistas o terceros deben aplicar la clasificación de información de la cooperativa. Las TRD, el inventario de activos de información y lineamientos para la administración de los archivos.
- 2.2. Procedimiento Responsabilidad Por Los Activos:** Todos los activos de la información mantenidos en el inventario deben tener un propietario.
- 2.3. Procedimiento De Manejo De Medios:** Es responsabilidad de cada servidor público o contratista tomar las medidas para la protección de información contenida en medios removibles para evitar acceso físico y lógicos no autorizados, daños, pérdida de información o extravíos del mismo.

3. Control De Acceso

En este dominio relacionado con el acceso a la información y a las instalaciones de procesamiento de la información, se pueden generar los siguientes procedimientos:

- 3.1. Procedimiento Para Ingreso Seguro A Los Sistemas De Información:** La cooperativa AAA- La Bellezana debe suministrar y garantizar el cambio de contraseña; a los usuarios cambios de credenciales para el acceso a los servicios de red y sistemas de información para quienes hallan sido autorizados, según su



perfil y rol, las credenciales de acceso son de uso personal e intransferible. La Gerencia velará por los servicios tecnológicos que sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico, teniendo en cuenta la matriz de roles y perfiles para cada sistema de información.

- 3.2. Procedimiento De Gestión De Usuarios Y Contraseñas:** El usuario del correo electrónico debe ser igual al usuario de red y la contraseña inicialmente será asignada por la entidad, por lo cual se deberá mantener, y en caso de cambio reportar la nueva clave. Los usuarios deben tener la responsabilidad que las contraseñas modificadas tengan algún grado de complejidad y no deberán ser palabras comunes que se puedan encontrar en diccionarios ni tener información personal por tanto se deben cambiar constantemente las credenciales y reportar su actualización a gerencia.

4. Seguridad Física Y Del Entorno

Este dominio está relacionado con la prevención del acceso a áreas no autorizadas, el daño a la infraestructura, las instalaciones o de la información.

- 4.1. Procedimiento De Control De Acceso Físico:** Las puertas y ventanas de las áreas seguras deben permanecer cerradas y bloqueada cuando no haya supervisión o estén desocupadas.
- 4.2. Procedimiento De Protección De Activos:** La Cooperativa de acueducto aseo y alcantarillado establece los lineamientos para el uso, mantenimiento de la red de energía, obteniendo regulación de los puestos de trabajo, en los cuales solo deben conectar equipos como computadores de escritorio, portátiles y pantallas, los demás deben conectarse a la red eléctrica no regulada.
- 4.3. Procedimiento De Retiro De Activos:** Los activos son retirados de la entidad con previa autorización y registro.



4.4. Procedimiento De Mantenimiento De Equipos: Se ejecutan mantenimientos preventivos o correctivos dentro de la entidad, con los respectivos intervalos de tiempo de ejecución.

5. Seguridad De Las Operaciones

Este dominio busca asegurar las operaciones correctas dentro de las instalaciones de procesamiento de información de la Cooperativa:

5.1. Procedimiento De Gestión De Cambios: Identificación y registro de cambios significativos, planificación y pruebas previas de los cambios a realizar en los procesos o sistemas de la bellezana, valoración de impactos, tiempos de no disponibilidad del servicio, comunicación a las áreas pertinentes, entre otros.

5.2. Procedimiento De Gestion De Capacidad: La entidad realiza una gestión de la capacidad para los sistemas de información críticos, en especial si los recursos requeridos son escasos, demorados en su arribo o costosos. La entidad realiza acciones como la eliminación de datos obsoletos, cierre de aplicaciones, ambientes y sistemas en desuso, restricción de ancho de banda etc...

6. Seguridad De Las Comunicaciones

Este dominio busca el aseguramiento y la protección de la información a través de los diferentes servicios de comunicaciones de la organización.



6.1. Procedimiento De Transferencia De Información: Se realiza la transmisión o transferencia de la información de manera segura dentro de la cooperativa, teniendo en cuenta las copias de seguridad de la información en equipos como en el portal web y los sistemas de la entidad, estableciendo previamente las condiciones sobre la información que se va a proteger, la duración del acuerdo, responsabilidades, propietarios de la información, acciones en caso de incumplimiento, entre otros.

7. Adquisición Desarrollo Y Mantenimiento De Sistemas De Información

7.1. Procedimiento Adquisición, Desarrollo Y Mantenimiento De Software: Se encuentra la descripción de las actividades ejecutadas en gestión de la seguridad de la información en los sistemas desarrollados internamente o adquiridos a un tercero, verificando que cada uno de ellos preserve la confidencialidad, integridad y disponibilidad de la información de la entidad

7.2. Procedimiento De Control Software: En este procedimiento la entidad indica como se realizaría la gestión de las solicitudes de instalación de software para los usuarios autorizados y se realiza el inventario de software dentro de la entidad entre otros aspectos.

8. Gestión De Incidentes De Seguridad De La Información

8.1. Procedimiento De Gestión De Incidentes De Seguridad De La Información: La entidad prepara y gestiona el incidente por medio del monitoreo y verificación de los elementos de control con el fin de detectar y analizar un posible incidente de seguridad de información, al cual se le brinda la atención pertinente, tomando en cuenta la comunicación para con los administrativos y contratistas de la entidad informando sobre las nuevas vulnerabilidades, actualizaciones a la plataforma y recomendaciones de seguridad informática a través del correo electrónico o sitio web de la entidad.



Roles Y Responsabilidades

Es responsabilidad de los funcionarios internos y externos que hacen parte del comité de las Tecnologías de Información de la Cooperativa, la implementación, aplicación, seguimiento y autorizaciones de la política de seguridad y privacidad de la información, que sean utilizadas como herramientas para los debidos procesos de la gestión en la misma, las cuales deben ser aplicadas de forma obligatoria a nivel general para el cumplimiento de los objetivos y normatividades vigentes concernientes a la preservación de la información como activo histórico de la entidad pública, como lo es la Cooperativa de Acueducto, Aseo y Alcantarillado la Bellezana.

Inventario De Activos De Información

La entidad cuenta con un inventario documental el cual se puede localizar en el portal web de la Cooperativa de Acueducto, aseo y alcantarillado La Bellezana, en el ítem Transparencia / Instrumentos de Gestión de Información Pública, el cual se encuentra en implementación como con junto de datos en la plataforma Datos Abiertos.

Comité Ti

Este comité es el encargado de toda el área de Tecnología de Información de la entidad, el cual lleva el seguimiento a las iniciativas de TI y seguridad/privacidad de la Información, entre otras la Gobernabilidad y seguridad, el cual refiere a la creación de planes propios de TIC, con el fin de llevar a cabo un óptimo resguardo de la información, en los diferentes medios digitales a nivel de Hardware y Software.



Cumplimiento

El cumplimiento de las políticas establecidas en el presente son de obligatoriedad, ya que si los funcionarios omiten alguna, es el deber de la Gerente de la entidad tomar las medidas correspondientes.

Comunicación

El presente documento será socializado con los funcionarios dando a conocer las políticas de la seguridad y privacidad de la información, así mismo, este se alojará en el portal web referenciado a continuación <https://aaalabellezana.org.co/index.html>, y el soporte físico estará a cargo de la administración documental de la misma, para que puedan ser consultados por la entidad de control que lo requiera u otros según corresponda.

Fase Implementación

En base a las políticas y procedimientos planteados se organizan actividades para llevar a cabo la implementación del plan de seguridad y privacidad de la información para la vigencia en curso

Divulgación De La Información

- La información publicada en redes sociales, o sitio web, debe hacerse a través del funcionario encargado, según su perfil profesional, quien debe hacerse responsable del manejo de la publicación de información de la entidad.
- Los diferentes funcionarios deben proteger los archivos para su divulgación, este con el fin de evitar modificación en los mismos.
- La Cooperativa no se hace responsable por las consecuencias que se deriven de la utilización inadecuada por parte de terceros.



Actualización De Recursos Informáticos

- Llevar a cabo el mantenimiento preventivo y correctivo de los recursos informáticos de la cooperativa, teniendo en cuenta la vida útil de los mismos.
- Se debe contar con personal apto para generar diagnósticos de equipos obsoletos y si es el caso dar de baja para renovación, sin perder información del anterior.
- Exigir a los funcionarios la utilización responsable de los recursos informáticos, teniendo en cuenta las medidas de control establecidas para proteger el software y hardware y datos almacenados.
- Correcta utilización de dispositivos móviles corporativos ya que la atención se está brindando por este medio y hay información que puede ser útil para algún proceso de peso en la entidad

Administración y control

- La conexión a la red, debe ser autorizada por la Gerente de la Cooperativa AAA. La Bellezana.

Sitio Web

- Actualizar constantemente el sitio web <https://aaalabellezana.org.co/index.html>, en el cual se encontrará gran parte de la documentación pública, como información de contacto y sitios electrónicos de la Cooperativa.
- Realizar las publicaciones con previa aprobación y autorización de la Gerencia y áreas dentro de la organización de la Bellezana.
- Una vez Publicada la actualización es responsabilidad del funcionario solicitante.



Licencias De Software

- La cooperativa debe adquirir software según la necesidad y su respectiva licencia para de esta manera poseer características ajustables a lo requerido en los procesos del área
- Emplear en lo posible las últimas versiones ofimáticas disponibles en el mercado para disminuir los problemas de incompatibilidad de formato debido al cambio de versiones.
- Todos los programas utilizados en los recursos informáticos deben ser licenciados

Gestión Documental

- Circulares y demás comunicaciones digitales deben ser enviadas por correo electrónico, publicación en redes sociales y portal web de la Cooperativa, con el ánimo de regir buenas prácticas y dar continuidad a la estrategia de cero papel.
- Responsabilizar al usuario y funcionario el estar consultando los diferentes medios establecidos para la socialización de noticias informativas, circulares, decretos y demás.
- La radicación de correspondencia interna y externa que requiera imprimirse es responsabilidad de cada área y el funcionario encargado de la gestión documental.

Identificación, Contraseñas Y Autorizaciones

- Todos los funcionarios que accedan a los sistemas de información de la cooperativa deberá tener su propio identificador el cual será asignado como parte del proceso de autorización , de esta manera todas las acciones realizadas por el usuario adquirido tendrá un responsable.
- Los usuarios, claves, y autorizaciones deberán ser deshabilitadas o modificadas una vez se tenga la desvinculación del funcionario.



Seguridad Física

Establecer protocolos de seguridad apropiados en el ingreso a las instalaciones de la cooperativa (funcionarios, contratistas y terceros)

Seguridad Informática

- Llevar a cabo la creación de Backup semestral del Sitio Web de la Cooperativa
- Llevar a cabo la creación de copias de seguridad de los quipos de la entidad
- Llevar a cabo la configuración de copia de seguridad a los dispositivos móviles y redes sociales (Facebook, Whatsapp entre otros)
- Llevar a cabo la correcta depuración del servicio de correo electrónico de Google Gmail, ya que esta por ser una herramienta gratuita tiende a limitar el espacio de almacenamiento a tan solo 15 GB, y al llegar al tope inhabilita las entradas y salidas de mensajería, un riesgo que es manejable pero que si llega a suceder puede durar un promedio de 3 días para su activación de servicio.
- Llevar a cabo resguardo del servicio de correo electrónico de Google Gmail, herramienta gratuita y multidispositivo, la cual tiene una historia de los procedimiento contractuales, PQRS y de diferentes entes de control, los cuales se deben conservar de forma segura la Cooperativa AAA La Bellezana
- Depuración correcta de correos electrónicos corporativos
- Llevar a cabo la copia de seguridad a correos electrónicos corporativos, en casos fortuitos.

Seguimiento Y Control

Las políticas de Seguridad y Privacidad de la Información, deberá ser revisado y ajustado anualmente, garantizando que el contenido se encuentre actualizada conforme a los



cambios surgidos en la entidad, realizando seguimiento constante de las actividades establecidas en el cronograma del Plan de Seguridad y Privacidad de la Información, quedando como evidencia la respectiva evaluación, seguimiento y mejoras de las actividades programadas para la nueva vigencia.

Actividades

- Revisión de la Política de Seguridad y Privacidad de la Información
- Seguimiento del comité de TI a las políticas de seguridad y Privacidad de la Información
- Implementación de las Políticas de Seguridad y Privacidad de la Información
- Aprobación y adopción de las Políticas de Seguridad y Privacidad de la Información
- Backup sitio web de la Cooperativa
- Backup computadores de la Bellezana
- Backup de dispositivos móviles y redes sociales (whatsapp entre otros).Backup de correo gratuito Gmail
- Backup de correos corporativos



Fase De Mejora Continua

La Bellezana tiene como objetivo principal la elaboración del plan de mejoramiento, el cual se trabaja con la consolidación de las evaluaciones de vigencias previas para este año 2024.

MEJORA CONTINUA			
METAS	RESULTADOS A OBTENER	INSTRUMENTOS	
		MSPI	MRAE
Plan de Mejora Continua	Documento con el Plan de Mejoramiento	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17 – Mejora Continua	LI.GO.03 LI.GO.12 LI.GO.13 LI.INF.14 LI.INF.15 LI.ST.15 LI.UA.9 LI.UA.10

Tabla 4. Meta propuesta para la vigencia 2024 de la AAA. La Bellezana