AGUAS DE
BARRANCABERMEJA S.A. E.S.P.
Nit. 900.045.408-1

RESOLUCION N° 33

(31 ENE. 2020)

POR MEDIO DE LA CUAL SE ADOPTA EL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN PETI, PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LAS VIGENCIAS 2020-2023.

El Gerente de la Empresa AGUAS DE BARRANCABERMEJA S.A. E.S.P., en uso de sus atribuciones legales y estatutarias, especialmente las conferidas en el artículo 64 de los Estatutos de la empresa,

CONSIDERANDO:

a. De acuerdo con el Decreto 612 del 4 de abril de 2018, "...las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión (MIPG), al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos relacionados y publicarlos en su respectiva página web, a más tardar el 31 de enero de cada año (31 de julio en esta vigencia)".

b. Que el Decreto 1083 de 2015, modificado por el Decreto 1499 de 2017, creó el Consejo para la Gestión y el Desempeño Institucional integrado por las entidades y organismos que, por su misión, tienen a cargo funciones transversales de gestión y desempeño a nivel nacional y territorial, instancia a la cual le corresponde, entre otras funciones, proponer políticas, normas. herramientas, métodos y procedimientos en materia de gestión y desempeño institucional, presentar al Gobierno Nacional recomendaciones para la adopción de políticas. estrategias o acciones para mejorar la gestión y el desempeño institucional de las entidades y organismos del Estado y proponer estrategias para la debida operación del Modelo Integrado de Planeación y Gestión – MIPG

c. Que el Decreto 1078 de 2015 "Por medio de la cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones" establece entre otros, los lineamientos generales de la estrategia de gobierno en línea, define los lineamientos, plazos y términos para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un estado más eficiente, más transparente y participativo y que preste.

d. Que la Ley 1712 de 2014, Ley de Transparencia y del Acceso a la información Publica tiene por objeto regular el derecho de acceso a la Información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y constituye el marco general de la protección del ejercicio del derecho de acceso a la información pública en Colombia.

e. Que la Ley 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales reglamentado por el Decreto 1377 de 2013, incorporó los lineamientos necesarios para que los organismos públicos y privados identificaran los roles y la tipología de datos que son objeto de protección constitucional, así mismo, dispuso las condiciones las cuales se deben recolectar los datos personales que posteriormente serán vinculados con la administración de una base de datos.

f. Que conforme a la normatividad citada surge la necesidad de adoptar lineamientos institucionales de seguridad y privacidad de la información considerando el papel estratégico de las tecnologías de información y comunicaciones -TIC; además de la importancia de mitigar riesgos alrededor de la información mediante la implementación de planes para el manejo de incidentes, así como las herramientas para respaldar las Actividades.

g. Que a través del acta No. 003 del Comité Institucional de Gestión y Desempeño del 28 de Enero de 2020, se socializaron el Plan PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información y Plan de Seguridad y Privacidad de la Información vigencia 2020-2023 y se aprobó su presentación ante el Comité Institucional de Coordinación de Control Interno.

h. Que a través del Acta No 01 del 30 de enero de 2019, el Comité Institucional de Coordinación de Control Interno, aprobó el Plan PETI, Tratamiento de Riesgos de Seguridad y Privacidad de la información y Seguridad y Privacidad de la Información vigencia 2020-2023.

i. Que de conformidad con el Decreto 612 de 2018 del Departamento Administrativo de la Función Pública DAFP, se Integran el Plan PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información y Plan de Seguridad y Privacidad de la Información al Plan de Acción Institucional Integrado vigencia 2020.

En mérito de lo expuesto;

RESUELVE:

ARTÍCULO PRIMERO: Adoptar el Plan Estratégico de Tecnologías de la Información y Comunicación PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Plan de Seguridad y Privacidad de la Información para la vigencia 2020-2023.

ARTÍCULO SEGUNDO: Ordenar a partir de la firma de la presente Resolución la implementación del Plan Estratégico de Tecnologías de la Información y Comunicación PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Plan de Seguridad y Privacidad de la Información para las vigencias 2020-2023, para que se desarrolle en la Empresa Aguas de Barrancabermeja SA ESP.

ARTICULO TERCERO: Publicar a través del Profesional III Adscrito a la Subgerencia Administrativa y Financiera, el Plan Estratégico de Tecnologías de la Información y Comunicación PETI, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, Plan de Seguridad y Privacidad de la Información vigencia 2020-2023.

ARTÍCULO CUARTO: La presente resolución rige a partir de la fecha de su expedición.

COMUNIQUESE Y CUMPLASE

Dado en Barrancabermeja, a los 31 ENE. 2020

ALFREDO GARCES ECHEVERRY
Gerente

	NOMBRE DEL FUNCIONARIO	FECHA	FIRMA
Proyectó	Rafael Andres Lastre Gomez	30-01-2020	
Revisó	Carlos Vasquez	30-01-2020	
Aprobó	Alfredo Garces Echeverry	30-01-2020	
Nota. Los firmantes declaramos que hemos suscrito el presente documento y lo encontramos ajustado a las normas y disposiciones legales vigentes dentro de cada una de nuestras competencias y , por lo tanto lo presentamos para la firma			

PLAN ESTRATEGICO EN TECNOLOGIAS DE LA INFORMACION Y LA COMUNICACIÓN PETI

AGUAS DE BARRANCABERMEJA S.A. E.S.P.

2020-2023

	ELABORADO POR	REVISADO POR	APROBADO POR
Firma			
Cargo	Profesional III Adscrito a la Subgerencia Administrativa y Financiera	Presidente Comité Institucional de Gestión y Desempeño	Presidente Comité Institucional de Coordinación de Control Interno
Nombre	Rafael Andres Lastre Gomez	Carlos Arturo Vasquez	Alfredo Garces Echeverry
Fecha	Enero 2020	Acta No. 3 del 2020 del CIGyD	Acta No 1 de 2020 del CICCI

CONTROL DE CAMBIOS		
VERSION	FECHA DE APROBACION	DESCRIPCION DEL CAMBIO
1	Acta No 1 de 2020 del CICCI	Creación, Aprobación de Documento.

TABLA DE CONTENIDO

1. Objetivo 4
1.1 Objetivo general 4
1.2 Objetivos específicos 4
2. Alcances 4
3. Marco de referencia 4
4. Antecedentes 5
5. Metodología 6
6. Análisis de situación actual 8
6.1 Detalle técnico de la situación actual hardware 8
6.2 Detalle técnico de la situación actual software 9
7. Servicios de tecnología 10
8. Estructura TI aguas de Barrancabermeja 13
9. Rupturas estratégicas 14
10. Estructura de actividades estratégicas 15
11. Plan de comunicaciones 16

INTRODUCCIÓN

Para las organizaciones que quieren mantenerse altamente competitivas, el acelerado crecimiento y la demanda de servicios, les exigen integrarse a través de nuevas tecnologías de información y comunicación.

El proceso de cambio y selección de productos de software y hardware con calidad es muy importante para las instituciones.

La información se constituye en el mayor activo, por esto la necesidad de proteger la confidencialidad, la integridad y disponibilidad de la información para tener una mayor oportunidad de la información y de que todos los componentes actúen a favor de la empresa.

1. OBJETIVOS

1.1 OBJETIVOS GENERAL

Realizar en la Empresa Aguas de Barrancabermeja S.A E.S.P. una actualización y optimización de los procesos institucionales apoyados en una mejor infraestructura informática que vaya más acorde con los cambios que ha venido presentando la institución y que le permita tener alta disponibilidad sobre la información, de manera eficaz y oportuna.

1.2 OBJETIVOS ESPECIFICOS

- Describir la situación actual tanto del sistema informáticos como de la plataforma de equipos de cómputo y de comunicaciones
- Emitir un concepto acerca del estado de la infraestructura tecnológica y de las acciones que hay que llevar a cabo para evolucionar hacia un mejor desempeño institucional
- Recomendar un plan de trabajo que permita obtener una plataforma informática eficiente y adecuada para apoyar a la institución en el logro de sus objetivos primarios de funcionamiento

2. ALCANCES

El plan estratégico de tecnologías de la Información PETI describe las estrategias que ejecutará la Empresa Aguas de Barrancabermeja S.A E.S.P., durante los años 2020-2023 en materia de tecnologías de información y comunicaciones (TICS), con el fin de concretar el logro de objetivos misionales de la entidad, Plan institucional y Plan de Desarrollo Municipal de Barrancabermeja.

3. MARCO DE REFERENCIA

El PETI de la empresa Aguas de Barrancabermeja SA ESP esta alineado con las siguientes normas y recomendaciones

Identificador	Nombre	Numero o año	Descripción	Capacidades o servicios impactados.
1	Servicios Públicos Domiciliarios	Ley 142 1994	Lineamiento para la prestación de los servicios públicos domiciliarios	Información
2	Plan de Desarrollo Municipal	2020-2023	Alineación estratégica con el Plan de Desarrollo Municipal de Barrancabermeja	
3	Política de Gobierno Digital	Decreto 1008 de 2018	Define los componentes de la política de Gobierno Digital	TIC Estado TIC para Sociedad
4	Servicios Ciudadanos Digitales	Decreto 1413 de 2017	Define los componentes de la política de Servicio Ciudadanos	Servicio al Ciudadano

4. Antecedentes

La empresa Aguas de Barrancabermeja SA ESP consideró necesario realizar un proceso de actualización del PETI, debido al gran esfuerzo realizado durante el año 2017-2020 en Pro del cumplimiento de los lineamientos de Gobierno Digital, así como los ejercicios previos realizados tales como proyectos y actividades de fortalecimiento de capacidades institucionales de Tics, esto contribuyó a identificar una nueva problemática la cual explicamos a continuación:

Dominio	Problemática Identificada
Estrategia	Falta de Alineación con los objetivos institucionales de la entidad.
Gobierno	Ausencia de Metodología de proyecto e inversión en Compras de TI
Información	Ausencia de la Arquitectura de Información de alto Nivel Política de Documentos Electrónicos. No se cuenta con un lenguaje común de Intercambio de Componentes de Información

Sistemas de Información	No se identifica Planes, procedimientos y políticas para garantizar la continuidad de los servicios tecnológicos. No se cuenta con una documentación del mecanismo implementado para la garantizar la disponibilidad de los servicios tecnológicos.
Servicios Tecnológicos	No se evidencio Diagramas arquitectónicos que representen los elementos de infraestructura involucrados en el intercambio de información al interior de la entidad y con sistemas externos.
Uso y Apropiación	Falto socialización del Plan Estratégico de Tecnologías de Información alineados con la política de seguridad digital

5. Metodología

La actualización del PETI de la empresa Aguas de Barrancabermeja SA ESP se basó en la metodología y lineamientos e instrumentos desarrollados por el Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC, que componen la Estrategia de Gobierno Digital, la cual está soportada en la construcción de la Arquitectura Empresarial TI del Estado y en el modelo de gestión estratégica con TI (IT4+) así como también en el Modelo de Seguridad y Privacidad de la Información.

El Plan Estratégico de la Empresa Aguas de Barrancabermeja S.A E.S.P. ha sido elaborado con la intensión de definir e implementar un conjunto de estrategias que sirvan como una plataforma sobre la que se pueda organizar la actividad de sistemas de información y tecnologías de la institución para el periodo comprendido entre los años 2020-2023. En este contexto el desarrollo del proyecto del Plan ha respondido a las pautas definidas por metodologías y directrices de entidades reguladoras.

Los lineamientos de entes reguladores como la contraloría general hacen necesario focalizar el Plan Estratégico hacia el desarrollo, implementación y consolidación de Sistema de Información y Tecnologías.

Por esta razón las principales políticas fueron definidas teniendo en cuenta principios básicos como:

a. Importancia estratégica de información en todos los niveles de la organización.
b. La tecnología Informática y de comunicaciones es un instrumento de Servicio a la comunidad y a la ciudadanía.
c. La tecnología informática y de comunicaciones es un pilar de la modernización y optimización de procesos y funciones.
d. La integración e interacción de información entre las entidades del gobierno es esencial en el desarrollo de servicios para la ciudadanía.

Estos principios son tomados en consideración para el desarrollo estratégico del Plan Estratégico. Principios como los mencionados anteriormente tienen un complemento con la aplicación, evaluación y diagnóstico de los Sistemas de Información y Tecnologías identificados mediante la aplicación de la metodología TICS.

La metodología TICS y su interacción con el Plan estratégico se enmarca dentro de los siguientes lineamientos:

- **Estrategia TI**: Este dominio tiene el fin de apoyar el proceso de diseño, implementación y evolución de la Arquitectura TI en las instituciones, para lograr que esté alineada con las estrategias organizacionales y sectoriales.
- **Gobierno TI**: Este dominio brinda directrices para implementar esquemas de gobernabilidad de TI y para adoptar las políticas que permitan alinear los procesos y planes de la institución con los del sector.
- **Información**: Este dominio permite definir el diseño de los servicios de información, la gestión del ciclo de vida del dato, el análisis de información y el desarrollo de capacidades para el uso estratégico de la misma.
- **Sistemas de Información**: Este dominio permite planear, diseñar la arquitectura, el ciclo de vida, las aplicaciones, los soportes y la gestión de los sistemas que facilitan y habilitan las dinámicas en una institución.
- **Servicios Tecnológicos**: Este dominio permite gestionar con mayor eficacia y transparencia la infraestructura tecnológica que soporta los sistemas y servicios de información en las instituciones.
- **Uso y Apropiación**: Este dominio permite definir la estrategia y prácticas concretas que apoyan la adopción del Marco y la gestión TI que requiere la institución para implementar la Arquitectura TI.

Fuente: MINTIC

De acuerdo con los dominios la empresa tendría la siguiente relación:

Dominio de Estrategia de TI

1. Plan Estratégico de Tecnologías de la Información (PETI)
2. Indicadores: medir para aprender y mejorar

Dominio de Gobierno de TI

3. CIO: Líder estratégico de TI
4. Contratar servicios antes de comprar infraestructura
5. Políticas de seguridad con un enfoque de gestión integral del riesgo

Dominio de Información

6. Información pública como derecho
7. La información debe ser un producto y servicio de calidad
8. Trazabilidad y auditoría

Dominio de Sistemas de Información

9. Sistemas nacidos para integrarse e interoperar

Dominio de Servicios Tecnológicos

10. Pactar acuerdos de niveles de servicio
11. Pago por consumo

Dominio de Uso y Apropiación

12. Estrategia de comunicación
13. Procesos de gestión del cambio

6. ANÁLISIS DE LA SITUACIÓN ACTUAL

Todo proceso comienza con un análisis de la situación actual, que genera una visión del modelo de gestión de TI existente, su propósito es entender apropiadamente la visión, prioridades, sus problemas, rupturas estratégicas y madurez tecnológica.

6.1 Detalle técnico de la situación actual hardware

Equipos de cómputos activos:

La empresa aguas de Barrancabermeja cuenta con 85 números de equipos de cómputo, servidores tipo Blade y rack de comunicación con más de 100 puntos de red y circuito cerrado de televisión.

Equipo de Cómputo por funcionarios:
Cada funcionario dispone de un equipo de cómputo portátil o de escritorio conectado al dominio de la empresa, una impresora local o en red y scanner de alta velocidad para sus labores de digitalización.

Equipos de Impresión Activos:
Las impresoras se encuentras activas y configuradas por área de trabajo y conectadas a la red (dominio) de la empresa, algunas de ellas por la necesidad del servicio fueron instaladas de manera local y el tóner es suministrado por el área de inventarios.

Tipo de Red Utilizada:
El tipo de red utilizada en la red de área local se implementó con cableado estructurado de categoría 6 y 6ª de la marca Ortronics debidamente certificados utiliza uno swtiches marca HP de 48 puertos conectados en pila mediante fibra óptica.

Equipos de Redes de Interconexión de Datos:
Se cuenta con un firewall marca Sonic Wall de referencia TZ500 para el control y filtrado de paquetes, dos router en modalidad de alquiler para la interconexión de las sedes de la empresa.

Equipos de Respaldos UPS:

Contamos con una UPS de 3KVA y un banco de baterías para soportar una interrupción de energía de hasta 5 horas, se encuentra conectada con los servidores y el rack de comunicaciones, y los equipos activos de la empresa.

6.2 Detalle Técnico de la Situación Actual Software

Licencias de Sistema Operativo:
Todos los equipos de cómputo se encuentran debidamente licenciados bajo el tipo de licencia OEM suministrada con el equipo bajo la modalidad de arrendamiento.

Licencias de Herramientas Ofimática
Se cuenta con el paquete ofimático de Office profesional en sus versiones 2007, 2010 y 2013 y Office 365 respectivamente como fueron siendo adquiridos.

Software de Gestión Administrativa

En la gestión administrativa se cuenta con un sistema de información integral compuesto por los siguientes módulos:

- Módulo de Contabilidad, Financiero y Presupuesto
- Módulo de Activos fijos y almacén
- Módulo de Nomina
- Sistemas de Información Comercial
- Sistema de Gestión Documental Mercurio
- Módulo de recuperación de consumo
- Módulo de recaudo en línea.
- Infomante Sistema de Programación de mantenimientos.

Desarrollo de Soporte y Mantenimiento

El desarrollo y soporte está contratado con una firma llamada Microshif que es la encargada del soporte, actualización y mantenimientos de los sistemas de la empresa.

7. Servicios de tecnología

La empresa Aguas de Barrancabermeja cuenta con los siguientes servicios de tecnología:

Conectividad WIFI

La empresa Aguas de Barrancabermeja SA ESP cuenta actualmente con una red inalámbrica que opera una velocidad máxima de 750 Mbps, basada en el estándar 802,11 a/b/g/n, que complementa a la red de datos cableada y que le permite acceder al servicio de internet a todos los funcionarios que requieran el servicio desde la planta de tratamiento y la oficina de atención al usuario.

Instalación y Configuración de Access Point

Esta actividad consiste en la instalación y configuración de dispositivos inalámbricos para cubrir las áreas como oficinas, auditorio para complementar la red cableada de la empresa.

Servicios de Red

La empresa Aguas de Barrancabermeja SA ESP a través de la red de datos presta el servicio de red compuesto por:

Infraestructura de conexión

a. Adquisición de equipos activos de la red de datos
b. Renovación de equipos activos de la red de datos
c. Mantenimiento y soporte de equipos activos de la red de datos

Asignación de usuarios de red

Se asigna un usuario en la red, de acuerdo con lo estandarizado según las políticas, normas, y estándares de seguridad informática de la empresa Aguas de Barrancabermeja.

Instalación de puntos de red

Este servicio consiste en el proceso de instalación física de los mecanismos de infraestructura necesarios para proveer a un equipo de cómputo acceso a la red.

Activación de puntos de red

Conexión de un físico de acceso a la red con los elementos activos de la red que posibilitan su uso.

Mantenimiento y Gestión de los puntos de acceso a la red

El Área de Sistemas tiene a su cargo el monitoreo permanente y el soporte para la resolución de fallas que afecten el acceso a la red de datos de Aguas de Barrancabermeja SA ESP por parte de sus usuarios.

Gestión de Direccionamiento IP

El Área de Sistemas es el encargado de mantener en funcionamiento la continua prestación del servicio de asignación de automática de direccionamiento IPv4 a todos los equipos de cómputo de la Red de Datos de la empresa.

Instalación y Configuración de Software de Red

Consiste en la instalación y configuración de la interfaz de red del equipo de computo del usuario, así como los programas de aplicaciones y comunicaciones básicas, tales como navegadores web (iexplore ,Mozilla, Chrome)

Gestión de DNS
El área de Sistemas es el encargado de mantener en funcionamiento la continua inclusión de los sistemas de información dentro de los DNS locales y externos.

Asistencia técnica y soporte a usuarios con problemas específicos de red de datos.
Gestión de Sistemas de Seguridad Centralizados.

a. Firewall
b. Detección de Intrusos
c. Monitoreo de Red

Mantenimiento Correctivos y Preventivos de Software

Este servicio es programado dos veces al año por el área de sistemas para todos los equipos de cómputo de la Planta de tratamiento y la Oficina de atención al Usuario.
Los mantenimientos correctivos son atendidos y reportados en el formato de requerimientos de soportes de usuarios.

Soporte a Usuarios

Escalamiento del soporte técnico de los equipos de cómputo y periféricos.
Este escalamiento se realiza a los equipos de cómputo y periféricos que tiene vigencia de garantía o depende de una asistencia técnica de un tercero, este escalamiento consiste en efectuar la respectiva articulación directa con el proveedor pertinente, que realiza el servicio técnico.

Revisión y Limpieza de virus a los equipos de cómputo.
Esta asistencia se efectúa a los usuarios que reportan problemas de anomalías con sus aplicaciones tecnológicas instaladas en los equipos de cómputo pertinentes a la empresa Aguas de Barrancabermeja SA ESP.

Instalación y configuración de Impresoras, scanner.
Este servicio se realiza a las dependencias o usuarios que solicitan instalación y configuración de periféricos pertenecientes a la Empresa Aguas de Barrancabermeja SA ESP.

Acompañamiento en el respaldo de la información.
Esta asistencia se realiza a las oficinas o usuarios que solicitan la creación de Backup de la información institucional que esta almacenada en el disco del equipo de computo, este

servicio consiste en facilitarle los medios de almacenamiento al usuario para que pueda realizar su copia de seguridad en la red.

Instalación de Aplicaciones Licenciadas.

Servicio de Actualizaciones
Servicio de Instalación y mantenimiento de Software

Tipos de soporte a usuarios

Soporte a usuario en sitio

Desplazamiento del personal capacitado a la locación física del problema

Soporte a Usuario Remoto

Por medio de instrucciones y herramientas de acceso remoto se le indica al usuario como proceder para resolver un incidente menor.

Los horarios de atención de Lunes a viernes 07:00 am – 12:00 y de 02:00 pm a 06:00 pm sujetos a modificaciones de horarios por parte de la empresa.

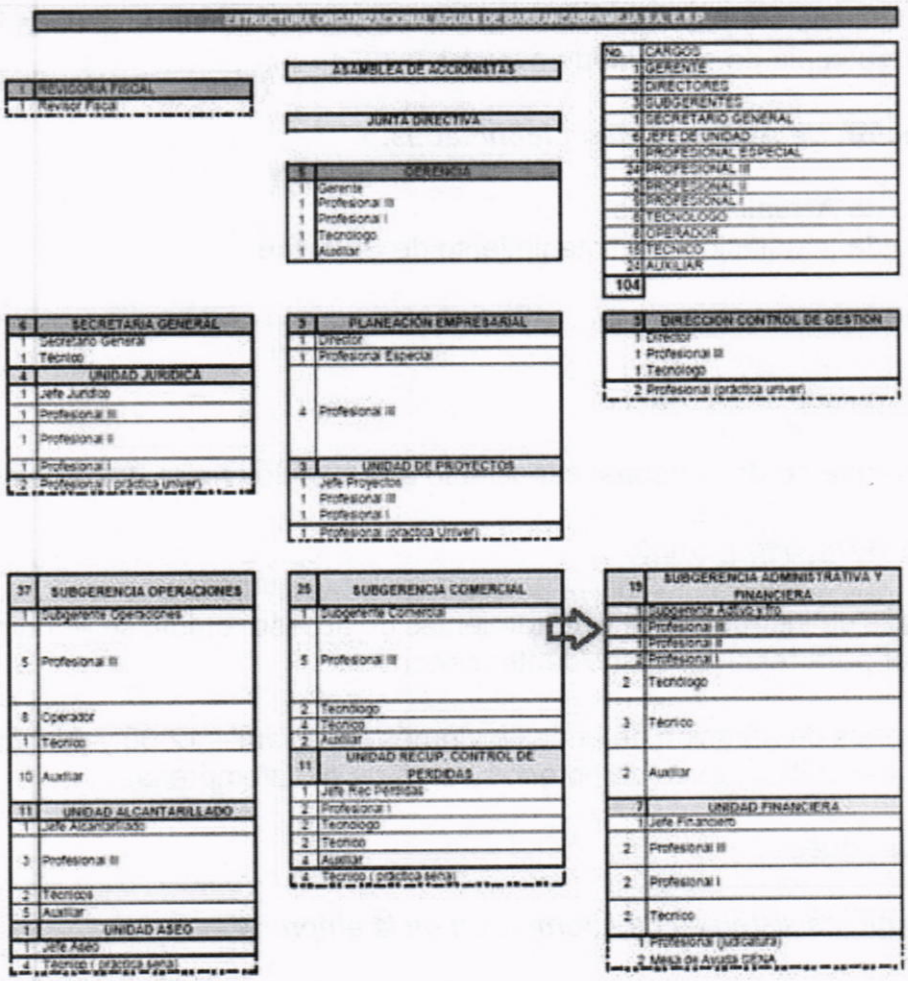
Capacitaciones

Manejo de los sistemas de información de la empresa

Estas capacitaciones se realizan de acuerdo con las necesidades de capacitación para el personal nuevo y/o refuerzo.

8. Estructura TI Aguas de Barrancabermeja

La Empresa Aguas de Barrancabermeja SA ESP tiene definida la siguiente estructura organizacional de la siguiente manera



9. RUPTURAS ESTRATÉGICAS

En la empresa Aguas de Barrancabermeja SA ESP con el objeto de fomentar el cambio de paradigmas y de adoptar pensamientos que permitan llevar a cabo la transformación de la gestión de TI, identifica las siguientes rupturas estratégicas.

- Los sistemas de información requieren ser integrales e interoperables
- La disponibilidad de la información para el desarrollo e implementación de soluciones al ciudadano, deben ser más oportunas, confiables y con mayor detalle.
- La tecnología debe ser considerada un factor de valor estratégico para la empresa.

- Fortalecer el equipo humano de la empresa en el desarrollo de las capacidades de uso y apropiación de TIC.

10. ESTRUCTURA DE ACTIVIDADES ESTRATÉGICAS

Definición de la Hoja de Ruta

En la hoja de ruta se analizó el modelo de gobierno de TI, las necesidades de Información, así como la alineación de los procesos de TI. Se definen los lineamientos y actividades estratégicas, para los próximos 4 años.

Proyecto e Iniciativa	Dominio AE	Producto	Actividad	Fuente	Tipo	Ejecución
Mejoramiento de la infraestructura tecnológica	Servicios Tecnológicos	Mejoramiento de la Infraestructura tecnológica para la prestación de servicios tecnológicos	Adquisición de equipos tecnológicos para el mejoramiento de la prestación de los servicios tecnológicos	Recursos Propios	Actualización	2020-2021
Tramites y Servicios al Ciudadano	Sistemas de Información	Racionalización de tramites	Implementación de servicios y/o tramite en línea para la ciudadanía	Propios	Nuevo	2020-2021
Servicios de almacenamiento en la Nube	Información	Custodia y respaldo de la información de la empresa	Adquisición de Servicios de Almacenamiento en la Nube	Propios	Nuevo	2021-2022
Gestión de Documentos y Expedientes Electrónicos	Sistemas de Información	Mejoramiento en el sistema de gestión documental	Actualización de Software y procedimientos para la implementación de documentos y expedientes electrónicos	Propios	Actualización	2020-2022
Canales de Atención al Ciudadano	Sistemas de Información	Mejoramiento en los canales de atención al ciudadano	Integración de los canales de PQRSD de la empresa	Propios	Actualización	2022-2023
Canales de Recaudo	Estrategia y Gobierno	Aumento en los canales de recaudos para los usuarios	Habilitación de canales de recaudo en línea.	Propios	Nuevo	2020-2021

11. Plan de Comunicaciones

Una vez aprobado el PETI por parte del comité Institucional de gestión y desempeño responsable de orientar la instrumentación del modelo integrado de planeación y gestión se procederá a socializar el plan con todos los funcionarios de la entidad. Se busca el PETI sea la herramienta para dirigir la gestión TI de la entidad y con su aplicación se aplique la Política de Gobierno Digital para favorecer a la entidad y a la comunidad, que son los dos componentes de la Política.
Se hará difusión del Plan Estratégico de Tecnología de la información PETI a través de página web institucional.

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

AGUAS DE BARRANCABERMEJA S.A. E.S.P.

2020-2023

	ELABORADO POR	REVISADO POR	APROBADO POR
Firma			
Cargo	Profesional III Adscrito a la Subgerencia Administrativa y Financiera	Presidente Comité Institucional de Gestión y Desempeño	Presidente Comité Institucional de Coordinación de Control Interno
Nombre	Rafael Andres Lastre Gomez	Carlos Arturo Vasquez	Alfredo Garces Echeverry
Fecha	Enero 2020	Acta No. 3 del 2020 del CIGyD	Acta No 1 de 2020 del CICCI

CONTROL DE CAMBIOS		
VERSION	FECHA DE APROBACION	DESCRIPCION DEL CAMBIO
1	Acta No 1 de 2020 del CICCI	Creación, Aprobación de Documento.

TABLA DE CONTENIDO

1. OBJETIVOS 4
2. ALCANCE 4
3. NIVEL DE CUMPLIMIENTO 4
4. IMPLEMENTACION DE POLITICAS DE SEGURIDAD DE LA INFORMACION 5
4.1 ROLES Y RESPONSABILIDADES 7
4.2 CUMPLIMIENTO 8
4.3 COMUNICACIÓN 8
4.4 MONITOREO 8
5. DESCRIPCION DE LOS LINEAMIENTOS 8
5.1 GENERALIDADES 8
5.2 DERECHOS MORALES Y PATRIMONIALES 9
5.3 DIVULGACION DE LA INFORMACION 9
5.4 INFORMACION CONFIDENCIAL 9
5.5 RECURSOS INFORMATICOS 10
5.6 ADMINISTRACION Y CONTROL 10
5.7 WEB SITE E INTRANET 10
5.8 DERECHOS DE AUTOR LICENCIAS DE SOFTWARE 10
5.9 CORREO ELECTRONICO 11
5.10 GESTION DOCUMENTAL 11
5.11 COMPUTADORES, SERVIDORES Y REDES 11
5.12 CUENTAS DE LOS USUARIOS 12
5.13 IDENTIFICACION, CONTRASEÑAS Y AUTORIZACION 12
5.14 SEGURIDAD FISICA Y DEL ENTORNO 12
6. CUMPLIMIENTO DE IMPLEMENTACION 13
7. MONITOREO Y REVISION 14

INTRODUCCIÓN

Los lineamientos de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Empresa Aguas de Barrancabermeja SA ESP con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan el Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus lineamientos, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Aguas de Barrancabermeja SA ESP, para asegurar el direccionamiento estratégico de la Entidad, establece la compatibilidad de lineamientos y objetivos de seguridad de la información, estos últimos correspondientes a:

a) Mitigar los riesgos de la entidad.
b) Cumplir con los principios de seguridad de la información.
c) Cumplir con los principios de la función administrativa.
d) Mantener la confianza de los funcionarios, contratistas y terceros.
e) Apoyar la innovación tecnológica.
f) Implementar el sistema de gestión de seguridad de la información.
g) Proteger los activos de información.
h) Establecer las políticas, procedimientos e instructivos en materia de
i) seguridad de la información.
j) Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos de Aguas de Barrancabermeja SA ESP
k) Garantizar la continuidad del servicio frente a incidentes.

1. OBJETIVOS

Definir los mecanismos y todas las medidas necesarias por parte de la Empresa Aguas de Barrancabermeja SA ESP, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2. ALCANCE

Este Plan de Seguridad y Privacidad de la Información y sus lineamientos, son aplicables a todos los funcionarios de Aguas de Barrancabermeja SA ESP, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

3. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a este Plan.
A continuación se establecen los lineamientos que soportan el plan de seguridad y privacidad de la información de Aguas de Barrancabermeja SA ESP.

a) La Empresa Aguas de Barrancabermeja SA ESP ha decidido definir, implementar, operar y mejorar de forma continua la Gestión de Seguridad de la Información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.
c) La Empresa Aguas de Barrancabermeja SA ESP protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.

d) La Empresa Aguas de Barrancabermeja SA ESP protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, 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.
e) Aguas de Barrancabermeja SA ESP protege su información de las amenazas originadas por parte del personal.
f) Aguas de Barrancabermeja SA ESP protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
g) Aguas de Barrancabermeja SA ESP controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
h) Aguas de Barrancabermeja SA ESP implementa controles de acceso a la información, sistemas y recursos de red.
i) Aguas de Barrancabermeja SA ESP garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
j) Aguas de Barrancabermeja SA ESP garantiza a través 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.
k) Aguas de Barrancabermeja SA ESP garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.
l) Aguas de Barrancabermeja garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
El incumplimiento a los lineamientos 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.

4. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Justificación

La Empresa Aguas de Barrancabermeja SA ESP con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos

y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la misma, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

a) Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

b) Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

c) Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

a) Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

b) Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

c) No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

d) Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

e) Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

A los efectos de una correcta interpretación del presente Plan, se realizan las siguientes definiciones:

a) Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

b) Sistema de Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

c) Tecnología de la Información: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

4.1 ROLES Y RESPONSABILIDADES

El plan establece la conformación del Comité de Seguridad de la Información de Aguas de Barrancabermeja SA ESP, que se encuentra adherido al comité de gestión y desempeño. La implementación, aplicación, seguimiento y autorizaciones de los lineamientos del Plan de Seguridad y Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de las directrices de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.

Comité de Seguridad de la Información. El comité está encargado de recomendar la formulación y actualización periódica de las políticas relativas a los recursos informáticos y a la seguridad de la información. La Gerencia, Subgerentes y Profesional de recursos informáticos de la Empresa. Es responsable de clasificar y proteger la información utilizada por ellos; cuando ocurra un incidente grave que refleje alguna debilidad, deberán tomar las acciones para reducir los riesgos.

Control de Gestión. Debe velar por el cumplimiento de las políticas, normas y procedimientos de seguridad de la información en la Empresa. Igualmente, advertir acerca de las vulnerabilidades detectadas.

Profesional III Adscrito a la Subgerencia Administrativa y Financiera. Responsable de implantar las políticas, normas y procedimientos de seguridad en la empresa; evaluar, proponer la adquisición e implantar productos de seguridad informática; acordar el análisis de riesgos, planes de contingencia y realizar las demás actividades necesarias para garantizar un ambiente informático seguro.

El Administrador del sistema. Es responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y llevar a cabo las tareas de seguridad relativas a los sistemas que administra.

Usuario. Todo servidor público o persona que asuma funciones públicas, es responsable de cumplir con todas las políticas informáticas y de seguridad de la Empresa.

4.2 CUMPLIMIENTO

El cumplimiento de los lineamientos de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, Aguas de Barrancabermeja SA ESP se reserva el derecho de tomar las medidas correspondientes.

4.3 COMUNICACIÓN

Mediante socialización a todos los funcionarios de la Empresa Aguas de Barrancabermeja SA ESP se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de los lineamientos, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.aguasdebarrancabermeja.gov.co.

4.4 MONITOREO

Se crearán los mecanismos y los indicadores correspondientes a los lineamientos de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

5. DESCRIPCIÓN DE LOS LINEAMIENTOS

5.1 GENERALIDADES

La Empresa Aguas de Barrancabermeja SA ESP en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importantante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son integridad, disponibilidad y confidencialidad de la información.

De acuerdo a estos lineamientos se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece los lineamientos de riesgos institucional.

Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los

objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad. Los lineamiento se detallan a continuación:

5.2 DERECHOS MORALES Y PATRIMONIALES

Los usuarios son responsables de la custodia y la confidencialidad de los datos y la información a la cual tengan acceso en forma directa e indirecta.
La empresa es propietaria de todos los datos e información que circule o se genere al interior de la misma o que esté disponible a través de sus sistemas de información y/o computadores.
En este sentido, el Gerente y Servidores públicos de nivel directivo clasificaran los datos y la información generados o utilizados por su Subgerencia solicitando a sus colaboradores y contratistas seguir los procedimientos establecidos por la Subgerencia Administrativa y Financiera para el resguardo de los mismos a través de copias de seguridad (Backup).

5.3 DIVULGACION DE LA INFORMACION

La información entregada a los medios de comunicación debe hacerse a través del funcionario encargado del manejo de la comunicación empresarial.
La empresa no se hace responsable por las consecuencias que se deriven de la utilización inadecuada por parte de terceros. Igualmente, se abstiene de suministrar la información que haya recibido de terceros para su uso interno y confidencial.

5.4 INFORMACIÓN CONFIDENCIAL

Exigir a los usuarios la protección de la información clasificada como confidencial o de uso restringido.
Incluir una cláusula de confidencialidad en los contratos u órdenes, cuando el contratista requiera acceder de manera directa o indirecta a los datos o información de la Empresa.
Todo empleado que participe en proyectos de la Empresa, o tenga acceso a su información, debe guardar confidencialidad sobre la misma. El responsable del proyecto debe solicitar a los participantes, como parte de los términos, compromiso y condiciones iniciales de su participación, que firmen un acuerdo de confidencialidad de la información.

5.5 RECURSOS INFORMÁTICOS

Establecer el cambio periódico de los recursos informáticos, dependiendo de la obsolescencia, la vida útil, el estado de los mismos y las necesidades de la Empresa.
Se dará de baja a los equipos teniendo en cuenta el procedimiento establecido para tal fin.
Exigir a los usuarios la utilización responsable y razonable de los recursos informáticos. Igualmente, el acatamiento de las medidas de control establecidas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde con la importancia de los datos y la naturaleza de los riesgos.

5.6 ADMINISTRACIÓN Y CONTROL

La conexión a la red debe ser autorizada por el Profesional de Recursos Informáticos con las directrices emitidas por la Subgerencia Administrativa y Financiera. No pueden conectarse computadores, servidores, hubs, switches, routers, o cualquier otro hardware a la red sin la autorización correspondiente.

5.7 WEBSITE E INTRANET

Adoptar el Website http://www.aguasdebarrancabermeja.gov.co y la intranet como los sitios electrónicos oficiales de la empresa, para la publicación de información externa e interna.
Realizar la publicación de información en la Website e intranet con la autorización de la Subgerencia Administrativa y Financiera y ejecutado por el administrador de la Web o quien haga sus veces, pero tratándose de información sobre la actividad contractual de la empresa. Cuando la información a publicar sea inherente a alguna Subgerencia específica, deberá el Subgerente o la Gerencia enviar dicha autorización. Una vez publicada, la actualización es responsabilidad del funcionario solicitante.

5.8 DERECHOS DE AUTOR LICENCIAS DE SOFTWARE

Proteger el Derecho de Autor y Derechos Conexos, de acuerdo con lo consagrado en la constitución política, los ordenamientos legales y acuerdos regionales.
Emplear, en lo posible, las últimas versiones del software disponible en el mercado, para disminuir los problemas ocasionados por las diferencia de versiones.
Todos los programas utilizados en los computadores de la empresa deben contar con sus respectivas licencias de uso vigentes y condiciones exigidas

5.9 CORREO ELECTRONICO

La empresa suministrara el acceso al correo electrónico y a internet, como herramientas para la realización de las labores, dependiendo de las responsabilidades y naturaleza del trabajo contratado, conforme a lo previsto en el manual de funciones.
El uso inadecuado de internet constituirá una falta grave, que se clasificara como tal por la magnitud del hecho o por no atender los requerimientos de la empresa para que se cese la utilización indebida. La comprobación y las sanciones disciplinarias se realizaran conforme lo establecido en la legislación aplicable.

5.10 GESTIÓN DOCUMENTAL

Propender porque las circulares y en general comunicaciones informáticas enviadas entre los servidores de la Empresa Aguas de Barrancabermeja S.A E.S.P, se realice por medios electrónicos.
Responsabilizar al funcionario de mantener consultando permanente la cuenta habilitada en el Sistema de Gestión Documental Mercurio y atender los compromisos definidos por este medio.
Cualquier comunicación registrada por otro medio, no será considerada como oficial y el funcionario responderá por las consecuencias derivadas de ello, todo documento será reconocido una vez haya sido enviado a su destinatario, el radicado de por sí solo no implica oficialización del documento y se entenderá por no tramitado, el funcionario que a sabiendas radique y no envié la comunicación responderá por las consecuencias que se deriven de dicho acto.
Solamente se exceptuarán situaciones que por dificultades del sistema o fallos en las redes no permita hacer en debido registro con el sistema de gestión documental, lo que sí requeriría un registro manual y ser certificado por la persona competente.
La radicación de correspondencia interna y externa que requiera imprimirse es responsabilidad de cada dirección y la oficina de gestión documental únicamente se encargara del envío local y/o nacional.

5.11 COMPUTADORES, SERVIDORES Y REDES

Prohibir a los usuarios la modificación de la configuración de hardware y software establecida por el funcionario encargado de administrar el sistema.
La Subgerencia administrativa y financiera será responsable que los equipos se protejan para disminuir el riesgo de hurto, destrucción, fluctuaciones de energía, incendio y medio ambiente (por ejemplo: agua), utilizando instalaciones en condiciones adecuadas,

cerraduras, vigilantes, protectores contra transitorios de energía eléctrica y, para los servidores, fuentes de poder interrumpibles (UPS).
Prohibir el uso de módems en computadores que tengan conexión a la red local (LAN), para prevenir la intrusión de hackers a través de las puertas traseras. Todas las comunicaciones de datos deben efectuarse a través de la red LAN de la empresa.

5.12 CUENTAS DE LOS USUARIOS

Exigir que la solicitud de una nueva cuenta o el cambio de privilegios se haga a través del funcionario encargado de la Subgerencia.
Cuando la empresa vincula a un respectivo funcionario este debe firmar un documento donde declara conocer las políticas informáticas y de seguridad de la información y acepta las responsabilidades.
No debe concederse una cuenta a personas que no sean empleados de la empresa, a menos que estén debidamente autorizados por la Subgerencia correspondiente. En este caso, la persona debe firmar un documento donde declare conocer las políticas informáticas y de seguridad de la información y acepta sus responsabilidades.

5.13 IDENTIFICACION, CONTRASEÑAS Y AUTORIZACIONES

Todos los usuarios que acceden a los sistemas de información requieren de un único e intransferible identificador, el cual será proporcionado como parte del proceso de autorización.
Los identificadores concedidos deberán eliminarse o deshabilitarse, por solicitud de la Subgerencia, cuando cese la vinculación del usuario con la empresa en forma permanente o temporal, o cuando se presente un uso indebido.
De esta manera, todas las acciones realizadas con un identificador de usuario son responsabilidad del titular del mismo.

5.14 SEGURIDAD FISICA Y DEL ENTORNO

Implantar los controles de seguridad apropiados para el ingreso a las instalaciones de la empresa de funcionarios, contratistas y terceros.
El acceso de personal contratista, se debe autorizar una vez se haya formalizado el contrato y de acuerdo con los controles de seguridad definidos.
Se debe exigir al personal contratista, cumplir igualmente con las políticas, procesos procedimientos establecidos en la empresa.
Esta guía, proporciona la metodología establecida por la Entidad para la administración y gestión de los riesgos a nivel de procesos; orienta sobre las actividades a desarrollar

desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

6. CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo con los lineamientos mencionadas anteriormente, se describe a continuación las actividades que se deben desarrollar y los plazos de implementación según lo establecido por Aguas de Barrancabermeja SA ESP.

1. Revisión de los lineamientos de Seguridad y Privacidad de la Información Aprobada.
2. Socialización en Comité de Gestión y Desempeño (Comité de Seguridad de la Información) la hoja de ruta para la puesta en marchas del cumplimiento de las políticas actuales.
3. Implementacion de las lineamientos de la Seguridad de la Informacion.
    3.1. Entrevistar con los líderes de los Procesos.
    3.2 Generación de procedimientos y Aprobación Comité.
4. Adopción de las políticas de seguridad y privacidad de la información.
5. Seguimiento y Control de las políticas

CRONOGRAMA DE ACTIVIDADES DEL PLAN DE SEGURIDAD DE LA INFORMACION		
ACTIVIDAD	**RECURSOS**	**Año de Implementación**
Revisión de la Política Actual y Socialización de la puesta en marcha de la Implementación de los Lineamientos.	Humanos	2020
Generar Procedimientos de los lineamientos de seguridad de la información	Humanos	2020-2023
Implementación de los Lineamientos de Seguridad de la Información.	Humanos, Financieros	2020-2023

7. MONITOREO Y REVISIÓN

La entidad debe asegurar el logro de sus objetivos anticipándose a los eventos negativos relacionados con la gestión de la entidad. El monitoreo y revisión se presentarán en el comité de gestión y desempeño encardado de las funciones de seguridad de la información, y la unidad de control de gestión tal como lo establece las líneas de defensa.

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

AGUAS DE BARRANCABERMEJA S.A. E.S.P.

2020-2023

	ELABORADO POR	REVISADO POR	APROBADO POR
Firma			
Cargo	Profesional III Adscrito a la Subgerencia Administrativa y Financiera	Presidente Comité Institucional de Gestión y Desempeño	Presidente Comité Institucional de Coordinación de Control Interno
Nombre	Rafael Andres Lastre Gomez	Carlos Arturo Vasquez	Alfredo Garces Echeverry
Fecha	Enero 2020	Acta No. 3 del 2020 del CIGyD	Acta No 1 de 2020 del CICCI

CONTROL DE CAMBIOS		
VERSION	FECHA DE APROBACION	DESCRIPCION DEL CAMBIO
1	Acta No 1 de 2020 del CICCI	Creación, Aprobación de Documento.

TABLA DE CONTENIDO

1. OBJETIVOS 4

1.1 Objetivo general 4

1.2 Objetivos específicos 4

2. ALCANCE 4

3. DEFINICIONES 4

4. TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: MAPA DE RISGOS DE SEGURIDAD DIGITAL 6

4.1 METODOLOGIA PARA LA IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 9

4.2 CUMPLIMIENTO DE IMPLEMENTACIÓN 9

5. PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION. 10

5.1 CRONOGRAMA PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 10

INTRODUCCIÓN

La Administración de Riesgos es un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de tal forma que permita a las entidades minimizar pérdidas y maximizar oportunidades.

Todos los servidores públicos, en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas, consecuencias de la materialización de dichos riesgos y los posibles controles que se puedan implementar para el tratamiento de dichos riesgos.

En este plan se pretende establecer las acciones de control que permitan una eficaz, eficiente y efectiva gestión del riesgo en el contexto de la seguridad y privacidad de la información, desde la identificación hasta el monitoreo; enfatizando en la importancia de la administración del riesgo, sus fundamentos teóricos y da una orientación para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y de lineamientos sencillos y claros para su adecuado tratamiento.

1. OBJETIVOS

1.1 Objetivo general

Definir las acciones necesarias que permitan la administración de los riesgos de seguridad y privacidad de la información contemplando: Identificación de activos de información, amenazas, vulnerabilidades, riesgos y controles, los niveles aceptables y tratamiento de riesgo en la empresa Aguas de Barrancabermeja SA ESP.

1.2 Objetivos específicos

- Realizar un análisis y valoración de los riesgos de seguridad de la información identificados para determinar la medida a implementar que permita lograr un nivel aceptable del riesgo.
- Identificar las medidas de protección que contribuyan al correcto tratamiento de los riesgos a través de una adecuada selección y relación de controles.

2. ALCANCE

En este plan de tratamiento se cubrirán todos aquellos posibles riesgos asociados a los activos de información de la empresa Aguas de Barrancabermeja SA ESP.

3. DEFINICIONES

Para la administración del riesgo, se tendrán en cuenta los siguientes términos y definiciones:

- **Acciones asociadas:** son las acciones que se deben tomar posterior a determinar las opciones de manejo del riesgo (asumir, reducir, evitar compartir o transferir), dependiendo de la evaluación del riesgo residual, orientadas a fortalecer los controles identificados.
- **Administración de riesgos:** conjunto de etapas secuenciales que se deben desarrollar para el adecuado tratamiento de los riesgos.
- **Amenaza:** situación externa que no controla la entidad y que puede afectar su operación

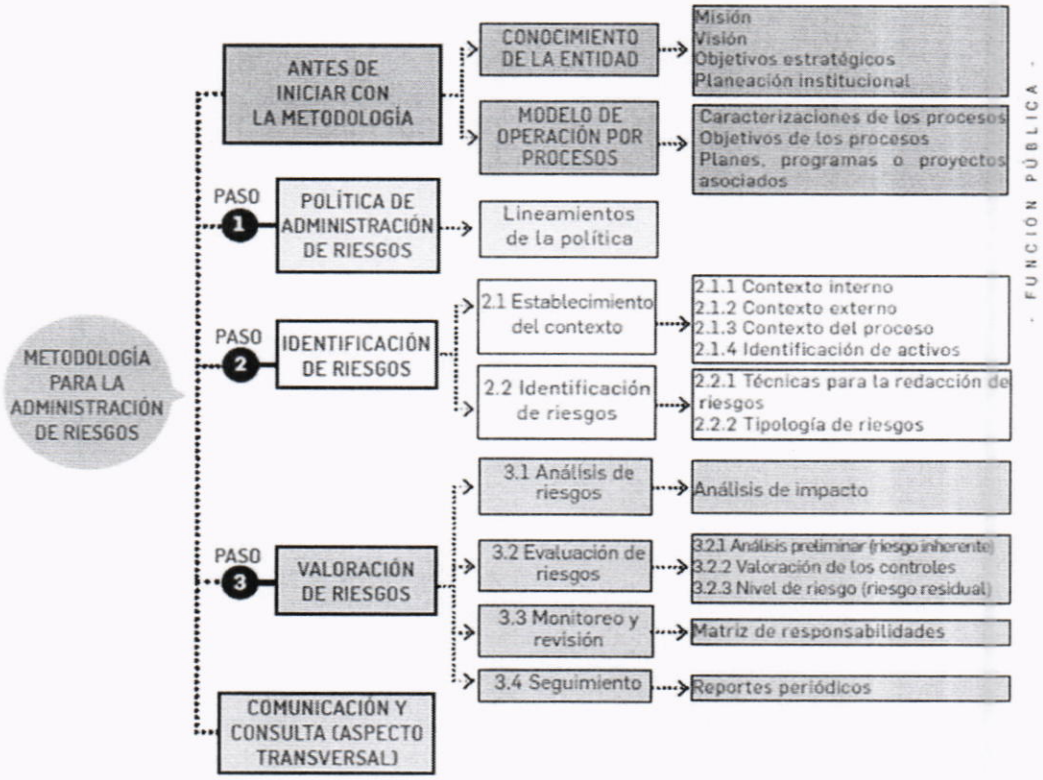
- **Análisis del riesgo:** etapa de la administración del riesgo, donde se establece la probabilidad de ocurrencia y el impacto del riesgo antes de determinar los controles (análisis del riesgo inherente).
- **Asumir el riesgo:** opción de manejo donde se acepta la pérdida residual probable, si el riesgo se materializa.
- **Causa:** medios, circunstancias y/o agentes que generan riesgos.
- **Calificación del riesgo:** estimación de la probabilidad de ocurrencia del riesgo y el impacto que puede causar su materialización.
- **Compartir o transferir el riesgo:** opción de manejo que determina traspasar o compartir las pérdidas producto de la materialización de un riesgo con otras organizaciones mediante figuras como outsourcing, seguros, sitios alternos.
- **Consecuencia:** efectos que se pueden presentar cuando un riesgo se materializa.
- **Contexto estratégico:** son las condiciones internas y del entorno, que pueden generar eventos que originan oportunidades o afectan negativamente el cumplimiento de la misión y objetivos de una institución.
- **Control:** acción o conjunto de acciones que minimiza la probabilidad de ocurrencia de un riesgo o el impacto producido ante su materialización.
- **Control preventivo:** acción o conjunto de acciones que eliminan o mitigan las causas del riesgo; está orientado a disminuir la probabilidad de ocurrencia del riesgo.
- **Control correctivo:** acción o conjunto de acciones que eliminan o mitigan las consecuencias del riesgo; está orientado a disminuir el nivel de impacto del riesgo.
- **Debilidad:** situación interna que la entidad puede controlar y que puede afectar su operación.
- **Evaluación del riesgo:** resultado del cruce cuantitativo de las calificaciones de probabilidad e impacto, para establecer la zona donde se ubicará el riesgo.
- **Evitar el riesgo:** opción de manejo que determina la formulación de acciones donde se prevenga la materialización del riesgo mediante el fortalecimiento de controles identificado.
- **Frecuencia:** ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.
- **Identificación del riesgo:** etapa de la administración del riesgo donde se establece el riesgo con sus causas (asociadas a factores externos e internos de riesgo), consecuencias y se clasifica de acuerdo con los tipos de riesgo definidos
- **Impacto:** medida para estimar cuantitativa y cualitativamente el posible efecto de la materialización del riesgo.
- **Mapa de riesgos:** documento que de manera sistemática, muestra el desarrollo de las etapas de la administración del riesgo.
- **Materialización del riesgo:** ocurrencia del riesgo identificado

- **Opciones de manejo:** posibilidades disponibles para administrar el riesgo posterior a la valoración de los controles definidos (asumir, reducir, evitar compartir o transferir el riesgo residual).
- **Plan de contingencia:** conjunto de acciones inmediatas, recursos, responsables y tiempos establecidos para hacer frente a la materialización del riesgo y garantizar la continuidad del servicio
- **Probabilidad:** medida para estimar cuantitativa y cualitativamente la posibilidad de ocurrencia del riesgo.
- **Procedimiento:** conjunto de especificaciones, relaciones, responsabilidades, controles y ordenamiento de las actividades y tareas requeridas para cumplir con el proceso.
- **Riesgo:** eventualidad que tendrá un impacto negativo sobre los objetivos institucionales o del proceso.
- **Riesgo de corrupción:** posibilidad de que por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y en consecuencia del Estado, para la obtención de un beneficio particular.
- **Riesgo inherente:** es aquel al que se enfrenta una entidad o proceso en ausencia de controles y/o acciones para modificar su probabilidad o impacto.
- **Riesgo institucional**: Son los que afectan de manera directa el cumplimiento de los objetivos o la misión institucional.
- **Riesgo residual:** nivel de riesgo que permanece luego de determinar y aplicar controles para su administración.
- **Valoración del riesgo:** establece la identificación y evaluación de los controles para prevenir la ocurrencia del riesgo o reducir los efectos de su materialización. En la etapa de valoración del riesgo se determina el riesgo residual, la opción de manejo a seguir, y si es necesita.

4. TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN: MAPA DE RISGOS DE SEGURIDAD DIGITAL

Para el tratamiento de los riesgos de seguridad y privacidad de la información se toma como base la estructura establecida por el DAFP "Guía para la Administración del Riesgo y el Diseño de Controles de las Entidades Públicas del DAFP v4".

Esquema 2. Metodología para la administración del riesgo



13

Estructura que ha permitido la identificación y valoración inicial de riesgos, cuyo resultado es insumo principal para la formulación del Plan de Tratamiento de Riesgos de Seguridad Y Privacidad De La Información.

Es de anotar que para la identificación de los riesgos se tuvo en cuenta la identificación de los Activos de Seguridad Digital e información, entre los que se mencionan: aplicaciones de la entidad pública, servicios Web, redes, información física o digital, Tecnologías de la Información - TI- o Tecnologías de la Operación -TO-) que utiliza la empresa para su funcionamiento.

TIPO DE ACTIVO	DESCRIPCION
INFORMACIÓN	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores), teniendo en cuenta lo anterior, se puede distinguir como información: Contratos, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, registros contables, estados financieros, archivos ofimáticos, documentos y registros del sistema integrado de gestión, bases de datos con información personal o con información relevante para algún proceso (bases de datos de nóminas, estados financieros) entre otros.
SOFTWARE	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades.
HARDWARE	Equipos físicos de cómputo y de comunicaciones como, servidores, biométricos que por su criticidad son considerados activos de información.
SERVICIOS	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos, tales como: Servicios WEB, intranet, CRM, ERP, Portales organizacionales, Aplicaciones entre otros (Pueden estar compuestos por hardware y software).
INTANGIBLES	Se consideran intangibles aquellos activos inmateriales que otorgan a la entidad una ventaja competitiva relevante, uno de ellos es la imagen corporativa, reputación o el good will, entre otros.
COMPONENTES DE RED	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red, por ejemplo, el cableado estructurado y tarjetas de red, routers, switches, entre otros.
PERSONAS	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información, por ejemplo: personal con experiencia y capacitado para realizar una tarea específica en la ejecución de las actividades.
INSTALACIONES	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa.

Identificar los activos es importante para saber lo que se debe proteger para garantizar tanto su funcionamiento interno (BackOffice) como su funcionamiento de cara al ciudadano (Front Office).

En el cuadro siguiente se detallan las cuatro (4) fases a seguir del proceso del Modelo de Seguridad y Privacidad de la Información (MSPI) que son:

ETAPAS MSPI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
PLANEAR	Establecer Contexto.
	Valoración del Riesgo.
	Planificación del Tratamiento del Riesgo.
IMPLEMENTAR	Implementación del Plan de Tratamiento de Riesgo
GESTIONAR	Monitoreo y Revisión Continuo de los Controles asociados a los Riesgos.
MEJORA CONTINUA	Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

4.1 METODOLOGIA PARA LA IMPLEMENTACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

- **Seguimiento de los Lineamientos de la Política de Administración de Riesgos de la empresa**

Para Aguas de Barrancabermeja S.A. E.S.P., la gestión del Riesgo es el proceso efectuado por la Gerencia, su equipo directivo y por todo el personal para proporcionar a la administración, un aseguramiento razonable con respecto al logro de los objetivos.

Así mismo, en relación con la gestión de los riesgos de seguridad digital y de seguridad de la información, la empresa ha designado como responsable de Seguridad Digital y Seguridad de la Información a la Subgerencia Administrativa y Financiera bajo la coordinación del Profesional III de Sistemas, líder del proceso Gestión Informática.

- **Actividades para la formulación e implementación del Plan de Tratamiento de Riesgos**

1. Priorización de los riesgos a tratar (Valorar del riesgo y del riesgo residual)

2. Seguimiento y control a los riesgos asociados a la Seguridad y Privacidad de la información, una vez aplicados controles internos.

3. Evaluación de los riesgos (efectividad de los controles asociados a los posibles riesgos).

4. Formulación de las medidas a asumir frente a los riesgos

5. Implementación de medidas a seguir para el tratamiento de los riesgos asociados a la Seguridad y Privacidad de la información.

- **Cronograma de actividades de acuerdo con el mapa de riesgos de seguridad digital**

4.2 CUMPLIMIENTO DE IMPLEMENTACIÓN

De acuerdo con las fases mencionadas anteriormente, se describe a continuación los dominios que se deben desarrollar y los plazos de implementación de acuerdo con lo establecido por el Aguas de Barrancabermeja SA ESP.

- Revisión de la Política de Seguridad de la Información, incluida en el manual de Informática
- Aspectos organizativos de la seguridad de la información
- Seguridad Ligada a los recursos humanos
- Revisión del Control de acceso
- Seguridad en la parte operativa
- Seguridad en las telecomunicaciones
- Gestión de Incidentes de Seguridad de la Información
- Aspectos de seguridad de la información en la gestión de continuidad del negocio.

Con base en el resultado del análisis de riesgos de la información y con el fin de gestionar el riesgo residual, se proponen acciones de mejora los cuales pueden estar en marcha por medio de planes de acción o de tratamiento con la finalidad de que la información siempre conserve las características de confidencialidad, integridad y disponibilidad de esta, desarrollándose como un proceso de seleccionar e implementar medidas para modificar el nivel de riesgo.

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

Para la elaboración del Plan de tratamiento de riesgos de seguridad y privacidad de la información se toma como base los riesgos identificados en el Mapa de Riesgos 2020 relacionados con la seguridad digital. y de acuerdo con los dominios de establecidos en el cumplimiento de implementación se podrán seguir identificados los riesgos para ser tratados usando la metodología expuesta en este plan.

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

AGUAS DE BARRANCABERMEJA S.A. E.S.P. NIt. 900.045.408-1	SISTEMA DE GESTION	**Código:** GIF-PL-003
		Página: 11 de 11
		Versión: 1
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	**Vigente a partir de:** 30-01-2020

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

ACTIVIDAD	TRIMESTRES VIG 2020				TRIMESTRES VIG 2021				TRIMESTRES VIG 2022				TRIMESTRES VIG 2022				RESPONSABLE	MEDIDA DE TRATAMIENTO
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4		
RIESGO 1. Alteración indebida de los datos de usuarios en el Sistema de Información Comercial																		Minimizar
Capacitación para el aprovechamiento del Modulo de Auditoria del Sistema de Información Comercial		X															Profesional III TIC	
Asignar Roles y responsabilidades frente a la implementación de las Seguimiento de Novedades al Sistema de Información Comercial		X															Profesional III TIC	
Realización de Seguimiento de Novedades al Sistema de Información Comercial (Depende de la Asignacion de Roles)		X		X		X		X									Según la Asignacion de Roles	
Seguimiento a las actividades de control			X														Profesional III TIC	
RIESGO 2. Daños en los Equipos Activos de la Infraestructura Tecnológica																		Minimizar
Mantenimiento Preventivo Equipos de actuales			X				X				X				X		Profesional III TIC	
RIESGO 3. Deficiente Parametrización del Sistema de Información Comercial en cuanto a pagos dobles	X				X				X				X					Minimizar
Desarrollo en el Sistema Comercial Neptuno modulo de saldos a favor del usuario			X	X													Subgerencia Comercial, Profesional TIC	