ANÁLISIS DE RIESGOS PARA EL PROCESO ADMINISTRATIVO: DEPARTAMENTO DE INFORMÁTICA EN LA EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE PEREIRA S.A E.S.P, BASADOS EN LA NORMA ISO 27005

INGENIERO ALEXIS ARMANDO ANGARITA VIVAS

INGENIERO CÉSAR AUGUSTO TABARES ISAZA

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y CIENCIAS DE LA COMPUTACIÓN

PROGRAMA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN

PEREIRA, DICIEMBRE DE 2012

ANÁLISIS DE RIESGOS PARA EL PROCESO ADMINISTRATIVO: DEPARTAMENTO DE INFORMÁTICA EN LA EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE PEREIRA S.A E.S.P, BASADOS EN LA NORMA ISO 27005

INGENIERO ALEXIS ARMANDO ANGARITA VIVAS

INGENIERO CÉSAR AUGUSTO TABARES ISAZA

Proyecto de Grado para optar por el título de Especialista en Redes de Datos

Dirigido por el Ingeniero Juan de Jesús Veloza Mora

UNIVERSIDAD TECNOLÓGICA DE PEREIRA
FACULTAD DE INGENIERÍAS ELÉCTRICA, ELECTRÓNICA, FÍSICA Y CIENCIAS DE LA COMPUTACIÓN
PROGRAMA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
PEREIRA, DICIEMBRE DE 2012

Nota de aceptación:

_____

_____

_____

_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Pereira, diciembre de 2012

CONTENIDO

LISTA DE ILUSTRACIONES

LISTA DE TABLAS

1 INTRODUCCIÓN

La información es el **principal activo** de toda organización según los más modernos paradigmas de la administración empresarial, pudiendo hacer su aparición de muchas formas: impresa o escrita en papel, almacenada electrónicamente, transmitida por correo, ilustrada en películas o hablada en conversaciones.

En el ambiente de negocios competitivo de hoy, esa información está constantemente bajo la amenaza de muchas fuentes, que pueden ser internas, externas, accidentales o maliciosas para con la organización. Con el incremento del uso de nueva tecnología para almacenar, transmitir y recobrar información se han abierto canales para un mayor número y variedad de amenazas.

Proteger la información y los recursos tecnológicos informáticos es una tarea continua y de vital importancia que debe darse en la medida en que avanza la tecnología, ya que las técnicas empleadas por aquellos que usan dichos avances para fines delictivos aumentan y como resultado los atacantes son cada vez más numerosos, mejor organizados y con mejores capacidades. Es importante que toda organización que quiera tener una menor probabilidad de pérdida de recursos por causa de los ataques a los que se expone defina una estrategia de seguridad fundamentada en políticas de seguridad que estén respaldadas por todos los miembros de la organización.

Se debe considerar que la violación de la seguridad en un sistema podría llegar a afectar gravemente las operaciones más importantes de la empresa, desmejorar sus procesos y dejarla expuesta a la quiebra.

Se requiere establecer por tanto, un sistema de gestión de seguridad de información dentro de cualquier tipo de organización. Es necesario asegurar la **confidencialidad, integridad, disponibilidad y auditabilidad** de la información vital para la corporación, el negocio y los clientes. Una estrategia de gestión de la información es esencial para sobrevivir en el mercado actual.

En este trabajo se plantea el tema de análisis de riesgos para la seguridad de la Información de acuerdo a los lineamientos de ISO 27005 para el proceso: “Departamento de Informática” de la Empresa Aguas y Aguas de Pereira S.A E.S.P, elemento fundamental para poder implementar políticas y procedimientos que permitan mantener la seguridad de la información en un nivel óptimo.

Este desarrollo es fundamental para en un futuro pensar en la implementación del sistema de gestión de seguridad de la información y para la creación de una estrategia de seguridad basada en políticas, apuntando hacia la certificación en la norma ISO 27000.

TÍTULO

ANÁLISIS DE RIESGOS PARA EL PROCESO ADMINISTRATIVO: GESTION DE INFORMÁTICA EN LA EMPRESA DE ACUEDUCTO Y ALCANTARILLADO DE PEREIRA S.A E.S.P, BASADOS EN LA NORMA ISO 27005.

2 DEFINICIÓN DEL PROBLEMA

En el ámbito de los sistemas transaccionales de información y el manejo adecuado de la ésta, se requiere proteger a la Empresa de las diferentes amenazas que en algún momento se podrían cristalizar y generar traumatismos en el manejo de la misma. Se debe garantizar que la información está siendo manejada correctamente y en un ambiente seguro, es decir que la información no sea alterada o modificada en ningún momento.

Actualmente el proceso: "Departamento de Informática" de la Empresa Aguas y Aguas de Pereira S.A E.S.P, no tiene dimensionados los riesgos de activos de información.

Ante esta situación se platean entonces los siguientes problemas:

¿Cómo se debe proteger la información almacenada en los servidores y medios Electrónicos que posee la Empresa?

¿Cuáles son los riesgos en los activos de información, que enfrenta el Departamento de informática de la empresa Aguas y Aguas de Pereira?

En este sentido, se propone como parte del trabajo de investigación, realizar un análisis de riesgos para el proceso administrativo: Departamento de Informática, basado en las normas de Seguridad de la Información a saber:

ISO/IEC 27001: Tecnologías de la Información, técnicas de seguridad, sistemas de Gestión de la seguridad de la información y requerimientos.

ISO/IEC 27005-2008: Esta norma establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la

aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

Hay que señalar de todas maneras, que ISO 27005 no proporciona una metodología concreta de Análisis de Riesgos, sino que describe a través de su clausulado el proceso recomendado de análisis incluyendo las fases que lo conforman:

- Establecimiento del contexto (Cláusula 7)
- Evaluación del riesgo (Cláusula 8)
- Tratamiento del riesgo (Cláusula 9)
- Aceptación del riesgo (Cláusula 10)
- Comunicación del riesgo (Cláusula 11)
- Monitorización y revisión del riesgo (Cláusula 12)

En pocas palabras, la norma servirá para no tener dudas sobre los elementos que debe incluir toda buena metodología de Análisis de Riesgos, por lo que, visto desde esta manera, puede constituirse como una metodología en sí misma.

3 JUSTIFICACIÓN

Aunque hoy en día todas las empresas tienen claro que su activo más valioso es la INFORMACIÓN, éstas no implementan acciones tendientes a proteger en su totalidad dicho activo, haciéndolas vulnerables a las amenazas existentes en su entorno.

El análisis y gestión de riesgos es un instrumento fundamental para proteger la información, la cual a su vez, tiene implícitas definiciones como Apetito al riesgo y Capacidad de riesgo; siendo la primera, el nivel de riesgo que cada organización está preparada para tolerar en sus negocios, y la segunda, el nivel de riesgo que cada organización no está, financieramente capacitada para exceder; por lo tanto, la gestión del riesgo es propia para cada organización.

En el caso particular de la Empresa Aguas y Aguas de Pereira no existen procedimientos, planes de gestión de riesgos, ni una cultura organizacional del riesgo, con las cuales se definan controles y acciones a tomar para llegar a un nivel de riesgo de seguridad de la información aceptable para la empresa.

Realizar un análisis de riesgos es crucial para en un futuro desarrollar y poner en funcionamiento un sistema de seguridad de la información en la Empresa. En esta etapa de análisis, se construye lo que será el "modelo de seguridad", esto es, una representación de todos los activos y sus dependencias jerárquicas, así como el mapa de riesgos y amenazas, es decir, todo aquello que pudiera ocurrir y que tuviera un impacto para la Empresa. Así mismo, esta etapa de análisis permitirá realizar la estimación de impactos (probabilidad de que se materialice la amenaza) y calcular el riesgo al que puede ser sometida la Empresa.

Es por ello que se hace necesario evaluar y analizar los riesgos de seguridad de la información que tiene actualmente la empresa específicamente el proceso administrativo: "Departamento de Informática", objetivo de esta investigación, con lo cual la empresa entenderá cuál es su situación actual a nivel de seguridad y tomará decisiones adecuadas para mitigar los riesgos, además de evaluar si las medidas que se implementen son las correctas.

4 OBJETIVOS

4.1 OBJETIVO GENERAL

Realizar el análisis de riesgos para el subproceso administrativo "Gestión de Informática" de la Empresa Aguas y Aguas de Pereira S.A E.S.P

4.2 OBJETIVOS ESPECÍFICOS

1. Realizar un inventario de Activos del departamento de Informática
2. Identificar Amenazas
3. Identificar vulnerabilidades
4. Calcular el riesgo
5. Desarrollar el mapa de riesgos
6. Definir el riesgo aceptable

5 MARCO REFERENCIAL

5.1 MARCO DE ANTECEDENTES

Mediante Decreto Extraordinario No.90 de 1957 se organizaron las Empresas Públicas de Pereira como establecimiento público autónomo, encargado de la administración de los servicios públicos de energía eléctrica, teléfonos, acueducto, alcantarillado, plaza de mercado y matadero. En 1959 mediante Acuerdo 043 del Concejo Municipal se le delegó a la Empresa la administración de las cuencas hidrográficas del municipio, para lo cual se creó el Departamento de Reforestación, dedicado especialmente a la conservación de la Cuenca del río Otún.

Gracias a la Ley 142 de 1994, se constituyó un nuevo régimen de servicios públicos domiciliarios en el cual se establecen, entre otros, los siguientes aspectos: los principios generales y la intervención del Estado en la regulación, control y vigilancia en los servicios públicos, el régimen jurídico de las empresas de servicios públicos, el régimen de actos y contratos, el régimen laboral y el régimen de transición; normas especiales para algunos servicios públicos y el régimen tarifario.

El Concejo Municipal de Pereira expidió el Acuerdo 30 de 1996 a través del cual transformó el establecimiento público Empresas Públicas de Pereira, escindiéndolo en cuatro sociedades por acciones: Empresa de Energía de Pereira S.A. E.S.P, Empresa de Aseo de Pereira S.A E.S.P., Empresa de Telecomunicaciones de Pereira S.A. E.S.P. y Empresa de Acueducto y Alcantarillado de Pereira S.A. E.S.P. e igualmente se constituyó la Empresa de Servicios Múltiples compartidos, Multiservicios S.A.

La Empresa de Acueducto y Alcantarillado de Pereira S.A. E.S.P, tiene por objeto principal la prestación de los servicios públicos domiciliarios de acueducto y alcantarillado incluyendo sus actividades complementarias. Fue constituida por medio de la escritura pública 1326 del 16 de Mayo de 1997 de la Notaría Cuarta del Circuito de Pereira. La nueva Empresa inició sus labores en forma autónoma el 24 de julio de 1997 y se inscribe ante la Cámara de Comercio de Pereira bajo el No. 5667 del 25 de Julio del mismo año.

Mediante acuerdo No.20 del 28 de julio de 2004, se transforma en sociedad anónima de economía mixta de Servicios Públicos Domiciliarios, constituida por medio de la escritura pública 2665 del 24 de agosto de 2004 de la Notaría Sexta del Circuito de Pereira. Para efectos comerciales, la Empresa adoptó el nombre de AGUAS Y AGUAS DE PEREIRA.

En el año 2001 la Gerencia de la Empresa contrató una evaluación del manejo de la información de Aguas y Aguas por parte de la empresa Multiservicios bajo los aspectos de calidad, seguridad y oportunidad de la información. Esta evaluación mostró falencias que afectaban tanto a la información, como el servicio al cliente. Por este motivo las directivas de la Empresa decidieron tener el control de su información y de sus clientes; para lo cual Aguas y Aguas de Pereira desarrolló su proyecto de modernización tecnológica.

Este proyecto incluyó la conformación de un grupo de sistemas dentro de la Dirección de Planeación y Sistemas, la implementación del sistema de información Empresarial, el desarrollo de una intranet, acceso controlado a internet, la instalación de un centro de cómputo adecuado para poder procesar la información de la Empresa y permitir las comunicaciones de los funcionarios. Este proyecto adicionalmente apoyó proyectos de todas las áreas de la Empresa con su personal y recursos informáticos.

Para el año 2004 la Empresa sufrió un cambio cultural bastante favorable ya que comenzó a utilizar la tecnología informática de una manera mucho más productiva, como se mostró en los múltiples proyectos en donde se aplicaron tecnologías informáticas para la implementación de sistemas de Información.

El grupo de sistemas se vio robustecido con la contratación de cuatro ingenieros de sistemas para apoyar el desarrollo de las actividades empresariales.

Se implementó en la red de datos el uso de un firewall, que permitió establecer políticas de conectividad con las demás sedes e implementar el servicio de Internet. En la parte de conectividad intra-empresarial, se puso en funcionamiento el servidor de dominios de red, el cual permitió garantizar el acceso a los servicios de red de datos disponibles sólo a personal autorizado de la institución. Se gestionó más eficientemente la comunicación y colaboración de archivos en red de las dependencias, con la asignación de grupos de trabajo.

La Empresa contrató un Leasing Operativo para servidores, software y equipos complementarios, los cuales fueron adquiridos en su totalidad en el año 2006. Posteriormente se adquirieron servidores para respaldo y contingencia de equipos de misión critica.

En cuanto a seguridad, se implementaron una serie de medidas de seguridad para la infraestructura informática y una política de seguridad informática para

los usuarios de la red. Ésto llevó al desarrollo de documentos que orientaron el uso de los sistemas informáticos, para obtener el mayor provecho de estas tecnologías, y evitar el uso indebido de las mismas.

En cuanto a la seguridad lógica de la red, se instaló un Firewall de Cisco modelo PIX 515e, el cual permitió proteger la red de intrusos informáticos. En el año 2008 se adquiere un Barracuda Spam Firewall, disminuyendo en un 98% la llegada de correo no deseado y virus a los buzones de correo electrónico de los usuarios.

Es importante aclarar que todas las implementaciones antes mencionadas, se realizaron sin tener una estrategia y una visión clara sobre el valor de la información como activo principal de la empresa, ni las amenazas que ponen en riesgo la seguridad de dicho activo.

5.2 MARCO TEÓRICO

La seguridad de la información es la preservación de los principios básicos de la confidencialidad, integridad y disponibilidad de la misma y de los sistemas implicados en su tratamiento. Estos tres pilares se definen como:

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

En la seguridad de la información, no sólo intervienen los aspectos tecnológicos, sino también los procesos, los ambientes (centro de cómputo, ubicación de oficinas) y principalmente las personas.

Por lo anteriormente expuesto es necesario adoptar un modelo aprobado internacionalmente, que permita definir adecuadamente todos los procesos que deben ser tenidos en cuenta a la hora de implementar un SGSI. Para los efectos de este proyecto de grado se definió que el modelo a utilizar es el ISO/IEC 27001.

ISO/IEC 27001: Uno de los modelos más utilizados para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) es la Norma ISO27001, la cual se basa en el ciclo de vida PHVA (Planear, Hacer, Verificar y Actuar; o ciclo Deming) de mejora continua, al igual que otras normas de sistemas de gestión (ISO 9001 para calidad, ISO 14001 para medio ambiente, etc.).

Este estándar es certificable, es decir, cualquier organización que tenga implantado un SGSI según este modelo, puede solicitar una auditoría externa por parte de una entidad acreditada y, tras superar con éxito la misma, recibir la certificación en ISO 27001.

El origen de la Norma ISO27001 está en el estándar británico BSI (British Standards Institution) BS7799-Parte 2, estándar que fue publicado en 1998 y era certificable desde entonces. Tras la adaptación pertinente, ISO 27001 fue publicada el 15 de Octubre de 2005.

ISO ha reservado la serie de numeración 27000 para las normas relacionadas con sistemas de gestión de seguridad de la información. En el 2005 incluyó en ella la primera de la serie (ISO 27001), las demás son:

ISO 27000 (Términos y definiciones)

ISO 27002 (Objetivos de control y controles)

ISO 27003 (Guía de implantación de un SGSI)

ISO 27004 (Métricas y técnicas de medida de la efectividad de un SGSI),

ISO 27005 (Guía para la gestión del riesgo de seguridad de la información) y

ISO 27006 (Proceso de acreditación de entidades de certificación y el registro de SGSI).

Existen otros estándares internacionalmente aceptados, relacionados con seguridad de la información, que la enfocan desde diferentes puntos de vista como controles de seguridad, buen gobierno, gestión de riesgo, etc.; entre los cuales se destacan los siguientes:

COBIT: Los Objetivos de Control para la Información y la Tecnología relacionada (COBIT®) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las

buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones facilitadas por la TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien. El Instituto ITGI Governance Institute (www.itgi.org) diseñó y creó esta publicación titulada COBIT® como un recurso educacional para los directores ejecutivos de información, para la dirección general, y para los profesionales de administración y control de TI.

NIST: National Institute of Standards and Technology, elabora y promueve patrones de medición, estándares y tecnología con el fin de realzar la productividad, facilitar el comercio y mejorar la calidad de vida. Destinados principalmente para el Gobierno de EE.UU. las fuerzas militares y el sector comercial, pero pueden ser adaptados a cualquier contexto. Las publicaciones del NIST son estándares concisos y claros, disponibles de forma gratuita. NIST tiene una división especial destinada para publicaciones relacionadas en seguridad de la información: Computer Security Division –Resource Center.

AS/NZ4360: Norma Australiana – Neozelandesa que suministra orientaciones genéricas para la gestión de riesgos. Puede aplicarse a una gran variedad de actividades, decisiones u operaciones de cualquier entidad pública, privada o comunitaria, grupos o individuos. Se trata de una instrucción amplia pero que permite la definición de objetivos específicos de acuerdo con las necesidades de cada implementación. La aplicación de la norma AS/NZS 4360, le garantiza a la organización una base sólida para la aplicación de cualquier otra norma o metodología de gestión de riesgos específica para un determinado segmento.

5.2.1 GESTIÓN DE RIESGO

Se puede definir como “el proceso de toma de decisiones en un ambiente de incertidumbre sobre una acción que puede suceder y sobre las consecuencias que existirán si esta acción ocurre”.

El Análisis de Riesgos implica:

• Determinar **qué** se necesita proteger**.**
• **De qué** hay que protegerlo**.**
• **Cómo** hacerlo.

5.2.2 REGULACIONES Y NORMAS QUE TRATAN EL RIESGO

COMUNICACIÓN "A" 4609 DEL BCRA PARA ENTIDADES FINANCIERAS

Requisitos mínimos de gestión, implementación y control de los riesgos relacionados con tecnología informática y sistemas de información.

NTC5254 – ICONTEC: Esta norma proporciona una guía genérica para la gestión de riesgo. Se puede aplicar a una gama muy amplia de actividades, decisiones u operaciones de cualquier empresa pública, privada o comunitaria, a grupo o a individuos.
Esta norma especifica los elementos del proceso de la gestión de riesgo, pero no tiene el propósito de imponer uniformidad de los sistemas de gestión de riesgo. Es genérica e independiente de cualquier industria o sector económico especifico.

MAGERIT: Es la Metodología de Análisis y Gestión de Riesgos de los sistemas de Información de las Administraciones públicas. MAGERIT, es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos. MAGERIT ha sido elaborada por un equipo interdisciplinario del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del Consejo Superior de Informática.

BASILEA II: Estándar internacional que sirva de referencia a los reguladores bancarios, con objeto de establecer los requerimientos de capital necesarios, para asegurar la protección de las entidades frente a los riesgos financieros y operativos.

LEY SARBANES OXLEY (SOX): Impulsada por el gobierno norteamericano como respuesta a los mega-fraudes corporativos que impulsaron Enron, Tyco International, WorldCom y Peregrine Systems. Es un conjunto de medidas tendientes a asegurar la efectividad de los controles internos sobre reportes financieros.

ISO/IEC 27005:2008: Esta Norma proporciona directrices para la Gestión del Riesgo de Seguridad de la Información en una Organización**.** Sin embargo, esta Norma no proporciona ninguna metodología específica para el análisis y la gestión del riesgo de la seguridad de la información.

Es aplicable a todo tipo de Organización:

- ✓ Empresas Comerciales
- ✓ Organismo Gubernamentales
- ✓ Organismos sin fines de lucro
- ✓ Entidades Financieras

Los pasos establecidos en esta norma son los siguientes:

1. Establecer el contexto.
2. Evaluación del riesgo.
    a. Identificación del riesgo
    b. Estimación del riesgo
    c. Valoración del riesgo
3. Tratamiento del riesgo.
4. Aceptación del riesgo.
5. Comunicación del riesgo.
6. Seguimiento del riesgo.

5.3 MARCO CONCEPTUAL

Activos

Recursos de los sistemas de información o relacionados con estos, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

El valor de los activos puede ser:

Subjetivo: Tiene un valor subjetivo es decir, “cuánto vale para la organización”

Intrínseco u Objetivo: El objeto tiene un valor económico.

LA INFORMACIÓN = ACTIVO

- Tiene valor para una organización y por consiguiente debe ser debidamente protegida.

- Garantiza la continuidad comercial, minimiza el daño a ésta y maximiza el retorno sobre las inversiones y las oportunidades.

- La seguridad que puede lograrse por medios técnicos es limitada y debe ser respaldada por una gestión y procedimientos adecuados.

Tipos de Activos:

Hardware: Infraestructura tecnológica de soporte
Software: Programas
Organización: Organización lógica y física del personal

Amenaza

Se entiende por una amenaza una condición del entorno del sistema de información (persona, máquina, suceso o idea) que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad (no cumplimiento de alguno de los aspectos mencionados) afectando alguno de los activos de la compañía.

Vulnerabilidad

Es un hecho o actividad que permite concretar una amenaza.

Impacto

Es el daño producido por la materialización de una amenaza.

Riesgo

Es la posibilidad de que se produzca un impacto en la organización.

Contramedidas o Salvaguardas

Protecciones u acciones que disminuyen el riesgo.

5.4 MARCO LEGAL

ISO 27000

En Colombia, las normas internacionales en seguridad de la información, han sido adoptadas por el Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC y el Gobierno Colombiano ha generado normativas de control interno

como el MECI1000 y de calidad como la NTCGP1000 apoyado por estándares internacionales (COSO, ISO9001 respectivamente).

Las normas NTC ISO/IEC 27001 y NTC ISO/IEC 27005 fueron liberadas por el Instituto Colombiano de Normas Técnicas y Certificación, ICONTEC en el año 2006 y 2008 respectivamente y son una copia idéntica por traducción de las normas ISO/IEC 27001 e ISO/IEC 27005. Estas normas permiten diseñar una herramienta para la implementación del sistema de gestión de seguridad de la información teniendo en cuenta la política, la estructura organizativa, los procedimientos y los recursos. La norma NTC ISO/IEC 27001 adopta el modelo de procesos "Planificar-Hacer-Verificar-Actuar" (PHVA) para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, SGSI.

COSO, un marco de referencia para el control interno, es la base del modelo de control interno MECI1000, adoptado mediante el Decreto 1599 de 2005. Y COBIT, un marco de referencia para el Gobierno y control de TI basado en un modelo de procesos de TI alineado con COSO mediante la ISO9000 y la ISO27002. La ISO 9000 es el estándar para gestión de calidad en las organizaciones que fue trasladado a las entidades del Estado en la NTCGP 1000, adoptada mediante el Decreto 4140 de 2004 y actualizada mediante el Decreto 4485 de 2009.
Tomado de "Normativa del Gobierno electrónico en Colombia" – Ministerio de las Tecnologías de la Información y las comunicaciones.

LEY 1266 DE 2008

Dicta disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
http://www.secretariasenado.gov.co/senado/basedoc/ley/2008/ley_1266_2008.html

LEY 1273 DE 2009 – LEY DE DELITOS INFORMÁTICOS

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

CAPÍTULO I

"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos"

•Acceso abusivo a un sistema informático

•Obstaculización ilegitima de sistema informático o red de telecomunicación
•Interceptación de datos informáticos
•Daño informático
•Uso de software malicioso
•Violación de datos personales
•Suplantación de sitios web para capturar datos personales

CAPÍTULO II

•Hurto por medios informáticos y semejantes
•Transferencia no consentida de activos
http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html

6 DISEÑO METODOLÓGICO PRELIMINAR

6.1 HIPÓTESIS

Considerando la los procedimientos, las acciones tomadas y la infraestructura tecnológica con la que cuenta actualmente el departamento de Informática de la Empresa Aguas y Aguas de Pereira S.A E.S.P, se puede afirmar que el nivel de riesgos de seguridad de la información en los activos para el proceso administrativo: "Departamento de Informática", se encuentra en **un nivel ALTO.**

6.2 TIPO DE INVESTIGACIÓN

La Investigación utiliza un método deductivo y analítico y se clasifica como de tipo descriptiva y explicativa.

6.3 METODOLOGÍA

Para alcanzar los objetivos propuestos en esta investigación, el proyecto se ejecutará en dos etapas. Durante la primera etapa se realizará el inventario de todos los activos del Departamento de Informática; mientras que en la segunda etapa se elaborará el mapa de riesgos del proceso administrativo y se definirá el nivel de riesgo aceptable por la entidad.

6.4 POBLACIÓN

El proyecto está enfocado principalmente al proceso administrativo de la empresa de Acueducto y Alcantarillado de Pereira S.A. E.S.P, en particular al Departamento de Informática. De igual manera, esta investigación es de interés para toda la comunidad universitaria de pregrado y postgrado, que pretendan adelantar trabajos sobre seguridad informática.

7 ESQUEMA TEMÁTICO

7.1 ESTABLECIMIENTO DEL CONTEXTO

7.1.1 CONSIDERACIONES GENERALES [1]

Entrada: Se refiere a toda la información acerca de la organización que es pertinente para establecer el contexto de la gestión del riesgo en la seguridad de la información.

Acción: Se debe establecer el contexto para la gestión del riesgo en la seguridad de la información, lo cual implica establecer los criterios básicos que son necesarios para la gestión del riesgo de la seguridad de la información, definir el alcance y los límites y establecer una organización adecuada que opere la gestión del riesgo de la seguridad de la información.

Guía para la implementación: Es esencial determinar el propósito de la gestión del riesgo en la seguridad de la información ya que esto afecta al proceso total y, en particular, al establecimiento del contexto. En el caso particular de este proyecto, el propósito de la gestión del riesgo en la seguridad de la información para la Empresa de Acueducto y Alcantarillado de Pereira S.A. ESP está dado por los siguientes temas:

- ✓ Dar soporte a un SGSI
- ✓ Conformidad legal y evidencias de una debida diligencia
- ✓ Preparación de un plan para la continuidad del negocio
- ✓ Preparación de un plan de respuesta a incidentes

[1] Tomado en su totalidad del NUMERAL 7.1 del documento NTC- ISO 27005

Salida: Especificación de los criterios básicos, alcance y límites, y organización del proceso de gestión del riesgo en la seguridad de la información.

7.1.2 CRITERIOS BÁSICOS

7.1.2.1 CRITERIOS DE EVALUACIÓN DEL RIESGO

Es muy importante definir los criterios para la evaluación del riesgo, con el fin de determinar el riesgo en la seguridad de la información de la organización. Para tal efecto, se tendrán en cuenta los siguientes aspectos:

- ✓ El valor estratégico del proceso de información del negocio
- ✓ La criticidad de los activos de información involucrados
- ✓ Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- ✓ La importancia de la disponibilidad, confidencialidad e integridad para las operaciones y el negocio.
- ✓ Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación.

Estos criterios de evaluación del riesgo se utilizarán para especificar las prioridades para el tratamiento del riesgo.

7.1.2.2 CRITERIOS DE IMPACTO

Se desarrollarán criterios de impacto del riesgo y se especificarán en términos del grado de daño o de los costos para la organización, causados por un evento de seguridad de la información, considerando aspectos tales como:

- ✓ El nivel de clasificación de los activos de información impactados
- ✓ Brechas en la seguridad de la información (por ejemplo, pérdida de confidencialidad, integridad y disponibilidad)
- ✓ Operaciones deterioradas (partes internas o terceras partes)
- ✓ Pérdida del negocio y del valor financiero
- ✓ Alteración de planes y fechas límite
- ✓ Daños para la reputación
- ✓ Incumplimiento de los requisitos legales, reglamentarios o contractuales

7.1.2.3 CRITERIOS DE LA ACEPTACIÓN DEL RIESGO

Los criterios de aceptación del riesgo no hacen parte del alcance de este documento.

7.1.3 ALCANCE Y LÍMITES [2]

Con el fin de definir el alcance y los límites de la gestión de la seguridad de la información para la Empresa Aguas y Aguas de Pereira se tomó en cuenta la siguiente información:

- **OBJETIVOS ESTRATÉGICOS DEL NEGOCIO**

  Misión

  Gestionamos el recurso hídrico como bien social, generando rentabilidad económica, social y ambiental.

  Visión

  Ser líderes en la gestión integral del agua a nivel nacional, y competir exitosamente en Latinoamérica en servicios de consultoría, comercialización y operación.

  Valores y Principios Corporativos

  Integridad: Hacemos lo correcto, SIEMPRE.

  Preferencia por el cliente: Nos anticipamos a las necesidades de las personas con el fin de superar sus expectativas, lograr su fidelidad y mantener su confianza.

  Responsabilidad Social: Contribuimos al mejoramiento de la calidad de vida basados en el respeto hacia los empleados, la comunidad y el ambiente.

  Mejoramiento Continuo: Buscamos la excelencia.

[2] Información tomada de la página web de la entidad, www.aguasyaguas.com.co

Interés Público: Actuamos con objetividad y responsabilidad en nuestras acciones, garantizando beneficios sociales.

Pensamiento Positivo: Mantenemos una actitud hacia el cambio y logro de los objetivos, alcanzando una dinámica empresarial permanente.

Solidez Empresarial: Generamos riqueza para beneficio de todos.

Política Integrada de Gestión y Control

"En la Empresa de Aguas y Aguas de Pereira es un compromiso permanente la prestación eficiente de los servicios de Agua Potable y Saneamiento Hídrico, conforme a las normas legales, con Responsabilidad Social Empresarial, en coherencia con los siguientes principios:

- Calidad en el agua, fluidez en el servicio y transparencia en la gestión.
- Prevención y mitigación de los impactos ambientales para beneficio de la empresa y su entorno.
- Actitud de servicio para la satisfacción de nuestros clientes y partes interesadas.
- Realización de ensayos de laboratorio técnicamente válidos con personal competente.
- Obtención del máximo bienestar laboral en seguridad y salud ocupacional.
- Gestión continua de los riesgos en todos los componentes del sistema.
- Mejoramiento continuo de los procesos y de la competencia del personal".

Objetivos acordes al principio de la política de calidad de la empresa:

- Crecimiento sostenido de los ingresos y un adecuado control de los costos y gastos de funcionamiento efectivos.
- Gestionar instrumentos de cobertura para deuda en moneda extranjera.
- Mitigación del riesgo financiero y cambiario.

- Mitigación del riesgo por pasivos laboral y pensional.
- Estructuración de un plan de negocios.
- Control Subprocesos de Facturación.
- Disminución tiempos de respuesta en la atención a clientes.
- Evaluación continua e integral del programa de AP y SP.
- Adopción, implementación y evaluación de una cultura que genere valor agregado por unidades de negocio.
- Aseguramiento Sistema Integrado de Calidad y Control.
- Formulación e implementación de la política para la participación de la Empresa en el manejo de las cuencas abastecedoras y receptoras.}
- Proteger la salud de los trabajadores contra los riesgos presentes en los lugares de trabajo.
- Contribuir con el desarrollo de la sociedad.
- Fortalecer la educación y la conciencia ambiental de los habitantes de Pereira, para el conocimiento de los servicios de la Empresa y la conservación del recurso hídrico.
- Actuar bajo criterios técnicos establecidos en la norma ISO IEC 17025 y normas legales.
- Tener altos niveles de desempeño en las labores cotidianas y con nuestros clientes.
- Implementar cultura de gestión de riesgos.
- Mejoramiento continuo de los procesos.
- Redefinir esquema integral de gestión comercial.
- Desarrollo e implementación de un modelo de Gestión por competencias.
- Desarrollar Cultura de Servicio al cliente.
- Monitoreo y seguimiento a la percepción del cliente.

- **PROCESOS DEL NEGOCIO**

Tabla 1. Macroproceso de Apoyo. Aguas y Aguas de Pereira

MACROPROCESO DE APOYO		
PROCESO	**SUBPROCESO**	**PROCEDIMIENTO**
SISTEMA DE INGENIERIA Y ADMINISTRACION DE PROYECTOS	FORMULACION Y EJECUCION DE PROYECTOS	Formulación y ejecución de proyectos (Preinversión)
	ADMINISTRACIÓN DE PROYECTOS	Precontractual para selección de proveedores y adquisiciones de bienes, consultorías, interventorías y obras
	INTERVENTORIA	Interventoria o coordinación de interventoria
	RECIBO A USUARIOS DE INFRAESTRUCTURAS NUEVAS	Requerimientos técnicos y comerciales para la conexión de los servicios públicos domiciliarios de Acueducto y Alcantarillado Aprobación proyectos hidrosanitarios de edificaciones y urbanizaciones Recibo nueva infraestructura de servicios de acueducto y alcantarillado
	GESTION SOCIOAMBIENTAL	Programa "Cultura del agua" Seguimiento Socioambiental de Obras
	CENTRO DE INFORMACIÓN GEOREFERENCIADA	Actualización Información Espacial
SISTEMA DE PROVISION DE RECURSOS	GESTION DE ALMACENAMIENTO	Recepción de Mercancías Manejo y almacenamiento de mercancía Entrega y legalización de mercancía Devolución de mercancía al proveedor
	GESTION JURIDICA	Contratación
	GESTION DEL TALENTO HUMANO	Gestión del Talento Humano
	GESTION INFORMATICA	Mantenimiento y soporte a plataforma tecnológica Gestión de usuarios sistema de información corporativo Soporte a usuario final Gestión de seguridad
	GESTION DE COMPRAS	Adquisición de bienes y servicios Selección y evaluación de proveedores Control y custodia de bienes muebles

Fuente: www.aguasyaguas.com.co

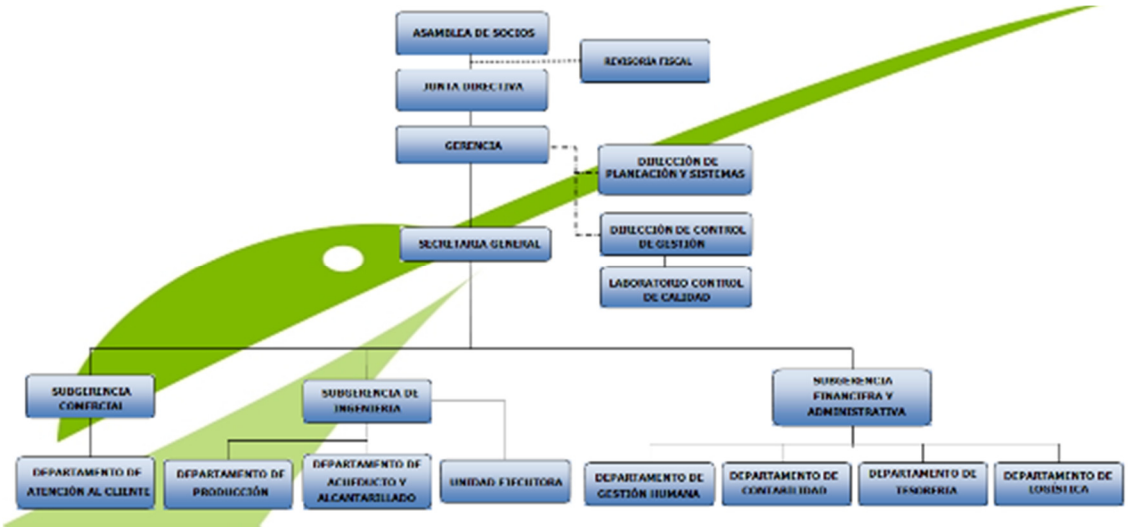
Tabla 2. Macroprocesos de Apoyo y Gerencial. Aguas y Aguas de Pereira

MACROPROCESO DE APOYO		
PROCESO	**SUBPROCESO**	**PROCEDIMIENTO**
SISTEMA DE REGISTRO E INFORMACION	GESTION CONTABLE Y TRIBUTARIA	Trámite de cuentas Interface de nómina Informes y trámites con entidades de control y vigilancia Declaraciones tributarias nacionales y municipales Conciliaciones Cierre contable Activación de obras Archivo de la información
	GESTION DE TESORERIA	Control de Egreso Control de Ingresos Deuda pública Inversiones Auditoría Financiera de Recaudos
	GESTION DE PRESUPUESTO	Formulación del presupuesto Ejecución del presupuesto Evaluación del presupuesto y presentación de informes
	GESTION DE COSTOS	Administración Sistema de Costos Conciliación Inventarios - Contabilidad Proyecciones Financieras e indicadores de corto plazo
MACROPROCESO GERENCIAL		
PROCESO	**SUBPROCESO**	**PROCEDIMIENTO**
SISTEMA DE DIRECCION	DIRECCION GERENCIAL	N/A
	PLANIFICACION	Aplicación tarifaria
	LABORATORIO CONTROL DE CALIDAD	Recolección de muestras Análisis de Calidad Equipos Servicio al Cliente Estimación de Incertidumbre de Medición Validación de Ensayos
	SISTEMA INTEGRADO DE CALIDAD Y CONTROL	Manual de Calidad Elaboración, revisión y aprobación de documentos Gestión de Riesgos Retos de calidad Control de registros Auditorías internas de Calidad Acciones Correctivas, Preventivas Actualización y Verificación del Cumplimiento Legal

Fuente: www.aguasyaguas.com.co

- **ESTRUCTURA DE LA ORGANIZACIÓN**

Ilustración 1. Organigrama Aguas y Aguas de Pereira



Fuente: www.aguasyaguas.com.co

- **IDENTIFICACIÓN DE ACTIVOS**

Los activos se identifican en el numeral 8.1.1.1.

El alcance del proceso de gestión del riesgo en la seguridad de la información dentro de este documento es la ejecución del análisis de riesgos para el proceso administrativo de la Empresa Aguas y Aguas de Pereira, y está limitado al Departamento de Informática de la entidad.

7.2 SITUACIÓN ACTUAL DE INFRAESTUCTURA TECNOLÓGICA

SERVIDORES

La empresa Aguas y Aguas cuenta con una granja de servidores Unix, Linux y Windows los cuales soportan las aplicaciones del negocio y los servicios de red para usuarios, brindando capacidad de almacenamiento, procesamiento, controles de seguridad y conectividad.

Actualmente la Empresa cuenta con una Plataforma robusta, estable y actualizada.

A continuación se presentan los servidores que soportan los respectivos servicios de TI en la Empresa:

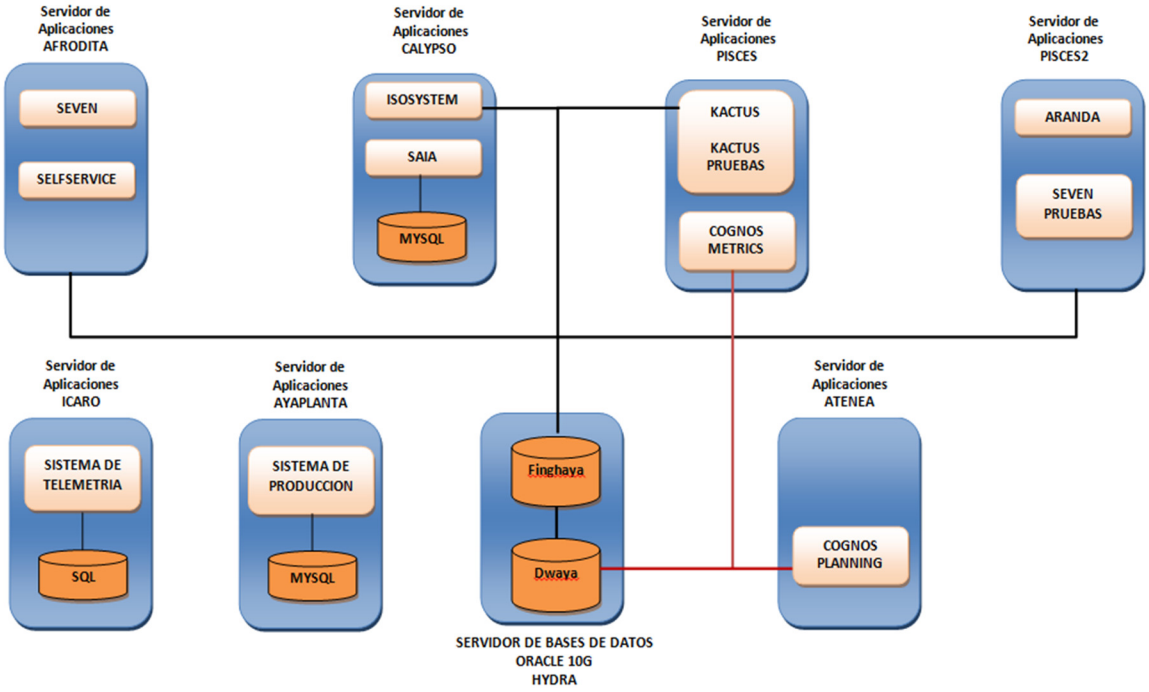
Tabla 3. Estado actual de la Plataforma Tecnológica de Aguas y Aguas de Pereira

ESTADO ACTUAL DE LA PLATAFORMA TECNOLOGICA DE SERVIDORES DE LA EMPRESA AGUAS Y AGUAS DE PEREIRA S.A. E.S.P			
SERVIDOR	**NOMBRE**	**SISTEMA OPERATIVO**	**SERVICIO**
IBM PSERIES 520	HYDRA	AIX 5L Versión 6.1	BASES DE DATOS ORACLE 10G SERVIDOR TSM
IBM PSERIES 630 (Contingencia)	NEPTUNO	AIX 5L Versión 6.1	BASES DE DATOS ORACLE 10G DE CONTINGENCIA
IBM XSERIES 3650	ATENEA	Windows 2003 Server SP2	COGNOS 8 (ORACLE 10G)
STORAGE MANAGER DS4300	-	DS Storage Manager 9 Client	ALMACENAMIENTO DE COPIAS DE SEGURIDAD (Discos Asignados a PISCES3)
STORAGE MANAGER DS4700	-	DS Storage Manager 10 Client	ALMACENAMIENTO DE BASES DE DATOS (Discos Asignados a servidores Hydra y Neptuno)
IBM BLADE CENTER S	Sistema compuesto por dos cuchillas HS22 las cuales tienen instalado el sistema de Virtualizacion VMware Vsphere Essentials Plus 4.0 con el cual se tienen virtualizados 9 servidores actualmente. 2 discos duros internos de 146 GB en raid 1 en cada cuchilla 2 discos discos Near Line SAS en Raid 1 en Storage del Blade Center 4 discos duros SAS de 146 GB en Raid 5 en Storage del Blade center 2 discos duros SAS de 2TB en Raid 1 en Storage del Blade Center 4 discos duros SAS de 2TB en Raid 5 en Storage del Blade Center	VMware Vsphere Essentials Plus 4.0	CUCHILLA 1 - Servidor de Correo AQUARIUS - Servicor de Aplicaciones Pisces2 - Servidor de Aplicaciones Calypso - Servidor VCENTER
		VMware Vsphere Essentials Plus 4.0	CUCHILLA 2 -Servidor de Aplicaciones Apolo - Servidor de Intranet Cetus - Servidor de Aplicaciones Afrodita - ServiDor de Aplicaciones Pisces - Servidor Web Atlas
SERVIDOR DE CORREO (VM)	AQUARIUS	Red Hat Enterprise Linux ES release 4	CORREO CORPORATIVO
SERVIDOR DE APLICACIONES (VM)	PISCES	Windows 2000 Server SP4	KACTUS COGNOS METRICS (ORACLE 10G) ARANDA
SERVIDOR DE APLICACIONES (VM)	CALYPSO	Windows 2003 Server SP1	SAIA (Mysql) ISOSYSTEM (ORACLE 10G)
SERVIDOR VCENTER (VM)	VCENTER	Windows 2008 Server SP1 64BIT	Pendiente por Instalcion de VCENTER
SERVIDOR DE APLICACIONES (VM)	APOLO	Windows 2008 Server SP1 64BIT	ORION COSTMANAGER (ORACLE 10G)
SERVIDOR INTRANET (MV)	CETUS	Red Hat Enterprise Linux ES release 4	INTRANET Y SERVICIOS DE RED (MYSQL)
SERVIDOR DE APLICACIONES (VM)	AFRODITA	Windows 2003 Server SP1	SISTEMA ERP SEVEN (ORACLE 10G)
SERVIDOR DE APLICACIONES (VM)	PICES2	Windows 2000 Server SP4	SEVEN de Pruebas
SERVIDOR WEB (MV)	ATHLAS	CentOS release 5.6	SITIO WEB EMPRESARIAL (MYSQL)
HP PROLIANT NL150 G6	ICARO	Windows 2008 Server SP1	SISTEMA DE TELEMETRIA SQL SERVER
HP PROLIANT NL150 G6	AYAPLANTA	Windows 2008 Server SP1	SISTEMA DE LABORATORIO (MYSQL)
IBM XSERIES 225(Contingencia)	CETUSBK	Red Hat Enterprise Linux ES release 4	INTRANET Y SERVICIOS DE RED CONTINGENCIA
IBM XSERIES 225(contingecia)	AQUIARIUSBK	Red Hat Enterprise Linux ES release 4	CORREO - WEB CONTINGENCIA
IBM XSERIES 225 (backups)	PISCES3	Windows 2000 Server SP4	COPIAS DE SEGURIDAD Y CONTINGENCIA
SWITCHES SAN 24B	-	-	Conectividad en fibra optica de servidores de bases de datos y sistemas de almacenamiento
TAPE DRIVE TS2240	Copias de Seguridad en unidades		
FIREWALL UTM FORTIGATE	Dispositivo de Seguridad Perimetral UTM FORTIGATE 200B	v4.0,build0324, 110520 (MR2 Patch 7)	FIREWALL - ANTIVIRUS - UTM - VPN
ANTISPAM FORTIMAL	Dispositivo de Seguridad Perimetral ANTISPAM FORTIMAIL 100C	v4.0,build0103,091223 (GA Patch 1)	ANTISPAM - ANTIVIRUS

Fuente: Elaboración propia

Diagrama de comunicación de Bases de Datos

Ilustración 2. Diagrama de comunicación de Bases de Datos



Fuente: Elaboración propia

ELEMENTOS DE RED Y SEGURIDAD

La red de la Empresa Aguas y Aguas de Pereira, se basa actualmente en Switches 3com de última generación y capacidad de trabajo en Capa 3, así como también algunas características de seguridad como soporte 802.1x, ACL y Calidad de Servicio.

El Switch CORE de la Red es un 3com 4900 de 12 puertos el cual interconecta a todos los pisos del edificio en los cuales esta situada la Empresa. Esta interconexión se hace a través de Transceivers con fibra Óptica a 1Gbps.

Los Switchs de Borde, son equipos 3com 4500 con capacidad de trabajo en capa3 y con conexiones redundantes al switch CORE.

Existe una red Wireless 3com administrada por un Wireless controller WX1200, el cual permite acceso tanto para los equipos de la Empresa como para equipos de Visitantes. En cada piso se establecen dos Access Point los cuales son administrador por el Switch WX1200.

El acceso a internet se realiza a través de un canal dedicado de 4Mbps el cual es gestionado por a través de una interface en un equipo Fortigate de propiedad de la Empresa.

Para la comunicación entre sedes, se cuenta con canales de datos dedicados con velocidades de 2MB para Almacén y 2Mb para Sede Producción.

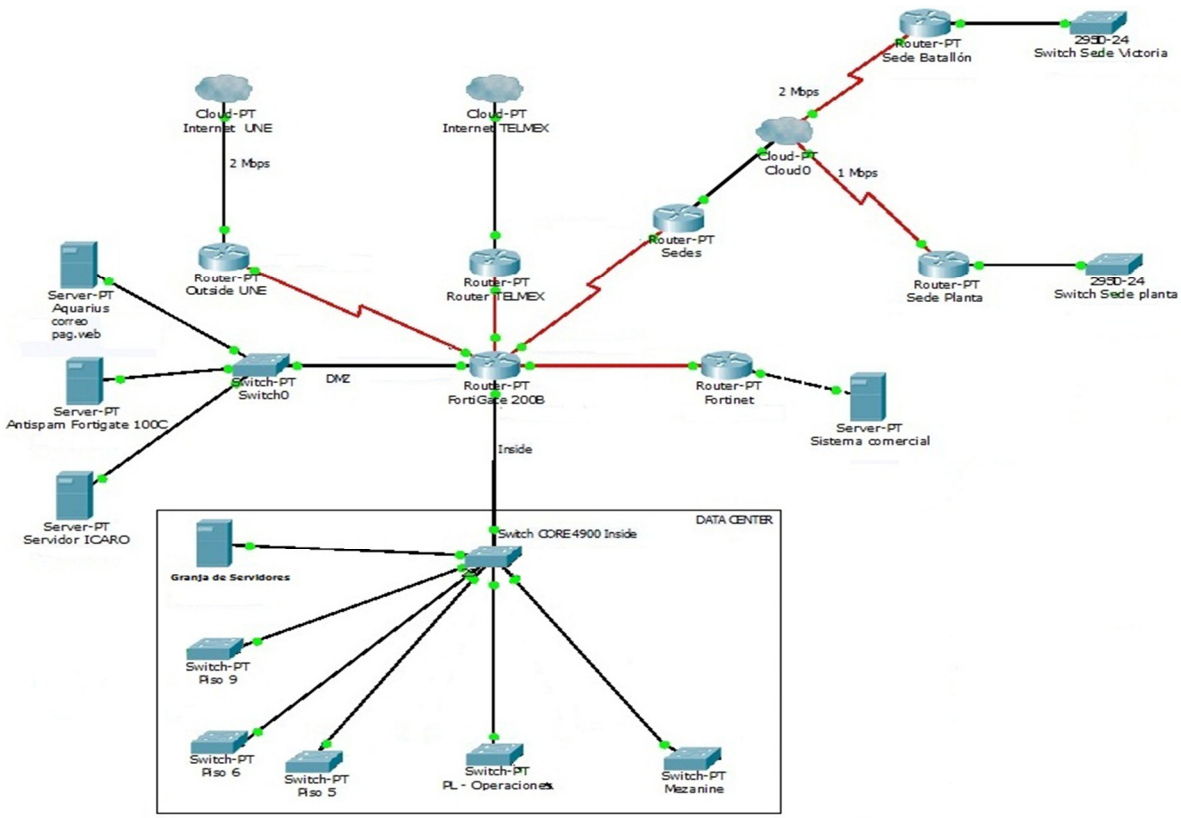
A nivel de Seguridad Perimetral, se cuenta con dos dispositivos Firewall Fortigate y Antispam for mail, los cuales a través de políticas definidas, permiten el servicio de internet, la interconexión entre las diferentes zonas como DMZ, Outside e Inside y restringen el paso de correo basura hacia los buzones de correo de los usuarios.

Todos los usuarios internos navegan a través de servicio Proxy interno que permite limitar y controlar la navegación.

A continuación se presenta el diagrama de conexión de red:

DIAGRAMA DE CONEXIÓN DE SWITCHES Y ROUTER DE INTERNET

Ilustración 3. Diagrama de conexión de switchs y router de internet



Fuente: Elaboración propia

En la arquitectura actual no hay evidencia de una red de gestión con monitoreo permanente de eventos de seguridad, sin embargo se usan herramientas de gestión basadas en SNMP v1 para detectar caídas del servicio.

Toda la arquitectura de red está enfocada a entregar un alto rendimiento a los servidores y aplicaciones que soporta, con controles de seguridad de capa 3 del modelo OSI hacia arriba, en particular en el perímetro de Internet.

APLICACIONES

Las aplicaciones de la Empresa Aguas y Aguas de Pereira están basadas fundamentalmente en Oracle y MySql.

La mayoría de las aplicaciones están desarrolladas en arquitectura Cliente Servidor y Cliente servidor Web.

A continuación se presenta el listado de aplicaciones de la división de sistemas

SIC - SISTEMA DE INFORMACIÓN COMERCIAL:

Es el sistema que se encarga de todo lo relacionado con la comercialización del servicio de acueducto y alcantarillado, contiene toda la información con que se realiza la facturación de los servicios que presta la empresa a los ciudadanos de Pereira.

Lo integran los módulos: Lectura y Crítica, Reclamos, Cartera, Corte, Recaudo, Solicitudes, Consultas y Reportes, Facturación.

SEVEN - SISTEMA DE INFORMACIÓN FINANCIERO Y ADMINISTRATIVO:

Sistema integrado para administrar la información financiera y administrativa de la Empresa. Compuesto por 3 módulos principales: Financiero, Administrativo, Gestión Comercial (Utilizado para facturas servicios adicionales prestados por la Empresa).

KACTUS - SISTEMA DE RECURSOS HUMANOS Y NÓMINA:

Sistema para la administración de los recursos humanos y nómina de la Empresa. Compuesto por 11 módulos (Reclutamiento, Selección, Análisis de cargos, Evaluación del Desempeño, Biodata, Nómina y Administración de Salarios,

Educación y Capacitación, Salud Ocupacional, Bienestar de Personal, Indicadores de Gestión, Formación y Desarrollo).

COGNOS METRICS MANAGER - COGNOS 8:

Es una aplicación Web que permite componer de una forma sencilla un cuadro de mando y ofrecer a la empresa la posibilidad de supervisar y gestionar un gran número de métricas clave en todos los niveles de la organización.

COGNOS 8 PLANNING:

Cognos 8 Planning es una solución completamente integrada, de vanguardia y escalable, para realizar los procesos de planificación, presupuestación y forecast. Cognos 8 Planning integra la planificación operacional y financiera en tiempo real para obtener una visibilidad inmediata sobre las necesidades de recursos y el rendimiento futuro del negocio.

INTRANET:

La Empresa cuenta con un sistema Intranet en ambiente web, el cual a través de su administración permite a los usuarios tener servicios de Red tales como Correo electrónico, Intranet corporativa, Internet y unidades de red compartidas.

SISTEMA DE CALIDAD – ISOSYSTEM

Sistema en ambiente web, para la gestión y administración de Calidad de la Empresa. Cuenta con 15 usuarios activos conectados en forma concurrente.

SISTEMA DE GESTIÓN DOCUMENTAL – SAIA

Sistema en ambiente web para la gestión y acceso unificado de documentos producidos y recibidos por la Empresa. Cuenta con 370 usuarios activos conectados en forma concurrente.

SISTEMA DE TELEMETRÍA

Sistema en ambiente web para la administración de la información referente a datos propios de telemetría en los tanques de almacenamiento ubicados en diferentes puntos de la ciudad.

TSM (TIVOLI STORAGE MANAGER)

Sistema en ambiente web para la administración de las copias de seguridad de la Información empresarial.

SISTEMA DE COSTOS – ABC

Sistema de información que agrupa los costos y gastos de acuerdo a las actividades de cada proceso. Actualmente se encuentran 5 usuarios activos.

8 VALORACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN

8.1 ANÁLISIS DEL RIESGO

8.1.1 IDENTIFICACIÓN DEL RIESGO

8.1.1.1 IDENTIFICACIÓN DE LOS ACTIVOS

Este capitulo presenta el inventario y clasificación de los activos de información que son manejados por los funcionarios de la empresa a través del proceso GESTIÓN DE INFORMÁTICA, con el fin principal de determinar qué activos posee el área de informática, reconocer el valor de cada activo, los niveles de acceso permitidos, y determinar su clasificación para que sea utilizada adecuadamente.

La realización de un inventario y clasificación de activos de información hace parte de la debida diligencia que a nivel estratégico ha considerado el área de informática dentro de sus elementos a tratar con respecto a la seguridad para los activos de información de la Empresa.

Las mejores prácticas de seguridad de la información a nivel nacional e internacional recomiendan de manera imperativa la realización de un inventario y clasificación de los activos de información de las organizaciones, para determinar cómo deben ser utilizados en los procesos del negocio, los roles y las

responsabilidades que tiene el personal sobre la misma, reconociendo adicionalmente los niveles de confidencialidad que a cada activo debe dársele.

De esta forma y con base en las normas técnicas colombianas NTC ISO/IEC 27001 y NTC ISO/IEC 27002 en el ítem "Gestión de Activos" se persigue dar cumplimiento a tres puntos principales que son explícitos en las mismas así:

Inventario de Activos: Todos los activos deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes de la entidad.

Propiedad de los Activos: Toda la información y los activos asociados con los servicios de procesamiento de información deben ser "propiedad"[3] de una parte designada de la entidad.

Directrices de Clasificación: La información debe clasificarse en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la entidad.

DEFINICIONES

Información: La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades de la organización y, en consecuencia, necesita una protección adecuada[4].

Seguridad de la Información: La seguridad de la información es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de inversiones y oportunidades de negocio[5]. Adicionalmente, se define como la preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.

---

[3] El término "Propietario" identifica a un individuo o a una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término "Propietario" no implica que la persona tenga realmente los derechos de propiedad de los activos.

[4] Tomado de NTC ISO/IEC 27002:2005

[5] Tomado de NTC ISO/IEC 27002:2005

Clasificación de la Información: Es el ejercicio por medio del cual se determina que la información pertenece a uno de los niveles de clasificación estipulados a nivel corporativo. Tiene como objetivo asegurar que la información recibe el nivel de protección adecuado. La información debe clasificarse en términos de la sensibilidad y la importancia para la organización.

Propietario de la Información: Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de definir quienes tienen acceso y que pueden hacer con la información y de determinar cuáles son los requisitos para que la misma se salvaguarde ante accesos no autorizados, modificación, pérdida de la confidencialidad o destrucción deliberada, y al mismo tiempo de definir que se hace con la información una vez ya no sea requerida.

Custodio Técnico: Es una parte designada de la organización, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad (Toma de copias de seguridad, asignar privilegios de: Acceso, Modificaciones, Borrado) que el propietario de la información haya definido, con base en los controles de seguridad disponibles en la organización.

Usuario: Cualquier persona que genere, obtenga, transforme, conserve o utilice información de la organización en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la compañía. Son las personas que utilizan la información para propósitos propios de su labor, adecuados y que tendrán el derecho manifiesto de uso dentro del inventario de información.[6]

INFORMACIÓN A DILIGENCIAR EN EL INVENTARIO

PROPIEDAD

Es un grupo de información que permite determinar la propiedad de los activos y para el cual la tabla de inventario define los siguientes campos:

Nombre del Activo: Es un campo que define la manera como se va a reconocer el activo de información en el proceso y la entidad, con un nombre particular y diferenciable.

[6] Las personas que se relacionan con la Empresa de Acueducto y alcantarillado de Pereira S.A E.S.P, están obligadas a utilizar la información a la cual tengan acceso en virtud de sus funciones o relación contractual, exclusivamente para el ejercicio de las mismas"

Descripción del activo: Información adicional que permita identificar de manera única el activo de información o su importancia dentro de la entidad o proceso. Esta información también permite determinar si el activo de información comprende otros activos.

Propietario[7].

Custodio Técnico[8].

TIPO

Se define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:

PROC (proceso): Procesos, subprocesos y actividades del negocio.

INF (Información): Corresponde a este tipo de activos, datos, sistemas de información e información almacenada o procesada física o electrónicamente como por ejemplo: las bases de datos, archivos de datos, contratos, acuerdos, documentación del sistema, información sobre investigaciones, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro, pruebas de auditoría e información archivada física o electrónicamente.

SOF (Software): Dentro de este tipo de activos se encuentran, ofimática, herramientas de propósito específico, herramientas de desarrollo, utilidades, aplicaciones para acceso a la información.

HAR (Hardware): Son activos como por ejemplo: Equipos de computación, equipos de comunicaciones, medios removibles, instrumentos particulares para la ejecución del proceso y otros equipos físicos.

RED (Redes): Todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información.

PER (Personal): Todos los grupos de personas involucradas en el sistema de información.

ACCESO

[7] Ver definiciones.

[8] Ver Definiciones

El grupo de información denominado “Acceso” permite identificar que usuarios han sido formalmente declarados y autorizados a hacer uso de la información y adicionalmente identificar que tipos de acceso se manejan del activo para cada usuario o grupo de usuarios. Los siguientes son los campos de información que se encuentran en la tabla de inventario:

Usuarios: son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

Derechos de Acceso: Hace referencia a los usuarios y permisos establecidos para el uso del activo de información. Se sugiere los siguientes:

(L) lectura, consulta o (E) Escritura.

(M) Modificación.

(B) Borrado, eliminación.

UBICACIÓN

Es la información acerca de donde se encuentra específicamente ubicado el activo, puede ser un archivo físico de oficina, archivo digital, sistema de información, computador, base de datos, o aplicación.

Para este grupo de información se indica si el activo se encuentra disponible en medio físico o en medio electrónico.

Física: Especifica la ubicación física del activo de información por ejemplo: archivadores, archivos de áreas, centro de cómputo, oficinas, entre otros.

Electrónica: Especifica la ubicación de los activos de información digitales que tienen ubicación electrónica por ejemplo: servidores, intranet, direcciones IP, equipos de trabajo, entre otros.

Atributos de Clasificación

A cada activo de información se le relacionó uno o más atributos, los cuales permiten identificar su sensibilidad y justificar el valor asignado al activo y adicionalmente permitirán obtener elementos que permitan darle un tratamiento adecuado. Los atributos asociados al activo de información y que se

tiene como información de referencia en la matriz de inventario y clasificación de activos de información es la siguiente:

A1: Activo de información de clientes o terceros que debe protegerse, de accesos no autorizados, pérdida de integridad o indisponibilidad.

A2: Activo de información que debe ser restringido a un número limitado de funcionarios.

A3: Activo de información que debe ser restringido a personas externas a la Empresa.

A4: Activo de información que puede ser alterado o comprometido para fraudes ó corrupción.

A5: Activo de información que es muy crítico para las operaciones internas de la Empresa.

A6: Activo de información que es muy crítico para la prestación de servicio a terceros, tales como ciudadanos, organismos de control, u otras organizaciones.

A7: Activo de información que ha sido declarado de conocimiento público por parte de la persona con autoridad para hacerlo o por alguna norma jurídica.

Valor

Este es un grupo de información para el cual se define y deben ser ingresados valores en el rango desde Muy Bajo hasta Muy Alto para cada uno de los campos. Esta información nos indica el valor que tiene el activo para La Empresa, o específicamente para el proceso, ya que uno de los criterios importantes de su clasificación es en términos de su valor. A continuación se define el significado de cada campo presente en la tabla de inventario:

C (Confidencialidad): Protección para que el activo de información sea accesible solamente por aquellas personas autorizadas para ello. En este campo en el inventario se presenta uno de los siguientes valores:

Tabla 4. Descripción de los criterios de confidencialidad para los activos de información

CRITERIO	DESCRIPCION	EXPLICACION
MA	Muy Alto	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente La Empresa.
A	Alto	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente a la Empresa
MA	Medio	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente de manera importante al proceso.
B	Bajo	El conocimiento o divulgación no autorizada de este activo de información impacta negativamente de manera leve al proceso.
MB	Muy Bajo	El conocimiento o divulgación no autorizada de este activo de información no tiene ningún impacto negativo en el proceso.

Fuente: Elaboración propia

I (Integridad): protección de la exactitud y estado completo de la información y sus métodos de procesamiento.

Tabla 5. Descripción de los criterios de integridad de la información

CRITERIO	DESCRIPCION	EXPLICACION
MA	Muy Alto	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos impacta negativamente La Empresa.
A	Alto	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos impacta negativamente a la Empresa.
MA	Medio	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos impacta negativamente de manera importante al proceso.
B	Bajo	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos impacta negativamente de manera leve al proceso.
MB	Muy Bajo	La pérdida de exactitud y estado completo de la información y de los métodos de procesamientos no tiene ningún impacto negativo en el proceso.

Fuente: Elaboración propia

D (Disponibilidad): Garantizar que los usuarios autorizados tengan acceso a los activos de información cada vez que los requieren.

Tabla 6. Descripción de los criterios de disponibilidad de los activos de información

CRITERIO	DESCRIPCION	EXPLICACION
MA	Muy Alto	La falta del activo de información impacta negativamente la Empresa
A	Alto	La falta del activo de información impacta negativamente a la Empresa
MA	Medio	La falta del activo de información impacta negativamente de manera importante al proceso.
B	Bajo	La falta del activo de información impacta negativamente de manera leve al proceso.
MB	Muy Bajo	La falta del activo de información no tiene ningún impacto negativo en el proceso.

Fuente: Elaboración propia

V (Valor): En este campo se encuentra definido el valor que tiene el activo de información para la Empresa, o específicamente para el proceso teniendo en cuenta las características valoradas:

Tabla 7. Descripción de los criterios del valor del activo de información

CRITERIO	DESCRIPCION	EXPLICACION
MA	Muy Alto	La perdida de confidencialidad, integridad o disponibilidad del activo de información impacta negativamente La Empresa.
A	Alto	La perdida de confidencialidad, integridad o disponibilidad del activo de información impacta negativamente La Empresa.
MA	Medio	La perdida de confidencialidad, integridad o disponibilidad del activo de información impacta negativamente de manera importante al proceso.
B	Bajo	La perdida de confidencialidad, integridad o disponibilidad del activo de información impacta negativamente de manera leve al proceso.
MB	Muy Bajo	La perdida de confidencialidad, integridad o disponibilidad del activo de información no tiene ningún impacto negativo en el proceso.

Fuente: Elaboración propia

CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados. La información con base en su valor y de acuerdo a los requisitos de confidencialidad tiene diferentes grados de protección o manejo especial que se definen en la clasificación de activos de información.

En este capítulo se define el esquema de clasificación para estipular los niveles de protección para cada activo de información y señalar las consideraciones especiales de manejo, restricciones, distribución, almacenamiento y destrucción de la información.

Definición

La clasificación de los activos de información del Área de Informática de Aguas y Aguas se basa en la información del inventario consignado en este documento. Se define un esquema de clasificación que se basa en los siguientes componentes:

1) Niveles de Clasificación

- ✓ Niveles de Acceso.
- ✓ Métodos de Distribución.
- ✓ Restricciones en la Distribución Electrónica.

- ✓ Almacenamiento y Archivado.
- ✓ Destrucción.
- ✓ Penalizaciones por revelación deliberada de la información.

Cada activo de información tendrá asociado un único nivel de clasificación. Cada nivel de clasificación posee características propias de protección, manejo y tratamiento del activo de información en cuanto a: Niveles de Acceso, Métodos de Distribución, Restricciones en la Distribución Electrónica, Almacenamiento, Archivado, Disposición y Destrucción. Una vez que a un activo de información le es asignado un nivel de clasificación este adquiere las características específicas anteriormente mencionadas para el nivel específico asignado.

Adicionalmente para cada activo de información se definen unos atributos de clasificación, estos indican propiedades adicionales y específicas que cada activo de información posee y las cuales permiten identificar el nivel de riesgo base inherente a cada activo de información.

Como resultado de esta clasificación se genera una tabla de clasificación de los activos de información del proceso Gestión de Informática.

Niveles de Clasificación y de Confidencialidad

Los Niveles de Clasificación y Confidencialidad de los activos del proceso Gestión de Informática son los siguientes:

Niveles de Clasificación

Pública: La información pública del proceso Gestión de Informática es la información que ha sido declarada de conocimiento público de acuerdo a alguna norma jurídica o por parte de la persona o grupo de personas del área con autoridad para hacerlo. Esta información puede ser entregada o publicada sin restricciones a los funcionarios o a cualquier persona sin que esto implique daños a terceros ni a las actividades y procesos de la Empresa.

Confidencial: La información confidencial del proceso Gestión de Informática es toda aquella información que no es Pública y que además no ha sido aún clasificada en este documento. A la información confidencial sólo pueden tener acceso las personas que expresamente han sido declaradas usuarios legítimos de

esta información, y con los privilegios asignados, tal como aparece consignado en el inventario de activos de información.

A esta categoría se asocia la información propiedad de terceros que el área de informática utiliza bajo acuerdos de confidencialidad o por licencias de uso. Los directores definirán cual información es Reservada o Confidencial.

La información confidencial debe ser entendida como: La existencia de información más crítica a nivel de pérdida de su confidencialidad que otra y que por ende debe tener una mayor protección.

La información que es confidencial hoy puede llegar a ser pública en un momento posterior, de conocimiento público para un conjunto de personas y parte de ella es pública para la comunidad en general en algunos casos.

Para saber cuándo puede permitírsele el acceso y uso de la información a personas distintas a las responsables de la misma y para poder establecer el grado de protección que se le debe aplicar a la información de la empresa, es necesario clasificarla totalmente en términos de su confidencialidad.

Para realizar una clasificación más precisa y fácil de manejar se definen tres grados de confidencialidad de la información para la Empresa: de uso interno, restringida y altamente restringida. A continuación encontramos su definición específica:

Uso Interno

Es toda información consignada en el inventario de activos de información que es utilizada por el personal de la Empresa para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma leve a terceros o a los sistemas y/o procesos de la Empresa.

Restringida

Información que es utilizada por solo un grupo de funcionarios para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin autorización del propietario de la información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma importante a terceros o a los sistemas y/o procesos de la institución.

Altamente Restringida

Información que es utilizada por solo un grupo de funcionarios para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin autorización especial de la entidad. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma grave a terceros o a los sistemas de la Empresa.

Para el esquema de clasificación de la confidencialidad de la información de la Empresa, la relación que se establece entre los niveles de Clasificación es como se muestra en la ilustración 4.

Ilustración 4. Niveles de Clasificación de confidencialidad de información de Aguas y Aguas

Fuente: Elaboración propia

CARACTERÍSTICAS Y RECOMENDACIONES DE MANEJO PARA LOS DIFERENTES NIVELES DE CLASIFICACIÓN

Tabla 8. Características y recomendaciones de manejo para los niveles de clasificación

	Nivel de clasificacion			
	Publica	**Uso Interno**	**restringida**	**Altamente restringida**
1. Definición	La información pública de la Empresa de Acueducto y Alcantarillado de Pereira. es la información que ha sido declarada de conocimiento público de acuerdo a alguna norma jurídica o por parte de la persona o grupo de personas de la Empresa de Acueducto y Alcantarillado de Pereira. con autoridad para hacerlo. Esta información puede ser entregada o publicada sin restricciones a los funcionarios o a cualquier persona sin que esto implique daños a terceros ni a las actividades y procesos de la Empresa.	Es toda información consignada en el inventario de activos de información que es utilizada por el personal de la Empresa de Acueducto y Alcantarillado de Pereira. para realizar sus labores en los procesos y que no puede ser conocida por terceros sin autorización del propietario del activo. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma leve a terceros o a los sistemas y/o procesos de la Empresa.	Información que es utilizada por solo un grupo de funcionarios para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin autorización del propietario de la información. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma importante a terceros o a los sistemas y/o procesos de la Empresa.	Información que es utilizada por solo un grupo de funcionarios para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin autorización especial de la Entidad. En caso de ser conocida, utilizada o modificada por personas sin la debida autorización, impactaría de forma grave a terceros o a los sistemas de información.
2. Criterio de Definición de Confidencialidad	Calificación del activo: Muy baja (MB):" La perdida de confidencialidad, integridad o disponibilidad del activo de información no tiene ningún impacto negativo en el proceso." Atributos: A2: "No está restringida a un número limitado de funcionarios". A3: "No restringida a personas externas". A7: "Declarado de conocimiento público". Baja (B): " La perdida de confidencialidad, integridad o disponibilidad del activo de información impacta negativamente de manera leve al proceso."	Calificación del activo Baja (B): " La perdida de confidencialidad, integridad o disponibilidad del activo de información impacta negativamente de manera leve al proceso." Media (M): " La perdida de confidencialidad, integridad o disponibilidad del activo de información impacta negativamente de manera importante al proceso." Atributos: A3: "Restringida a personas externas"	Calificación del activo: Alta (A): " La perdida de confidencialidad, integridad o disponibilidad del activo de información impacta negativamente a la Empresa". Atributos: A2: "Restringido a un número determinado de funcionarios".	Calificación del activo: Muy Alta (MA): " La perdida de confidencialidad, integridad o disponibilidad del activo de información impacta negativamente a la Empresa".
3. Acceso permitido	Todos (Cualquier persona Interna o Externa)	Todos los funcionarios de la Empresa de Acueducto y Alcantarillado de Pereira y contratistas con un compromiso firmado de confidencialidad y con autorización del propietario para su uso.	Solo los Usuarios expresamente autorizados en el Inventario de activos y subcontratistas con un compromiso firmado confidencialidad y con autorización del propietario para su uso.	Funcionarios de Aguas y Aguas con un compromiso firmado de confidencialidad de información y con autorización formal de la gerencia para acceder a esta información.

4. Etiquetado				
a. Documentos en Papel	a. No es requerido	a. No es requerido, queda a discreción del propietario de la información. En caso de etiquetarse, si un documento que se haya impreso no posee el campo "Nivel de Confidencialidad", prediligenciado por medio de formato electrónico, entonces se deberá etiquetar con un sello de tinta correspondiente a su clasificación en su primera página como mínimo.	SI, es obligatorio por parte del Propietario de la información. Si un documento que se haya impreso no posee el campo "Nivel de Confidencialidad", prediligenciado por medio de formato electrónico, entonces se deberá etiquetar con un sello de tinta correspondiente a su clasificación en su primera página como mínimo.	SI, es obligatorio por parte del Propietario de la información. Si un documento que se haya impreso no posee el campo "Nivel de Confidencialidad", prediligenciado por medio de formato electrónico, entonces se deberá etiquetar con un sello de tinta correspondiente a su clasificación en su primera página como mínimo.
b. Archivos Electrónicos (Texto, Word, Excel, dibujos, planos, etc.)	b. No es requerido.	b. No es requerido, queda a discreción del propietario de la información. En caso de etiquetarse los documentos o información que estén en archivos electrónicos se les deben agregar un campo de información que indique el nivel de clasificación del mismo y que hagan parte de los formatos manejados.	SI, es obligatorio por parte del Propietario de la información. Los documentos o información que estén en archivos electrónicos se les deben agregar un campo de información que indique el nivel de clasificación del mismo y que hagan parte de los formatos manejados.	SI, es obligatorio por parte del Propietario de la información. Los documentos o información que estén en archivos electrónicos se les deben agregar un campo de información que indique el nivel de clasificación del mismo y que hagan parte de los formatos manejados.
c. Aplicaciones	c. No es requerido.	c. No es requerido, queda a discreción del propietario de la información. En caso de etiquetarse, las aplicaciones que procesen o almacenen temporal o indefinidamente información, y si lo permiten, se les debe agregar un cuadro de diálogo en donde se informe su nivel de clasificación.	SI, es obligatorio por parte del Propietario de la información. Las aplicaciones que procesen o almacenen temporal o indefinidamente información, y si lo permiten, se les debe agregar un cuadro de diálogo en donde se informe su nivel de clasificación.	SI, es obligatorio por parte del Propietario de la información. Las aplicaciones que procesen o almacenen temporal o indefinidamente información, y si lo permiten, se les debe agregar un cuadro de diálogo en donde se informe su nivel de clasificación.

d. Carpetas en Sistemas	d. No es requerido	d. No es requerido, queda a discreción del propietario de la información. En caso de etiquetarse, las carpetas en servidores de archivos o en PCS se les deben colocar un nombre o identificador distintivo (icono en algunos sistemas) con el nivel de clasificación a cada carpeta que almacena la información clasificada.	SI, es obligatorio por parte del Propietario de la información. Las carpetas en servidores de archivos o en PCS se les debe colocar un nombre o identificador distintivo (ícono en algunos sistemas) con el nivel de clasificación a cada carpeta que almacena la información clasificada.	SI, es obligatorio por parte del Propietario de la información. Las carpetas en servidores de archivos o en PCS se les debe colocar un nombre o identificador distintivo (ícono en algunos sistemas) con el nivel de clasificación a cada carpeta que almacena la información clasificada.
5. Método de distribución recomendado				
a. Internamente	a. Ninguno. Esta información puede distribuirse en cualquier medio al público en general, incluso a cualquier ente o persona por fuera de la Empresa.	Electrónica: Mediante el sistema de correo electrónico de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. y a través de las redes de datos y sistemas de La Alcaldía Mayor de Bogotá D.C. únicamente. Se debe evitar en lo posible manejar esta información en dispositivos de almacenamiento externo (Diskets, CDS, DVD's, memorias USB, SD, etc.) que no sean autorizados por La Alcaldía Mayor de Bogotá D.C. Física: Proceso de manejo de correspondencia interno.	Electrónica: Mediante el sistema de correo electrónico de la Secretaría General de la Alcaldía Mayor de Bogotá D.C. y a través de las redes de datos y sistemas de la únicamente. Se debe evitar en lo posible manejar esta información en dispositivos de almacenamiento externo (Diskets, CDS, DVD's, memorias USB, SD, etc.) que no sean autorizados por la Secretaría General de la Alcaldía Mayor de Bogotá D.C. Física: Proceso de manejo de correspondencia interno, verificando que el destinatario si es un usuario autorizado en el inventario de activos de información, de otra forma se requiere de autorización por parte del propietario de la información.	Electrónico: Solo en la red de la Alcaldía Mayor de Bogotá D.C. y los archivos deberán estar cifrados, la entrega se hace solo a un destinatario legitimo del inventario de activos de información. (Se recomienda el uso de certificado digital en el correo electrónico) Física: Entrega directa, firma de recepción personal requerida no transferible, entregada por el propietario de la información directamente.

b. Hacia Terceros	b. Ninguno. Esta información puede distribuirse en cualquier medio al público en general, incluso a cualquier ente o persona por fuera de la entidad.	Debe ser entregada a un tercero solo si es una obligación contractual o de negocio bien conocida o si hay una autorización formal del propietario de la información para su entrega. Electrónica: Si se entrega en medio electrónico en lo posible se debe tener los archivos y/o datos de acceso de solo lectura. Se puede entregar la información vía e-mail a destinatarios con cuentas por fuera de la Empresa. Se debe evitar utilizar listas de distribución al momento de enviar este tipo de información. Física: Si es posible se debería entregar solo en medio físico (Papel), el menor número de copias posible, y solo al receptor autorizado, firmando una carta de recibido.	Debe ser entregada a un tercero solo si es una obligación contractual o de negocio bien conocida o si hay una autorización formal del propietario de la información para su entrega. Electrónica: Si se entrega en medio electrónico en lo posible se debe tener los archivos y/o datos de acceso de solo lectura. No se puede entregar la información vía e-mail a destinatarios con cuentas por fuera de los sistemas de correo de la Empresa si la información no posee clave. Se debe evitar utilizar listas de distribución al momento de enviar este tipo de información. Física: Si es posible se debería entregar solo en medio físico (Papel), el menor número de copias posible, y solo al receptor autorizado, firmando una carta de recibido, mediante la empresa de mensajería contratada para tal fin o directamente por parte del propietario de la información.	Debe ser entregada a un tercero solo si es una obligación contractual o de negocio bien conocida o si hay una autorización formal del propietario de la información para su entrega. Electrónico: Siempre se debe entregar esta información de manera cifrada al destinatario legítimo directamente. (Se debe utilizar certificado digital si se requiere obligatoriamente transmitir por correo electrónico) Físico: En este caso debe utilizarse una empresa de transporte de valores con un proceso formal de verificación del destinatario y entrega directa.
6. Almacenamiento y archivado				
a. Información Impresa.	a. No requiere precauciones especiales. A	a. Se debe establecer una política de escritorio limpio, asegurar el acompañamiento y seguimiento de las acciones de personas externas en las instalaciones.	a. Se debe archivar en áreas seguras bajo llave (Cajones, Cuarto de archivo, estantes, etc.)	a. Se debe archivar en áreas seguras bajo llave (Cajones, Cuarto de archivo, estantes, etc.). Se recomienda guardar este tipo de información en caja fuerte si es posible. Cada vez que se archive asegúrese de que sea por fuera de la vista de otras personas.
b. Información Electrónica	b. No requiere precauciones especiales.	b. Se puede almacenar en cualquier sistema o repositorio siempre y cuando se asegure que no es accesible a personas por fuera de las redes y sistemas de información de Aguas y Aguas (i.e. desde Internet,servicios FTP, Web, etc.). Debe existir copia de la información solamente en los medios, sistemas de información o recursos indicados en el campo ubicación del inventario de activos de información.	b. Se debe almacenar en sistemas o repositorios centralizados, bien administrados desde donde se comparta la información, está prohibido dejar sin protección de autenticación de usuario/password esta información y con los privilegios indicados en el inventario de activos de información y los asignados por el propietario a los usuarios autorizados. Debe evitarse almacenar este tipo de información en PCS que no tengan administración formal de seguridad. Debe existir copia de la información solamente en los medios, sistemas de información o recursos indicados en el campo ubicación del inventario de activos de información.	b. Los controles individuales mínimos sugeridos para la información digital son: la autenticación con usuario y contraseña al sistema donde reposa la información y adicionalmente usuario y contraseña para el archivo (si es posible se debe cifrar la información). Si esta información se encuentra en un PC o portátil, al equipo deben tener acceso solo las personas autorizadas, preferiblemente utilizando autenticación fuerte de mínimo dos factores. Debe existir copia de la información solamente en los medios, sistemas de información o recursos indicados en el campo ubicación del inventario de activos de información.

c. e-mail	c. No requiere precauciones especiales.	c. Se debe asegurar que esta información no se envíe a terceros no autorizados para recibirla por este medio.	c. asegúrese de que la información no queda en los elementos enviados y adicionalmente asegúrese de que el backup del correo electrónico se realiza de manera segura (protegido con usuario y contraseña).	c. Se debe evitar en lo posible el uso de este medio, en caso de que sea necesario debe manejarse a través de certificados digitales.
7. Destrucción				
a. Información Impresa.	a. No requiere precauciones especiales.	a. No requiere precauciones especiales.	a. Se deben utilizar máquinas destructoras de papel.	a. Debe utilizarse una destructora de papel pero preferiblemente debe incinerarse y esta acción debe ser llevada a cabo por el propietario del activo.
b. Reciclaje de Papel	b. Es permitido sin restricciones.	b.Es permitido solo para uso interno.	b. No es permitido.	b. No es permitido.
d. Medios de almacenamiento	d. No requiere precauciones especiales.	d. Borrado seguro de información, destrucción física de medios que vayan a desecharse.	d. Borrado seguro de información, destrucción física de medios que vayan a desecharse.	d. Borrado seguro de información, destrucción física de medios que vayan a desecharse.
8. Transmisión Oral				
a. Conversaciones y reuniones	a. No requiere precauciones especiales.	a. Se debe evitar referenciar esta información por fuera de las instalaciones laEmpresa, cuando se lleven a cabo deben ser en conversaciones privadas y en voz baja, evitando en lo posible zonas públicas, tales como elevadores, pasillos, cafeterías, etc.	a. Se debe evitar referenciar esta información por fuera de las instalaciones de la Empresa. al menos que sea una reunión formal por fuera de las mismas. Evite reunirse en salas que no sean cerradas y que no permitan aislar el ruido. Si la información fue anotada en papelógrafos o tableros, o documentos no formales (trozos de papel, libretas o agendas personales, etc.), esta debe ser borrada o destruida inmediatamente se abandone el sitio o se transfiera a un medio formal dispuesto por Empresa (Archivo de Acta, archivo formal de notas, etc.).	a. Se debe evitar referenciar esta información por fuera de las instalaciones de la Empresa al menos que sea una reunión formal por fuera de las mismas. Evite reunirse en salas que no sean cerradas y que no permitan aislar el ruido. En lo posible asegúrese que esta información solo es transmitida solo a las mínimas personas necesarias. Si la información fue anotada en papelógrafos o tableros, o documentos no formales (trozos de papel, libretas o agendas personales, etc.), esta debe ser borrada o destruida inmediatamente se abandone el sitio o se transfiera a un medio formal dispuesto por la Empresa (Archivo de Acta, archivo formal de notas, etc.).

b. Telefónica	b. No requiere precauciones especiales.	b. No se debería entregar información de uso interno a personas no autorizadas por este medio.	b. Evite en lo posible establecer conversaciones telefónicas en donde se maneje este tipo de información, más aun si hay posibles escuchas no autorizados cerca del sitio en donde se encuentra. Si se requiere haga uso de un teléfono en una zona segura o aislada (Sala de reuniones, tele conferencia)	b. Evite establecer conversaciones telefónicas en donde se maneje este tipo de información, más aun si hay posibles escuchas no autorizados cerca del sitio en donde se encuentra. Si se requiere haga uso de un teléfono en una zona segura o aislada (Sala de reuniones, tele conferencia)
c. Voice Mail o maquina de grabación automática de mensajes	c. No requiere precauciones especiales.	c. No se debería entregar información de uso interno a personas no autorizadas por este medio.	c. No se deberían dejar mensajes con este tipo de información	c. No se deberían dejar mensajes con este tipo de información
9. Transmisión por FAX				
a. Localización de la Máquina de FAX	a. No debe estar disponible al público en general (externo)	a. No debe estar disponible al público en general (externo)	a. No debe estar disponible a personas no autorizadas y se debe tener bajo supervisión específica (i.e. Asistente, secretaria, etc.).	a. No debe estar disponible a personas no autorizadas y se debe tener bajo supervisión específica (i.e. Asistente, secretaria, etc.) y en oficina cerrada.
b. Uso de Cubierta de FAX	b. Si se requiere cubierta. Debe identificar a la compañía	b. Si se requiere cubierta. Debe identificar a la compañía	b. Si se requiere cubierta. Debe identificar a la compañía y debe estar etiquetado como confidencial.	b. Se debe evitar la transmisión por FAX, solo con autorización de la gerencia se debe llevar a cabo. En tal caso se debe etiquetar como altamente confidencial.
c. Cuidados en la transmisión	c. No requiere precauciones especiales	b. No se debería entregar información de uso interno a personas no autorizadas por este medio.	c. Es permitido sin restricciones.	c. No se deberían dejar mensajes con este tipo de información

10. Seguridad Física				
a. Estaciones de Trabajo	a. Se debe bloquear el equipo con protección de contraseña apenas se abandone y adicionalmente tener un protector de pantalla que bloquee el equipo en un tiempo corto automáticamente en caso de olvido. En un tiempo más largo se puede configurar la estación para que se apague automáticamente y no quede disponible en la red. Se debe tener un estricto control de vigilancia para el retiro de estaciones de trabajo por fuera de las instalaciones.	a. Se debe bloquear el equipo con protección de contraseña apenas se abandone y adicionalmente tener un protector de pantalla que bloquee el equipo en un tiempo corto automáticamente en caso de olvido. En un tiempo más largo se puede configurar la estación para que se apague automáticamente y no quede disponible en la red. Se debe tener un estricto control de vigilancia para el retiro de estaciones de trabajo por fuera de las instalaciones.	a. Se debe bloquear el equipo con protección de contraseña apenas se abandone y adicionalmente tener un protector de pantalla que bloquee el equipo en un tiempo corto automáticamente en caso de olvido. En un tiempo más largo se puede configurar la estación para que se apague automáticamente y no quede disponible en la red. Se debe tener un estricto control de vigilancia para el retiro de estaciones de trabajo por fuera de las instalaciones.	a. Se debe bloquear el equipo con protección de contraseña apenas se abandone y adicionalmente tener un protector de pantalla que bloquee el equipo en un tiempo corto automáticamente en caso de olvido. En un tiempo más largo se puede configurar la estación para que se apague automáticamente y no quede disponible en la red. Se debe tener un estricto control de vigilancia para el retiro de estaciones de trabajo por fuera de las instalaciones. Conecte lo menos posible la estación a la red de la Empresa o a Internet.
b. Información Impresa en zona de impresión	b. No requiere precauciones especiales.	b. Se debe tener las impresoras por fuera del alcance del público en general y se debe buscar la impresión inmediatamente.	b. Se debe tener las impresoras por fuera del alcance del público en general y se debe buscar la impresión inmediatamente.	b. Se debe tener una persona atendiendo todo el proceso de impresión en la zona de impresoras desde el inicio, esta debe estar autorizada a ver la información.
c. Lap Tops, PDA's	c. No requiere precauciones especiales.	c. No descuide el equipo en zonas que no posean vigilancia o control de salida de equipos.	c. Nunca debe dejarlo solo el equipo y siempre debe utilizar cable de aseguramiento (lockdown cable), y si no es posible se debe dejar bajo vigilancia y cuando se salga de la oficina se debe dejar este bajo llave.	c. Nunca debe dejarlo solo el equipo y siempre debe utilizar cable de aseguramiento (lockdown cable) y si no es posible se debe dejar bajo vigilancia y cuando se salga de la oficina se debe dejar este bajo llave. Se debe procurar tener la información cifrada.

d. Acceso a Oficina	d. No requiere precauciones especiales.	d. No requiere precauciones especiales.	d. El acceso a las áreas que poseen información confidencial debe tener algún tipo de restricción física de acceso (Puerta con llave, tarjeta, vigilancia), este control debe ser aplicado cuando la oficina este desatendida.	d. El acceso a las áreas que poseen información confidencial debe tener algún tipo de restricción física de acceso (Puerta con llave, tarjeta, vigilancia), este control debe ser aplicado cuando la oficina este desatendida.
11.Fotocopiado de Información				
a. Tipo de copias permitidas.	a. No requiere precauciones especiales.	a. No requiere precauciones especiales.	a. Solo cuando sea necesario.	a. Debe ser autorizado por el propietario de la información.

Fuente: Elaboración propia

Procedimiento de clasificación

La clasificación de la información se lleva a cabo bajo el mismo procedimiento del inventario de activos de información (Definición, Revisión, Actualización y Publicación). La diferencia que se suscita es que en la definición después de que el líder de proceso lleva a cabo el levantamiento de información, el responsable del proceso de Gestión de Informática es quien asigna los niveles de clasificación de acuerdo a la información consignada para en matriz de Inventario y clasificación. En este sentido lo que se realiza es el llenado de la columna clasificación con alguno de los siguientes valores:

Pública
Uso Interno
Restringida
Altamente Restringida

Estos valores se consiguen a partir del valor consignado en el campo Valor total del activo y los atributos sobre la información:

Tabla 9. Criterios de clasificación de la información de la empresa Aguas y Aguas de Pereira

Nivel de clasificacion	Definicion	Criterios de clasificacion	
		valor	atributos
Altamente restringida	Utilizada por un grupo de funcionarios y que no puede ser conocida por otros funcionarios o terceros sin autorizacion especial del AREA DE INFORMATICA. En caso de ser conocida, utilizada o modificada por personas sin la debida autorizacion impactaria de forma grave a terceros a los sitemas ya la empresa en general.	**Muy Alto**	
restringida	Utilizada por un grupo de funcionarios y que no puede ser conocida por otros funcionarios o terceros sin autorizacion del PROPIETARIO. En caso de ser conocida, utilizada o modificada por personas sin la debida autorizacion impactaria de forma importante a terceros o a los sisstemas y/o procesos de la Empresa.	**Alto**	**A2**
uso interno	Utilizada por un grupo de funcionarios y que no puede ser conocida por terceros sin autorizacion del PROPIETARIO. En caso de ser conocida, utilizada o modificada por personas sin la debida autorizacion, impactaria de forma leve a terceros o a los sisstemas y/o procesos del area de Informatica.	**Medio o Bajo**	**A3**
Publica	Informacion que ha sido declarada de conocimiento publico de acuerdo a alguna norma juridica o por parte d ela persona o grupo de personas con autoridad para hacerlo. Esta informacion puede ser entregada o publicada sin restricciones a los funcionarios o a culaquier persona sin que esto implique daños a terceros ni a las actividades y procesos del Area de Informatica.	**Muy Bajo**	**A2, A3, A7**

Fuente: Elaboración propia

IDENTIFICACIÓN DE ACTIVOS

✓ ACTIVOS PRIMARIOS

PROCESOS DEL NEGOCIO

Tabla 10. Identificación de activos

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
PROCESO: GESTIÓN DE INFORMÁTICA	Brindar soporte a los sistemas de información corporativa y al usuario final.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Información	Lectura, Consulta, Escritura	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

INFORMACIÓN

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
BASES DE DATOS ORACLE	Datos almacenados y con los cuales se alimentan los siguientes sistemas de información: -Sistema de información financiero (SEVEN) -Sistema de información de Recursos Humanos (KACTUS) -Sistema de inteligencia de Negocios BI (COGNOS) -Sistema de Recursos Informáticos (ARANDA)		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Información	Lectura, Consulta, Escritura	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A1,A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
BASES DE DATOS MYSQL	Datos almacenados y con los cuales se alimentan los siguientes sistemas de información: -Sistema de Gestión Documental (SAIA) -Sistema INTRANET		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Información	Lectura, Consulta, Escritura	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A1,A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

- ✓ **ACTIVOS DE SOPORTE**

HARDWARE

EQUIPOS TRANSPORTABLES

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
EQUIPOS DE CÓMPUTO PORTÁTILES **Cantidad: 15**	Computadores portátiles asignados a la Gerencia y subgerencias de la Empresa, así como a la sala de capacitación perteneciente al grupo de información de sistemas.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta, Escritura	Gerencia, Subgerencias y Sala de Capacitación	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Medio

EQUIPOS FIJOS

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SERVIDOR IBM PSERIES 520	Servidor de Bases de Datos ORACLE 10G y Servidor de Backup Tivoli Storage Manager TSM 6.1		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta, Escritura	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SERVIDOR IBM PSERIES 630	Servidor de Bases de Datos ORACLE 10G. Funciona como contingencia de Servidor IBM pseries 520.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta, Escritura	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN	
SERVIDOR IBM XSERES 3650	Servidor de aplicaciones. Sistema de inteligencia de Negocios BI COGNOS	
PROPIETARIO	**CUSTODIO TÉCNICO**	
Grupo de Información y Sistemas	Ingeniero de Servidores	
TIPO	**ACCESO**	**UBICACIÓN**
Hardware	Lectura, Consulta	Datacenter

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SISTEMA IBM BLADECENTER-S	Sistema Blade Center con dos cuchillas HS 22 (servidores físicos) utilizadas para virtualización de servidores.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SERVIDOR DE CORREO (MÁQUINA VIRTUAL)	Servidor de correo corporativo QMAIL.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta, Escritura	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN
SERVIDOR DE APLICACIONES (MÁQUINA VIRTUAL)	Servidor de aplicaciones con los siguientes sistemas de información: - Sistema de Recursos Humanos (KACTUS) - Sistema BI (COGNOS METRICS) - Sistema de recursos informáticos (ARANDA)

PROPIETARIO	CUSTODIO TÉCNICO		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SERVIDOR DE APLICACIONES (MÁQUINA VIRTUAL)	Servidor de aplicaciones con los siguientes sistemas de información: - Sistema de Gestión Documental SAIA - Sistema de Calidad ISOSYSTEM		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta, Escritura	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SERVIDOR DE APLICACIONES (MÁQUINA VIRTUAL)	Servidor de aplicaciones con los siguientes sistemas de información: - Sistema de Costos ORION Cost Manager		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**

A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	**DESCRIPCIÓN**		
SERVIDOR DE APLICACIONES (MÁQUINA VIRTUAL)	Servidor de aplicaciones con los siguientes sistemas de información: - Sistema de información financiera ERP SEVEN		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	**DESCRIPCIÓN**		
SERVIDOR DE APLICACIONES (MÁQUINA VIRTUAL)	Servidor de aplicaciones con los siguientes sistemas de información: - Sistema financiero SEVEN en ambiente de pruebas		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	**DESCRIPCIÓN**
SERVIDOR DE INTRANET Y SERVICIOS DE RED (MÁQUINA VIRTUAL)	Servidor de Intranet y servicios de red. - Servidor Proxy - Servidor DHCP - Servidor de dominio SAMBA - Servidor DNS

	- Servidor mensajería instantánea Openfire		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Ingeniero de Servidores		
TIPO Hardware	**ACCESO** Lectura, Consulta, Escritura	**UBICACIÓN** Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO **SERVIDOR WEB (MÁQUINA VIRTUAL)**	**DESCRIPCIÓN** Servidor del sitio Web de la Empresa.		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Ingeniero de Servidores		
TIPO Hardware	**ACCESO** Lectura, Consulta, Escritura	**UBICACIÓN** Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO **SERVIDOR HP PROLIANT NL150 G6**	**DESCRIPCIÓN** Servidor del Sistema de información de telemetría de la Empresa.		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Ingeniero de Servidores		
TIPO Hardware	**ACCESO** Lectura, Consulta	**UBICACIÓN** Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**

A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO		**DESCRIPCIÓN**	
SERVIDOR HP PROLIANT NL150 G6		Servidor del Sistema de información de Laboratorio de la Empresa.	
PROPIETARIO		**CUSTODIO TÉCNICO**	
Grupo de Información y Sistemas		Ingeniero de Servidores	
TIPO	**ACCESO**		**UBICACIÓN**
Hardware	Lectura, Consulta		Datacenter
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO		**DESCRIPCIÓN**	
SERVIDOR IBM XSERIES 225		Servidor de intranet y servicios de red (CONTINGENCIA)	
PROPIETARIO		**CUSTODIO TÉCNICO**	
Grupo de Información y Sistemas		Ingeniero de Servidores	
TIPO	**ACCESO**		**UBICACIÓN**
Hardware	Lectura, Consulta		Datacenter
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	**DESCRIPCIÓN**
SERVIDOR IBM XSERIES 225	Servidor de Correo y Servidor Web (CONTINGENCIA)
PROPIETARIO	**CUSTODIO TÉCNICO**
Grupo de Información y Sistemas	Ingeniero de Servidores

TIPO	ACCESO	UBICACIÓN
Hardware	Lectura, Consulta	Datacenter

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN
SERVIDOR IBM XSERIES 225	Servidor de copias de respaldo para las Bases de Datos de misión critica (CONTINGENCIA)
PROPIETARIO	**CUSTODIO TÉCNICO**
Grupo de Información y Sistemas	Ingeniero de Servidores

TIPO	ACCESO	UBICACIÓN
Hardware	Lectura, Consulta	Datacenter

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN
EQUIPOS DE CÓMPUTO PC **Cantidad: 6**	Computadores de mesa (PC) asignados al área de Gerencia.
PROPIETARIO	**CUSTODIO TÉCNICO**
Grupo de Información y Sistemas	Profesional III

TIPO	ACCESO	UBICACIÓN
Hardware	Lectura, Consulta, Escritura	Gerencia

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN
	Computadores de mesa (PC) asignados al área de

EQUIPOS DE CÓMPUTO PC **Cantidad: 11**	Secretaría General.		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Profesional III		
TIPO Hardware	**ACCESO** Lectura, Consulta, Escritura	**UBICACIÓN** Secretaría General	
ATRIBUTOS A2,A3,A4	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
	Medio	Medio	Medio

NOMBRE DEL ACTIVO **EQUIPOS DE CÓMPUTO PC** **Cantidad: 13**	**DESCRIPCIÓN** Computadores de mesa (PC) asignados al área de Dirección de Planeación y Sistemas.		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Profesional III		
TIPO Hardware	**ACCESO** Lectura, Consulta, Escritura	**UBICACIÓN** Dirección de Planeación y Sistemas	
ATRIBUTOS A2,A3,A4	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
	Medio	Medio	Medio

NOMBRE DEL ACTIVO **EQUIPOS DE CÓMPUTO PC** **Cantidad: 15**	**DESCRIPCIÓN** Computadores de mesa (PC) asignados al área de Dirección de Control de Gestión.
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Profesional III

TIPO	ACCESO	UBICACIÓN
Hardware	Lectura, Consulta, Escritura	Dirección de Control de Gestión

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN
EQUIPOS DE CÓMPUTO PC **Cantidad: 52**	Computadores de mesa (PC) asignados al área de Subgerencia Comercial.
PROPIETARIO	**CUSTODIO TÉCNICO**
Grupo de Información y Sistemas	Profesional III

TIPO	ACCESO	UBICACIÓN
Hardware	Lectura, Consulta, Escritura	Subgerencia Comercial

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN
EQUIPOS DE CÓMPUTO PC **Cantidad: 85**	Computadores de mesa (PC) asignados al área de Subgerencia de Ingeniería.
PROPIETARIO	**CUSTODIO TÉCNICO**
Grupo de Información y Sistemas	Profesional III

TIPO	ACCESO	UBICACIÓN
Hardware	Lectura, Consulta, Escritura	Subgerencia de Ingeniería

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
EQUIPOS DE CÓMPUTO PC **Cantidad: 46**	Computadores de mesa (PC) asignados al área de Subgerencia Financiera		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura, Consulta, Escritura	Dirección de Subgerencia Financiera	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Medio

PERIFÉRICOS DE PROCESAMIENTO

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet 4515	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Atención al cliente	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Mezanine	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
HP LaserJet 3015	Impresora Láser
PROPIETARIO	**CUSTODIO TÉCNICO**
Medición	Profesional III

TIPO Hardware	**ACCESO** Lectura	**UBICACIÓN** Mezanine	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO **HP LaserJet 2420**	**DESCRIPCIÓN** Impresora Láser		
PROPIETARIO Cartera	**CUSTODIO TÉCNICO** Profesional III		
TIPO Hardware	**ACCESO** Lectura	**UBICACIÓN** Mezanine	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO **HP LaserJet Personal**	**DESCRIPCIÓN** Impresora Láser		
PROPIETARIO Atención al Cliente	**CUSTODIO TÉCNICO** Profesional III		
TIPO Hardware	**ACCESO** Lectura	**UBICACIÓN** Mezanine	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	**DESCRIPCIÓN** Impresora Láser

HP LaserJet 3005			
PROPIETARIO	**CUSTODIO TÉCNICO**		
Almacén	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Almacén	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	**DESCRIPCIÓN**		
HP LaserJet 3005	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Medición	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Salón Herramientas	Lectura	Almacén	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	**DESCRIPCIÓN**		
HP LaserJet 3800	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet 3055	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet 2420	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Control de Gestión	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet 3005	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Secretaría General	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**

A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO		**DESCRIPCIÓN**	
HP LaserJet 4350		Impresora Láser	
PROPIETARIO		**CUSTODIO TÉCNICO**	
Facturación		Profesional III	
TIPO	**ACCESO**		**UBICACIÓN**
Hardware	Lectura		Piso 5
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO		**DESCRIPCIÓN**	
HP LaserJet 3800 (Color)		Impresora Láser	
PROPIETARIO		**CUSTODIO TÉCNICO**	
Subgerencia Comercial		Profesional III	
TIPO	**ACCESO**		**UBICACIÓN**
Hardware	Lectura		Piso 5
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO		**DESCRIPCIÓN**	
HP LaserJet Personal		Impresora Láser	
PROPIETARIO		**CUSTODIO TÉCNICO**	
Subgerencia Comercial		Profesional III	
TIPO	**ACCESO**		**UBICACIÓN**
Hardware	Lectura		Piso 5

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet 2420	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Base de Redes	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Local 101	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet 3005	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Departamento de Acueducto	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Local 102	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
HP LaserJet 3015	Impresora Láser
PROPIETARIO	**CUSTODIO TÉCNICO**
Subgerencia de Ingeniería	Profesional III

TIPO	ACCESO	UBICACIÓN
Hardware	Lectura	Piso 6

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
HP LaserJet 2420	Impresora Láser
PROPIETARIO	**CUSTODIO TÉCNICO**
Departamento de Gestión Humana	Profesional III

TIPO	ACCESO	UBICACIÓN
Hardware	Lectura	Piso 6

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
HP LaserJet Personal	Impresora Láser
PROPIETARIO	**CUSTODIO TÉCNICO**
Archivo	Profesional III

TIPO	ACCESO	UBICACIÓN
Hardware	Lectura	Piso 6

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
HP LaserJet 3015	Impresora Láser

PROPIETARIO	CUSTODIO TÉCNICO	
Logística	Profesional III	
TIPO	**ACCESO**	**UBICACIÓN**
Hardware	Lectura	Piso 6

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN	
HP LaserJet 3005 color	Impresora Láser	
PROPIETARIO	**CUSTODIO TÉCNICO**	
Subgerencia de Ingeniería	Profesional III	
TIPO	**ACCESO**	**UBICACIÓN**
Hardware	Lectura	Piso 6

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN	
HP LaserJet 3005	Impresora Láser	
PROPIETARIO	**CUSTODIO TÉCNICO**	
Subgerencia de Ingeniería	Profesional III	
TIPO	**ACCESO**	**UBICACIÓN**
Hardware	Lectura	Piso 6

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN

HP LaserJet 3005	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Tesorería	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Piso 6	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	**DESCRIPCIÓN**		
HP LaserJet 2420	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Contabilidad	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Piso 6	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	**DESCRIPCIÓN**		
HP LaserJet 3015	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Gerencia	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Piso 9	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet 4015	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Planeación	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Piso 9	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet 3005 color	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Gerencia	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Piso 9	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet Personal	Impresora Laser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Planeación	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Piso 9	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**

A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO		**DESCRIPCIÓN**	
HP LaserJet 1522		Impresora Láser	
PROPIETARIO		**CUSTODIO TÉCNICO**	
Departamento de Producción		Profesional III	
TIPO	**ACCESO**		**UBICACIÓN**
Hardware	Lectura		Planta de Tratamiento
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO		**DESCRIPCIÓN**	
HP LaserJet 3015		Impresora Láser	
PROPIETARIO		**CUSTODIO TÉCNICO**	
Departamento de Producción		Profesional III	
TIPO	**ACCESO**		**UBICACIÓN**
Hardware	Lectura		Planta de Tratamiento
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO		**DESCRIPCIÓN**	
HP LaserJet 1522		Impresora Láser	
PROPIETARIO		**CUSTODIO TÉCNICO**	
Departamento de Producción		Profesional III	
TIPO	**ACCESO**		**UBICACIÓN**
Hardware	Lectura		Planta de Tratamiento

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet 2605 color	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Mantenimiento	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Planta de Tratamiento	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
HP LaserJet 4100	Impresora Láser		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Departamento de Producción	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Planta de Tratamiento	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Alto

MEDIOS PARA ALMACENAMIENTO DE DATOS

NOMBRE DEL ACTIVO	DESCRIPCIÓN
IBM STORAGE MANAGER DS4700	Sistema de almacenamiento en discos, el cual aloja toda la información referente a bases de datos Oracle y sistemas operativos de servidor de bases de datos en producción y servidor de bases de datos de contingencia.

PROPIETARIO	CUSTODIO TÉCNICO		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
IBM STORAGE MANAGER DS4300	Sistema de almacenamiento en discos, el cual aloja copias de seguridad realizadas a diferentes servidores de la Empresa.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
IBM TAPE DRIVE TS2240	Sistema de Copias de seguridad en unidades de cinta magnética.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Hardware	Lectura	Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
CINTAS IBM TAPE ULTRIUM 4 **Cantidad 5**	Cintas magnéticas para copias de seguridad de la información de los servidores y bases de datos de la Empresa.
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Ingeniero de Servidores

TIPO	ACCESO	UBICACIÓN
Hardware	Lectura, Consulta, Escritura	Datacenter

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

SOFTWARE

SISTEMAS OPERATIVOS

NOMBRE DEL ACTIVO	DESCRIPCIÓN
SISTEMA OPERATIVO WINDOWS XP	Licencias de Sistema Operativo Windows XP instalado en equipos de cómputo de la Empresa.
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Profesional III

TIPO	ACCESO	UBICACIÓN
Software	Consulta	Piso 5

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A1,A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN
SISTEMA OPERATIVO WINDOWS VISTA	Licencias de Sistema Operativo Windows Vista instalado en equipos de cómputo de la Empresa.

PROPIETARIO	CUSTODIO TÉCNICO		
Grupo de Información y Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Consulta	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A1,A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SISTEMA OPERATIVO WINDOWS 7	Licencias de Sistema Operativo Windows 7 instalado en equipos de cómputo de la Empresa.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Consulta	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A1,A2,A3,A4	Medio	Medio	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SISTEMA OPERATIVO WINDOWS 2000 Server	Licencias de Sistema Operativo Windows 2000 Server instalado en Servidores de la Empresa.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Consulta	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A1,A2,A3,A4	Alto	Alto	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SISTEMA OPERATIVO WINDOWS 2003 Server	Licencias de Sistema Operativo Windows 2003 Server instalado en Servidores de la Empresa.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Consulta	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A1,A2,A3,A4	Alto	Alto	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SISTEMA OPERATIVO WINDOWS 2008 Server	Licencias de Sistema Operativo Windows 2008 Server instalado en Servidores de la Empresa.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Consulta	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A1,A2,A3,A4	Alto	Alto	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN	
SISTEMA OPERATIVO LINUX	Licencias de Sistema Operativo Linux Server instalado en Servidores de la Empresa.	
PROPIETARIO	**CUSTODIO TÉCNICO**	
Grupo de Información y Sistemas	Ingeniero de Servidores	
TIPO	**ACCESO**	**UBICACIÓN**
Software	Consulta	Piso 5

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A1,A2,A3,A4	Alto	Alto	Alto

SOFTWARE ESTANDAR

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
MOTOR DE BASES DE DATOS ORACLE 10G	Software de administración de bases de Datos para la administración de la información almacenada para los diferentes sistemas de información.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero Administrador de Bases de Datos		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Consulta	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A1,A2,A3,A4	Alto	Alto	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
MOTOR DE BASES DE DATOS MYSQL	Software de administración de bases de Datos para la administración de la información almacenada para los diferentes sistemas de información.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero Administrador de Bases de Datos		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Consulta	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A1,A2,A3,A4	Alto	Alto	Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
SOFTWARE DE ANTIVIRUS	Software de prevención y detección de amenazas antivirus que pueden surgir en la Empresa a través de diferentes

NORTON SERVER	medios.		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Profesional III		
TIPO Software	**ACCESO** Consulta, Escritura	**UBICACIÓN** Piso 5	
ATRIBUTOS A1,A2,A3,A4	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
	Alto	Alto	Alto

NOMBRE DEL ACTIVO **IBM TIVOLI STORAGE MANAGER**	**DESCRIPCIÓN** Software de administración de copias de Seguridad empresarial.		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Ingeniero de Servidores		
TIPO Software	**ACCESO** Consulta, Escritura	**UBICACIÓN** Piso 5	
ATRIBUTOS A1,A2,A3,A4	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
	Muy Alto	Muy Alto	Muy Alto

APLICACIONES DEL NEGOCIO

NOMBRE DEL ACTIVO **SISTEMA ERP DE LA EMPRESA SEVEN**	**DESCRIPCIÓN** Sistema ERP de la Empresa. Permite realizar la gestión financiera y administrativa de la Empresa		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Tecnólogo III		
TIPO Software	**ACCESO** Lectura, consulta, Escritura	**UBICACIÓN** Subgerencia Financiera	
ATRIBUTOS	**VALOR**		

	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A1,A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SISTEMA DE GESTION HUMANA KACTUS	Sistema HR de la Empresa. Permite realizar la administración del recurso humano y nómina de la Empresa		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Tecnólogo III		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Lectura, consulta, Escritura	Subgerencia Financiera	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A1,A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SISTEMA DE GESTIÓN DOCUMENTAL SAIA	Sistema de administración de archivo y administración del flujo documental de la Empresa.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Lectura, consulta, Escritura	Todas las Dependencias	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
SISTEMA DE BUSINESS INTELLIGENCE - COGNOS	Sistema de inteligencia de negocios de la Empresa. Permite realizar la administración de indicadores de gestión y bodega de datos de la Empresa.

PROPIETARIO	CUSTODIO TÉCNICO
Grupo de Información y Sistemas	Ingeniero de Servidores

TIPO	ACCESO	UBICACIÓN
Software	Lectura, consulta, Escritura	Subgerencia Financiera

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
SISTEMA DE CALIDAD DE LA EMPRESA ISOSYSTEM	Sistema de calidad de la Empresa. Permite realizar la administración financiera de la Empresa

PROPIETARIO	CUSTODIO TÉCNICO
Grupo de Información y Sistemas	Ingeniero de Servidores

TIPO	ACCESO	UBICACIÓN
Software	Lectura, consulta, Escritura	Todas las Dependencias

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A1,A2,A3,A4,A5,A6	Alto	Alto	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN
SISTEMA DE COSTOS DE LA EMPRESA COSTMANAGER	Sistema de costos ABC de la Empresa.

PROPIETARIO	CUSTODIO TÉCNICO
Grupo de Información y Sistemas	Tecnólogo III

TIPO	ACCESO	UBICACIÓN
Software	Lectura, consulta, Escritura	Subgerencia Financiera

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SISTEMA ARANDA	Sistema de administración de recursos informáticos de la Empresa. Permite administrar el inventario de hardware, software y mesa de ayuda.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Profesional III		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Lectura, consulta, Escritura	Grupo de Información y Sistemas	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Alto	Alto	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SISTEMA INTRANET	Sistema de colaboración interna de la Empresa		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	**ACCESO**	**UBICACIÓN**	
Software	Lectura, consulta, Escritura	Todas las Dependencias	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Muy Alto	Muy Alto	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN	
SISTEMA DE CORREO ELECTRÓNICO	Sistema de correo electrónico de la Empresa.	
PROPIETARIO	**CUSTODIO TÉCNICO**	
Grupo de Información y Sistemas	Ingeniero de Servidores	
TIPO	**ACCESO**	**UBICACIÓN**
Software	Lectura, consulta, Escritura	Todas las Dependencias

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Muy Alto	Muy Alto	Medio

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
SITIO WEB EMPRESARIAL	Sitio Web de la Empresa.		
PROPIETARIO	CUSTODIO TÉCNICO		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	ACCESO	UBICACIÓN	
Software	Lectura, consulta, Escritura	Todas las Dependencias	
ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Bajo	Alto	Alto

RED

MEDIOS Y SOPORTE

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
CANAL DE INTERNET UNE	Canal de Internet para el servicio de navegación.		
PROPIETARIO	CUSTODIO TÉCNICO		
Grupo de Información y Sistemas	Ingeniero de Servidores		
TIPO	ACCESO	UBICACIÓN	
Red	consulta	Datacenter	
ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Medio	Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN

CANAL DE INTERNET TELMEX	Canal de Internet para el servicio de Telemetría.		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Ingeniero de Servidores		
TIPO Red	**ACCESO** consulta	**UBICACIÓN** Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Alto	Muy Alto

NOMBRE DEL ACTIVO **RED INALÁMBRICA INTERNA**	**DESCRIPCIÓN** Red de datos Wi-Fi para uso empresarial.		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Tecnólogo III		
TIPO Red	**ACCESO** consulta	**UBICACIÓN** Todas las Áreas de la Empresa	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Alto	Muy Alto

NOMBRE DEL ACTIVO **CANAL DE DATOS SEDES REMOTAS**	**DESCRIPCIÓN** Canal de Datos para la comunicación de la sede principal con las sedes remotas.		
PROPIETARIO Grupo de Información y Sistemas	**CUSTODIO TÉCNICO** Ingeniero de Servidores		
TIPO Red	**ACCESO** consulta	**UBICACIÓN** Datacenter	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Medio	Alto	Muy Alto

RELEVOS PASIVOS O ACTIVOS

NOMBRE DEL ACTIVO	DESCRIPCIÓN
FIREWALL FORTIGATE 200B	Sistema Firewall y dispositivo de seguridad perimetral UTM de la Empresa.
PROPIETARIO	**CUSTODIO TÉCNICO**
Grupo de Información y Sistemas	Ingeniero de Servidores

TIPO	ACCESO	UBICACIÓN
Red	Lectura, Consulta	Datacenter

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
ANTISPAM FORTIMAIL 100C	Sistema AntiSpam y dispositivo de seguridad perimetral de la Empresa.
PROPIETARIO	**CUSTODIO TÉCNICO**
Grupo de Información y Sistemas	Ingeniero de Servidores

TIPO	ACCESO	UBICACIÓN
Red	Lectura, Consulta	Datacenter

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
SWITCHES SAN 24B	Switches para conectividad en fibra óptica de servidores de Bases de Datos y sistema de almacenamiento.
PROPIETARIO	**CUSTODIO TÉCNICO**
Grupo de Información y Sistemas	Ingeniero de Servidores

TIPO	ACCESO	UBICACIÓN
Red	Lectura, Consulta	Datacenter

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
SWITCHES 3com 4500	Switches para conectividad en entre los diferentes pisos del edificio y el Datacenter.
PROPIETARIO	**CUSTODIO TÉCNICO**
Grupo de Información y Sistemas	Ingeniero de Servidores

TIPO	ACCESO	UBICACIÓN
Red	Lectura, Consulta	Datacenter

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4,A5,A6	Muy Alto	Muy Alto	Muy Alto

PERSONAL

PERSONA A CARGO DE LA TOMA DE DESICIONES

NOMBRE DEL ACTIVO	DESCRIPCIÓN
DIRECTOR DE SISTEMAS	Persona encargada de la toma de decisiones del Área de Sistemas.
PROPIETARIO	**CUSTODIO TÉCNICO**
Director de Sistemas	No Aplica

TIPO	ACCESO	UBICACIÓN
Personal	No aplica	Piso 9

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Muy Alto	Muy Alto	Muy Alto

USUARIOS

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
USUARIOS SISTEMAS DE INFORMACION	Usuarios de las diferentes dependencias de la empresa que hacen uso de los sistemas de información.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Grupo de Información y Sistemas	No aplica		
TIPO	**ACCESO**	**UBICACIÓN**	
Personal	No aplica	Todas las Áreas	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Muy Alto	Muy Alto	Muy Alto

PERSONAL DE OPERACIÓN MANTENIMIENTO

NOMBRE DEL ACTIVO	DESCRIPCIÓN		
PROFESIONAL III	Persona encargada del soporte a usuario final y al sistema de información ARANDA.		
PROPIETARIO	**CUSTODIO TÉCNICO**		
Profesional III	No Aplica		
TIPO	**ACCESO**	**UBICACIÓN**	
Personal	No aplica	Piso 5	
ATRIBUTOS	**VALOR**		
	CONFIDENCIALIDAD	**INTEGRIDAD**	**DISPONIBILIDAD**
A2,A3,A4	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
TECNÓLOGO III	Persona encargada del soporte a los sistemas de información SEVEN, KACTUS, SAIA.
PROPIETARIO	**CUSTODIO TÉCNICO**
Tecnólogo III	No Aplica

TIPO	ACCESO	UBICACIÓN
Personal	No aplica	Piso 5

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
TECNÓLOGO I	Persona encargada del soporte a los sistemas de información SEVEN, KACTUS Y COSTMANAGER.
PROPIETARIO	**CUSTODIO TÉCNICO**
Tecnólogo I	No Aplica

TIPO	ACCESO	UBICACIÓN
Personal	No aplica	Piso 5

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Muy Alto	Muy Alto	Muy Alto

NOMBRE DEL ACTIVO	DESCRIPCIÓN
INGENIERO DE SERVIDORES	Persona encargada del soporte y administración de la plataforma de servidores de la Empresa, así como de la seguridad y los canales de comunicación.
PROPIETARIO	**CUSTODIO TÉCNICO**
Ingeniero de servidores	No Aplica

TIPO	ACCESO	UBICACIÓN
Personal	No aplica	Piso 5

ATRIBUTOS	VALOR		
	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
A2,A3,A4	Muy Alto	Muy Alto	Muy Alto

Fuente: Elaboración propia

8.1.1.2 IDENTIFICACIÓN DE AMENAZAS

Tabla 11. Nomenclatura para identificación de amenazas

A	Accidental
D	Deliberada
E	Ambiental

Fuente: Elaboración propia

Tabla 12. Identificación de amenazas

TIPO	AMENAZA	ORIGEN
Daño fisico	Fuego	A,D,E
	Daño por Agua	A,D,E
	Polvo, Corrosion,Congelamiento	A,D,E
	Destruccion de Equipos o Medios	A,D,E
Eventos Naturales	Fenomenos Climaticos	E
	Fenomenos Sismicos	E
	inundación	E
Perdida de los Servicios esenciales	Falla en el suministro de Agua o de aire acondicionado	A,D
	Perdida de Suministro de Energia	A,D,E
	Falla en equipo de telecomunicaciones	A,D
Perturbacion debida a la radiacion	Radiacion electromagnetica	A,D,E
Compromiso de la Información	Espionaje remoto	D
	Pirateria	D
	Ingenieria social	D
	Accesos no autorizados a los sistemas	D
	Escucha Subrepticia	D
	Suplantacion de Identidad	D
	Hurto de medios o documentos	D
	Hurto de Equipo	D
	Recuperacion de Medios reciclados o Desechados	D
	Divulgación	A,D
	Datos provenientes de fuentes no confiables	A,D
	Manipulacion con Hardware	D
	Manipulacion con software	A,D
	Software Malicioso	A,D
Fallas Técnicas	Falla del equipo	A
	Mal funcionamiento de equipo	A
	Saturacion del sistema de informacion	A,D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimieno del sistema de información	A,D
	Incumplimiento en el mantenimieno de equipo	A,D
Acciones no autorizadas	Uso no autorizado de Equipos	A,D
	Copia fraudulenta de software	D
	Uso de Sofware falso o copiado	A,D
	Corrupcion de los datos	D
	Procesamiento ilegal de los datos	D
	Allanamieto Ilegal	A,D

Fuente: Elaboración propia

8.1.1.3 IDENTIFICACIÓN DE CONTROLES EXISTENTES

Tabla 13. Nomenclatura para la identificación de controles

ESTADO		
INEFICAZ	INSUFICIENTE	INJUSTIFICADO

Fuente: Elaboración propia

Tabla 14. Identificación de Controles existentes

CONTROLES EXISTENTES	ESTADO DE IMPLEMENTACION	UTILIZACION
FIREWALL DE SEGURIDAD PERIMETRAL	IMPLEMENTADO 100%	100%
ANTISPAM	IMPLEMENTADO 100%	100%
ANTIVIRUS DE SEGURIDAD PERIMETRAL	IMPLEMENTADO 100%	100%
ANTIVIRUS DE SEGURIDAD INTERNA	IMPLEMENTADO 100%	100%
POLITICAS DE NAVEGACION Y DE USO DE CORREO INTERNO	INSUFICIENTE	70%
SISTEMAS SE AUTENTICACION MAGNETICA EN ACCESOS	INSUFICIENTE	90%
AUTENTICACION A NIVEL DE DOMINIO EN LA RED	INSUFICIENTE	90%
PERMISOS DE ACCESOS A LA INFORMACION COMPARTIDA EN AL RED	INSUFICIENTE	90%
COPIAS DE SEGURIDAD DE LA INFORMACION DE LOS SERVIDORES	INSUFICIENTE	90%
COPIAS DE SEGURIDAD DE LA INFORMACION DE LOS USUARIOS	INSUFICIENTE	90%
SISTEMAS DE RESPALDO ELECTRICO	IMPLEMENTADO 100%	100%

Fuente: Elaboración propia

8.1.1.4 IDENTIFICACIÓN DE VULNERABILIDADES

Tabla 15. Identificación de vulnerabilidades

TIPO	VULNERABILIDAD	AMENAZA
HARDWARE	Mantenimiento insuficiente de los medios de almacenamiento	Incumplimiento en el mantenimieno del sistema de información
	Falta de esquemas de reemplazo periódico.	Destrucción del equipo o los medios.
	Susceptibilidad a la humedad, el polvo y la suciedad.	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Falta de control de cambio con configuración eficiente	Error en el uso
	Susceptibilidad a las variaciones de tensión	Pérdida del suministro de energía
	Susceptibilidad a las variaciones de temperatura	Fenómenos meteorológicos
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Defectos de Fabrica en el HW	Incumplimiento en el mantenimieno del sistema de información
	Obsolecencia de Hardware	Incumplimiento en el mantenimieno del sistema de información
	Falta de configuracion de respaldos o equipos de contingencia	Incumplimiento en el mantenimieno del sistema de información
	Copia no controlada	Hurto de medios o documentos
SOFTWARE	Falta o insuficiencia de la prueba del software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Falta de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	Abuso de los derechos
	Falta de pruebas de auditoría	Abuso de los derechos
	Distribución errada de los derechos de acceso	Abuso de los derechos
	Software de distribución amplia	Corrupción de datos
	Utilización de los programas de aplicación a los datos errados en términos de tiempo	Corrupción de datos
	Interfase de usuario complicada	Error en el uso
	Falta de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Falta de mecanismos de identificación y autentificación, como la autentificación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Procesamiento ilegal de datos
	Software nuevo o inmaduro	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación con software
	Falta de copias de respaldo	Manipulación con software
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de medios o documentos
	Falta de Actualizacion de Sisitemas Operativos y Aplicaciones	Mal funcionamiento del software Software Malicioso
	Falla en la producción de informes de gestión	Uso no autorizado del equipo

RED	Falta de prueba del envío o la recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha subrepticia
	Tráfico sensible sin protección	Escucha subrepticia
	Conexión deficiente de los cables	Falla del equipo de telecomunicaciones
	Punto único de falla	Falla del equipo de telecomunicaciones
	Arquitectura insegura de la red	Espionaje remoto Piratería
	Transferencia de contraseñas autorizadas	Espionaje remoto Piratería
	Gestión inadecuada de la red (capacidad de recuperación del enrutamiento)	Saturación del sistema de información
PERSONAL	Ausencia del personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error en el uso Uso no autorizado de Equipos
	Uso incorrecto de software y hardware	Error en el uso
	Falta de conciencia acerca de la seguridad	Error en el uso
	Falta de mecanismos de monitoreo	Procesamiento ilegal de los datos
	Falta de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado del equipo Piratería
LUGAR	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Falta de protección física de las puertas y ventanas de la edificación	Hurto de equipo Fuego
ORGANIZACIÓN	Falta de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Falta de procedimiento de monitoreo de los recursos de procesamiento información	Abuso de los derechos
	Falta de auditorías (supervisiones) regulares	Abuso de los derechos
	Falta de procedimientos de identificación y evaluación de riesgos	Abuso de los derechos
	Falta de reportes sobre fallas incluidos en los registros de administradores y operador	Abuso de los derechos
	Falta o insuficiencia en el acuerdo a nivel de servicio	Incumplimiento en el mantenimiento del sistema de información
	Falta de procedimiento de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Falta de planes de continuidad	Falla del equipo
	Faltas de politicas de Seguridad	Hurto de equipo Hurto de medios o documentos Uso no autorizado del equipo Uso de software falso o copiado Espionaje remoto

Fuente: Elaboración propia

8.1.1.5 IDENTIFICACIÓN DEL IMPACTO

En relación al impacto, se consideran las siguientes posibilidades:

- Se pierde la información/conocimiento.
- Terceros podrían tener acceso a la información/conocimiento.
- La información ha sido manipulada o está incompleta.
- La información/conocimiento o persona no está disponible.
- Hay dudas acerca de la legitimidad de la fuente de la información.

8.1.2 ESTIMACIÓN DEL RIESGO

8.1.2.1 METODOLOGÍA PARA LA ESTIMACION DEL RIESGO

Este análisis de riesgo se realiza con diferentes grados de detalle teniendo en cuenta la criticidad de los activos y las vulnerabilidades conocidas para la empresa. Se utiliza una metodología de estimación con datos cualitativos. Se utiliza una estimación cualitativa para obtener una indicación general del nivel de riesgo y revelar los riesgos más importantes.
Para la estimación cualitativa se utiliza una escala de atributos calificativos para describir la magnitud de las consecuencias potenciales (insignificante, bajo, mediano, alto) y la probabilidad de que ocurran dichas consecuencias.

8.1.2.2 EVALUACIÓN DE LAS CONSECUENCIAS (IMPACTO)

Para valorar el impacto en los elementos de información, se considera la siguiente escala:

Tabla 16. Evaluación del impacto

1	**Insignificante**	No causa ningún tipo de impacto o daño al Área o la organización.
2	**Bajo**	Causa daño aislado, que no perjudica a ningún componente del Área o de la organización.
3	**Mediano**	Provoca la desarticulación de un componente del Área o de la de la organización. Si no se atiende a tiempo, a largo plazo puede provocar la desarticulación de la organización.
4	**Alto**	En el corto plazo desmoviliza o desarticula a la organización.

Fuente: Elaboración propia

8.1.2.3 EVALUACIÓN DE LA PROBABILIDAD DE INCIDENTES

Valorar la Probabilidad de amenaza que podría causar perjuicio de disponibilidad, confidencialidad, integridad y autenticidad de la información o de los datos institucionales.

Para determinar la probabilidad de amenaza se utilizan las siguientes consideraciones:

• ¿Cuál es el interés o la atracción por parte de individuos externos, de atacarnos?

• ¿Cuáles son nuestras vulnerabilidades?

• ¿Cuántas veces ya han tratado de atacarnos?

Tabla 17. Evaluación probabilidad de ocurrencia de incidentes

1	**Insignificante (Ninguna)**	No existen condiciones que impliquen que el hecho se presente
2	**Baja**	Existen condiciones que hacen muy lejana la posibilidad de que el hecho se presente.
3	**Mediana**	Existen condiciones que hacen poco probable un hecho en el corto plazo pero que no son suficientes para evitarlo en el largo plazo.
4	**Alta**	La realización del hecho es inminente. No existen condiciones internas y externas que impidan el desarrollo del hecho.

Fuente: Elaboración propia

8.1.2.4 NIVEL DE ESTIMACION DEL RIESGO

Tabla 18. Nivel de estimación del riesgo

VULNERABILIDADES - NIVEL DE RIESGO	
NIVEL 1	Se requiere de acciones preventivas inmediatas.
NIVEL 2	Se requiere de acciones preventivas.
NIVEL 3	Se requiere de Acciones preventivas
NIVEL 4	Se requiere seguimiento

Fuente: Elaboración propia

8.2 EVALUACION DEL RIESGO

Criterios para la evaluación del riesgo:

Tabla 19. Criterios para la evaluación del riesgo

CRITERIO	VALORACION DEL RIESGO
No existen controles	Se mantiene el resultado de la evaluación antes de controles.
Los controles existentes no son efectivos	Se mantiene el resultado de la evaluación antes de controles.
Los controles existentes son efectivos pero no están documentados	Cambia el resultado a una casilla inferior de la matriz de evaluación antes de controles (el desplazamiento depende de sí el control afecta el impacto o la probabilidad).
Los controles existentes son efectivos y están documentados	Pasa a escala inferior (el desplazamiento depende de si el control afecta el impacto o la probabilidad).

Fuente: Elaboración propia

Tabla 20. Nivel de riesgo

NIVEL DE RIESGO	
ALTO	Se requiere de acciones inmediatas.
MEDIO	Se requiere de Acciones a mediano plazo.
BAJO	Se requiere acciones a largo plazo

Fuente: Elaboración propia

- **MAPA DEL RIESGO (MATRIZ DE RIESGO)**

Tabla 21. Mapa del riesgo de la Empresa Aguas y Aguas de Pereira

Matriz de Análisis de Riesgo		Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																																			
ACTIVOS SUBPRECESO GESTION DE INFORMATICA	Magnitud de Daño: [1= Insignificante 2 = Baja 3 = Mediana 4 = Alta]	DAÑO FISICO				EVENTOS NATURALES			PERDIDA DE LOS SERVICIOS ESCENCIALES			PERTURBACION DEBIDA A LA RADIACION	COMPROMISO DE LA INFORMACION														FALLAS TECNICAS						ACCIONES NO AUTORIZADAS					
		Fuego	Daño por Agua	Polvo, Corrosión,Congelamiento	Destruccion de Equipos o Medios	Fenomenos Climaticos	Fenomenos Sismicos	inundación	Falla en el suministro de Agua o de aire acondicionado	Perdida de Suministro de Energia	Falla en equipo de telecomunicaciones	Radiacion electromagnetica	Espionaje remoto	Piratería	Ingeniería social	Accesos no autorizados a los sistemas	Escucha Subrepticia	Suplantacion de Identidad	Hurto de medios o documentos	Hurto de Equipo	Recuperacion de Medios reciclados o Desechados	Divulgación	Datos provenientes de fuentes no confiables	Manipulacion con Hardware	Manipulacion con software	Software Malicioso	Falla del equipo	Mal funcionamiento de equipo	Saturacion del sistema de informacion	Mal funcionamiento del software	Incumplimiento en el mantenimiento del sistema de información	Incumplimiento en el mantenimiento de equipo	Uso no autorizado de Equipos	Copia fraudulenta de software	Uso de Sofware falso o copiado	Corrupcion de los datos	Procesamiento ilegal de los datos	Allanamieto Ilegal
		2	1	2	3	2	3	2	2	2	3	2	4	4	3	3	2	2	4	3	2	3	3	3	3	4	3	3	2	2	2	2	2	3	3	3	3	2
Procesos del Negocio	4	8	4	8	12	8	12	8	8	8	12	8	16	16	12	12	8	8	16	12	8	12	12	12	12	16	12	12	8	8	8	8	8	12	12	12	12	8
Bases de Datos	4	8	4	8	12	8	12	8	8	8	12	8	16	16	12	12	8	8	16	12	8	12	12	12	12	16	12	12	8	8	8	8	8	12	12	12	12	8
Equipos Portatiles	2	4	2	4	6	4	6	4	4	4	6	4	8	8	6	6	4	4	8	6	4	6	6	6	6	8	6	6	4	4	4	4	4	6	6	6	6	4
Servidores	4	8	4	8	12	8	12	8	8	8	12	8	16	16	12	12	8	8	16	12	8	12	12	12	12	16	12	12	8	8	8	8	8	12	12	12	12	8
Equipos PC	3	6	3	6	9	6	9	6	6	6	9	6	12	12	9	9	6	6	12	9	6	9	9	9	9	12	9	9	6	6	6	6	6	9	9	9	9	6
Impresoras	2	4	2	4	6	4	6	4	4	4	6	4	8	8	6	6	4	4	8	6	4	6	6	6	6	8	6	6	4	4	4	4	4	6	6	6	6	4
Sistemas de Almacenamiento	4	8	4	8	12	8	12	8	8	8	12	8	16	16	12	12	8	8	16	12	8	12	12	12	12	16	12	12	8	8	8	8	8	12	12	12	12	8
Sistemas Operativos	4	8	4	8	12	8	12	8	8	8	12	8	16	16	12	12	8	8	16	12	8	12	12	12	12	16	12	12	8	8	8	8	8	12	12	12	12	8
Motores de Bases de Datos	4	8	4	8	12	8	12	8	8	8	12	8	16	16	12	12	8	8	16	12	8	12	12	12	12	16	12	12	8	8	8	8	8	12	12	12	12	8
Antivirus	3	6	3	6	9	6	9	6	6	6	9	6	12	12	9	9	6	6	12	9	6	9	9	9	9	12	9	9	6	6	6	6	6	9	9	9	9	6
Aplicaciones del Negocio	4	8	4	8	12	8	12	8	8	8	12	8	16	16	12	12	8	8	16	12	8	12	12	12	12	16	12	12	8	8	8	8	8	12	12	12	12	8
Canales de Internet	3	6	3	6	9	6	9	6	6	6	9	6	12	12	9	9	6	6	12	9	6	9	9	9	9	12	9	9	6	6	6	6	6	9	9	9	9	6
Red Inalamabrica Interna	2	4	2	4	6	4	6	4	4	4	6	4	8	8	6	6	4	4	8	6	4	6	6	6	6	8	6	6	4	4	4	4	4	6	6	6	6	4
Canal de Datos Sedes Remotas	3	6	3	6	9	6	9	6	6	6	9	6	12	12	9	9	6	6	12	9	6	9	9	9	9	12	9	9	6	6	6	6	6	9	9	9	9	6
Firewall	4	8	4	8	12	8	12	8	8	8	12	8	16	16	12	12	8	8	16	12	8	12	12	12	12	16	12	12	8	8	8	8	8	12	12	12	12	8
Antispam	3	6	3	6	9	6	9	6	6	6	9	6	12	12	9	9	6	6	12	9	6	9	9	9	9	12	9	9	6	6	6	6	6	9	9	9	9	6
Suitches de Comunicación	4	8	4	8	12	8	12	8	8	8	12	8	16	16	12	12	8	8	16	12	8	12	12	12	12	16	12	12	8	8	8	8	8	12	12	12	12	8
Persona a Cargo de la Toma de desiciones	3	6	3	6	9	6	9	6	6	6	9	6	12	12	9	9	6	6	12	9	6	9	9	9	9	12	9	9	6	6	6	6	6	9	9	9	9	6
Usuarios	3	6	3	6	9	6	9	6	6	6	9	6	12	12	9	9	6	6	12	9	6	9	9	9	9	12	9	9	6	6	6	6	6	9	9	9	9	6
Personal de Operación y mantenimiento	4	8	4	8	12	8	12	8	8	8	12	8	16	16	12	12	8	8	16	12	8	12	12	12	12	16	12	12	8	8	8	8	8	12	12	12	12	8

Fuente: Elaboración propia

MATRIZ DE PROBABILIDAD/IMPACTO

Tabla 22. Matriz de Probabilidad/Impacto

PROBABILIDAD					
	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		IMPACTO			

Fuente: Elaboración propia

Para el **NIVEL DE RIESGO ACEPTABLE**, se toma como base la siguiente tabla:

Tabla 23. Nivel de Riesgo Aceptable

NIVEL DE RIESGO		
Insignificante	Igual a 1	**NIVEL DE RIESGO ACEPTABLE**
Leve	Entre 2 y 4	
Importante	Entre 5 y 8	**NIVEL DE RIESGO NO ACEPTABLE**
Muy Importante	Entre 9 y 11	
Inaceptable	Entre 12 y16	

Fuente: Elaboración propia

9 RECOMENDACIONES

El análisis de riesgos es una actividad fundamental en el proceso de implementación de un Sistema de Gestión de Seguridad Informática y por tal razón es aconsejable realizar las siguientes recomendaciones:

1. Debe existir un compromiso total de parte de todos y cada uno de los integrantes de la empresa.

2. Es necesario capacitar al personal en la importancia de la seguridad informática y en la importancia de conocer las vulnerabilidades y amenazas existentes.

3. Se recomienda a la empresa Aguas y Aguas de Pereira, continuar con las actividades requeridas para hacer la implementación del SGSI.

4. Este documento no es estático, ya que se trata de una fotografía tomada en un instante de tiempo, por lo tanto se recomienda que periódicamente se revise y se hagan los ajustes pertinentes.

5. Es necesario crear en la empresa la cultura de la seguridad informática, mediante campañas de sensibilización empresarial, así como mediante capacitaciones focalizadas en el tema de la cultura organizacional.

10 CONCLUSIONES

Una vez realizado el análisis de riesgos para el proceso administrativo: Departamento de Informática de la empresa Aguas y Aguas de Pereira, se pudo confirmar que la hipótesis planteada al inicio de la investigación era verdadera.

Dicha confirmación de la hipótesis plantea la necesidad de aplicar los controles requeridos para minimizar el riesgo y de esta forma llevarlo a un nivel aceptado por parte de la organización.

Hoy en día la información es más valiosa que nunca, las redes son una infraestructura crítica, los usuarios no tienen control sobre toda su información, los ataques son más rápidos que los parches y el usuario final es una amenaza. Por lo anteriormente expuesto, es necesario crear el cargo de Jefe de Seguridad Informática dentro del organigrama de la organización.

La Seguridad Informática no es un producto que se pueda comprar en un almacén y por lo tanto es necesario conocer a fondo la empresa, para de esta manera integrar adecuadamente los tres pilares fundamentales de la seguridad: Tecnología, Procedimientos y el Recurso Humano. De estos pilares, el más importante es el recurso humano, y por lo tanto, los esfuerzos institucionales deben estar concentrados en gran medida a fortalecer el personal, mediante programas de capacitación y concientización.

11 BIBLIOGRAFÍA

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS. Proyecto de Norma Técnica Colombiana NTC-ISO 27005. Bogotá D.C.: ICONTEC, 2008. 96p.

BURGOS, Jorge y CAMPOS, Pedro. Modelo Para Seguridad de la Información en TIC. 2008, versión 2. Available from Internet: <ceur-ws.org/Vol-488/paper13.pdf>

GARCÍA, Edgar. Sistema de Gestión de Seguridad de la Información Caso de Estudio. 2010. Available from internet: <MAGGETSI2_104-controles.pdf>

IT GOVERNANCE INSTITUTE. Enterprise Risk: Identify, Govern and Manage IT Risk. Rolling Meadows, IL. USA: 2009. 94p.

RAMIÓ, Jorge. Libro Electrónico de Seguridad Informática y Criptografía. Madrid, España. 2006. 1106 diapositivas