PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Empresa de Servicios Públicos
Administración Pública
Cooperativa AAA

EMPRESA DE SERVICIOS PÚBLICOS AAA

LA BELLEZANA

CUADRO DE CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
Inicial	**2020**	Emisión Inicial
1.0	**2021**	Ajustes y Publicación
2.0	**2022**	Actualización
3.0	**2023**	Actualización, cronograma y evaluación vigencia anterior
4.0	**2024**	Reestructuración
5.0	**2025**	Actualización

CONTENIDO

INTRODUCCIÓN

La Cooperativa de acueducto, aseo y alcantarillado La Bellezana, adopta la “Guía para la administración del riesgo y el diseño de controles de entidades públicas” y el “Anexo 4 Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas”, para de esta manera crear la estrategia en mejora del tratamiento de riesgos de esta entidad, llevando a cabo la identificación de riesgos de seguridad digital sobre los activos de información creación de controles y su respectivo seguimiento, teniendo en cuenta las categorías como lo son: Aceptar, reducir, evitar y compartir el riesgo.

De esa manera los servidores públicos en general están sometidos a riesgos que pueden afectar la gestión realizada por ende es propuesto el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, con el objetivo de orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo identificando las posibles causas, definiendo controles sobre los mismos.

OBJETIVOS

- Realizar un proceso de mejora continua para el tratamiento de riesgos de seguridad digital.
- Aplicar los lineamientos indicados en la “Guía para la administración del riesgo y el diseño de controles en entidades públicas” y procesos internos para tratar de manera integral los riesgos de seguridad y privacidad de la información y de esta manera propender por la integridad, confidencialidad y disponibilidad.
- Gestionar los riesgos de seguridad y privacidad de información
- Fortalecer y apropiar los conocimientos referentes a la gestión de riesgos y seguridad de la información.

ALCANCE

El plan presentado aplica a todos los funcionarios de la Cooperativa con el fin de realizar una eficiente gestión del riesgo del seguridad y privacidad de la información.

REFERENCIAS NORMATIVAS

Normativa	Descripción	Link de consulta
Riesgos de Gestión, Corrupción y Seguridad Digital.	Guía para la administración del riesgo y el diseño de controles en entidades públicas.	https://gobiernodigital.mintic.gov.co/692/articles-82062_recurso_1.pdf
ISO 27001:2013	Tecnologías de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos	https://dgsei.edomex.gob.mx/sites/dgsei.edomex.gob.mx/files/manuales/Norma%20ISO%2027001-2013.pdf

Ley 1712 de 2014	Transparencia y Del Derecho de Acceso a la Información Pública	https://funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882
Anexo 4	Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas	https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

Tabla 1. Referencias normativas

Fuente: Autor

CONCEPTOS BÁSICOS

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 consecuencia.

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo. Esta puede ser medida con criterios de frecuencia o factibilidad.

Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Consecuencia: los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

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.

Riesgo inherente: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

Gestión del riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

Mapa de riesgos: documento con la información resultante de la gestión del riesgo.

Plan Anticorrupción y de Atención al Ciudadano: plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.

Confidencialidad: propiedad de la información que la hace no disponible, es decir, divulgada a individuos, entidades o procesos no autorizados.

Vulnerabilidad: es una debilidad, atributo, causa o falta de control que permitiría la explotación por parte de una o más amenazas contra los activos.

Integridad: propiedad de exactitud y completitud.

Tolerancia al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

Activo: en el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

Control: medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones).

Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

Disponibilidad: propiedad de ser accesible y utilizable a demanda por una entidad.

Apetito al riesgo: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

Ciberseguridad: Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan.

Confidencialidad: Atributo de la información que determina quien está autorizado a acceder a ella y previene su divulgación no autorizada dentro de la Cooperativa AAA La Bellezana.

Contraseña Fuerte: Contraseña que consta mínimo de nueve caracteres, mayúsculas, minúsculas, números y caracteres especiales.

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

Copias de Seguridad: Es el proceso mediante el cual se realiza la copia de la información existente, con el fin de poder recuperarla, en caso en que ocurra un fallo que afecta a esta y pueda estar disponible.

Custodio de Activo de Información: Parte designada de la organización, un cargo, proceso o grupo de trabajo encargado de administrar, modificar, leer, procesar y hacer efectivos los controles de seguridad definidos, tales como copias de seguridad.

Disponibilidad: Atributo de la información que determina para quien está disponible y los permisos de su uso dentro de las gestiones que adelante la Cooperativa

Gestión de Claves: Son controles que se realizan mediante la gestión de claves criptográficas.

Gestión de Incidentes de Seguridad de la Información: Son las acciones de control para garantizar la seguridad de los activos de información y su apropiada gestión, implementando las acciones para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la Cooperativa.

Gestión de Riesgos: Son las acciones que realiza la Cooperativa para la identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo.

Impacto: El costo de la organización de un incidente (de la escala que sea) que puede o no ser medido en términos estrictamente financieros.

Incidente de Seguridad de la Información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que compromete a la Cooperativa.

Información: Es un activo de valor que hace parte de la Agencia Nacional Digital, por la cual asume funciones, como responsable o encargada de la misma en cumplimiento de los requisitos legales, normativos e institucionales. La información corresponde a todo dato de la entidad (tecnológico, administrativo, financiero, contable, entre otros), propio o de terceros, con las cuales dispone de un acuerdo o convenio; y datos personales de los cuales asume un rol como responsable o encargado.

Integridad: Atributo de la información que protege los activos de información, software, sobre posibles alteraciones, modificaciones no autorizadas, formalmente por la Cooperativa.

Inventario de Activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, intangibles, etc) dentro del alcance dentro del SGSI, que tenga valor para la Cooperativa y necesiten por tanto ser protegidos de potenciales riesgos.

Principios de Seguridad de la Información: Son características propias de la protección de la información: La Confidencialidad, Integridad y Disponibilidad.

Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Responsable 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: Es la probabilidad de que una amenaza o vulnerabilidad pueda ocasionar la perdida y/o alteración de la información de la Cooperativa.

Seguridad de la Información: Preservación de la confidencialidad integridad y disponibilidad de la información.

Sistema de Gestión de Seguridad de la Información (SGSI): Es un conjunto de políticas, de seguridad de la información, que siguen la norma ISO/IEC/27001. Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, minimizando a la vez los riesgos de seguridad de la información.

Vulnerabilidad: Es la debilidad o fallo del sistema que pone en riesgo la confidencialidad, integridad y disponibilidad de la información de la Cooperativa.

Norma: Principio que se dispone de carácter general, donde se establecen las obligaciones, restricciones y orientaciones para el acceso y uso de los activos de información.

Política: Declaración de alto nivel que describe la posición de la Cooperativa sobre un tema específico.

ESTABLECIMIENTO CONTEXTO

Teniendo como base la identificación de los servicios ofrecidos por la Administración Pública Cooperativa de Acueducto, Aseo y Alcantarillado la Bellezana, y que se soportan en los activos de información los cuales deben ser identificados previamente, según su proceso, en segunda instancia se debe realizar la estimación de probabilidad y el impacto de las amenazas halladas para el contexto externo o interno de la cooperativa.

Dentro del contexto de la cooperativa se listan a continuación algunas amenazas que pueden llegar a impactar los objetivos y que deberán ser tenidas en cuenta al momento del tratamiento del riesgo para cada proceso:

- Accidente laboral
- Atención a emergencias sanitarias en el menor tiempo posible
- Fenómenos meteorológicos extremos (incendios forestales)
- Interrupción del suministro de agua potable
- Disturbios civiles
- Enfermedad no profesional
- Interrupción de TI y telecomunicaciones
- Ataque cibernético
- Fallas en infraestructura crítica
- Desastres naturales
- Pandemias (por ejemplo Covid 19)

METODOLOGÍA

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información expone las actividades a desarrollar en el proceso de cumplimiento del plan, con el fin de mitigar los riesgos sobre los activos de información, en base a las recomendaciones de la guía para la administración del riesgo y el diseño de controles en entidades públicas V6 (2022)

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso del MSPI planteada desde el 2023, relacionadas con las cuatro fases del modelo de seguridad y privacidad de la información.

ETAPAS DEL MSPI	PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN
Planear	Establecer Contexto Valoración del Riesgo Planificación del Tratamiento del Riesgo Aceptación del Riesgo
Implementación	Implementación del Plan de Tratamiento del Riesgo
Gestionar	Monitoreo y Revisión continuo de los Riesgos
Mejora Continua	Mantener y mejorar el Proceso de Gestión del en la Riesgo Seguridad de la Información

Tabla 2. Resumen de las actividades de Gestión del Riesgo en la seguridad de la información

Fuente: MSPI

DESARROLLO METODOLÓGICO

Para llevar a cabo la realización del tratamiento de los riesgos de seguridad de la información en la cooperativa AAA. La bellezana se toma como base la metodología para la administración de riesgos propuesto en la “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas”.

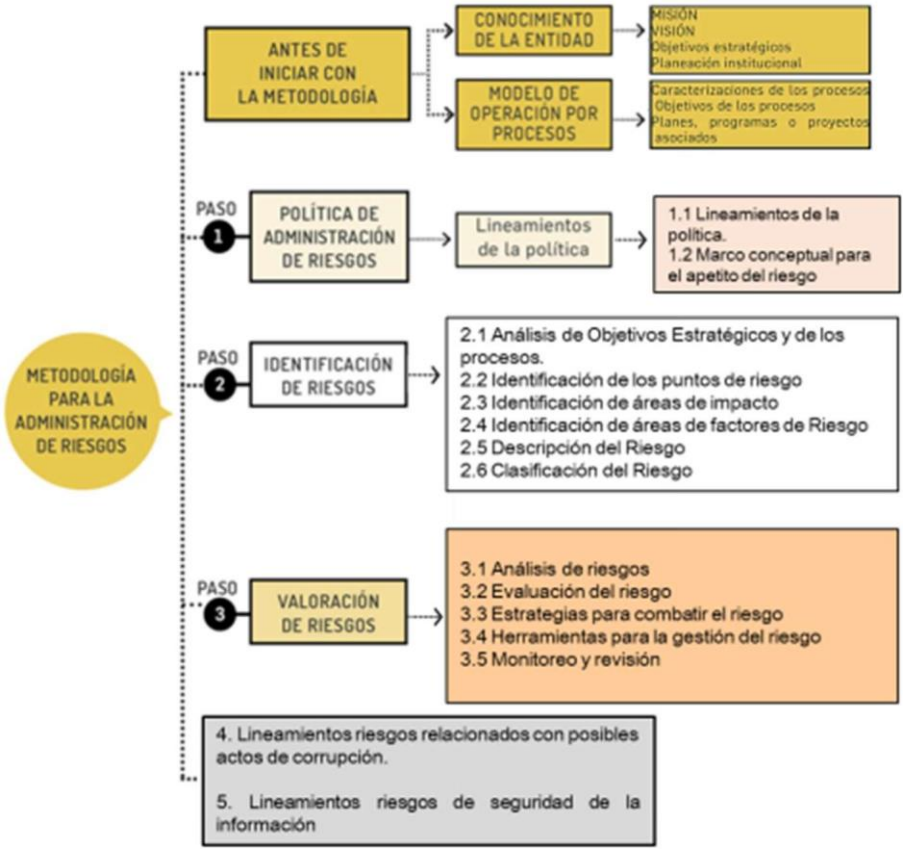

Imagen 1. Metodología para la administración del riesgo

Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.

PASO 1. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO – LINEAMIENTO DE LA POLÍTICA DE RIESGOS

La cooperativa La Bellezana, en base al modelo integrado de gestión del MinTic, se compromete a crear una cultura de la gestión del riesgo con el apoyo de la creación de los diferentes planes creados del sector TIC.

La política de administración del riesgo ofrece opciones para tratar y manejar los riesgos basados en un análisis para la toma de decisiones adecuadas, estimando los lineamientos para administración de los mismos.

- **Evitar:** después del análisis propuesto en donde se detecta las actividades que ocasionan riesgos se trabaja en la eliminación la exposición de la misma.
- **Prevenir:** Teniendo como base las revisiones periódicas de los mantenimientos preventivos se planean estrategias indicadas a que el evento de riesgo no ocurra.
- **Reducir o Mitigar:** hace referencia a la protección estimada en el plan de contingencia TIC, equipos de protección de los sistemas de información, copias de respaldo entre otros.
- **Dispersar:** es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en una misma área.

Los riesgos detectados deben ser analizados de tal forma que se pueda determinar cuál va a ser tu tratamiento.

INFORMACIÓN SOBRE LA EVALUACIÓN DE RIESGOS DE SEGURIDAD

La Administración Pública Cooperativa de Acueducto, Aseo y Alcantarillado, en el 2024 lleco a cabo el cargue de conjuntos de datos como activos de información de los diferentes procesos de la entidad, en plataforma de Datos Abiertos en estado público, lo cual se encuentra en constante implementación, adicional con el apoyo de las diferentes herramientas de resguardo de información de entidades que ejercen control sobre la

cooperativa se mantiene una constante actualización, tanto de documentos como de información procesada en la entidad de las diferentes áreas como lo son: el área contractual, activos de información, talento humano y contabilidad, con esta información recolectada se alimentan el SecopI y SecopII, Sia Observa Contraloría, SIGA, SUIT, SUI, SIGEP II y sitio web de la entidad.

Un punto importante al momento de levantar riesgos es que, adicional a los riesgos operativos, es importante tener en cuenta los riesgos de contratación, los riesgos de seguridad digital entre otros.

Como lo indica el Paso 2 de la "Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas" emitida por el DAFP, para efectos del presente modelo se podrán identificar los siguientes tres (3) riesgos inherentes de seguridad digital:

- Pérdida de la Confidencialidad
- Pérdida de la Integridad
- Pérdida de la Disponibilidad

PASO 2. IDENTIFICAR LOS RIESGOS INHERENTES DE SEGURIDAD DIGITAL

Siguiendo el anexo 4 "Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas" sección 4.1.7, para la identificación de los riesgos inherentes de seguridad digital de la coopertiva, se toma como base el siguiente listado de amenazas, que representan situaciones o fuentes que pueden hacer daño a los activos y materializar los riesgos.

Deliberadas (D),Extremo(E), Fortuito(F) o Ambientales(A).

Tipo	Amenaza	Origen
Daño Físico	Fuego	F,D,A
	Agua	F,D,A
Eventos Naturales	Fenómenos Climáticos	E

	Fenómenos Sísmicos	E
Pérdidas de los servicios prestados	Falla en el sistema de servicio del agua	E
	Falla en el mantenimiento de la bocatoma	E
Fallas técnicas	Fallas del equipo de cómputo	D, F
	Mal funcionamiento del equipo	D, F
	Saturación del sistema de información (SUI, Financiero o sitio web entre otros..)	D, F
	Mal funcionamiento del sistema(SUI, Financiero o sitio web entre otros..)	D, F
Acciones no autorizadas	Uso no autorizado del equipo de cómputo	D, F
	Copia fraudulente del software (Financiera)	D, F

Tabla 3. Tabla de amenazas comunes en la Cooperativa AAA. La Bellezana

Fuente: ISO/IEC 27005:2009(Anexo 4 Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas)

Amenazas dirigidas por el hombre: empleados con o sin intención, proveedores y piratas informáticos, entre otros.

Fuente de Amaneza	Motivación	Acciones Amenazantes
Pirata informático, Intruso ilegal	Reto	Piratería
	Ego	Ingeniería Social
Criminal de la Computación	Destrucción de la Información	Crimen por Computador
	Divulgación Ilegal de la Información	Acto Fraudulento
Terrorismo	Chantaje	Ataque contra el sistema (financiero)
	Destrucción	Penetración en el sistema

Tabla 4. Tabla de amenazas dirigida por el Hombre en la AAA. La Bellezana

Fuente: ISO/IEC 27005:2009 (Anexo 4 Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas)

Identificación de Vulnerabilidades

La Cooperativa puede identificar vulnerabilidades (debilidades) en las siguientes áreas:

Tipo	Vulnerabilidades
Hardware	Mantenimiento Insuficiente
	Susceptibilidad a las variaciones de temperatura (o al polvo y suciedad)
	Almacenamiento sin protección
	Falta de cuidado en la disposición final
	Copia no Controlada
Software	Ausencia de registros de auditoría
	Ausencia de documentación
	Ausencia de mecanismos de identificación y autenticación de usuarios
	Contraseña sin protección
Red	Ausencia de pruebas de envío o recepción de mensajes
	Líneas de comunicación sin protección
	Conexión deficiente de cableado
	Tráfico sensible sin protección
	Punto único de falla
Personal	Ausencia del personal
	Falta de conciencia en seguridad
	Trabajo no supervisado de personal externo (contratistas)
Lugar	Falta de controles de acceso a la oficina de la cooperativa
	Ausencia de protección en puertas o ventanas

Organización	Ausencia de control de los activos de la entidad
	Ausencia de la implementación de los mecanismos de monitoreo para brechas en la seguridad.

Tabla 5. Tabla de Vulnerabilidades comunes en la AAA. La Bellezana

Fuente ISO/IEC 27005 (Anexo 4 Lineamientos Para La Gestión De Riesgos De Seguridad Digital En Entidades Públicas)

PASO 3. VALORACIÓN DE RIESGOS

Riesgos de Seguridad Digital: Estos riesgos resultan de la combinación de amenazas y vulnerabilidades tales como:

- **Fuga o Pérdida de la Información:** ocasionando que la información llegue a personas no autorizadas.
- **Pérdida de la Confidencialidad:** Violación o incidente a la propiedad de la información que impide su divulgación a individuos, entidades o procesos no autorizados.
- **Pérdida de la Integridad:** Pérdida de la propiedad de mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizadas.
- **Pérdida de la Disponibilidad:** Perdida de la cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.
- **Riesgos de Privacidad:** Son aquellos riesgos que afectan a los usuarios catalogándose como violación de sus derechos en el riesgo del tratamiento inadecuado de datos personales.

Análisis De Riesgos

Se identifican las causas, vulnerabilidades, amenazas (identificación, descripción, tipo), consecuencias y se determina la clase de riesgo (probabilidad e impacto), todo esto asociado a aquellos eventos o situaciones que afecten los activos de la información que pueden entorpecer el normal desarrollo de los procesos.

A continuación, se muestra tabla con la información correspondientes a los controles de la entidad.

ADMINISTRACION PUBLICA COOPERATIVA ACUEDUCTO, ASEO, ALCANTARILLADO
LA BELLEZA NIT: 900. 348.296 -2

N Control	Descripción del control	Afectación		Atributos						Probabilidad Residual (2 Controles)	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							
1	El profesional encargado de la publicación de contratos en las plataformas online obligatorias por los diferentes entes de control, verifica que la información suministrada por el contratista corresponda a los requisitos establecidos de la contratación directa, a través de una lista de chequeo donde están los requisitos de información y la revisión con la información física y digital suministrada, los contratos que cumplen son registrados en las diferentes plataformas de contratación tales como: Secop II, Sigep II y Sia Observa Contraloría entre otras	x		Preventivo	Manual de contratación	40%	Documentado	Continua	Registro de Material	36%	Baja	25.2%	Mayor	80%	Alta	Reducir

ADMINISTRACION PUBLICA COOPERATIVA ACUEDUCTO, ASEO, ALCANTARILLADO
LA BELLEZA NIT: 900. 348.296 -2

N Control	Descripción del control	Afectación		Atributos						Probabilidad Residual (2 Controles)	Probabilidad Residual Final	%	Impacto Residual Final	%	Zona de Riesgo Final	Tratamiento
		Probabilidad	Impacto	Tipo	Implementación	Calificación	Documentación	Frecuencia	Evidencia							
2	El profesional encargado del control interno realiza la respectiva auditoría en el proceso de contratación, según programación de auditorías internas.	x		Detectivo	Manual de contratación	70%	Documentado	Continua	Con Registro	18%	Baja	42%	Mayor	80%	Alta	Reducir

3	El profesional encargado de los procesos de tic de la entidad realiza la constante revisión y actualización de planes e informes de TI, para la gestión de publicación en el portal web de la entidad. Teniendo en cuenta los periodos de cumplimiento ante los entes de control, basado en la información del índice de transparencia y acceso a la información pública.	x		Detectivo	Matriz ITA	85%	Documentado	Continua	Con Registro	12.6%	Baja	47.4%	Mayor	80%	Alta	Reducir
4	El profesional encargado del área de contabilidad realiza los registros presupuestales y de tesorería relacionados en las operaciones presupuestales de ingresos financieros de la empresa en el sistema, a su vez elabora informes de ejecución presupuestal, estados financieros y plan anual de adquisiciones, los cuales deben ser trasladados al área de TIC para poder gestionar la publicación en el sitio web de la entidad.	x		Detectivo	Manual de Funciones	50%	Documentado	Continua	Con Registro	30%	Baja	30%	Mayor	80%	Alta	Reducir

Tabla 6. Valoración del Riesgo – Bellezana 2024

ACTIVIDADES PARA EL DESARROLLO DEL PLAN DE GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	Actividad	**Responsable**	**Periodo Límite**
Actualización de Lineamiento de Riesgos	Entender y actualizar la política de Gestión de Riesgos.	Planeación	5 meses
	Actualización de inventario de activos de información	Contratista /Gerencia	11 meses
	Actualización del conjunto de datos abiertos publicados en datos abiertos.	Contratista TIC	11 meses
	Mínimo 2 Copias de Respaldo de Sitio web	Contratista Admon Sitio web	11 meses
Tratamiento de Riesgos de Seguridad y Privacidad de Información	Identificación, análisis y evaluación de riesgos de seguridad y privacidad de la información	Comité TI	8 meses
	Realimentación, Revisión y verificación de los riesgos identificados	Comité TI	8 meses
	Evaluación del nivel de impacto vs probabilidad y los controles existentes para calcular el nivel de riesgo.	Comité TI	8 meses
	Aprobación de riesgos identificados e inclusión en la matriz de riesgos de la empresa	Comité TI/Gerente	6 meses

Seguimiento	Seguimiento al tratamiento de riesgos	Comité TI	11 meses
Evaluación Riesgos	Calculo de riesgos basado en la eficacia de los controles existentes.	Comité TI	11 meses
Mejoramiento y control	Seguimiento a los controles de los riesgos de seguridad y privacidad de la información	Comité TI	11 meses

Tabla 7. Actividades para implementar en el Plan de Tratamiento de Seguridad y Privacidad de la Información en la Cooperativa AAA. La Bellezana.