ETAPA DE PLANIFICACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, PARA LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

ADRIANA DIAZ LENIS
GERARDO CAMPOS MOLINA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2022

ETAPA DE PLANIFICACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, PARA LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

ADRIANA DIAZ LENIS
GERARDO CAMPOS MOLINA

Proyecto Aplicado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

MSC. KATERINE MARCELES
Directora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUE
2022

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ibagué, 31 de mayo de 2022

TABLA DE CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE IMAGENES

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO: cualquier cosa que tiene valor para la organización[1].

ACTIVOS DE INFORMACIÓN Y RECURSOS: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo[2].

AMENAZAS: evento que puede generar daño a la información, generada por una vulnerabilidad que puede ser explotada.

CONFIDENCIALIDAD: característica en la seguridad de la información, que limita el acceso a la información a personas no autorizadas.

CONTROL: conjunto de técnicas utilizadas en la seguridad informática, para proteger la información y mitigar los riesgos.

DISPONIBILIDAD: característica de la información que determina que solamente estará accesible a personas autorizadas.

EVALUACIÓN DEL RIESGO: proceso mediante el cual se identifican los activos, las vulnerabilidades y amenazas, igualmente su probabilidad e impacto, con el fin de identificar los controles a implementar, para mitigar el riesgo.

---

[1] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. [Sitio web]. Bogotá: ICONTEC, Norma Técnica NTC-ISO/IEC colombiana 27001. [Consulta: 2021-05-30]. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

[2] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. [Sitio web]. Bogotá: CONPES, 3854 de 2016. [Consulta: 2021-05-30]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

EVENTO DE SEGURIDAD DE LA INFORMACIÓN: ocurrencia de una novedad que comprometa la seguridad informática o la seguridad de la información.

GESTIÓN DEL RIESGO: actividades coordinadas para garantizar la integridad, confidencialidad y disponibilidad de la información.

INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN: un evento o serie de eventos que comprometen la seguridad de la información.

INTEGRIDAD: propiedad de salvaguardar la exactitud y estado completo de los activos[3].

PLAN DE CONTINUIDAD: documento que brinda una guía de pasos a seguir para continuar operando posterior a un evento o incidente de seguridad de la información.

PARTES INTERESADAS (*STAKEHOLDER*): persona u organización que puede percibirse a sí misma como afectada por una decisión o actividad[4].

RIESGO: probabilidad de materialización de una amenaza.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (*Accountability*), no repudio y fiabilidad[5].

---

[3] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Guía para la Implementación de Seguridad de la Información en una MIPYME. [Consulta: 2021-04-30]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf

[4] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Modelo de Seguridad y privacidad de la Información. [Consulta: 2021-04-30]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

[5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. [Sitio web]. Bogotá: ISO/IEC, NTC-ISO/IEC 17799:2006. [Consulta: 2021-04-30]. Disponible en: https://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

SEGURIDAD DIGITAL: preservación de la confidencialidad, integridad, y disponibilidad de la información que se encuentra en medios digitales[6].

VULNERABILIDAD: debilidad que puede ser explotada por una o varias amenazas.

[6] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Modelo de Seguridad y Privacidad de la Información. [Consulta: 2021-05-30]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

RESUMEN

Durante los últimos años el gobierno nacional de Colombia, ha promovido el uso de las TIC, como un instrumento esencial para la optimización de la gestión pública en las entidades del estado, es por ello que inició con la estrategia de “Gobierno en Línea”, la cual tenía como objetivo, automatizar los procesos y procedimientos con el fin de volverlos más eficientes. La evolución de las TIC y el continuo enfoque de satisfacer las necesidades de los ciudadanos, impulso que el gobierno nacional evolucionara su visión digital hacia un nuevo enfoque denominado “Gobierno Digital”.

A través de la política de “Gobierno Digital”, busca que las entidades del estado sean más innovadoras, competitivas y proactivas en un entorno digital, que garanticen la prestación de los servicios informáticos, con calidad, confiabilidad y un alto grado de seguridad, con el fin de lograr un estado más eficiente, transparente, que ayude a construir ecosistemas digitales entre los ciudadanos, aprovechando el uso de las TIC.

En este orden de ideas, es fundamental que las entidades del orden nacional y territorial desarrollen la política de “Gobierno Digital”, en cumplimiento del marco normativo y legal, con el objetivo de lograr eficiencia administrativa, mediante la creación de un entorno de confianza digital, alineado con las exigencias del ministerio de las TIC, acordes con los nuevos desafíos tecnológicos, con una gestión de riesgo que satisfagan las necesidades y la protección de los derechos de los ciudadanos.

ABSTRACT

In recent years, the national government of Colombia has been promoting the use of ICT as an essential instrument for optimizing public management in state entities, which is why it began with the strategy of "Gobierno en Línea" (Goverment Online, in english), which aimed to automate processes and procedures in order to make them more efficient. The evolution of ICTs and the continuous focus on meeting the needs of citizens, prompted the national government to evolve its digital vision towards a new approach called “Gobierno Digital” (Digital Goverment, in english).

Through the Digital Government policy, it seeks for state entities to be more innovative, competitive and proactive in a digital environment, ensuring the provision of computer services, with quality, reliability and a high degree of security, in order to to achieve a more efficient, transparent state that helps build digital ecosystems among citizens, taking advantage of the use of ICT.

In this line, it is essential that national and territorial entities develop the Digital Government policy, in compliance with the regulatory and legal framework, with the aim of achieving administrative efficiency, by creating an environment of digital trust, aligned with the demands of the ICT ministry, in accordance with the new technological challenges, with risk management that satisfies the needs and the protection of citizens' rights.

INTRODUCCIÓN

La EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO SA ESP OFICIAL (en adelante **IBAL**), es una empresa de servicios públicos domiciliarios oficial, del orden territorial, que presta los servicios públicos domiciliarios de acueducto y alcantarillado en la ciudad de Ibagué, con más de 25 años de experiencia, se ha caracterizado por el compromiso en el mejoramiento continuo a través de la gestión del riesgo en todos sus procesos, es por ello que tiene implementadas y certificadas las normas NTC-ISO9001, NTC-ISO14001 y NTC-ISO 4500, las cuales están inmersas un sistema integrado de gestión (en adelante **SIG**).

De acuerdo con el SIG se observa que el IBAL, tiene identificados procesos estratégicos, misionales, de apoyo y de evaluación, a través de los cuales desarrollan su objeto misional. Revisando el proceso de Gestión Tecnológica[7], se puede observar qué este proceso de apoyo, gestiona todos los recursos tecnológicos de la empresa, mediante una serie de actividades enmarcadas en el ciclo PHVA.

En el marco del cumplimiento de los objetivos de la política de gobierno digital, en aras de apoyar la adopción del Modelo Integrado de Planeación y Gestión (en adelante **MIPG**) y como parte del mejoramiento continuo del SIG, el IBAL deberá avanzar con el diseño de la etapa de planificación del modelo de privacidad y seguridad de la información (en adelante MSPI) establecido por el ministerio de tecnologías de la información y las comunicaciones MINTIC (en adelante MinTic), con el objetivo articular la gestión con las políticas públicas, y así garantizar la seguridad de la información en todos sus procesos, trámites y servicios ofrecidos

[7] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué. IBAL, SIG-Sistema Integrado de Gestión. [Consultado: 10 de mayo de 2021]. Disponible en https://www.ibal.gov.co/sistema-de-gestion-de-calidad

de manera digital, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El IBAL es una empresa industrial y comercial de estado, dedicada a la prestación de los servicios públicos domiciliarios de acueducto y alcantarillado en la ciudad de Ibagué, su máximo accionista y propietario es el municipio de Ibagué, en nombre del Instituto de Financiamiento, Promoción y Desarrollo de Ibagué – INFIBAGUE, el cual tiene el 99% de sus acciones. Normativamente se encuentra regida por la ley 142 de 1994[8] y su control, inspección y vigilancia, están atribuidas a la Superintendencia de Servicios Públicos Domiciliarios.

Legalmente EL IBAL se deberá acoger a todos los decretos, resoluciones, circulares etc., que se establezcan el ámbito de aplicación del artículo 39 de Ley 489 de 1998[9], motivo por el cual, deberá atender los lineamientos de la política de gobierno digital, establecidos en el Decreto 1008 de 14 de junio de 2018[10] por ministerio de las tecnologías de la información y las comunicaciones.

Es por ello que el IBAL mediante Resolución 0668 de 29 de julio de 2019[11], adoptó la Política de seguridad y privacidad de la información, conforme con los lineamientos del MinTic (Ministerio de las Tecnologías de la información y

[8] COLOMBIA. SECRETARIA DEL SENADO. Ley 142 de 1994. Ley de Servicios Públicos Domiciliarios. [en línea]. Bogotá D.C.1994. [Consultado: 13 mayo de 2021]. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_0142_1994.html

[9] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 489 de 1998. Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones. [en línea]. Bogotá D.C. [Consultado: 13 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186

[10] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Decreto 1008 de 2018 [en línea]. Bogotá D.C. [Consultado: 13 de mayo de 2021]. Disponible en: https://estrategia.gobiernoenlinea.gov.co/623/articles-74795_recurso_1.pdf

[11] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL, Por la cual se adopta la política de seguridad y privacidad de la información [Consultado: 10 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/Politica%20de%20seguridad%20de%20la%20infromaci%C3%B3n.pdf

comunicaciones), la cual estaba enfocada en la estrategia de gobierno en línea, y que con el tiempo evolucionó a la Política de Gobierno Digital.

Igualmente el IBAL en los últimos años ha elaborado algunos documentos relacionados con el Modelo de seguridad y privacidad de la Información (en adelante **MSPI**), en los cuales observa ejecución hasta la fase de diagnóstico como se puede evidenciar en el documento de octubre de 2018 denominado "DIAGNOSTICO Seguridad y privacidad de la información"[12], y en el documento "MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN MSPI"[13].

A raíz de todo esto, se hace imperante para el IBAL el cumplimiento de todos los lineamientos establecidos por el MINTIC para el MSPI, con el fin de garantizar una óptima gestión de trámites y servicios, adoptando mecanismos que brinden la seguridad y la privacidad de la información. Todo esto en cumplimiento de las políticas del orden nacional y las convergentes con MIPG, so pena de las actuaciones disciplinarias que puede acarrear el incumplimiento de estas, las cuales están establecidas en la Ley 734 de 2002, modificada por la Ley 1952 de 2019 y reformada por la Ley 2094 de 2021.

1.2 FORMULACIÓN DEL PROBLEMA

En el marco del Decreto 1008 de 2018, se definieron los lineamientos de la política de Gobierno Digital, se estableció el ámbito de aplicación y se desarrollaron los principios sobre los cuales se iba a regir; igualmente entre los elementos que

[12] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL, Diagnóstico Seguridad y Privacidad de la información. [Consultado: 10 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/Plan%20de%20seguridad%20y%20privacidad%20de%20la%20informacion%20-%20(DIAGNOSTICO)%20%20IBAL.pdf

[13] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL, MSPI. [Consultado: 10 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/Plan%20de%20seguridad%20y%20privacidad%20de%20la%20informaci%C3%B3n.pdf

componen la política de Gobierno Digital (componentes, habilitadores y propósitos), se establece las qué, las entidades del estado deberán implementar una política de seguridad y privacidad de la información, con base en el modelo de que establezca el ministerio de las TIC para este fin, situación en la cual se plantea la siguiente pregunta: ¿***Cómo mediante el diseño de la etapa de planificación de un modelo de seguridad y privacidad de la información, se puede mejorar la privacidad y seguridad de la información en la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL***?***.***

2 JUSTIFICACIÓN

De acuerdo con el Manual para la Implementación de la Política de Gobierno Digital en su versión 7 de abril de 2019[14], existen dos componentes esenciales: TIC para estado y TIC para la sociedad, los cuales son habilitados por tres componentes transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, con el desarrollo de estos 5 componentes las entidades del estado podrán cumplir con los logros definidos en esta política. En la ilustración 1 se pueden observar los elementos.

Ilustración 1. Elementos de la política de gobierno digital

Fuente: Manual para la implementación de la Política de Gobierno Digital, Versión 7, abril de 2019, página 17.

[14] COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Manual para la Implementación de la Política de Gobierno Digital. Versión 7 de abril de 2019. 89 p. [Consultado: 15 de mayo de 2021]. Disponible en: https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf

Es importante mencionar qué, para el desarrollo de estos cinco componentes, el MinTic ha desarrollo una serie de guías y modelos basados en estándares internacionales que buscan orientar a las entidades del estado en la implementación de esta política.

Uno de los componentes transversales de la política de gobierno digital es la ***seguridad de la información***, la cual busca qué, mediante la implementación del MSPI, las entidades del estado desarrollen en sus procesos, trámites, servicios, sistemas de información, infraestructura y en general en todos los activos de información, lineamientos de seguridad con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de la información.

Es importante mencionar que el IBAL en cumplimiento de los lineamientos de la política de gobierno digital, y con el desarrollo del componente de seguridad de la información, podrá establecer los procesos y procedimientos necesarios en su SIG, encaminados a garantizar una óptima prestación de trámites y servicios en un entorno digital, mediante la gestión del riesgo de los elementos que conforman su arquitectura de TI, con el fin de controlar las vulnerabilidades que se puedan presentar en ellos, y así lograr la satisfacción del usuario que se beneficia de los servicios públicos que presta el IBAL.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Diseñar la fase de planificación del modelo de seguridad y privacidad de la información para el proceso de gestión tecnológica de la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, adoptando los lineamientos de la ISO/IEC 27001:2013 y del ministerio de las Tecnologías de la Información y las Comunicaciones, con el fin de apoyar la gestión la seguridad y privacidad de la información.

3.2 OBJETIVOS ESPECÍFICOS

Evaluar el nivel de madurez de la implementación del modelo de seguridad y privacidad de la información del proceso de Gestión Tecnológica, mediante el desarrollo de la herramienta de autodiagnóstico del MINTIC, que permita identificar la brecha en la implementación del modelo y las vulnerabilidades técnicas y administrativas.

Analizar los activos de información y recursos del proceso de Gestión Tecnológica, mediante la aplicación de la guía de riesgos del DAFP, para su valoración, clasificación y tratamiento, con el fin de gestionar la confidencialidad, disponibilidad e integridad de la información.

Proponer una actualización de la política de seguridad de la información vigente, para guiar el comportamiento de las partes interesadas, logrando que la empresa trabaje bajo buenas prácticas de seguridad, minimizando la ocurrencia de incidentes informáticos.

Elaborar un procedimiento en seguridad y privacidad de la información, basado en un dominio crítico identificado en la herramienta de evaluación de efectividad de los controles establecidos en la norma ISO/IEC 27001:2013, con el fin de documentar el procedimiento que se ajuste al proceso de Gestión Tecnológica.

4 MARCOS DE REFERENCIA

4.1 MARCO TEÓRICO

4.1.1 Importancia de un MSPI en instituciones Públicas. Las empresas de servicios públicos domiciliarios, qué, en nombre del estado provean servicios públicos esenciales para una comunidad, por ejemplo: acueducto, alcantarillado, aseo, energía, gas natural, etc, deberán garantizar una adecuada gestión de la información en cada uno de sus procesos (estratégicos, misionales, apoyo y evaluación), para que desarrollen las actividades necesarias que permitan garantizar la continuidad en la operación y por ende el suministro de los servicios públicos.

Es importante mencionar que los volúmenes de información que se trabajan en este tipo de organizaciones es bastante alto, ya que periódicamente, tienen que realizar el procesamiento de los datos de los consumos registrados por los dispositivos que se encuentran en los predios (micromedidores de agua, contador de energía, medidor de gas natural, etc), con el fin de liquidarlos y generar la facturación de los servicios y posteriormente registrar el recaudo por los conceptos facturados. Esta actividad es crítica en las empresas de servicios públicos, ya que de su adecuada gestión se generan los recursos necesarios para su operación.

Otro factor muy importante para este tipo de empresas u organizaciones, son los servicios que se prestan a los usuarios y/o suscriptores, de manera presencial en las oficinas destinadas para este fin o virtual a través del uso de los diferentes canales de comunicación que se tienen destinados, de la efectiva gestión que se realizan de estos servicios y la información que en ellos se realiza, dependerá del nivel de satisfacción de los usuarios y/o suscriptores, quien en última son los responsables de pagar los servicios públicos suministrados.

4.1.2 Identificación de los activos mediante la metodología del DAFP. La Guía para la administración del riesgo y el diseño de controles en entidades públicas, el Departamento Administrativo de la Función Pública (DAFP)[15], compiló la metodología necesaria para que las empresas del sector público, desarrollen una adecuada gestión del riesgo de los activos más importantes para cada entidad; esto se realiza a través de tres pasos: una política de administración del riesgo, la identificación del riesgo y la valoración de los riesgos.

Para el presente trabajo se desarrollará esta metodología relacionada con los lineamientos de los riesgos asociados con la seguridad de la información, en la cual se pueden mencionar: identificación de activos de seguridad de la información, identificación del riesgo, la valoración del riesgo y los controles asociados a la seguridad de la información.

4.1.3 Problemas generados con la no implementación del MSPI. Con el desarrollo y evolución de las políticas enfocadas al aprovechamiento del ecosistema digital, el gobierno nacional busca que las entidades sector público, adopten mecanismos necesarios para la optimización de su gestión a través del uso y manejo de las tecnologías de la información y las comunicaciones, con el fin de lograr un estado más eficiente y prestar mejores servicios a los ciudadanos, y que esta actividad brinde una oportunidad para la generación de nuevas alternativas que permitan innovar y mejorar continuamente el funcionamiento de las empresas del estado.

El incumplimiento de estas directrices del orden nacional, traerá consigo para las empresas del estado, rezago en los procesos internos de cada entidad, ya que, a

[15] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. [Sitio web]. Bogotá: DAFP, Guía para la administración del riesgo y el diseño de controles en entidades públicas versión 5. [Consulta: 15 de mayo de 2021] Disponible en: https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238&download=true

través de estas, lo que se busca es agilizar y optimizar la gestión de las entidades públicas, a través del uso de las tecnologías de la información y comunicaciones, de una manera confiable y segura, con el fin de mejorar el portafolio de servicios que estas entidades ofrecen a los ciudadanos.

Así mismo, el incumplimiento a estas directrices, puede acarrear sanciones de tipo disciplinario a los funcionarios que se encuentren a cargo de estas empresas o procesos internos de la organización, los cuales pueden encontrarse inmersos en una sanción en el marco de la Ley 734 de 2002, modificada por la Ley 1952 de 2019 y reformada por la Ley 2094 de 2021.

4.2 MARCO CONCEPTUAL

4.2.1 Las empresas de servicios públicos en Colombia. Son entidades públicas o privadas qué en nombre del estado, prestan los servicios domiciliarios de acueducto, alcantarillado, aseo, energía eléctrica, distribución de gas combustible, telefonía fija pública básica conmutada y la telefonía local móvil en el sector rural, a una población o comunidad; estas organizaciones se encuentran reglamentadas en la Ley 142 de 1994 y su control, inspección y vigilancia están atribuidas a la superintendencia de servicios públicos domiciliarios.

4.2.2 Política de gobierno digital. Busca en las entidades del estado y en todas las partes interesadas, “Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado ciudadano, competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”. Esta política es compuesta por dos (2) componentes: TIC para Estado y TIC para la sociedad, tres habilitadores transversales: seguridad de la información, arquitectura y servicios ciudadanos digitales y cinco (5) propósitos: servicios digitales de confianza y calidad, procesos internos seguros y eficientes,

decisiones basadas en datos, empoderamiento ciudadano a través de un estado abierto y territorios y ciudades inteligentes a través de las TIC.

4.2.3 Modelo de seguridad y privacidad de la información (MSPI). Es un conjunto metodologías y buenas prácticas basadas en estándares internacionales, relacionadas con la seguridad y privacidad de la información, que busca apoyar a las entidades del estado en la implementación de la política de gobierno digital, mediante la gestión del riesgo, incentivando el uso y aprovechamiento de las tecnologías de la información y las comunicaciones.

La seguridad de la información, hace mención a garantizar la integridad, confidencialidad y disponibilidad de la información.

- La integridad es la propiedad de mantener atomizada la información, tal cual como fue concebida, sin ser modificada por personas o entidades no autorizadas.

- La disponibilidad es la capacidad de mantener accesible la información para que pueda ser consultada o gestionada por una persona o entidad con permiso para realizarlo.

- La confidencialidad es la propiedad que tiene la información de permanecer restringida, que sólo estará disponible para ciertos grupos de interés, los cuales tienen los recursos y los medios para acceder a ella de manera formal.

4.2.4 Familia de estándares ISO/IEC 27000. La familia de estándares de la norma ISO/IEC 27000, definen un conjunto de buenas prácticas relacionadas con la seguridad y privacidad de la información, a través de la implementación de controles y objetivos de control, la medición de la gestión relacionada con la seguridad de la

información, todo esto enmarcado en la gestión del riesgo y el mejoramiento continuo de todos los procesos involucrados en esta actividad.

4.2.5 Infraestructuras críticas. Hace mención a la infraestructura física, el entorno administrativo, técnico y operativo que tienen las organizaciones públicas o privadas, para prestar un servicio público o un servicio básico esencial a una población o comunidad, y qué a partir de ella, se generan sinergias con otros factores productivos de la sociedad, contribuyendo al mejoramiento de la calidad de vida de los habitantes que se benefician de ella. El estado colombiano tiene previstas en el proyecto de Ley 245 de 2019[16] los siguientes sectores como infraestructura crítica ver cuadro 1.

Cuadro 1. Sectores que conforman el SNICC

Nro	Sector
1	Defensa y Seguridad
2	Salud
3	Agua Potable y Saneamiento Básico
4	Infraestructura para el transporte
5	Energía
6	Industria química y nuclear
7	Financiero y tributario
8	Tecnologías de la Información y las Comunicaciones, Espectro electromagnético y órbita geoestacionaria
9	Monumentos nacionales y patrimonio cultural
10	Alimentación y seguridad alimentaria
11	Entidades administrativas de todas las ramas del poder público y de los diferentes niveles de gobierno

Fuente: Proyecto de Ley 245 de 2019 - Por la cual se crea el sistema nacional de protección de las infraestructuras críticas –SNINC–, y se dictan otras disposiciones

4.2.6 Modelo integrado de planeación y gestión v2 (MIPG)[17]. Es un modelo de gestión, que busca que las entidades del estado integren los sistemas de desarrollo administrativo y gestión de calidad, para articularlos con el sistema de control interno y así garantizar una eficiencia en la prestación de los servicios que ofrecen las

[16] CONGRESO DE LA REPÚBLICA DE COLOMBIA. [Sitio web]. Bogotá: Proyectos de Ley Radicados 2018-2019. Proyecto de Ley 245 de 2019 [Consulta: 03 de mayo de 2021]. Disponible en http://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2018-2019/1403-proyecto-de-ley-245-de-2019

[17] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. [Sitio web]. Bogotá: DAFP, MiPg. [Consulta: 15 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/web/mipg/inicio

entidades para satisfacer las necesidades, problemas y garantizar los derechos de todos.

4.3 MARCO CONTEXTUAL

La Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, es una empresa industrial y comercial del estado, que presta los servicios públicos domiciliarios de acueducto y alcantarillado en la ciudad de Ibagué, nace del proceso de liquidación de la Empresa de Obras Sanitarias de Ibagué (Empoibagué), cuando en el año de 1991 a raíz de la iniciativa de una nueva constitución para la nación, desaparecieron los institutos de fomento municipal **Insfopal y los Empos** para dar paso a empresas del orden municipales, las cuales podría ejercer la prestación de los servicios públicos en los municipios.

A través de los últimos años el IBAL ha ido evolucionando como empresa y organización, lo que le ha permitido implementar y certificar las normas de calidad NTC-ISO9001, NTC-ISO14001 y NTC-ISO 45001, consolidándose como la empresa pública número uno en el departamento del TOLIMA. La implementación de estas normas de calidad enmarcadas en la gestión del riesgo, le permite articular de una manera más sencilla y eficiente, nuevos marcos de referencia basados en estándares internacionales como lo son los establecidos por el ministerio de las TIC, para el tema de la seguridad y privacidad de la información.

El objetivo primordial del desarrollo de la etapa de planificación del MSPI, es la adopción e implementación por parte del IBAL, de la política de seguridad y privacidad de la información, la cual deberá ser construida mediante la siguiente temática: identificación y valoración de activos, controles en los activos, monitoreo de las vulnerabilidades, detección de amenazas, planes y programas de recuperación ante incidentes en la seguridad de información, los cuales deberán implementarse y evaluarse periódicamente en cumplimiento de ciclo PHVA que

indica el MSPI.

4.4 MARCO LEGAL

La estrategia de gobierno en línea se estableció a partir del Decreto 1151 de 2008[18], el cual tenía como objetivo "Contribuir con la construcción de un estado más eficiente, más transparente y participativo, prestando mejores servicios a los ciudadanos y a las empresas, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación". Su ámbito de aplicación era para las entidades de la administración pública.

Mediante la Ley 1341 de 2009[19] se definieron los principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones y transformó el Ministerio de las Comunicaciones en el Ministerio de las Tecnologías de la Información y las Comunicaciones (MINTIC).

A través del Decreto 2573 de 2014[20] se definieron los lineamientos generales de la Estrategia de Gobierno en Línea y su ámbito de aplicación era para las entidades que conforman la administración pública y los particulares que cumplen funciones administrativas.

El Decreto Único Reglamentario del sector de tecnologías de la información y las comunicaciones – DUR-TIC o Decreto 1078 de 2015[21], tiene como objetivo compilar y racionalizar las normas de carácter reglamentario en el sector TIC. Así mismo,

---

[18] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. [Sitio web]. Bogotá: DAFP, Decreto 1151 de 2008. [Consulta: 15 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=29774

[19] CONGRESO DE LA REPÚBLICA DE COLOMBIA. [Sitio web]. Bogotá: LEY 1341 DE 2009 [Consulta: 03 de mayo de 2021]. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_1341_2009.html

[20] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. [Sitio web]. Bogotá: DAFP, Decreto 2573 de 2014. [Consulta: 15 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=60596#14

[21] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. [Sitio web]. Bogotá: DAFP, Decreto 1078 de 2015. [Consulta: 22 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888

mediante este decreto surgió la Política de Gobierno Digital, cuyo ámbito de aplicación sería para las entidades que conforman la administración pública y los particulares que cumplen funciones administrativas, estará definida por el ministerio de las TIC y se desarrollaría a través de componentes y habilitadores trasversales, acompañados de lineamientos y estándares internacionales.

5 DISEÑO METODOLÓGICO

De acuerdo con el modelo de seguridad y privacidad de la información elaborado por MINTIC, el cual contempla su operación basado en el ciclo PHVA (planear, hacer, verificar y actuar), la metodología que se va utilizar para la realización de este proyecto aplicado, consiste en desarrollar etapa previa a la fase de implementación como lo son la fase de diagnóstico y la fase de planificación.

5.1 FASE DE DIAGNOSTICO

En la fase de diagnóstico se busca identificar el estado actual que tiene el IBAL, con relación a la implementación del MSPI, en esta fase se van a desarrollar las siguientes actividades: determinación del estado actual de la seguridad y privacidad de la información a través de uso de la herramienta llamada Instrumento de Evaluación MSPI[22], la cual desarrolló MINTIC, y como resultado de su diligenciamiento se podrá identificar el nivel de madurez del IBAL e identificar las vulnerabilidades administrativas y técnicas de acuerdo con los dominios del anexo A de la norma ISO/IEC 27001:2013. Los insumos de información para desarrollar esta fase, serán tomados de las fuentes de información primaria como la página web del IBAL, documentos del sistema integrado de gestión y el conocimiento propio que tenemos de la empresa.

5.2 FASE DE PLANIFICACIÓN

Una vez agotada la fase de diagnóstico, se desarrollará la fase de planificación, en la cual, con base a los resultados de autodiagnóstico, se establecerán las acciones a desarrollar a nivel de seguridad y privacidad de la información, esto a través de la

[22] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Instrumento de Evaluación MSPI. [Consulta: 18 de mayo de 2021]. Disponible en: : https://gobiernodigital.mintic.gov.co/692/articles-150507_Instrumento_Evaluacion_MSPI.xlsx

metodología de gestión de riesgo que establece el DAFP. Con el fin de determinar el alcance que se tendrá para el MSPI, el cual se define en esta fase, es importante tener en cuenta los siguientes aspectos: contexto del IBAL, liderazgo, planeación y soporte.

Es importante resaltar que para desarrollo de la fase de planificación, se van a consultar las guías e instructivos relacionadas con ésta, las cuales proporciona MINTIC a través de su portal web https://gobiernodigital.mintic.gov.co/. Entre ellas se encuentran, las siguientes:

- Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información[23].
- Guía 2 – Política General MSPI[24].
- Guía 3 – Procedimientos de Seguridad y Privacidad de la Información[25].
- Guía 4 – Roles y responsabilidades de seguridad y privacidad de la información[26].
- Guía 5 – Gestión de Activos[27].
- Guía 7 – Gestión de Riesgos[28].

[23] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información. [Consulta: 18 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150519_Instructivo_instrumento_Evaluacion_MSPI.pdf

[24] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Guía 2 Política General MSPI. [Consulta: 18 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150520_G2_Politica_General.pdf

[25] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Guía 3 Procedimientos de Seguridad y Privacidad de la Información. [Consulta: 18 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150514_G3_Procedimiento_de_Seguridad.pdf

[26] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Guía 4 Roles y responsabilidades de seguridad y privacidad de la información. [Consulta: 18 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150523_G4_Roles_responsabilidades.pdf

[27] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Guía 5 Gestión De Activos. [Consulta: 18 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150528_G5_Gestion_Clasificacion.pdf

[28] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Guía 7 Gestión de Riesgos. [Consulta: 18 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150516_G7_Gestion_Riesgos.pdf

- Guía 8 – Controles de Seguridad[29].
- Guía para la administración del riesgo y el diseño de controles en entidades públicas. DAFP Versión 5 diciembre de 2020[30].

[29] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Guía 8 Controles de Seguridad. [Consulta: 18 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150511_G8_Controles_Seguridad.pdf

[30] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: DAFP, Guía para la administración del riesgo y el diseño de controles en entidades pública. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238&download=true

6 EVALUACIÓN DEL NIVEL DE MADUREZ DE LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL PROCESO DE GESTIÓN TECNOLÓGICA, MEDIANTE EL DESARROLLO DE LA HERRAMIENTA DE AUTODIAGNÓSTICO DEL MINTIC, QUE PERMITA IDENTIFICAR LA BRECHA EN LA IMPLEMENTACIÓN DEL MODELO Y LAS VULNERABILIDADES TÉCNICAS Y ADMINISTRATIVAS

De acuerdo con los lineamientos de MINTIC, se debe realizar una fase previa a la implementación del modelo, en la cual se identifiquen aspectos importantes en la organización relacionados con la seguridad y privacidad de la información, que serán el insumo para desarrollar la fase de planificación.

La primera actividad que se va a desarrollar en el presente documento, es el diagnóstico del estado actual del IBAL con relación a los requerimientos del MSPI, para desarrollar esta fase se tomó como guía el instrumento evaluación MSPI[31], en el cual se pueden identificar las siguientes actividades que se muestran en la ilustración 2:

[31] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información. [Consulta: 18 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150519_Instructivo_instrumento_Evaluacion_MSPI.pdf

Ilustración 2. Actividades fase de diagnóstico

Fuente: MinTic - Instructivo para el Diligenciamiento de la Herramienta de Diagnostico de Seguridad y Privacidad de la Información. Versión 1. junio de 2017 Página 18.

6.1 LEVANTAMIENTO DE INFORMACIÓN

Para el desarrollo de esta actividad de la fase de autodiagnóstico, se tomó como fuente primaria de información la página web de la empresa www.ibal.gov.co, relacionada con el sistema integrado de gestión (en adelante SIG), la caracterización de los procesos de gestión tecnológica y gestión comercial; así mismo, se tomó el conocimiento de los autores de este proyecto, quienes laboran en el IBAL en el proceso de gestión comercial y gestión tecnológica como profesionales universitarios y cuentan con la experiencia e información necesaria de los procesos internos de la empresa para desarrollar a plenitud este tipo de proyecto.

Proceso de Gestión Tecnológica de acuerdo con la matriz de caracterización[32], se define como un proceso de apoyo, el responsable es el líder del proceso, está

[32] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL, Matriz de caracterización gestión tecnológica. [Consulta: 18 de mayo de 2021]. Disponible en:

conformado por el área de Gestión Tecnológica del IBAL y tiene como objetivo: "Garantizar el efectivo apoyo tecnológico a las diferentes áreas del IBAL S.A. ESP OFICIAL, mediante la asignación, administración y mejora de los recursos tecnológicos disponibles (hardware, software, redes y comunicaciones)". A continuación, se hace una relación de la información relacionada con el proceso de acuerdo con el SIG y que está disponible en la página web del IBAL:

a) Matriz de caracterización proceso de Gestión Tecnológica.

- Planeación del proceso.

- Plan de Trabajo o Plan de Acción del Proceso.
- Plan Estratégico de Sistemas (PETI).
- Cronograma de mantenimiento preventivo hardware.
- Planificación de copias de respaldo.
- Planes de contingencia.

- Administración de redes y comunicaciones.

- Gestión del servicio de internet.
- Seguridad de la información (antivirus).
- Conexión de dispositivos (asignación de Ip).
- Gestión Canales de datos.
- Administración plataforma Call Center.
- Equipos instalados a la plataforma o red corporativa.
- Actualización firewall(firmware).

https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/CARACTERIZACI%C3%93N%20GESTI%C3%93N%20TECNOLOGICA%20v14.pdf

- Administración, desarrollo y soporte de software (incluido ofimática).

- Software actualizado, nueva versión.
- Registro de capacitación o reentrenamiento.
- Información respaldada.
- Nuevos Programas.
- Equipo con software operativo.

- Soporte a usuarios internos (hardware).

- Suministro de mantenimiento preventivo y correctivo de equipos.
- Equipos con hardware operativo.
- Actualización página web y certificación de la publicación.
- Página web con lineamientos de Gobierno en Línea, y lo estipulado en la Ley 1712 de 2014" Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones" y Resolución 3564 del 31 de diciembre de 2015 Anexo 1, Anexo 2.
- Tramites en línea.
- Creación y configuración de correos institucionales.

- Administración bases de datos y seguridad de la información.

- Implementación de bases de datos corporativas.
- Administración y monitoreo de la integridad de la información.
- Monitoreo de los servidores de Bases de datos.
- Diseño de las soluciones de almacenamiento.
- Seguridad de las bases de datos y a recuperación de desastres.
- Implementación de los planes de contingencia.
- Diagramas de flujo de datos y relacionales.

- Seguimiento y verificación del proceso.

- Informes de Gestión.
- Planes de Mejoramiento.
- Resultados de Auditorías Internas del SIG.
- Medición y análisis de Indicadores de Gestión.

b) Procedimientos.

- GT-P-001 Procedimiento de Gestión Tecnológica
- GT-P-002 Procedimiento manejo de licencias adquiridas por el IBAL

c) Instructivos.

- GT-I-001 Instructivo Mantenimiento Pagina Web y Correos Institucionales
- GT-I-002 Instructivo Administración de Redes y Comunicaciones
- GT-I-003 Instructivo para realización de copias de respaldo
- GT-I-004 Instructivo para Reporte de Requerimientos de Software
- GT-I-005 Instructivo Administración Bases de Datos y Seguridad de la Información

d) Otros.

- GT-O-001 Política de Seguridad y Privacidad de la Información IBAL SA ESP Oficial

e) Registros.

- GT-R-001 Soporte en Hardware y/o Software
- GT-R-002 Mantenimiento de equipos

- GT-R-003 Seguimiento Copias de Respaldo
- GT-R-004 Encuesta de satisfacción del cliente interno
- GT-R-005 Configuración e instalación de licencias

f) Recurso humano proceso de gestión tecnológica.

Mediante Resolución IBAL 0755 de 2018[33] se adoptó el manual específico de funciones y competencias laborales en EL IBAL, en el cual se puede identificar los cargos asociados al proceso de Gestión Tecnológica así como las funciones que realizan cada uno de ellos, a continuación se hace una relación de los funcionarios que conforman en proceso, los cuales son los responsables de garantizar el efectivo cumplimiento de los objetivos del proceso:

- Un (1) Profesional Especializado Grado 3 – Líder del proceso de Gestión Tecnológica.
- Dos (2) Profesionales Universitarios Grado 1, ingenieros de sistemas.
- Un (1) Técnico Grado 2.
- Adicionalmente se tiene una persona contratada de apoyo a la gestión quien realiza las funciones de un técnico 2, para realizar soporte técnico, mantenimiento preventivo y correctivo al parque computacional del IBAL[34].

[33] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL, Manual específico de funciones y competencias laborales 2018. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/MANUAL-DE-FUNCIONES-RESOLUCION-0755-DEL-03-DE-AGOSTO-DE-2018_0.pdf

[34] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL, Relación de Contratistas de Servicios Profesionales y de Apoyo a la Gestión 2018. [Consultado: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/Contratistas%20Servicios%20Profesionales%20y%20Apoyo%202018.pdf

6.2 PRUEBAS Y ANÁLISIS

Continuando con las actividades de la fase de diagnóstico, de acuerdo con los lineamientos del instrumento de evaluación del MSPI, se realizan las pruebas administrativas y técnicas las cuales se desarrollan en el archivo de Excel **articles-5482_Instrumento_Evaluacion_MSPI.xlsx**[35], el cual dispuso MINTIC para realizar esta actividad y busca que a través de su diligenciamiento, tener una visión más real del nivel de implementación del MSPI y su avance en el ciclo PHVA, también identificar la brecha con relación a la ISO/IEC 27001:2013 y una calificación del IBAL frente a las mejores prácticas relacionadas en el marco de ciberseguridad de NIST.

Las pruebas administrativas del instrumento de evaluación, están orientadas a los temas de seguridad de la información relacionados con los controles de la norma ISO/IEC 27001:2013 en los dominios A5, A6, A7, A8, A17 y A18.

Pruebas técnicas del instrumento de evaluación, están orientadas a la evaluación de controles y requisitos, asociados con la norma ISO/IEC 27001:2013 en los dominios A9, A10, A11, A12, A13, A14 y A16.

De acuerdo con la guía instrumento de Evaluación MSPI, se tiene la siguiente escala de valores para la evaluación de las pruebas técnicas y administrativas, ver cuadro 2.

[35] MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [sitio web]. Bogotá: MINTIC. Instrumento de Evaluación MSPI. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Instrumento_Evaluacion_MSPI.xlsx

Cuadro 2. Escala de valoración de controles

Tabla de Escala de Valoración de Controles ISO/IEC 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	Total, falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Fuente: Instrumento de Evaluación MSPI – articles-5482_Instrumento_Evaluacion_MSPI.xlsx. Versión 1. junio de 2017. Hoja Escala de Evaluación.

Esta actividad se elaboró con la información que se recolectó en la actividad anterior y se desarrolló realizando una lectura de las pruebas descritas por MINTIC en el archivo de Excel relacionadas con los controles de la ISO/IEC 27001:2013, y en cada una de ellas se otorgó un puntaje de acuerdo con la información del IBAL y la escala de valores que se presenta en el cuadro 2. El desarrollo estuvo a cargo de los autores de este documento, en compañía de los funcionarios del proceso de gestión tecnológica del IBAL.

6.3 RESULTADOS Y ANÁLISIS DE LAS PRUEBAS ADMINISTRATIVAS Y TÉCNICAS

Como resultado de la aplicación de las pruebas administrativas y técnicas de acuerdo con el Instrumento de Evaluación MSPI, se obtuvieron los siguientes resultados para el IBAL, el cual se puede observar en el cuadro 3.

Cuadro 3. Resultado de la evaluación de los controles

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	51	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	76	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	22	100	REPETIBLE
A.9	CONTROL DE ACCESO	60	100	EFECTIVO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	59	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	62	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	49	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	45	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	14	100	INICIAL
A.18	CUMPLIMIENTO	86.5	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		**40**	**100**	EFECTIVO

Fuente: elaboración grupo de trabajo - Instrumento de Evaluación MSPI – articles-5482_Instrumento_Evaluacion_MSPI.xlsx. Versión 1. marzo 2021.

Según el resultado de la evaluación de los controles, el promedio para el IBAL fue de **40 puntos**, qué, de acuerdo con la escala de valoración de controles (cuadro 2), se puede concluir que "***Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin***

embargo, es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada".

Esto se puede traducir en que el IBAL gracias a tener implementado el SIG, tiene documentado y gestionado algunos controles que le permiten mitigar el riesgo ante posibles incidentes relacionados con la seguridad de la información, sin embargo, estos controles no están siendo gestionados adecuadamente y no existen roles y responsabilidades claras en la organización para la gestión de cada uno de ellos.

6.3.1 Análisis Avance del ciclo PHVA. Una vez se realizadas las pruebas técnicas y administrativas, se puede identificar el nivel de avance del IBAL con relación al ciclo PHVA. Como resultado se puede determinar que la empresa está en un 16%, lo que indica que existen procesos del ciclo ya iniciados como la planificación e implementación, pero un porcentaje muy bajo 12% y 4%. Lo que sugiere que el IBAL deberá enfocar sus esfuerzos a lograr el avance del 100% con relación a todos los componentes del ciclo y así dar cumplimiento a los requisitos legales con relación al MSPI. El resultado se puede ver en el cuadro 4.

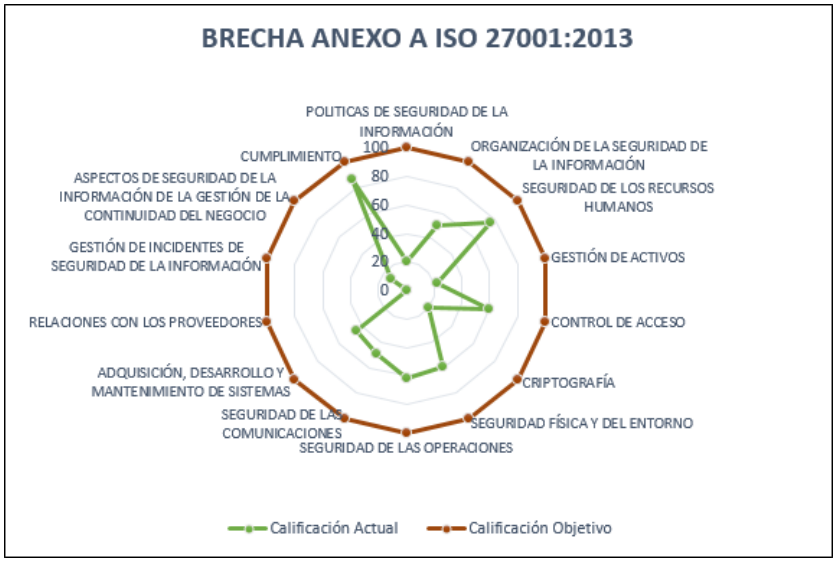
Cuadro 4. Avance del ciclo PHVA

Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2015	Planificación	12%	40%
2016	Implementación	4%	20%
2017	Evaluación de desempeño	0%	20%
2018	Mejora continua	0%	20%
TOTAL		16%	100%

Fuente: Elaboración grupo de trabajo - Instrumento de Evaluación MSPI – articles-5482_Instrumento_Evaluacion_MSPI.xlsx. Versión 1. marzo 2021.

6.3.2 Brecha de seguridad. Las brechas de seguridad de los controles que tiene implementado el IBAL frente a la norma ISO/IEC 27001:2013, se puede observar en la ilustración 3.

Ilustración 3. Brecha de seguridad del IBAL según anexo A ISO/IEC 27001:2013



Fuente: Elaboración grupo de trabajo Instrumento de Evaluación MSPI – articles-5482_Instrumento_Evaluacion_MSPI.xlsx. Versión 1. marzo 2021.

- La brecha con relación al dominio A.18 CUMPLIMIENTO, el IBAL obtuvo un promedio de 86.5 puntos, lo que indica que la brecha está cerca con relación a los lineamientos de la ISO/IEC 27001:2013, lo que muestra el compromiso de la empresa en el cumplimiento de los requisitos legales y regulatorios relacionados con la seguridad de la información.

- La brecha con relación al dominio A.7 SEGURIDAD DE LOS RECURSOS HUMANOS, el IBAL obtuvo un promedio de 76 puntos, lo que indica que la brecha está cerca con relación a los lineamientos de la ISO/IEC 27001:2013, esto muestra que el IBAL tiene muy bien definidos los procedimientos (en el

proceso de gestión humana) para que los funcionarios comprendan y tengan conciencia de las responsabilidades y funciones relacionados con las actividades que tienen que desarrollar en la empresa.

- La brecha con relación al dominio A.12 SEGURIDAD DE LAS OPERACIONES, el IBAL obtuvo un promedio de 62 puntos, lo que indica que la brecha está medianamente cerca con relación a los lineamientos de la ISO/IEC 27001:2013, esto muestra que el IBAL gestiona las instalaciones para el procesamiento de información y la seguridad la infraestructura tecnológica.

- La brecha con relación al dominio A.9 CONTROL DE ACCESO, el IBAL obtuvo un promedio de 60 puntos, lo que indica que la brecha está medianamente cerca con relación a los lineamientos de la ISO/IEC 27001:2013, esto muestra que el IBAL tiene definido procedimientos para limitar el acceso a la información, garantizar el acceso no deseado a los sistemas y servicios, y vela por que los usuarios tangan salvaguardada la información.

- La brecha con relación al dominio A.11 SEGURIDAD FÍSICA Y DEL ENTORNO, el IBAL obtuvo un promedio de 59 puntos, lo que indica que la brecha está medianamente cerca con relación a los lineamientos de la ISO/IEC 27001:2013, esto muestra que el IBAL tiene definido procedimientos para limitar el acceso físico al centro de datos y tiene sistemas de monitoreo y seguridad, que garantizan el acceso no autorizado a estos.

- La brecha con relación al dominio A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, el IBAL obtuvo un promedio de 51 puntos, lo que indica que la brecha está medianamente cerca con relación a los lineamientos de la ISO/IEC 27001:2013, esto muestra que el IBAL tiene definido algunas funciones y responsabilidades relacionados con la seguridad de la información, garantiza

la seguridad del teletrabajo y el uso de dispositivos móviles, pero le hace falta adoptar políticas con concretas con relación a estos temas.

- La brecha con relación al dominio A.13 SEGURIDAD DE LAS COMUNICACIONES, el IBAL obtuvo un promedio de 49 puntos, lo que indica que la brecha está medianamente distanciada con relación a los lineamientos de la ISO/IEC 27001:2013, esto muestra que el IBAL tiene algunos procedimientos para la gestión de la seguridad en las redes, lo cual es efectivo, pero tendrá que implementar mecanismos de apoyen la gestión de este elemento.

- La brecha con relación al dominio A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS, el IBAL obtuvo un promedio de 45 puntos, lo que indica que la brecha está distanciada con relación a los lineamientos de la ISO/IEC 27001:2013, esto muestra que el IBAL tiene algunos procedimientos no muy bien definidos que garantizan el ciclo de vida de los sistemas de información y tiene separados los entornos de producción y desarrollo de aplicaciones.

- La brecha con relación al dominio A.8 GESTION DE ACTIVOS, el IBAL obtuvo un promedio de 22 puntos, lo que indica que la brecha está muy distanciada con relación a los lineamientos de la ISO/IEC 27001:2013, esto muestra que el IBAL tiene algunos procedimientos relacionados con la gestión de activos, pero estos no están acordes con alguna metodología y no se tiene reglamentada la gestión de medios removibles. Para lo cual deberá revisar y ampliar su política de seguridad de la información que le permita desarrollar estos conceptos.

- La brecha con relación al dominio A.10 CRIPTOGRAFÍA Y A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN, el IBAL obtuvo un promedio de 20 puntos, lo que indica que la brecha está muy distanciada con relación a los lineamientos de la ISO/IEC 27001:2013, esto muestra que el IBAL debe revisar su política de

seguridad de la información periódicamente, con el fin tener sus lineamientos directrices con relación a conceptos como la criptografía entre otros.

- La brecha con relación al dominio A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO, el IBAL obtuvo un promedio de 14 puntos, lo que indica que la brecha está muy lejana con relación a los lineamientos de la ISO/IEC 27001:2013, esto muestra que el IBAL debe desarrollar e implementar planes para la recuperación, que le garanticen la continuidad de la seguridad de la información.

- La brecha con relación al dominio A.15 RELACIONES CON LOS PROVEEDORES, el IBAL obtuvo un promedio de cero, en donde se puede evidenciar que la empresa no tiene una política asociada con la seguridad de la información relacionada con sus proveedores, para lo cual deberá identificar los riesgos asociados con la relación de los proveedores, identificar los controles que se van a aplicar y verificar el cumplimiento de los compromisos pactados en esta política.

6.3.3 Dominios a fortalecer por parte del IBAL. De acuerdo con el análisis de la brecha que tiene el IBAL en sus controles frente a la norma ISO/IEC 27001:2013 Anexo A, los dominios a fortalecer son:

- **A.15 Relaciones con los proveedores.** A través del proceso de gestión jurídica y contractual, el IBAL deberá evaluar la posibilidad de implementar una política específica, relacionada con la seguridad de la información con las relaciones con los proveedores, esto con el fin de mitigar los riesgos asociados con los proveedores del IBAL.

- **A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio**. Con relación los planes y programas para la

continuidad del negocio, el IBAL deberá elaborar un plan de continuidad del negocio y asociar los activos más críticos en la organización, esto con el fin de tener planificado una estrategia que le permita recuperarse ante un incidente relacionado con la seguridad de la información.

- **A.5 Políticas de seguridad de la información**. Con relación a las políticas asociadas a la seguridad de la información, el IBAL deberá reformularla con base a los dominios que se tienen que fortalecer, así mismo, deberá ampliar el contenido con la especificación de los roles y responsabilidades relacionados con la seguridad, y por último deberá definir los términos en los cuales se va a revisar anualmente esta política, con el fin de aplicar los cambios que hayan surgido durante la vigencia de revisión y que sean necesarios establecerlos.

- **A.8 Gestión de activos**. El IBAL deberá realizar un inventario de activos de información, en el cual se puedan determinar los criterios de importancia del activo en la empresa, quien o quienes son los propietarios de los activos, quien o quienes son los responsables de gestionar estos activos, así mismo se debe realizar una gestión del riesgo que permita identificar los controles que se tendrían que implementar para mitigar el impacto ante un incidente.

6.3.4 Dominios a mantener por parte del IBAL. De acuerdo con norma ISO/IEC 27001:2013 Anexo A, los dominios a mantener y organizar son:

- **A.6 Organización de la seguridad de la información**. El IBAL deberá especificar en su manual específico de funciones, los roles y responsabilidades relacionados con la seguridad de la información, igualmente se deberá documentar los lineamientos para garantizar la seguridad del teletrabajo, así como el uso de los dispositivos móviles en los procesos de la empresa, esto con el fin de garantizar la protección de la información que se gestiona a través de las conexiones y medios digitales.

- **A.7 Seguridad de los recursos humanos**. Deberán revisarse los procedimientos con el proceso de gestión humana del IBAL, con el fin de articular las funciones seguridad de la información, los procedimientos cuando exista alguna novedad en la nómina que tenga relación con un funcionario de la empresa, y por último los procesos de inducción y reinducción.

- **A.18 Cumplimiento**. Se deberán documentar en el proceso de gestión tecnológica del IBAL, procedimientos para la detección de vulnerabilidades en la infraestructura tecnológica, con el fin de evaluar la eficacia de los procesos de seguridad que tienen implementados.

6.3.5 Resultados y Análisis Mejores Prácticas en Ciberseguridad. Continuando con el análisis de resultados del cumplimiento el IBAL frente a las mejores prácticas definidas por el marco de NIST (ver cuadro 5 e ilustración 4), se obtuvo con relación a este los siguientes resultados:

Cuadro 5. Calificación del IBAL frente a NIST

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
FUNCIÓN NIST	**CALIFICACIÓN ENTIDAD**	**NIVEL IDEAL CSF**
IDENTIFICAR	27	100
DETECTAR	25	100
RESPONDER	14	100
RECUPERAR	13	100
PROTEGER	45	100

Fuente: Elaboración grupo de trabajo - Instrumento de Evaluación MSPI – articles-5482_Instrumento_Evaluacion_MSPI.xlsx. Versión 1. marzo 2021.

- Núcleo Proteger, el IBAL obtuvo 45 puntos, lo que se puede concluir que la empresa tiene una gran inclinación a proteger los activos de información, controlar el acceso a la información, planes de capacitación y sensibilización a

los funcionarios y partes interesadas con relación a la seguridad de la información.

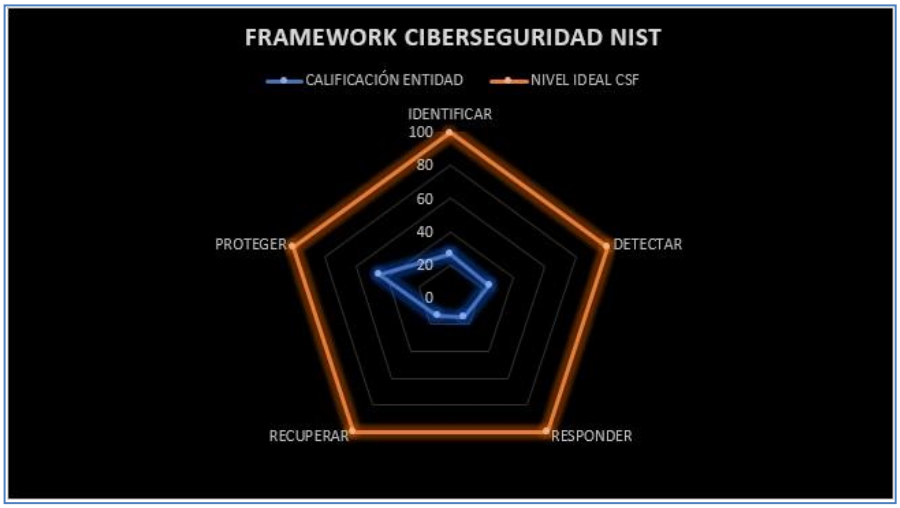
- Núcleo identificar, el IBAL obtuvo 27 puntos, lo que permite concluir que la empresa tiene algunos procedimientos para la gestión de activos, evaluación y gestión del riesgo, probablemente heredados del SIG.

- Núcleo detectar, el IBAL obtuvo 28 puntos, lo que permite concluir que la empresa tiene documentados algunos procedimientos relacionados con la identificación de eventos de ciberseguridad, pero no los está gestionando adecuadamente.

- Núcleo responder, el IBAL obtuvo 14 puntos, lo que permite concluir que la empresa tiene documentando algunas acciones relacionadas con eventos de ciberseguridad, pero no lo gestiona de una manera adecuada.

- Núcleo recuperar, el IBAL obtuvo 13 puntos, lo que permite concluir que la empresa debe desarrollar e implementar planes de resiliencia, que le permitan garantizar la recuperación ante un incidente de ciberseguridad.

Ilustración 4. Resultado según el framework NIST



Fuente: Elaboración grupo de trabajo - Instrumento de Evaluación MSPI – articles-5482_Instrumento_Evaluacion_MSPI.xlsx. Versión 1. marzo 2021.

6.4 INFORMES Y RECOMENDACIONES

Una vez realizadas las actividades de recolección de información y pruebas y análisis, la última actividad de esta fase de diagnóstico, son los informes y recomendaciones, lo cuales se presentan a continuación.

6.4.1 Nivel de Madurez frente al MSPI. De acuerdo con el resultado obtenido al diligenciar la herramienta Instrumento de Evaluación MSPI, se evidencia que el IBAL ***NO ALCANZA EL NIVEL INICIAL DE MADUREZ*** y de cumplimiento de acuerdo con la implementación del Modelo de Seguridad y Privacidad de la Información como se puede ver en el cuadro 6.

Cuadro 6. Nivel de madurez

NIVEL	CUMPLE ?
OPTIMIZADO	FALSO
GESTIONADO CUANTITATIVAMENTE	FALSO
DEFINIDO	FALSO
GESTIONADO	FALSO
INICIAL	FALSO
Nivel de madurez alcanzado	**NO ALCANZA NIVEL INICIAL**

Fuente: Elaboración grupo de trabajo - Instrumento de Evaluación MSPI – articles-5482_Instrumento_Evaluacion_MSPI.xlsx. Versión 1. marzo 2021.

En este nivel se encuentran las entidades, que aún no cuentan con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto, los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información.

6.4.2 Identificación de brecha con relación a ISO/IEC 27001:2013. Para la identificación de la brecha de la seguridad y privacidad de la información con relación a ISO/IEC 27001:2013, se tuvo en cuenta los puntajes obtenidos en el cuadro 3 Resultado de evaluación de efectividad de controles pruebas administrativas y técnicas, columna evaluación de efectividad de controles inexistente, inicial y repetible.

- **A.16 Gestión de incidentes de seguridad de la información**.

Las acciones y/o controles que deberá realizar el IBAL son: en el proceso de gestión tecnológica se deberá implementar un procedimiento relacionado con la gestión de incidentes relacionados con la seguridad de la información, el cual se garantice

registro y seguimiento adecuado de los incidentes relacionados con la seguridad de la información, con el fin de evaluar los riesgos a que están expuestos los activos de información en la empresa. El procedimiento deberá ser socializado entre todos los funcionarios del IBAL, con el fin que ellos notifiquen cualquier evento asociado a un posible incidente de seguridad. Así mismo, se deberá crear un protocolo de respuesta que permita mitigar los incidentes más frecuentes y que pongan en riesgo la seguridad de la información.

- **A.15 Relaciones con los proveedores**.

Las acciones y/o controles que deberá realizar el IBAL son: a través del proceso de gestión jurídica y contractual, el IBAL deberá evaluar la posibilidad de implementar una política específica, relacionada con la seguridad de la información con las relaciones con los proveedores, esto con el fin de mitigar los riesgos asociados con los proveedores del IBAL. En esta evaluación se deberá determinar el nivel de acceso a la información que requieran los proveedores del IBAL, con el fin de cumplir el objeto contractual, y si es necesario fijar cláusulas de confidencialidad que blinden los activos de información.

- **A.5 Políticas de seguridad de la información.**

Las acciones y/o controles que deberá realizar el IBAL son: incluir un apartado relacionado con los activos de información en el alcance de la política, ajustar los principios de la política relacionados con la alineación del SGSI en el IBAL, ya que este sistema de gestión no existe en la empresa, ajustar la política general de seguridad de la información relacionadas con gobierno en línea, y reemplazarlos por gobierno digital. Así mismo, en la política, se deberá incluir los plazos y términos de las revisiones y los responsables de realizarla, esto con el fin de implementar los cambios que puedan presentarse en la empresa y que se consideren necesarios adoptarlos.

- **A.10 Criptografía.**

Las acciones y/o controles que deberá realizar el IBAL son: se deberá implementar mecanismos criptográficos, que permitan garantizar la confidencialidad de los datos o activos de información críticos en la empresa. Estos mecanismos deberán documentarse en el proceso de gestión tecnológica, implementarse y revisarse periódicamente para verificar su efectividad.

- **A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio.**

Las acciones y/o controles que deberá realizar el IBAL son: se deberá elaborar un plan de continuidad del negocio, con el fin de planear las acciones que se deben realizar en la empresa para prevenir y recuperar los activos de información, cuando se materialice un incidente de seguridad, que afecte la seguridad de la información. Este plan deberá ser elaborado con base en la NTC/ISO 22301:2012 y contendrá todas las tareas, roles, responsables y actividades detalladas que permitan reestablecer los servicios en el menor tiempo posible con la menor implicación posible para el IBAL.

- **A.8 Gestión de activos.**

Las acciones y/o controles que deberá realizar el IBAL son: deberá realizar un inventario de activos asociados a la información, identificar los propietarios, identificar y mantener reglas para el uso de estos activos, cuales mecanismos se deberán adoptar para la devolución, mecanismos para la identificación y el su etiquetado.

7 ANÁLISIS DE LOS ACTIVOS DE INFORMACIÓN Y RECURSOS DEL PROCESO DE GESTIÓN TECNOLÓGICA, MEDIANTE LA APLICACIÓN DE LA GUÍA DE RIESGOS DEL DAFP, PARA SU VALORACIÓN, CLASIFICACIÓN Y TRATAMIENTO, CON EL FIN DE GESTIONAR LA CONFIDENCIALIDAD, DISPONIBILIDAD E INTEGRIDAD DE LA INFORMACIÓN.

Una vez concluida la fase de diagnóstico del estado actual del IBAL con relación a al MSPI, se procedió a desarrollar la fase de planificación, para lo cual se toma como insumo los resultados obtenidos en la fase anterior.

7.1 CONTEXTO DEL IBAL

El IBAL es una empresa de servicios públicos, que presta los servicios domiciliarios de acueducto y alcantarillado en la ciudad de Ibagué, actualmente tiene las siguientes sedes en la ciudad:

- Sede principal en la K 3 1 04 Barrio La Pola, en esta sede funciona la sede administrativa de la empresa, en ella se encuentran entre otros, el proceso de gestión tecnológica, el datacenter donde se ubican los servidores de la empresa, se tienen centralizadas las comunicaciones (internet de 50 Mbps y canales de datos) y se gestiona toda la seguridad perimetral de la red local y las otras sedes de la empresa.

- Sede la 15. En esta sede localizada en la calle 15 6 48, se encuentran la oficina de los subprocesos de Gestión de Cartera y una parte del proceso de Gestión Atención al cliente y PQR.

- Sede Fontainebleau. En esta sede localizada en la K 5 con 37, se encuentra la oficina del proceso de Gestión Documental.

- Sede Cádiz. En esta sede localizada en la calle 35 4ª 05 Barrio Cádiz, se encuentra la oficina del subproceso de facturación y recaudo.

- Sede F25. En esta sede localizada en 5 # 41-16 edificio F25, se encuentra la oficina del subproceso de Gestión Atención al cliente y PQR.

Con relación a la infraestructura tecnológica, la empresa tiene una topología de red en estrella en donde hay un datacenter principal y las estaciones de trabajo de los usuarios finales (pc con sistema operativo Windows) de todas las sedes se conectan a él por medio de canales de datos (MPLS), los cuales están contratados con la empresa de comunicaciones de Bogotá (ETB). EL IBAL tiene una conexión a internet de 50 Mbps (con reúso 1:1) contratado con la empresa Media Commerce, la cual es distribuida a las sedes por los canales de datos. Los computadores de los usuarios finales están bajo una red de dominio de Windows Server, lo que permite administrarlos eficientemente mediante una serie de directivas de grupo (GPO) las cuales se encuentran en el servidor de dominio principal y son propagadas por todas las sedes de la empresa, por los canales de datos.

Con relación al aspecto administrativo y organizacional, la empresa tiene un sistema integrado de gestión (SIG), que de acuerdo con el mapa de procesos vigente (ver ilustración 5), se observan los siguientes procesos misionales: Producción de agua potable, Aseguramiento y calidad de agua, Saneamiento Básico, Gestión comercial y Gestión Ambiental.

Profundizando en los procesos misionales del IBAL encontramos que:

- El proceso de producción de agua potable, hace referencia a las actividades que desarrolla el IBAL para captar, transportar, tratar, conducir, almacenar y distribuir el agua potable a los suscriptores de la empresa[36].

- El proceso de aseguramiento de la calidad de agua, hace referencia al monitoreo de la calidad del agua antes, durante y después de su tratamiento, mediante el análisis de las condiciones físico químicas, organolépticas y bacteriológicas[37].

Ilustración 5. Mapa de procesos IBAL

Fuente: EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, sitio web. Disponible en: https://www.ibal.gov.co/sites/default/files/inline-images/Mapa%20de%20procesos%20octubre%202021.jpg

---

[36] SUPERINTENDENCIA DE SERVICIOS PÚBLICOS DOMICILIARIOS. [sitio web]. Bogotá D.C. SSPD. Sistema único de información Sui. [Consultado: 18 de mayo de 2021]. Disponible en: http://www.sui.gov.co/web/acueducto

[37] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué. IBAL. Laboratorio de control de calidad. [Consultado: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/laboratorio-de-control-de-calidad-luis-eduardo-de-le-n-caicedo

- El proceso de Saneamiento básico, hace referencia a las actividades que desarrolla el IBAL para la recolección de residuos líquidos, la conducción de residuos líquidos, el tratamiento de residuos líquidos y su disposición final[38].

- El proceso de gestión comercial, hace referencia a las actividades para facturar los servicios de acueducto y alcantarillado a los suscriptores de la empresa, este proceso se inicia con la lectura de los consumos que se han registrado el micromedidor de agua hasta el recaudo de los servicios prestados. Este conjunto de actividades se realizan de manera mensual y se realizan a la totalidad de los suscriptores de la empresa, que para agosto de 2021 están en 158,706[39].

- El proceso de gestión ambiental, hace referencia a las actividades para la conservación ambiental, haciendo uso racional y sostenible de los recursos, con el fin de mitigar los aspectos e impactos ambiental que puedan surgir por la prestación de los servicios de acueducto y alcantarillado[40].

Si bien es cierto cada uno de los procesos misionales que tiene EL IBAL son importantes para su operación, se puede observar el proceso de gestión comercial tienen un alto contenido de datos e información, la cual debe gestionarse de manera ágil, oportuna y confiable, ya que, a través de la liquidación de la facturación mensual y el recaudo de la misma, la empresa percibe los ingresos necesarios para realizar las inversiones en las redes de acueducto y alcantarillado y así garantizar la prestación de sus servicios.

---

[38] SUPERINTENDENCIA DE SERVICIOS PÚBLICOS DOMICILIARIOS [sitio web]. Bogotá: SSPD, Sistema único de información Sui. [Consulta: 18 de mayo de 2021]. Disponible en: http://www.sui.gov.co/web/alcantarillado

[39] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL. Información de suscriptores facturados servicio de acueducto, periodo de agosto 2021 en SOLIN CLOUD ERP.

[40] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Sistema de gestión ambiental. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/pol-tica-del-sistema-de-gesti-n-ambiental

Debido a la gran importancia del proceso de gestión comercial para el objeto misional del IBAL, es vital profundizar un poco más en las actividades que se realizan al interior de este, con el fin de brindar un mejor contexto a la fase de planificación. El proceso de gestión comercial desarrolla mensualmente las siguientes actividades:

- Toma de lecturas a los micromedidores. Este proceso se realizar de manera mensual, a través del uso de dispositivos móviles (celulares) y una aplicación APK instalada en él, para la captura de las lecturas del micromedidor de agua, que se encuentra en cada uno de los predios de los suscriptores de la empresa.

- Análisis y determinación de los consumos a facturar. En este proceso posterior a la toma de lectura, permite identificar el consumo a facturar, esto se realiza a través del desarrollo de las siguientes actividades: crítica, post crítica, relecturas, notificaciones para revisión y revisiones internas.

- Liquidación de la facturación. Este proceso liquida los consumos de acuerdo con las tarifas para los servicios de acueducto y alcantarillado y los conceptos asociados a cada suscriptor.

- Entrega de la facturación a los suscriptores en los predios.

- Recaudo de la facturación a través de bancos y convenios con otras entidades.

- Registro de novedades de la facturación (pqr, abonos, financiaciones, etc).

Se puede concluir que, el conjunto de actividades que se realizan mensualmente en el proceso de gestión comercial, deben estar coordinadas de principio a fin, y tener un buen apoyo tecnológico que permita agilizar las actividades y garantice la integridad de la información en cada una de ellas, ya que, a través de este, la

empresa percibe los recursos necesarios para el cumplimiento del objeto social y un problema en el flujo de actividades del proceso, generaría graves consecuencias económicas para el IBAL.

Por otra parte, continuando con el contexto de los procesos que tiene el IBAL en el SIG, es importante mencionar que a través del proceso de Gestión Tecnológica se tiene que "*Garantizar el efectivo apoyo tecnológico a las diferentes áreas del IBAL S.A. ESP OFICIAL, mediante la asignación, administración y mejora de los recursos tecnológicos disponibles (hardware, software, redes y comunicaciones)*" [41]. Este enfoque que se presenta en la matriz de caracterización del proceso de gestión tecnológica, indica qué a través de este, se deben brindar todas las condiciones técnicas y tecnológicas, para que el cada uno de los funcionarios del IBAL, tenga a su disposición, todas las plataformas informáticas que tiene la entidad con el fin de desarrollar las actividades diarias, en función de los procesos a que pertenecen.

7.2 NECESIDADES Y EXPECTATIVAS DE LAS PARTES INTERESADAS

Con el fin de identificar las partes interesadas con relación al MSPI, a continuación, se hace una relación de cargos que pueden verse afectados en caso que ocurra un incidente relacionado con la seguridad de la información.

- **Gerente**. Encargado desarrollar los procesos de planeación, organización, control, orientación, ejecución y dirección, así como ejecutar las disposiciones de la asamblea general, y la junta directiva[42]. Deberá ser el responsable de velar

[41] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL, Matriz de caracterización gestión tecnológica. [Consultado: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/CARACTERIZACI%C3%93N%20GESTI%C3%93N%20TECNOLOGICA%20v14.pdf

[42] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Manual específico de funciones y competencias laborales 2018. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/MANUAL-DE-FUNCIONES-RESOLUCION-0755-DEL-03-DE-AGOSTO-DE-2018_0.pdf

por la implementación de las políticas relacionadas con la seguridad y privacidad de la información, en el marco del cumplimiento de su función legales establecidas en la resolución IBAL 0755 de 03 de agosto de 2018.

- **Dirección comercial y de servicio al cliente**. Responsable de la planeación, ejecución y control de las políticas, planes, programas y proyectos comerciales, mediante una adecuada y oportuna gestión comercial[43]. Deberá velar por la planeación y ejecución de las actividades del proceso de gestión comercial, con el fin de garantizar el correcto tránsito de información entre actividades que conforman el proceso.

- **Líder del proceso de facturación y recaudo.** Responsable de planear, coordina y controlar la ejecución del proceso de facturación, el cual incluye las actividades de cargue de información, lectura, crítica, post-crítica, visitas de desviación, liquidación, impresión y entrega de facturas[44]. Con relación a las necesidades y expectativas el líder del proceso de facturación y recaudo, es el responsable de coordinar y velar por la ejecución de todas las actividades del proceso de facturación.

- **Líder del proceso de gestión tecnológica**. Responsable de la administración, control de la infraestructura, seguridad integral de la plataforma tecnológica y los sistemas de información del IBAL, contribuyendo a garantizar la protección, confidencialidad, integridad y disponibilidad de la información y los sistemas de

[43] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Manual específico de funciones y competencias laborales 2018. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/MANUAL-DE-FUNCIONES-RESOLUCION-0755-DEL-03-DE-AGOSTO-DE-2018_0.pdf

[44] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Manual específico de funciones y competencias laborales 2018. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/MANUAL-DE-FUNCIONES-RESOLUCION-0755-DEL-03-DE-AGOSTO-DE-2018_0.pdf

información[45]. Con relación a las necesidades y expectativas el líder del proceso de gestión tecnológica, es el responsable de la garantizar la disponibilidad, integridad, confidencialidad y seguridad de la información en el IBAL.

7.3 ALCANCE DEL MSPI

Para determinar el alcance del MSPI para el IBAL, es importante conjugar varios factores con el fin de determinar los límites y la aplicabilidad que se le dará al modelo en la fase de implementación.

- Como primer factor se tiene que, el proceso de gestión comercial es, por su alta complejidad, altos volúmenes de información e importancia para la operación de la empresa, el proceso sobre el cual se va a centrar la planificación del modelo.

- Como segundo factor se tiene que el proceso de gestión tecnológica, será el responsable de realizar la gestión de los riesgos asociados a la seguridad de la información del proceso de gestión comercial, así como el de diseñar e implementar los controles necesarios con el fin de eliminar las vulnerabilidades que se puedan detectar en los elementos que conforman los sistemas de información de este proceso, con el fin de reducir el impacto que puede generar un incidente de seguridad. Así mismo deberá elaborar y auditar periódicamente los planes de contingencia y de recuperación ante posibles fallas o incidentes, que comprometan de la información del proceso comercial.

- Como tercer factor que se debe tener en cuenta para la planificación del modelo, es el resultado de diagnóstico que se obtuvo a través del diligenciamiento del Instrumento de Evaluación MSPI, el cual permite determinar el estado actual de

[45] EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Manual específico de funciones y competencias laborales 2018. [Consultado: 18 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/MANUAL-DE-FUNCIONES-RESOLUCION-0755-DEL-03-DE-AGOSTO-DE-2018_0.pdf

la gestión de seguridad y privacidad de la información en el IBAL y las vulnerabilidades administrativas y técnicas con relación a los dominios del anexo A de la norma ISO/IEC 27001:2013. Los resultados que se van a reforzar durante la planificación son los que resultaron INEXISTENTE, INICIAL Y REPETIBLE según la evaluación de efectividad de control, los cuales son:

- A.5 Políticas de seguridad de la información.
- A.8 Gestión de activos.
- A.10 Criptografía.
- A.15 Relaciones con los proveedores.
- A.16 Gestión de incidentes de seguridad de la información.
- A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio.

7.4 LIDERAZGO Y COMPROMISO DE LA ALTA DIRECCIÓN

El IBAL su sistema integrado de gestión (SIG), tiene delegado por acto administrativo a un funcionario encargado de liderar las actividades encaminadas a la gestión de los sistemas certificados por la empresa (OHSAS 18001, ISO 14001 e ISO 9001:2015), por ende, a este funcionario se le deberán las responsabilidades asociadas al MSPI, como parte de sus funciones.

Así mismo acorde con lo dispuesto en el Decreto 1499 de 2017[46] "*…Decreto Único Reglamentario del Sector Función Pública..*" en cada una de las entidades públicas del estado, deberá existir un **Comité Institucional de Gestión y Desempeño,** el cual atenderá todos los temas relacionados con la implementación y desarrollo de

[46] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: DAFP, Decreto 1499 (11, septiembre, 2017). Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83433

las políticas de gestión de la empresa, motivo por el cual es importante definir que, a través de este comité, se realizarán todas las gestiones encaminadas a implementar, operar, evaluar y garantizar el mejoramiento continuo del modelo a través de las siguientes funciones:

- Coordinar la inclusión en el manual especifico de funciones y competencias laborales de la empresa, funciones relacionadas con seguridad y privacidad de la información, así como los funcionarios a los que se les delegará esta responsabilidad.

- Planear y coordinar las estrategias relacionadas con la publicación y adopción de la política general del modelo, los objetivos y las políticas específicas de seguridad y privacidad de la información.

- Planear y coordinar los recursos necesarios para la implementación, seguimiento y mejoramiento continuo del MSPI.

- Realizar las revisiones periódicas al MSPI, con el fin de planear las posibles acciones de mejora o acciones correctivas, que garanticen la continuidad del modelo.

- Entre otras que resulten de la planificación e implementación del MSPI.

7.5 ROLES Y RESPONSABILIDADES

Para el desarrollo del MSPI es importante definir los roles y responsabilidades para garantizar el cumplimiento de los objetivos del modelo.

- **Gerencia.**

- Adoptar la política de seguridad y privacidad de la información, sus objetivos y políticas específicas.

- Garantizar la disponibilidad de recursos financieros, humanos, técnicos y tecnológicos que se requieran para implementar la política de seguridad y privacidad de la información.

- Comunicar a la empresa la importancia del MSPI.

- Asegurar que el MSPI logre los resultados previstos.

- Realizar las revisiones periódicas a la adopción del MSPI.

- **Líder del Proceso de Gestión Tecnológica.**

- Apoyar las actividades relacionadas con el autodiagnóstico, planificación, operación, evaluación y mejoramiento continuo del MSPI.

- Realizar la difusión y socialización de la presente política de seguridad y privacidad de la información.

- Elaborar y actualizar la documentación de todos los procedimientos, protocolos, instructivos, guías y manuales, que se deriven de la presente política de seguridad y privacidad de la información.

- Garantizar la adopción y realizar seguimiento de los controles relacionados en la política de seguridad y privacidad de la información del IBAL.

- Gestionar de una manera adecuada, el inventario de activos de información y recursos tecnológicos de propiedad o bajo custodia del IBAL, relacionados en el MSPI.

- **Líder del Proceso de Gestión Humana.**

- Garantizar qué se incluya en el programa de capacitaciones planeadas por la empresa, la política de seguridad y privacidad de la información y los cambios que en ella se realicen.

- Gestionar la inclusión de los artículos necesarios en el manual especifico de funciones y competencias laborales de la empresa, relacionados con las actividades desarrolladas en el MPSI.

- **Líder del Proceso de Gestión Jurídica y Contractual**

- Gestionar la inclusión en las minutas de los contratos suscritos entre el IBAL y terceros, acuerdos de confidencialidad relacionadas con los activos de información que tengan acceso por el desarrollo del objeto contractual.

- **Director de Control Interno de Gestión.**

- Incluir en el plan anual de auditorías, mecanismos de verificación para evaluar e informar sobre el cumplimiento de la implementación de la política de seguridad y privacidad de la información.

- Elaborar informes para la gerencia sobre el cumplimiento de la política de seguridad y privacidad de la información.

- Realizar las recomendaciones necesarias para el cumplimiento de la política de seguridad y privacidad de la información.

- **Funcionarios, contratistas y demás partes interesadas.**

- Deberán conocer y cumplir a cabalidad la política de seguridad y privacidad de la información y los requisitos que ella impone, so pena las sanciones disciplinarias que acarreé el incumplimiento de la misma.

- Participar activamente en las capacitaciones relacionadas con la política de seguridad y privacidad de la información.

7.6 PLANIFICACIÓN

Para elaborar fase de planificación del MSPI, se tuvieron en cuenta los factores qué en el desarrollo del este documento, han tenido una alta incidencia con la seguridad y privacidad de la información en el IBAL:

- **Diagnóstico:** con el desarrollo de esta fase se logró identificar el estado actual del IBAL, con relación a los requerimientos del MSPI y los dominios con relación a la ISO/IEC 27001:2013, en los cuales el IBAL estaba débil.

- **Contexto de la entidad:** a través del contexto se identificaron los procesos de gestión tecnológica y gestión comercial, como los procesos con un alto grado de relevancia en la planificación del modelo.

- **Liderazgo, roles y responsabilidades:** a través de la identificación de los actores más importantes para gestionar y administrar el MSPI, se podrá garantizar la implementación de todos los procedimientos que se describan en él MSPI.

7.6.1 Gestión del riesgo. Una vez identificado los factores más relevantes para la fase de planificación, se procede a detallar la metodología realizar la gestión del riesgo en los activos de información. Para esto se tomará como base la *GUÍA PARA LA ADMINISTRACIÓN DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PÚBLICAS DEL DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA (EN ADELANTE DAFP)* Versión 5 de diciembre de 2020[47].

De acuerdo con la guía del DAFP, se tiene que realizar los siguientes pasos para la gestión del riesgo:

7.6.1.1 Identificación y valoración de los activos de información. Inicialmente, es importante conocer que un activo es cualquier componente que juega un papel importante dentro de los procesos que se realizan en el grupo de gestión tecnológica y en el proceso de gestión comercial, por ejemplo: aplicaciones, servicios web, redes de comunicaciones, datos físicos o digitales, bases de datos, dispositivos, entre otros. Es por ello, que se hace relevante identificar y determinar cuáles son los elementos que se deben de proteger y con esto garantizar que la prestación de los servicios dentro del IBAL se realice dentro de un entorno digital seguro.

Para realizar la adecuada gestión de los activos de seguridad de la información en el IBAL, deberán realizarse las siguientes preguntas:

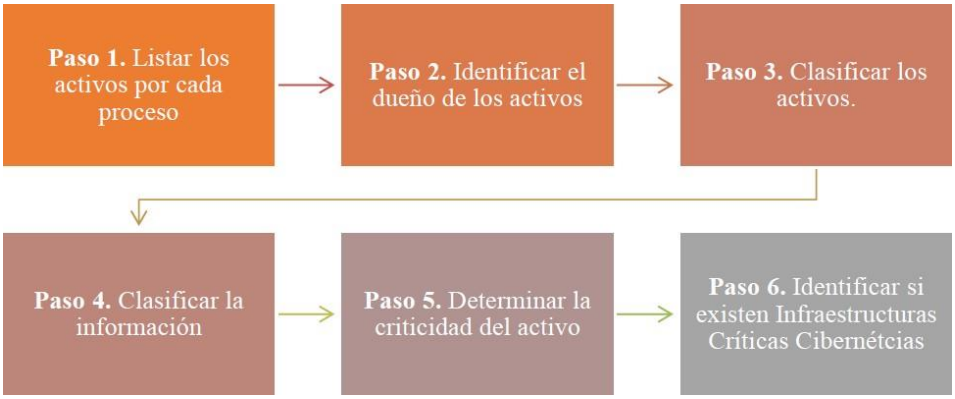
¿Qué activos son esenciales para que el proceso de gestión tecnológica cumpla con los objetivos plasmados en él SIG?

[47] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: DAFP, Guía para la administración del riesgo y el diseño de controles en entidades pública. Versión 5 diciembre de 2020. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238&download=true

¿Cuáles son los activos esenciales para el desarrollo de las actividades del proceso de gestión comercial?

Una vez planteados estos dos interrogantes, es importante desarrollar los pasos que se mencionan en el Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas en adelante ***MGRSD***[48]. De acuerdo con el MGRSD, se deben realizar los siguientes pasos para la identificación y valoración de activos, como se muestra en la ilustración 6.

Ilustración 6. Pasos para la identificación y valoración de activos



Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, Versión 1. Página 12.

A continuación, se detallan cada uno de los pasos:

- **Paso 1. Listar los activos para cada proceso**. Dentro de los procesos de Gestión Tecnológica y Dirección Comercial del IBAL, se identificaron y se listaron

[48] DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: DAFP, Anexo 4 - Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. [Consulta: 18 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

los activos señalando el identificador único, nombre del activo, su respectiva descripción y el proceso al que pertenece. El listado que se puede consultar en el cuadro 7.

Cuadro 7. Listado de activos de información IBAL

ID Activo	Proceso	Nombre del Activo	Descripción del Activo
GC-001	Gestión Comercial	Dispositivos Celulares	Permiten capturar los datos de las lecturas mensualmente de los micromedidores de agua de los suscriptores del IBAL.
GC-002	Gestión Comercial	Catastro de suscriptores	Datos de los suscriptores de la empresa a los cuales se les presta el servicio de acueducto y alcantarillado. Con estos datos, los consumos y tarifas, se realiza proceso de liquidación de la factura.
GC-003	Gestión Comercial	Recurso Humano	Funcionarios administrativos y operarios encargados de la toma de lecturas, relecturas, revisiones internas y entrega de facturas, análisis de consumos, liquidación de la factura y gestión de las novedades del proceso comercial (pqr, pagos, abonos, financiaciones, etc).
GC-004	Gestión Comercial	Documentos en papel	Conformado por los documentos en físico necesarios para realizar algunas de las actividades del proceso comercial, entre los cuales están: las notificaciones para revisión interna, las revisiones internas y toma de lecturas manual.
GT-001	Gestión Tecnológica	Solin CLOUD ERP	Software ERP para gestionar la información de todos los procesos del IBAL, responsable de realizar el proceso de liquidación de la factura del servicio a los suscriptores. Software on-premise.
GT-002	Gestión Tecnológica	Base de datos SOLIN CLOUD ERP	Base de datos relacional en MS SQL SERVER 2014, con la información de todos los procesos del IBAL, entre ellos el catastro de suscriptores.
GT-003	Gestión Tecnológica	Intranet	Software de aplicación basada en la web, para gestionar los datos de la toma de lecturas a través de los dispositivos celulares. Software on-premise.
GT-004	Gestión Tecnológica	Base de datos Intranet	Base de datos relacional en MS SQL SERVER 2017 EXPRESS, con los datos del proceso de toma de lecturas a través de los dispositivos celulares.
GT-005	Gestión Tecnológica	Servidor de Aplicaciones SOLIN CLOUD ERP	Compuesto por el hardware y el software de sistema, software de servicios, por medio del cual se ejecuta el software SOLIN ERP.
GT-006	Gestión Tecnológica	Servidor de Base de datos SOLIN CLOUD ERP	Compuesto por el hardware y el software de sistema y software de servicios, por medio del cual se almacenan los datos e información del software SOLIN ERP.
GT-007	Gestión Tecnológica	Servidor de Aplicaciones INTRANET	Compuesto por el hardware y el software de sistema y software de servicios por medio del cual se ejecutan el software de aplicaciones de la intranet.
GT-008	Gestión Tecnológica	Servidor de Base de datos INTRANET	Compuesto por el hardware y el software de sistema y software de servicios por medio del cual se almacenan los datos e información de la intranet.
GT-009	Gestión Tecnológica	Canales de Datos	Canales de comunicación de datos entre las sedes de la empresa y la sede principal del IBAL, contratados con ETB, tienen un ancho de banda de 15 Mbps.
GT-010	Gestión Tecnológica	Servicio de Internet	Canal dedicado para la conexión a internet de 50 Mbps, con reúso 1:1, el servicio de internet es gestionado y distribuido a todas las sedes de la empresa desde la sede principal del IBAL.

GT-011	Gestión Tecnológica	Firewall	Sistema de seguridad perimetral, con funciones de control de puertos, IDS, IPS y control de navegación, entre otros.
GT-012	Gestión Tecnológica	Switch Core Comunicaciones	Switch capa 2, localizado en el rack de comunicaciones, permite conectar el firewall con los otros dispositivos de comunicación.
GT-013	Gestión Tecnológica	Switch Core Servidores	Switch capa 2, localizado en el rack de servidores, permite la comunicación entre los servidores y el Switch del rack de comunicaciones.
GT-014	Todos	Computadores usuarios finales	Dispositivos de trabajo de los funcionarios de la empresa, por medio del cual acceden al software SOLIN, la intranet e internet para realizar sus actividades diarias.
GT-015	Todos	Antivirus	Sistema de protección contra malware que se instala en los computadores de los usuarios finales y servidores de la empresa.
GT-016	Gestión Tecnológica	Datacenter	Espacio físico para el alojamiento de los servidores y centralización de las comunicaciones del IBAL. En él se encuentran el rack de servidores y el rack de comunicaciones con unas condiciones ambientales y eléctricas controladas para su funcionamiento.

Fuente: elaboración grupo de trabajo.

- **Paso 2. Identificar el dueño de los activos**. En este paso, se debe de reconocer el propietario designado para cada uno de los activos identificados, con el propósito de designar los responsables de la protección y mantenimiento de estos elementos, esta información se puede ver en el cuadro 8.

Cuadro 8. Propietario de los activos de información IBAL

ID Activo	Proceso	Nombre del Activo	Propietario Designado del Activo
GC-001	Gestión Comercial	Dispositivos Celulares	Operarios de facturación
GC-002	Gestión Comercial	Catastro de suscriptores	Líder del proceso de gestión comercial
GC-003	Gestión Comercial	Recurso Humano	Líder del proceso de gestión comercia
GC-004	Gestión Comercial	Documentos en papel	Líder subproceso de Gestión Cartera Líder subproceso de facturación y recaudo Líder subproceso de Gestión de atención al cliente y pqr
GT-001	Gestión Tecnológica	Solin CLOUD ERP	Líder del proceso de Gestión tecnológica
GT-002	Gestión Tecnológica	Base de datos SOLIN CLOUD ERP	Líder del proceso de Gestión tecnológica
GT-003	Gestión Tecnológica	Intranet	Líder del proceso de Gestión tecnológica
GT-004	Gestión Tecnológica	Base de datos Intranet	Líder del proceso de Gestión tecnológica
GT-005	Gestión Tecnológica	Servidor de Aplicaciones SOLIN CLOUD ERP	Líder del proceso de Gestión tecnológica
GT-006	Gestión Tecnológica	Servidor de Base de datos SOLIN CLOUD ERP	Líder del proceso de Gestión tecnológica
GT-007	Gestión Tecnológica	Servidor de Aplicaciones INTRANET	Líder del proceso de Gestión tecnológica
GT-008	Gestión Tecnológica	Servidor de Base de datos INTRANET	Líder del proceso de Gestión tecnológica
GT-009	Gestión Tecnológica	Canales de Datos	Líder del proceso de Gestión tecnológica
GT-010	Gestión Tecnológica	Servicio de Internet	Líder del proceso de Gestión tecnológica
GT-011	Gestión Tecnológica	Firewall	Líder del proceso de Gestión tecnológica
GT-012	Gestión Tecnológica	Switch Core Comunicaciones	Líder del proceso de Gestión tecnológica
GT-013	Gestión Tecnológica	Switch Core Servidores	Líder del proceso de Gestión tecnológica
GT-014	Todos	Computadores usuarios finales	Funcionarios del IBAL
GT-015	Todos	Antivirus	Líder del proceso de gestión tecnológica
GT-016	Gestión Tecnológica	Datacenter	Líder del proceso de gestión tecnológica

Fuente: elaboración grupo de trabajo.

- **Paso 3. Clasificar los activos**. Se determinó para cada activo identificado, a que grupo de activos según su naturaleza pertenece. Para realizar esta clasificación se tomó como referencia la tipología de activos que sugiere el MGRSD (Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas), como se muestra en el cuadro 9.

Cuadro 9. Tipo de activos según MGRSD

Tipo de Activo	Descripción
Información	Información almacenada en formatos físicos (papel, carpetas, CD, DVD) o en formatos digitales o electrónicos (ficheros en bases de datos, correos electrónicos, archivos o servidores)
Software	Activo informático lógico como programas, herramientas ofimáticas o sistemas lógicos para la ejecución de las actividades
Hardware	Equipos físicos de cómputo y de comunicaciones
Servicios	Servicio brindado por parte de la entidad para el apoyo de las actividades de los procesos,
Intangibles	activos inmateriales que otorgan a la entidad una ventaja competitiva
Componentes de red	Medios necesarios para realizar la conexión de los elementos de hardware y software en una red
Personas	Roles que, por su conocimiento, experiencia y criticidad son considerados activos de información
Instalaciones	Espacio o área asignada para alojar y salvaguardar los datos considerados como activos críticos para la empresa

Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Versión 1. Página 13 y 14.

A continuación, se realiza la clasificación de los activos de información identificados en el IBAL, de acuerdo con la tipología del MGRSD, como se puede ver en el cuadro 10.

Cuadro 10. Clasificación de los activos según el tipo

ID Activo	Proceso	Nombre del Activo	Tipo de Activo
GC-001	Gestión Comercial	Dispositivos Celulares	Hardware
GC-002	Gestión Comercial	Catastro de suscriptores	Información
GC-003	Gestión Comercial	Recurso Humano	Personas
GC-004	Gestión Comercial	Documentos en papel	Información
GT-001	Gestión Tecnológica	Solin CLOUD ERP	Software
GT-002	Gestión Tecnológica	Base de datos SOLIN CLOUD ERP	Información
GT-003	Gestión Tecnológica	Intranet	Software
GT-004	Gestión Tecnológica	Base de datos Intranet	Información
GT-005	Gestión Tecnológica	Servidor de Aplicaciones SOLIN CLOUD ERP	Hardware y software
GT-006	Gestión Tecnológica	Servidor de Base de datos SOLIN CLOUD ERP	Hardware y software
GT-007	Gestión Tecnológica	Servidor de Aplicaciones INTRANET	Hardware y software
GT-008	Gestión Tecnológica	Servidor de Base de datos INTRANET	Hardware y software
GT-009	Gestión Tecnológica	Canales de Datos	Componente de red
GT-010	Gestión Tecnológica	Servicio de Internet	Servicios
GT-011	Gestión Tecnológica	Firewall	Hardware
GT-012	Gestión Tecnológica	Switch Core Comunicaciones	Componente de red
GT-013	Gestión Tecnológica	Switch Core Servidores	Componente de red
GT-014	Todos	Computadores usuarios finales	Hardware y software
GT-015	Todos	Antivirus	Software
GT-016	Gestión Tecnológica	Datacenter	Instalaciones

Fuente: elaboración grupo de trabajo.

- **Paso 4. Clasificar la información**. Para realizar la clasificación de la información se tomó como directrices las leyes 1712 de 2014 y 1581 de 2012, así como también la guía 5 Gestión de activos del Modelo de Seguridad y Privacidad de la Información, como se muestra en el cuadro 11.

Cuadro 11. Clasificación de la información

Clasificación	Descripción
Información pública	Información de acceso libre para cualquier persona u o entidad que la requiera. / No contiene datos personales.
Información pública clasificada	Información confidencial para la gestión de los procesos de la empresa. Puede ser accedida por terceros con autorización. / Contiene datos personales.
Información pública reservada	Información disponible únicamente para procesos de la empresa. / Contiene datos personales

Fuente: COLOMBIA. Congreso de la República, Ley 1712 de 2014. Página 3. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201712%20DEL%2006%20DE%20MARZO%20DE%202014.pdf

En el cuadro 12, se puede ver la clasificación de los activos según el tipo de información.

Cuadro 12. Clasificación de los activos según el tipo de información

ID Activo	Proceso	Nombre del Activo	Clasificación de los activos según el tipo de información
GC-001	Gestión Comercial	Dispositivos Celulares	Información pública clasificada
GC-002	Gestión Comercial	Catastro de suscriptores	Información pública reservada
GC-003	Gestión Comercial	Recurso Humano	Información pública
GC-004	Gestión Comercial	Documentos en papel	Información pública clasificada
GT-001	Gestión Tecnológica	Solin CLOUD ERP	Información pública clasificada
GT-002	Gestión Tecnológica	Base de datos SOLIN CLOUD ERP	Información pública reservada
GT-003	Gestión Tecnológica	Intranet	Información pública clasificada
GT-004	Gestión Tecnológica	Base de datos Intranet	Información pública clasificada
GT-005	Gestión Tecnológica	Servidor de Aplicaciones SOLIN CLOUD ERP	Información pública reservada
GT-006	Gestión Tecnológica	Servidor de Base de datos SOLIN CLOUD ERP	Información pública reservada
GT-007	Gestión Tecnológica	Servidor de Aplicaciones INTRANET	Información pública reservada
GT-008	Gestión Tecnológica	Servidor de Base de datos INTRANET	Información pública reservada
GT-009	Gestión Tecnológica	Canales de Datos	Información pública clasificada
GT-010	Gestión Tecnológica	Servicio de Internet	Información pública
GT-011	Gestión Tecnológica	Firewall	Información pública reservada
GT-012	Gestión Tecnológica	Switch Core Comunicaciones	Información pública reservada
GT-013	Gestión Tecnológica	Switch Core Servidores	Información pública reservada
GT-014	Todos	Computadores usuarios finales	Información pública clasificada
GT-015	Todos	Antivirus	Información pública reservada
GT-016	Gestión Tecnológica	Datacenter	Información pública reservada

Fuente: elaboración grupo de trabajo.

- **Paso 5. Determinar la criticidad del activo**. Para realizar la evaluación de la criticidad de los activos, se tuvo en cuenta el grado de importancia de cada uno respecto a la confidencialidad, integridad y disponibilidad, así se logró identificar el nivel de importancia o criticidad para el proceso de gestión tecnológica y el proceso de gestión comercial. Las escalas utilizadas para esta valoración fueron referidas de la Guía 5. Gestión de Activos del MSPI.

  Para la clasificación de los activos de acuerdo con la integridad, se utilizará ALTA MEDIA y BAJA, los activos de información que aún no se puedan clasificar según su integridad, serán tratados como ALTA. Ver cuadro 13.

Cuadro 13. Criticidad del activo con respecto a la integridad

Clasificación	Criticidad	Descripción
Información pública	(B) BAJA	La Información debe ser precisa coherente y completa, su pérdida no genera consecuencias
Información pública clasificada	(M) MEDIA	La Información debe ser precisa coherente y completa, su pérdida genera impacto negativo leve
Información pública reservada	(A) ALTA	La Información debe ser precisa coherente y completa, su pérdida genera graves consecuencias

Fuente: Elaboración del grupo de trabajo

Para la clasificación de los activos de acuerdo con la disponibilidad (por que puede ser consultada o utilizada por una individuo, proceso o entidad), se utilizará ALTA, MEDIA y BAJA, los activos de información que aún no se puedan clasificar según la disponibilidad, serán tratados como ALTA, ver cuadro 14.

Cuadro 14. Criticidad del activo con respecto a la disponibilidad

Clasificación	Criticidad	Descripción
Información pública	(B) BAJA	La no disponibilidad no con lleva implicaciones de ningún índole
Información pública clasificada	(M) MEDIA	La no disponibilidad genera implicaciones índole legal o económico
Información pública reservada	(A) ALTA	La no disponibilidad genera implicaciones índole legal y pérdidas de tipo económico.

Fuente: Elaboración del grupo de trabajo

Para la clasificación de los activos de acuerdo con la confidencialidad (la información no esté disponible ni será revelada a individuos, entidades o procesos no autorizados), se utilizará ALTA, MEDIA y BAJA, los activos de información que aún no se puedan clasificar según la confidencialidad, serán tratados como ALTA Ver cuadro 15.

Cuadro 15. Criticidad del activo con respecto a la confidencialidad

Clasificación	Criticidad	Descripción
Información pública	(B) BAJA	La Información está sin restricción de uso o conocimiento, la pérdida de confidencialidad no genera consecuencias
Información pública clasificada	(M) MEDIA	Información de la entidad y de sus terceros, puede ser accedida con autorización. la pérdida de confidencialidad genera consecuencias leves
Información pública reservada	(A) ALTA	Información de uso exclusivo para la empresa. la pérdida de confidencialidad genera consecuencias graves

Fuente: Elaboración del grupo de trabajo

Teniendo en cuenta que el nivel de criticidad, es el cálculo que determina el valor del activo en relación con la clasificación de la información, se tienen la siguiente escala de en el cuadro 16.

Cuadro 16. Nivel de criticidad con relación a la clasificación

Nivel de Criticidad	Clasificación
BAJA	Activos en los cuales la clasificación con relación a la confidencialidad, integridad y disponibilidad, es baja
MEDIA	Activos en los cuales la clasificación con relación a la confidencialidad, integridad y disponibilidad, en una de sus propiedades es alta o al menos en una de ella es de nivel medio
ALTA	Activos en los cuales la clasificación con relación a la confidencialidad, integridad y disponibilidad es alta.

Fuente: Elaboración del grupo de trabajo

Una vez establecidos los parámetros para evaluar el nivel de criticidad de los activos identificados en el IBAL, se realiza la respectiva clasificación y se determina el nivel de criticidad de cada uno de estos activos, como se puede ver en el cuadro 17.

Cuadro 17. Clasificación y nivel de criticidad de los activos

ID Activo	Nombre del Activo	Integridad	Disponibilidad	Confidencialidad	Nivel de Criticidad
GC-001	Dispositivos Celulares	M	M	M	M
GC-002	Catastro de suscriptores	A	A	A	A
GC-003	Recurso Humano	B	M	B	B
GC-004	Documentos	M	M	M	M
GT-001	Solin CLOUD ERP	A	A	A	A
GT-002	Base de datos SOLIN CLOUD ERP	A	A	A	A
GT-003	Intranet	M	A	M	M
GT-004	Base de datos Intranet	M	A	M	M
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	A	A	A	A
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	A	A	A	A
GT-007	Servidor de Aplicaciones INTRANET	M	A	M	M
GT-008	Servidor de Base de datos INTRANET	M	A	M	M
GT-009	Canales de Datos	M	M	M	M
GT-010	Servicio de Internet	B	M	M	M
GT-011	Firewall	A	A	A	A
GT-012	Switch Core Comunicaciones	A	A	A	A
GT-013	Switch Core Servidores	A	A	A	A
GT-014	Computadores usuarios finales	M	B	A	A
GT-015	Antivirus	A	A	A	A
GT-016	Datacenter	A	A	A	A

Fuente: elaboración grupo de trabajo.

- **Paso 6. Identificar si existen infraestructuras críticas cibernéticas ICC**. Realizados los pasos anteriores, se procedió a determinar si los activos de información que se identificaron son servicios esenciales y si estos están catalogados como Infraestructura Critica Cibernética (ICC), por que superan alguno de los tres criterios de acuerdo con los lineamientos impartidos por la DAFP, en la ilustración 7.

Ilustración 7. Criterios para identificar ICC

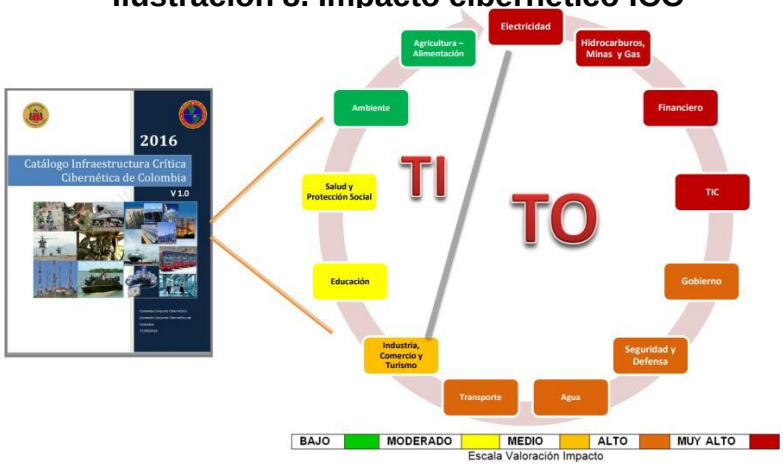
IMPACTO SOCIAL (0,5%) de Población Nacional	IMPACTO ECONÓMICO PIB de un Día o 0,123% del PIB Anual	IMPACTO AMBIENTAL
250.000 personas	$464.619.736	3 años en recuperación

Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Versión 1. Página 18.

Teniendo en cuenta el concepto del Comando Conjunto Cibernético (CCOC) de las Fuerzas Militares de Colombia, sobre infraestructura crítica cibernética "*Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales*[49]", se puede concluir ante un eventual incidente o perturbación que afecte alguno de los activos de información que se identificaron en el IBAL, ninguno de ellos tendría un grave impacto para los usuarios y/o suscriptores de la empresa, que supere los criterios para clasificarlos como ICC, porque ninguno de ellos está enfocado a las TO, como se muestra en la ilustración 8.

[49] ASOCIACION COLOMBIANA DE INGENIEROS DE SISTEMAS [sitio web]. Bogotá: ACIS. Conferencia Comando Conjunto Cibernético, fuerzas militares de Colombia. [Consultado: 18 de mayo de 2021]. Disponible en: https://acis.org.co/archivos/Conferencias/2016/GuiaICC.pdf

Ilustración 8. Impacto cibernético ICC



Fuente: Comando Conjunto Cibernético (CCOC) Página 3. Disponible en: https://www.ccit.org.co/wp-content/uploads/sesion-5-panel-infraestructuras-criticas-ciber-en-colombia.pdf

7.6.1.2 Identificación del riesgo. Una vez realizada la identificación de los activos información, se realiza la definición de los riesgos asociados a los procesos de gestión tecnológica y gestión Comercial del IBAL, donde se tomaron para esta identificación todos los activos valorados en la fase anterior.

Según lo indica la “Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas” presentada por el DAFP, se podrán identificar los siguientes tres (3) riesgos asociados a la seguridad digital: ***perdida de confidencialidad, perdida de integridad y perdida de la disponibilidad***.

Para cada uno de los riesgos identificados, se deben relacionar el grupo de activos específicos del proceso y, simultáneamente, identificar las posibles amenazas y vulnerabilidades que podrían ocasionar la materialización de estos. Es por ello, que para realizar la identificación de los riesgos que pueden afectar los activos, se deben evaluar las amenazas y las vulnerabilidades en razón a las perdidas en la

confidencialidad, integridad y disponibilidad de la información, de la coexistencia de estas dos, depende el riesgo.

La identificación de riesgos, amenazas y vulnerabilidades, se realizó a través del ***análisis de escenarios***, en la cual se expusieron una serie de situaciones las cuales pueden generar perdida de la confidencialidad, integridad y disponibilidad de la información, en los procesos de gestión tecnológica y gestión comercial.

A continuación, en el cuadro 18, se identificaron las siguientes amenazas relacionadas con los objetivos del proceso de gestión tecnológica y gestión comercial, los cuales pueden generar daño a los activos por medio de la explotación de las vulnerabilidades.

Cuadro 18. Amenazas identificadas

Amenaza	Descripción
Acceso no autorizado	Hace referencia al acceso indebido a los recursos de software (sistema operativo, aplicaciones, etc) o al centro de datos por falta de controles efectivos que impidan esta situación.
Destrucción de información	Hace referencia a la pérdida parcial o completa de los datos o información.
Fallas en el hardware	Posibles fallos técnicos que se pueden presentar en la infraestructura tecnológica, como servidores, computadores, terminales portátiles, etc.
Fallas en el software	Posibles fallas a nivel de aplicaciones que suscitan que los procesos tecnológicos presenten resultados inesperados, lo que genera retrasos en las actividades y hasta parálisis en los procesos.
Fallas en las comunicaciones	Problemas técnicos en la red de comunicaciones, lo que genera retrasos en las actividades y hasta parálisis en los procesos.
Hurto o Vandalismo	Se refiere a actos delictivos que ocasionan robos de activos de la información y/o actos vandálicos para sabotear los procesos de las empresas publicas
Malware	Es un software código malicioso diseñado para causar daño a los dispositivos y la información. Entre estos tipos de programas, se encuentra spyware, ransomware, rootkits y muchos más.
Falta de capacitación	Hace referencia a la falta de capacitación o entrenamiento del personal de la empresa, en la gestión de algunas herramientas de software o en la manipulación de hardware que puede generar daño con su manipulación.
Procedimientos desactualizados	Se refiere a que los procedimientos no cuentan con la documentación justificada de cada una de las actividades y/o procesos dentro de las áreas que componen las organizaciones.
Comportamiento no ético	Conductas inapropiadas de los usuarios tanto externos como internos, y que pueden llegar a atentar contra los activos de la información.
Factores ambientales	Es cualquier factor que proviene del medio ambiente, como temperaturas, lluvias, entre otros y puede ocasionar daños en los activos.
Orden público	Se pueden hacer una asonada en las instalaciones físicas de la empresa y puede ocasiones daños en la infraestructura tecnológica
Software desactualizado	Sistema operativo desactualizado, firmware desactualizado
Falta de monitoreo en la infraestructura de TI	Hace referencia a la falta de seguimiento de parámetros críticos en la infraestructura de software y hardware.
Incumplimiento del cronograma	Hace relación al incumplimiento de las actividades planeadas, generadas por el ausentismo laboral, lo que genera retraso en el proceso.

Fuente: elaboración trabajo grupo

A continuación, en el cuadro 19, se identificaron las vulnerabilidades en virtud del tipo de activo.

Cuadro 19. Vulnerabilidades identificadas

Tipo de Activo	Vulnerabilidad
Hardware	Falta de mantenimiento
	Sobrecarga de trabajo
	Fallas en las conexiones eléctricas
	Falta de UPS
	Falla en el suministro de energía alterna
	No existen planes de continuidad y recuperación
Software	Contraseñas débiles o predeterminadas
	Inadecuada gestión o protección de contraseñas
	Configuración predeterminada de servicios
	No existen copias de seguridad
	Software desactualizado
	Aplicaciones sin control de acceso
	Revisión de actualizaciones
	Falta de directivas de grupo
	Falta de antivirus
	No existen planes de continuidad y recuperación
	Falta de documentación/ciclo de vida
Servicios	Servicios no administrados
	Servicios mal configurados o por defecto
Red	Conexiones no controladas
	Falta de administración
	Falta de Documentación y procedimientos
	Falta de acuerdos de nivel de servicio (ANS) en comunicaciones
	Falta de gestión en las políticas
	Administración de red inadecuada
	Conexiones mal estructuradas
Personas	Entrenamiento Insuficiente
	Trabajo no supervisado
	Roles y responsabilidades no establecidas
	Falta de sensibilización en seguridad informática
	Errores humanos
	Planes de Contingencia para la realización de actividades
Instalaciones	Falta de Controles de acceso
	Falta de monitoreo factores críticos (temperatura, eléctrica y respaldo)
	Malas Condiciones eléctricas
	Desastre natural
	Falta de mantenimiento a la infraestructura
	Procedimientos no definidos
	No existen infraestructuras redundantes

Fuente: elaboración grupo de trabajo

A continuación, en el cuadro 20, se relacionan las amenazas y las vulnerabilidades de acuerdo con los tipos de riesgos asociados a la seguridad digital: perdida de confidencialidad, perdida de integridad y perdida de la disponibilidad.

Cuadro 20. Riesgos asociados a la seguridad digital IBAL

ID Activo	Nombre del Activo	Riesgo	Amenazas	Vulnerabilidades
GC-001	Dispositivos Celulares	Pérdida de disponibilidad	Hurto o vandalismo	Errores humanos
GC-002	Catastro de suscriptores	Pérdida de integridad	Acceso no autorizado	No existen copias de seguridad
GC-003	Recurso Humano	Pérdida de disponibilidad	Incumplimiento del cronograma	Falta de Planes de Contingencia para la realización de actividades
		Pérdida de Integridad	Comportamiento no ético	Trabajo no supervisado
				Falta de sensibilización en seguridad informática
GC-004	Documentos en papel	Pérdida de disponibilidad	Destrucción de información	Errores humanos
		Perdidas de confidencialidad	Comportamiento no ético	Trabajo no supervisado
GT-001	Solin CLOUD ERP	Pérdida de integridad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
		Pérdida de disponibilidad	Fallas en la comunicación	Administración de red inadecuada
				Conexiones mal estructuradas
				No existen planes de continuidad y recuperación
				No existen copias de seguridad
		Pérdida de la integridad	Fallas en el software	Software desactualizado
GT-002	Base de datos SOLIN CLOUD ERP	Pérdida de confidencialidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
		Pérdida de disponibilidad	Destrucción de información	No existen planes de continuidad y recuperación
				Servicios mal configurados o por defecto
GT-003	Intranet	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
				No existen copias de seguridad
		Pérdida de la integridad	Fallas en el software	Falta de documentación/ciclo de vida
		Pérdida de confidencialidad	Acceso no autorizado	Aplicaciones sin control de acceso
GT-004	Base de datos Intranet	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	Pérdida de disponibilidad	Fallas en hardware	Falta de mantenimiento
				Fallas en las conexiones eléctricas
				Falta de UPS
				Falla en el suministro de energía alterna
			Malware	Servicios mal configurados o por defecto
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
			Malware	Servicios mal configurados o por defecto
GT-007	Servidor de Aplicaciones INTRANET	Pérdida de disponibilidad	Fallas en hardware	Falta de mantenimiento
				Fallas en las conexiones eléctricas
				Falta de UPS
				Falla en el suministro de energía alterna
			Malware	Servicios mal configurados o por defecto
		Pérdida de la integridad	Fallas en el software	Falta de documentación/ciclo de vida
GT-008	Servidor de Base de datos INTRANET	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas
			Malware	Servicios mal configurados o por defecto
GT-009	Canales de Datos	Pérdida de disponibilidad	Factores ambientales	Falta de acuerdos de nivel de servicio (ANS) en comunicaciones
GT-010	Servicio de Internet	Pérdida de disponibilidad	Factores ambientales	Falta de acuerdos de nivel de servicio (ANS) en comunicaciones
GT-011	Firewall	Pérdida de confidencialidad	Software desactualizado	Revisión de actualizaciones
			Acceso no autorizado	Inadecuada gestión o protección de contraseñas
			Falta de monitoreo en la infraestructura de TI	Falta de gestión en las políticas
		Pérdida de disponibilidad	Fallas en el hardware	Fallas en las conexiones eléctricas

				Falta de UPS
				Falla en el suministro de energía alterna
GT-012	Switch Core Comunicaciones	Pérdida de disponibilidad	Fallas en el hardware	Fallas en las conexiones eléctricas
				Falta de UPS
				Falla en el suministro de energía alterna
			Acceso no autorizado	Inadecuada gestión o protección de contraseñas
GT-013	Switch Core Servidores	Pérdida de disponibilidad	Fallas en el hardware	Fallas en las conexiones eléctricas
				Falta de UPS
				Falla en el suministro de energía alterna
			Acceso no autorizado	Inadecuada gestión o protección de contraseñas
GT-014	Computadores usuarios finales	Pérdida de confidencialidad	Malware	Software desactualizado
		Pérdida de disponibilidad	Fallas en las comunicaciones	Administración de red inadecuada
			Fallas en el software	Falta de directivas de grupo
			Fallas en el Hardware	Falta de mantenimiento
				Fallas en las conexiones eléctricas
				Falta de UPS
				Falla en el suministro de energía alterna
GT-015	Antivirus	Pérdida de confidencialidad	Malware	Software desactualizado
			Falta de monitoreo en la infraestructura de TI	Falta de Documentación y procedimientos
GT-016	Datacenter	Pérdida de disponibilidad	Falta de monitoreo en la infraestructura de TI	Falta de Documentación y procedimientos
				Falta de monitoreo factores críticos
			Fallas en hardware	Falta de mantenimiento a la infraestructura
				Sobrecarga de trabajo
				Fallas en las conexiones eléctricas
				No existen infraestructuras redundantes
				Falta de UPS
				Falla en el suministro de energía alterna
				Desastre natural
			Acceso no autorizado	Falta de Controles de acceso
			Fallas en las comunicaciones	Falta de Documentación y procedimientos
			Procedimientos desactualizados	Falta de Documentación y procedimientos

Fuente: elaboración grupo de trabajo

7.6.1.3 Valoración del riesgo. En esta fase de la administración del riesgo se estableció la probabilidad de ocurrencia de los riesgos identificados y el nivel de consecuencia o impacto, con el fin de identificar la zona de riesgo inicial, para el desarrollo de esta valoración se tuvo en cuenta el nivel de frecuencia que se observa en el cuadro 21.

Cuadro 21. Probabilidad de ocurrencia del riesgo

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	0% - 20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	20.01% - 40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	40.01% - 60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	60.01% - 80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	80.01% - 100%

Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Versión 1. página 39.

Con el fin de determinar la probabilidad de ocurrencia del riesgo, se realizó el análisis del número de veces que se realiza la actividad con relación a cada uno de los activos de información como se muestra en el cuadro 22.

Cuadro 22. Actividades relacionadas con el activo

ID Activo	Nombre del Activo	Nro de Veces aproximado que se ejecuta la actividad por mes	Descripción (fórmula)
GC-001	Dispositivos Celulares	264.51	Total, lecturas suscriptores: 158,706 (Agosto/2021) Lecturas por Operario: 600 registros día Fórmula: 158,706/600
GC-002	Catastro de suscriptores	171.43	Total, novedades catastro de suscriptores: 1,200 (cambios de uso, estrato) Total, Ciclos facturación: 7 Fórmula: 1,200/7
GC-003	Recurso Humano	1,300	Días laborales en el mes: 26 Número de Operarios Lecturas: 50 Fórmula: 26x50
GC-004	Documentos en papel	15,000	Total de actividades de lecturas realizadas en papel.
GT-001	Solin CLOUD ERP	28	Total, Ciclos facturación: 7

			Procesos en ciclos: 1. Lecturas 2. Liquidación 3. Recaudo 4. Novedades Fórmula: 7 x 4
GT-002	Base de datos SOLIN CLOUD ERP	28	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Liquidación 3. Recaudo 4. Novedades Fórmula: 7 x 4
GT-003	Intranet	14	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Relecturas Fórmula: 7 x 2
GT-004	Base de datos Intranet	14	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Relecturas Fórmula: 7 x 2
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	28	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Liquidación 3. Recaudo 4. Novedades Fórmula: 7 x 4
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	28	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Liquidación 3. Recaudo 4. Novedades Fórmula: 7 x 4
GT-007	Servidor de Aplicaciones INTRANET	14	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Relecturas Fórmula: 7 x 2
GT-008	Servidor de Base de datos INTRANET	14	Total, Ciclos facturación: 7 Procesos en ciclos: 1. Lecturas 2. Relecturas Fórmula: 7 x 2
GT-009	Canales de Datos	130	Número de sede: 5 Días laborales en el mes: 26 Fórmula: 7 x 26
GT-010	Servicio de Internet	264.51	Total, lecturas suscriptores: 158,706 Lecturas por Operario: 600 registros día Fórmula: 158,706/600
GT-011	Firewall	7,500	Inventario de Computadores: 250 Días mes: 30 Fórmula: 250 x 30
GT-012	Switch Core Comunicaciones	7,500	Inventario de Computadores: 250 Días mes: 30 Fórmula: 250 x 30
GT-013	Switch Core Servidores	234	Número de Servidores físicos y virtuales: 9 Días laborales en el mes: 26 Fórmula: 9 x 26
GT-014	Computadores usuarios finales	6,266	Inventario de Computadores: 241 Días laborales en el mes: 26 Fórmula: 241 x 26
GT-015	Antivirus	6,500	Inventario de Computadores: 250

			Días laborales en el mes: 26 Fórmula: 250 x 30
GT-016	Datacenter	7,500	Inventario de Computadores: 250 Días mes: 30 Fórmula: 250 x 30

Fuente: elaboración grupo de trabajo

Para medir el impacto del riesgo, se definieron los siguientes criterios en el caso que se llegue a materializar dichos riesgos. Ver cuadro 23.

Cuadro 23 Niveles de medición del Impacto del riesgo

AFECTACION		IMPACTO	
Económica	**Reputacional**	**Cualitativo**	**Cuantitativo**
Afectación en SMLMV	El riesgo afecta la imagen de:		
Menor a 10	Alguna área de la organización	20%	Leve
Entre 10 y 50	La entidad internamente, la junta directiva y/o de proveedores	40%	Menor
Entre 50 y 100	La entidad frente a algunos usuarios en referencia al logro de los objetivos	60%	Moderado
Entre 100 y 500	La entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.	80%	Mayor
Mayor a 500	La entidad a nivel nacional, con divulgación a todo el país	100%	Catastrófico

Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Versión 1. página 40.

De acuerdo con el cuadro 24, se calculó el nivel de impacto en caso de materializarse un riesgo debido a un incidente de seguridad.

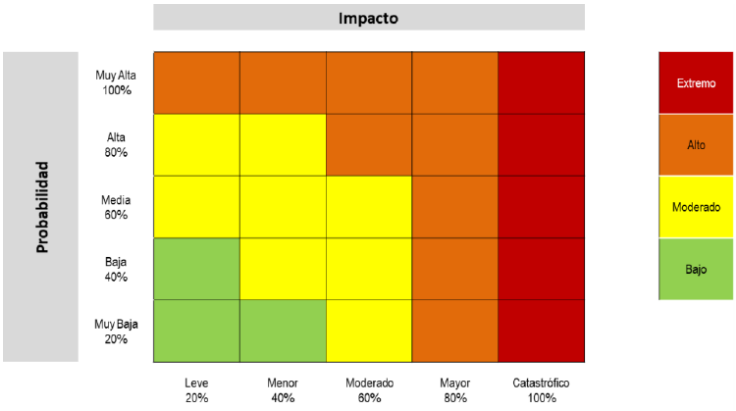
Cuadro 24. Nivel de impacto en caso de materializarse el riesgo

ID Activo	Nombre del Activo	Afectación Económica aproximada	Descripción (formula)
GC-001	Dispositivos Celulares	$ 1,000,000	Valor de un dispositivo móvil año 2021.
GC-002	Catastro de suscriptores	$42,000,000	Total, novedades catastro de suscriptores: 1,200 en el mes. Valor promedio de 1 factura: $ 35,000
GC-003	Recurso Humano	$ 0	Aunque el personal operativo no esté disponible, el IBAL cuenta con mecanismos de ley que le permitan liquidar una factura con consumos promedios por eventualidad.
GC-004	Documentos en papel	$ 40,000	Salario Mensual operario: $ 1,200,000 Días del Mes: 30
GT-001	Solin CLOUD ERP	$ 6,000,000,000,000	Recaudo promedio mensual por facturación de servicios: $ 6,000,000,000,000
GT-002	Base de datos SOLIN CLOUD ERP	$ 6,000,000,000,000	Recaudo promedio mensual por facturación de servicios: $ 6,000,000,000,000
GT-003	Intranet	$ 0	Si se materializa el riesgo, las actividades se puede realizar manualmente.
GT-004	Base de datos Intranet	$ 0	Si se materializa el riesgo, las actividades se puede realizar manualmente.
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	$ 6,000,000,000,000	Recaudo promedio mensual por facturación de servicios: $ 6,000,000,000,000
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	$ 6,000,000,000,000	Recaudo promedio mensual por facturación de servicios: $ 6,000,000,000,000
GT-007	Servidor de Aplicaciones INTRANET	$ 0	Si se materializa el riesgo, las actividades se puede realizar manualmente.
GT-008	Servidor de Base de datos INTRANET	$ 0	Si se materializa el riesgo, las actividades se puede realizar manualmente.
GT-009	Canales de Datos	$ 0	Si se materializa el riesgo se puede realizar las actividades en sede principal del IBAL
GT-010	Servicio de Internet	$ 0	Si se materializa el riesgo se puede realizar las actividades en sede principal del IBAL
GT-011	Firewall	$ 30,000,000	Precio del appliance y configuración de las políticas y servicios
GT-012	Switch Core Comunicaciones	$ 3,000,000	Precio del swtich capa 2
GT-013	Switch Core Servidores	$ 3,000,000	Precio del swtich capa 2
GT-014	Computadores usuarios finales	$ 4,500,000	Valor del computador o de la reconfiguración o de las piezas afectadas.
GT-015	Antivirus	Moderado	Teniendo en cuenta que el riesgo al no tener una solución protección contra virus, se pueden generar daños en los computadores de los usuarios finales, la cual con el tiempo se puede volver a reconstruir. Con relación a los servidores, el riesgo de afectación por malware, generaría la aplicación de los planes de contingencia, lo cual paralizaría los procesos por 5 días aproximadamente, afectando la imagen de la entidad con los usuarios del servicio.
GT-016	Datacenter	$ 6,000,000,000,000	Recaudo promedio mensual por facturación de servicios: $ 6,000,000,000,000

Fuente: Elaboración grupo de trabajo

Para estimar el nivel de riesgo inicial – inherente, se realizó a través de la determinación de la probabilidad y el impacto que puede ocasionar la materialización del riesgo, para esto se tuvo en cuenta el cuadro 25, de acuerdo con la guía del DAFP.

Cuadro 25. Matriz de Calor Inherente



Fuente: DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PUBLICA. Anexo 4 lineamientos para la gestión de riesgos de seguridad digital en entidades públicas. Versión 1. Página 82.

Basado en los criterios anteriormente mencionados, se procedió a determinar la probabilidad y el impacto que puede ocasionar la materialización de los riesgos anteriormente mencionados durante la ejecución de las actividades de los procesos de gestión tecnológica y gestión comercial en el IBAL, ver cuadro 26.

Cuadro 26. Zona de riesgo inherente

ID Activo	Nombre del Activo	Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Inherente Zona de Riesgo
GC-001	Dispositivos Celulares	Pérdida de disponibilidad	Hurto o vandalismo	Errores humanos	Alta (80%)	Leve (20%)	Moderado
GC-002	Catastro de suscriptores	Pérdida de integridad	Acceso no autorizado	No existen copias de seguridad	Alta (80%)	Mayor (80%)	Alto
GC-003	Recurso Humano	Pérdida de disponibilidad	Incumplimiento del cronograma	Falta de Planes de Contingencia para la realización de actividades	Muy Alta (100%)	Leve (20%)	Alto
		Pérdida de Integridad	Comportamiento no ético	Trabajo no supervisado			
				Falta de sensibilización en seguridad informática			
GC-004	Documentos en papel	Pérdida de disponibilidad	Destrucción de información	Errores humanos	Muy Alta (100%)	Leve (20%)	Alto
		Perdidas de confidencialidad	Comportamiento no ético	Trabajo no supervisado	Muy Alta (100%)	Leve (20%)	Alto
GT-001	Solin CLOUD ERP	Pérdida de integridad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Catastrófico (100%)	Extremo
		Pérdida de disponibilidad	Fallas en la comunicación	Administración de red inadecuada			
				Conexiones mal estructuradas			
				No existen planes de continuidad y recuperación			
				No existen copias de seguridad			
		Pérdida de la integridad	Fallas en el software	Software desactualizado			
GT-002	Base de datos SOLIN CLOUD ERP	Pérdida de confidencialidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Catastrófico (100%)	Extremo
		Pérdida de disponibilidad	Destrucción de información	No existen planes de continuidad y recuperación			
				Servicios mal configurados o por defecto			
GT-003	Intranet	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Leve (20%)	Moderado
				No existen copias de seguridad			
		Pérdida de la integridad	Fallas en el software	Falta de documentación/ciclo de vida			
		Pérdida de confidencialidad	Acceso no autorizado	Aplicaciones sin control de acceso			
GT-004	Base de datos Intranet	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Leve (20%)	Moderado
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	Pérdida de disponibilidad	Fallas en hardware	Falta de mantenimiento	Media (60%)	Catastrófico (100%)	Extremo
				Fallas en las conexiones eléctricas			
				Falta de UPS			
				Falla en el suministro de energía alterna			
			Malware	Servicios mal configurados o por defecto			
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Catastrófico (100%)	Extremo
			Malware	Servicios mal configurados o por defecto			
GT-007		Pérdida de disponibilidad	Fallas en hardware	Falta de mantenimiento	Media (60%)	Leve (20%)	Moderado
				Fallas en las conexiones eléctricas			

	Servidor de Aplicaciones INTRANET			Falta de UPS			
				Falla en el suministro de energía alterna			
			Malware	Servicios mal configurados o por defecto			
		Pérdida de la integridad	Fallas en el software	Falta de documentación/ciclo de vida			
GT-008	Servidor de Base de datos INTRANET	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Leve (20%)	Moderado
			Malware	Servicios mal configurados o por defecto			
GT-009	Canales de Datos	Pérdida de disponibilidad	Factores ambientales	Falta de acuerdos de nivel de servicio (ANS) en comunicaciones	Alta (80%)	Leve (20%)	Moderado
GT-010	Servicio de Internet	Pérdida de disponibilidad	Factores ambientales	Falta de acuerdos de nivel de servicio (ANS) en comunicaciones			
GT-011	Firewall	Pérdida de confidencialidad	Software desactualizado	Revisión de actualizaciones	Muy Alta (100%)	Leve (20%)	Alto
			Acceso no autorizado	Inadecuada gestión o protección de contraseñas			
			Falta de monitoreo en la infraestructura de TI	Falta de gestión en las políticas			
		Pérdida de disponibilidad	Fallas en el hardware	Fallas en las conexiones eléctricas			
				Falta de UPS			
				Falla en el suministro de energía alterna			
GT-012	Switch Core Comunicaciones	Pérdida de disponibilidad	Fallas en el hardware	Fallas en las conexiones eléctricas	Muy Alta (100%)	Leve (20%)	Alto
				Falta de UPS			
				Falla en el suministro de energía alterna			
			Acceso no autorizado	Inadecuada gestión o protección de contraseñas			
GT-013	Switch Core Servidores	Pérdida de disponibilidad	Fallas en el hardware	Fallas en las conexiones eléctricas	Alta (80%)	Leve (20%)	Moderado
				Falta de UPS			
				Falla en el suministro de energía alterna			
			Acceso no autorizado	Inadecuada gestión o protección de contraseñas			
GT-014	Computadores usuarios finales	Pérdida de Confidencialidad	Malware	Software desactualizado	Muy Alta (100%)	Leve (20%)	Alto
		Pérdida de disponibilidad	Fallas en las comunicaciones	Administración de red inadecuada			
			Fallas en el software	Falta de directivas de grupo			
			Fallas en el Hardware	Falta de mantenimiento			
				Fallas en las conexiones eléctricas			
				Falta de UPS			
				Falla en el suministro de energía alterna			
GT-015	Antivirus	Pérdida de confidencialidad	Malware	Software desactualizado	Muy Alta (100%)	Moderado (60%)	Alto
			Falta de monitoreo en la infraestructura de TI	Falta de Documentación y procedimientos			
GT-016	Datacenter	Pérdida de disponibilidad	Falta de monitoreo en la infraestructura de TI	Falta de Documentación y procedimientos	Muy Alta (100%)	Catastrófico (100%)	Extremo
				Falta de monitoreo factores críticos			
			Fallas en hardware	Falta de mantenimiento a la infraestructura			
				Sobrecarga de trabajo			
				Fallas en las conexiones eléctricas			
				No existen infraestructuras redundantes			
				Falta de UPS			
				Falla en el suministro de energía alterna			
				Desastre natural			

			Acceso no autorizado	Falta de Controles de acceso			
			Fallas en las comunicaciones	Falta de Documentación y procedimientos			
			Procedimientos desactualizados	Falta de Documentación y procedimientos			

Fuente: Elaboración grupo de trabajo

7.6.1.4 Controles asociados a la seguridad de la información. De acuerdo con la Guía para la administración del riesgo y el diseño de controles en entidades pública de la DAFP, se tiene que emplear como mínimo los controles del anexo 4 Del “Modelo Nacional de Gestión de riesgo de seguridad de la Información en entidades públicas”, referidos en el capítulo 5 páginas 29 a 38, siempre y cuando se ajusten al análisis de riesgos.

Como primera medida para identificar los controles a implementar, se van a tomar los riesgos qué resultaron en la zona de riesgo extremo (ver cuadro 27), debido al nivel de impacto que alguno de ellos puede generar sobre la información y la continuidad del negocio, a su vez el impacto económico que generaría la materialización de estos para el IBAL.

Adicionalmente, como se logró evidenciar en el resultado de la evaluación de los controles con la herramienta del autodiagnóstico de MINTIC (ver cuadro 3), el ***dominio A.17 Aspectos de seguridad de la información de la gestión de la continuidad del negocio,*** obtuvo un puntaje de 14, lo que demuestra que debe tomarse como referencia para diseñar los controles que permitan reducir la brecha de seguridad con relación a la ISO/IEC 27001:2013.

Cuadro 27. Zona de riesgo inherente extremo para la selección de controles

ID Activo	Nombre del Activo	Riesgo	Amenazas	Probabilidad	Impacto	Riesgo Inherente Zona de Riesgo
GT-001	Solin CLOUD ERP	Pérdida de integridad	Acceso no autorizado	Media (60%)	Catastrófico (100%)	Extremo
		Pérdida de disponibilidad	Fallas en la comunicación			
		Pérdida de la integridad	Fallas en el software			
GT-002	Base de datos SOLIN CLOUD ERP	Pérdida de confidencialidad	Acceso no autorizado	Media (60%)	Catastrófico (100%)	Extremo
		Pérdida de disponibilidad	Destrucción de información			
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	Pérdida de disponibilidad	Fallas en hardware	Media (60%)	Catastrófico (100%)	Extremo
			Malware			
GT-006	Servidor de Base de datos SOLIN CLOUD ERP	Pérdida de disponibilidad	Acceso no autorizado	Media (60%)	Catastrófico (100%)	Extremo
			Malware			
GT-016	Datacenter	Pérdida de disponibilidad	Falta de monitoreo en la infraestructura de TI	Muy Alta (100%)	Catastrófico (100%)	Extremo
			Fallas en hardware			
			Acceso no autorizado			
			Fallas en las comunicaciones			
			Procedimientos desactualizados			

Fuente: Elaboración grupo de trabajo

A continuación, en el cuadro 28, se listan los controles que se deben de implementar para mitigar los riesgos identificados (Zona de Riesgo: Extremo), según el Anexo A del estándar ISO/IEC 27001:2013, los cuales se ajustan al análisis de riesgos realizados en la Dirección Comercial y el grupo de Gestión Tecnológica del IBAL.

Cuadro 28. Controles a implementar en la zona de riesgo inherente extremo

ID Activo	Nombre del Activo	Riesgo	Amenazas	Vulnerabilidades	Probabilidad	Impacto	Riesgo Inherente Zona de Riesgo	ACTIVIDAD DE CONTROL	Soporte
GT-001	Solin CLOUD ERP	Pérdida de integridad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Catastrófico (100%)	Extremo	**A.9.1.1** Política de control de acceso **A.13.1.1** Controles de redes **A.17.1.2** Implementación de la continuidad de la seguridad de la información **A.14.2.7** Desarrollo contratado externamente	**A.9.1.1** En la política de seguridad y privacidad de la información, se debe establecer una política de control de acceso más coherente con el nivel del riesgo, con el fin de minimizarlo. **A.13.1.1** Se deben implementar directrices relacionadas con la gestión de seguridad de las redes, encaminadas a establecer las responsabilidades y procedimientos para la gestión de equipos. **A.17.1.2** Se deberán implementar un procedimiento orientado a garantizar el nivel de continuidad en la seguridad de la información, que permita servir de guía ante una situación adversa que se pueda presentar. **A.14.2.7** Se deben implementar directrices relacionadas con el desarrollo de software contratado externamente, con el fin de realizar los ensayos de aceptación para determinar la calidad y exactitud de los entregables.
		Pérdida de disponibilidad	Fallas en la comunicación	Administración de red inadecuada					
				Conexiones mal estructuradas					
				No existen planes de continuidad y recuperación					
				No existen copias de seguridad					
		Pérdida de la confidencialidad	Fallas en el software	Software desactualizado					
GT-002	Base de datos SOLIN CLOUD ERP	Pérdida de confidencialidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Catastrófico (100%)	Extremo	**A.9.1.1** Política de control de acceso **A.17.1.2** Implementación de la continuidad de la seguridad de la información	**A.9.1.1** En la política de seguridad y privacidad de la información, se debe establecer una política de control de acceso enfocada en gestionar los usuarios que se conectan a la base de datos. **A.17.1.2** Se deberán implementar un procedimiento
		Pérdida de disponibilidad	Destrucción de información	No existen planes de continuidad y recuperación					
				Servicios mal configurados o por defecto					

								A.12.3.1 Respaldo de información	orientado a garantizar el nivel de continuidad en la seguridad de la información, que permita servir de guía ante una situación adversa que se pueda presentar. **A.12.3.1** Se deben implementar procedimientos para la verificación de la funcionalidad de las copias de respaldo, ante un evento, así como los roles y responsables de realizar esta actividad.
GT-005	Servidor de Aplicaciones SOLIN CLOUD ERP	Pérdida de disponibilidad	Fallas en hardware	Falta de mantenimiento Fallas en las conexiones eléctricas Falta de UPS Falla en el suministro de energía alterna	Media (60%)	Catastrófico (100%)	Extremo	**A.11.2.4** Mantenimiento de equipos **A.12.6.1** Gestión de las vulnerabilidades técnicas **A.12.7.1** Información controles de auditoria de sistemas **A.17.1.2** Implementación de la continuidad de la seguridad de la información	**A.11.2.4** Se deben implementar procedimientos para la elaboración de los mantenimientos periódicos de los servidores, según las especificaciones del fabricante. Se debe llevar registro de fallas o sospechas con el fin de planear mantenimientos preventivos o correctivos. **A.12.6.1** Se deben implementar procedimientos que permitan la detección y análisis de vulnerabilidades al sistema operativo y los servicios que se tengan configurados. **A.12.7.1** Se deben implementar procedimientos para la auditoria de los registros del sistema, con el fin de evitar eventos que puedan afectar su disponibilidad. **A.17.1.2** Se deberán implementar un procedimiento orientado a garantizar el nivel de continuidad en la seguridad de la información, que permita servir de guía ante una situación adversa que se pueda presentar.
			Malware	Servicios mal configurados o por defecto					
GT-006	Servidor de Base de	Pérdida de disponibilidad	Acceso no autorizado	Inadecuada gestión o protección de contraseñas	Media (60%)	Catastrófico (100%)	Extremo	**A.12.6.1** Gestión de las vulnerabilidades técnicas	**A.12.6.1** Se debe llevar registro de fallas o sospechas con el fin de planear

	datos SOLIN CLOUD ERP		Malware	Servicios mal configurados o por defecto				**A.12.7.1** Información controles de auditoria de sistemas **A.17.1.2** Implementación de la continuidad de la seguridad de la información	mantenimientos preventivos o correctivos. **A.12.6.1** Se deben implementar procedimientos que permitan la detección y análisis de vulnerabilidades al sistema operativo y los servicios que se tengan configurados. **A.12.7.1** Se deben implementar procedimientos para la auditoria de los registros del sistema, con el fin de evitar eventos que puedan afectar su disponibilidad. **A.17.1.2** Se deberán implementar un procedimiento orientado a garantizar el nivel de continuidad en la seguridad de la información, que permita servir de guía ante una situación adversa que se pueda presentar.
GT-016	Datacenter	Pérdida de disponibilidad	Falta de monitoreo en la infraestructura de TI	Falta de Documentación y procedimientos	Muy Alta (100%)	Catastrófico (100%)	Extremo	**A.11.1.1** Perímetro de seguridad física. **A.11.1.2** Controles físicos de entrada. **A.11.2.1** Ubicación y protección de los equipos. **A.11.2.2** Servicios de suministro. **A.11.2.4** Mantenimiento de equipos. **A.17.1.2** Implementación de la continuidad de la seguridad de la información. **A.17.2.1** Disponibilidad de instalaciones de	**A.11.1.1** En la política de seguridad y privacidad de la información, se debe establecer las directrices para el control de acceso a los funcionarios a las instalaciones de procesamiento de información crítica, así como los controles físicos de entrada. **A.11.1.2** Se deben implementar procedimientos relacionados con el registro del ingreso del personal autorizado. **A.11.2.1** Se deben implementar procedimientos relacionados con los controles para minimizar el riesgo de amenazas físicas y ambientales, así como el seguimiento de las condiciones críticas de este entorno.
				Falta de monitoreo factores críticos					
			Fallas en hardware	Falta de mantenimiento a la infraestructura					
				Sobrecarga de trabajo					
				Fallas en las conexiones eléctricas					
				No existen infraestructuras redundantes					
				Falta de UPS					
				Falla en el suministro de energía alterna					
				Desastre natural					
			Acceso no autorizado	Falta de Controles de acceso					
			Fallas en las comunicaciones	Falta de Documentación y procedimientos					
			Procedimientos desactualizados	Falta de Documentación y procedimientos					

								procesamiento de información.	**A.11.2.2** Se deben llevar un registro con el fin de validar el funcionamiento que brindan el suministro eléctrico **A.11.2.4** Se deben implementar procedimientos para la elaboración de los mantenimiento periódicos a los equipos que se encuentran en el centro de datos según las especificaciones del fabricante. Se debe llevar registro de fallas o sospechas con el fin de planear mantenimientos preventivos o correctivos. **A.17.1.2** Se deberán implementar un procedimiento orientado a garantizar el nivel de continuidad en la seguridad de la información, que permita servir de guía ante una situación adversa que se pueda presentar. **A.17.2.1** Se deberá gestionar la disponibilidad de una infraestructura redundante que permita la disponibilidad de la información, ante una situación que afecte el centro de datos principal del IBAL.

Fuente: Elaboración grupo de trabajo

8 PROPUESTA DE ACTUALIZACIÓN EN LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN VIGENTE, PARA GUIAR EL COMPORTAMIENTO DE LAS PARTES INTERESADAS, LOGRANDO QUE LA EMPRESA TRABAJE BAJO BUENAS PRÁCTICAS DE SEGURIDAD, MINIMIZANDO LA OCURRENCIA DE INCIDENTES INFORMÁTICOS.

La EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, siguiendo los lineamientos del Decreto 1008 del 14 de junio de 2018 del Ministerio de Tecnologías de la Información y las Comunicaciones, determina la importancia de preservar la confidencialidad, integridad y disponibilidad de los activos de información de cada proceso que se realizan dentro de la empresa, mediante la implementación de un modelo de seguridad y privacidad de la información, con base en el estándar ISO/IEC 27001:2013.

Por lo anterior es necesario la declaración de una Política de Seguridad y Privacidad de la Información, la cual representa la posición de la EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL con respecto a la protección de los activos de la información, tales como: información, procesos, tecnologías de la información y el factor humano, que soporten los procesos que se realizan dentro de la empresa.

8.1 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política de seguridad y privacidad de la información de LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, aplica para toda la entidad, sus recursos y la totalidad de los procesos vigentes y futuros del SIG, por tal motivo rige para todos los funcionarios de la empresa, contratistas y personal provisto por terceros que desarrollen actividades en la empresa, con el fin de conseguir un adecuado nivel de protección de la información. La política se debe socializar con todo el personal de la empresa y será obligatoria

en los procesos de inducción y reinducción, así mismo estará disponible para todas las partes interesadas según sea lo determinado.

Para la EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, es relevante el cumplimiento de la misión, la visión y los objetivos estratégicos, ciñéndose a los valores corporativos establecidos dentro de la empresa. Es por ello, que se establece la Política de Seguridad y Privacidad de la Información con el objetivo de:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa (MIPG).
- Mantener la confianza de los empleados, contratistas y ciudadanos.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, contratistas, proveedores y usuarios externos de la EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL.
- Garantizar la continuidad del negocio frente a incidentes de seguridad.

Alcance y aplicabilidad de la política.

La presente política aplica para toda la EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, incluyendo empleados, contratistas, proveedores, terceros, suscriptores y usuarios del servicio en la cuidad de Ibagué, los cuales hacen uso de la información y de los recursos tecnológicos; con el fin de asegurar la integridad, confidencialidad y disponibilidad de la información.

Nivel de Cumplimiento.

Todas las personas cubiertas por el alcance y aplicabilidad de este, se adhieren en un 100% a la política, y el cumplimiento de esta se realizará a través de herramientas de monitoreo, generación de indicadores y auditorías internas.

A continuación, se establecen las políticas de seguridad que ha adoptado LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, en adelante IBAL:

- El IBAL define, implementa, opera y realiza mejoramiento continuo al MSPI, alineado con las necesidades de la empresa y los requerimientos legales que aplican por ser una empresa de servicios públicos.

- El IBAL establece las responsabilidades en lo referente a la seguridad de la información, las cuales deben de ser definidas, compartidas, socializadas, publicadas y aceptadas por cada uno de los funcionarios, contratistas, tercero o ciudadanos.

- El IBAL protegerá la información generada, procesada o resguardada por los procesos realizados en la empresa, con el fin de minimizar impactos financieros, operativos o legales debido a la utilización incorrecta de la información. Para que esto se cumpla es necesario la aplicación de controles establecidos por el estándar ISO/IEC 27001:2013.

- El IBAL protegerá la información corporativa de las amenazas originadas por parte de los funcionarios y agentes externos.

- El IBAL tiene el compromiso de resguardar las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- El IBAL controlará la operación de sus cuatro procesos: Estratégicos, Misionales, de Apoyo y de Evaluación, garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- El IBAL implementará los controles necesarios relacionados con el acceso a la información, sistemas y recursos de red.

- El IBAL garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- El IBAL garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- El IBAL garantizará la disponibilidad de sus cuatro procesos: Estratégicos, Misionales, de Apoyo y de Evaluación y la continuidad de su operación basado en el impacto que pueden generar la ejecución de incidentes contra la infraestructura tecnológica.

- El IBAL garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

- El IBAL proporcionará las herramientas o mecanismos necesarios, utilizando la criptografía, para garantizar la protección de las contraseñas de acceso a los sistemas informáticos y en general servicios tecnológicos que ofrece la empresa.

- El IBAL definirá las directrices para la clasificación y valoración de activos de información utilizados en los cuatro procesos: Estratégicos, Misionales, de Apoyo y de Evaluación.

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

Política de Gestión de Activos**.**

- El IBAL realizará y actualizará periódicamente el inventario y clasificación de activos de información, que hacen parte del contexto y alcance definidos en la planificación del MSPI. La gestión de los activos de información se realizará con base en los lineamientos que brinde el ministerio de las TIC para esta actividad.

- EL IBAL deberá preservar la confidencialidad de los activos de información, mediante una herramienta de software que le permita garantizar la seguridad de esta información.

- EL IBAL deberá realizar la gestión del riesgo de los activos de información periódicamente, de acuerdo con los lineamientos definidos por el ministerio de las TIC.

Política de control de acceso**.**

- El proceso de gestión tecnológica del IBAL, deberá garantizar la protección de la infraestructura de TI, por medio de controles físicos y lógicos, limitando el acceso a las personas no autorizadas, con el fin de preservar la seguridad de la información.

- Los funcionarios nuevos que lleguen a la empresa deberán realizar una sensibilización por parte del proceso de Gestión Tecnológica, referente a las directrices impartidas sobre la seguridad de la información. Del mismo modo,

para que estos nuevos funcionarios accedan a los recursos informáticos de la empresa, debe existir una solicitud realizada por el líder de cada proceso, la cual deberá ser gestionada por el proceso de Gestión Tecnológica.

- Los funcionarios que deseen conectar sus dispositivos personales a la red de la empresa, deberán cumplir con las exigencias técnicas establecidas por el proceso de Gestión Tecnológica del IBAL.

- Todos los funcionarios del IBAL y partes interesadas de la empresa, que tengan acceso a un sistema informático, deberán tener su propio usuario y contraseña, estos datos son personales e intransferibles y deberán renovarse de acuerdo con los lineamientos del proceso de Gestión Tecnológica del IBAL.

- La revocación del acceso a los sistemas de información del IBAL, será responsabilidad del proceso de Gestión Tecnológica. La solicitud de revocación de acceso a un sistema deberá realizarse por escrito o por correo electrónico desde una cuenta corporativa, firmada o aprobada por el líder del proceso y detallando el motivo por el cual se realizará esta actividad.

Política de protección contra software malicioso y no legal**.**

- Es responsabilidad del proceso de Gestión Tecnológica proporcionar las herramientas necesarias para la protección de la información y los recursos tecnológicos de propiedad de la empresa, con el fin de evitar que los sistemas de información se vean afectados por software malicioso o malware, así como impedir el uso o instalación de software no legal.

- Queda prohibido la desinstalar el software de protección (antivirus), así como la instalación de software no autorizado por el proceso de Gestión Tecnológica, en

los equipos de propiedad del IBAL, proporcionados para la ejecución de las actividades laborales.

- Si un funcionario detecta una actividad sospechosa o un incidente de seguridad relacionado con el equipo que tenga a su cargo, o con un equipo de su propiedad que se encuentre conectado a un sistema de información del IBAL o una red de comunicaciones de la empresa, deberá notificarlo al proceso de gestión Tecnológica para que se realice el respectivo análisis y las acciones necesarias para mitigar o eliminar el riesgo.

Política de privacidad y confidencialidad.

- EL IBAL se compromete a que la información personal de los usuarios y suscriptores, la cual es recopilada a través de los diferentes canales de comunicación que utiliza la empresa, esté sujeta a lo establecido por la ley 1581 de 2012.

- EL IBAL utilizará la información personal de los suscriptores y los predios a su nombre, serán utilizados exclusivamente para fines del proceso de Gestión Comercial, por la prestación de los servicios públicos domiciliarios de acueducto y alcantarillado.

- El IBAL garantizará a los usuarios y suscriptores, el acceso a la información personal que la empresa tenga en sus bases de datos, así como la actualización o rectificación de los datos, en el marco de los requisitos legales.

- El IBAL no expondrá información confidencial de los usuarios y/o suscriptores en ningún servicio, que ponga en riesgo la seguridad de esta información.

- Los funcionarios y las partes interesadas en la empresa, deberán velar por la protección y confidencialidad de los datos personales que se tengan almacenados en las bases de datos de la empresa, su uso y consulta serán por motivos laborales exclusivamente.

Política de integridad**.**

- Cada uno de los funcionarios del IBAL y partes interesadas, deberán hacer uso de los datos e información en forma íntegra, con el fin de garantizar su autenticidad al momento de ser procesada, entregada o transmitida hacia otro proceso.

- Los Activos de información que tengan a cargo los funcionarios o partes interesadas, deberán ser devueltos a la empresa, una vez se finalice el vínculo contractual, garantizando que su estado e integridad estén en óptimas condiciones.

- El proceso de Gestión Tecnológica deberá velar por la integridad de la información que se gestione a través de medios removibles (Usb, CD, DvD, SD, MicroSD, Entre Otros) por parte de los funcionarios de la empresa y de las partes interesadas.

- El proceso de Gestión Tecnológica deberá garantizar que los dispositivos que no se utilicen y que vayan a ser entregados por donación o a dar de baja en el inventario no contengan información sensible del IBAL.

Política de disponibilidad**.**

- El proceso de Gestión Tecnológica, deberá contar con un plan de continuidad del negocio y recuperación de desastres, con el fin de asegurar, recuperar o

reestablecer los sistemas de información y lo activos de información que resulten afectados, ante la materialización de un incidente de seguridad.

- El proceso de Gestión Tecnológica deberá tener segregados los ambientes informáticos de producción y desarrollo, debidamente documentados, con el fin de minimizar los riesgos de puesta en funcionamiento de cambios y nuevos desarrollos.

- El proceso de Gestión Tecnológica deberá establecer y aplicar metodologías para el desarrollo de software de aplicaciones que se realicen al interior de la empresa, con el fin de asegurar el ciclo de vida de estos sistemas.

Política de registro y auditoria**.**

- EL IBAL en cabeza de la oficina de control interno de gestión, deberá realizar auditoria y revisión periódica, de los sistemas de información y la gestión que se realice de los activos de información.

- El proceso de Gestión Tecnológica deberá tener un registro para el control de las copias de seguridad que se realizan periódicamente, así como las evidencias del restablecimiento de estas copias en un ambiente diferente al de producción.

- EL IBAL periódicamente se deben realizar evaluaciones a los controles implementados, relacionados con la seguridad de la información, con el fin de evidenciar la eficiencia y efectividad de los mismo. Esto se debe realizar a través de auditorías internas al modelo.

- EL IBAL deberá periódicamente revisar y evaluar los riesgos relacionados con los activos de información, con el fin de implementar las acciones necesarias

con el fin de minimizar o eliminar el nivel de impacto ante una materialización de un incidente de seguridad.

Política de capacitación y sensibilización en seguridad de la información**.**

- El IBAL deberá capacitar a los funcionarios y partes interesadas de la empresa, en temas relacionados con la seguridad y privacidad de la de la información, cada vez que se realice un ingreso y/o periódicamente realizar sensibilizaciones a los funcionarios sobre esta política.

- Todos los funcionarios y partes interesadas deberán participar de estas capacitaciones en cumplimiento al MSPI.

- El proceso de gestión tecnológica del IBAL será el responsable de coordinar y gestionar estas capacitaciones, de acuerdo con los riesgos identificados para los activos de información.

Política para dispositivos móviles.

- Los funcionarios del IBAL que tengan a cargo dispositivos móviles de propiedad de la empresa los cuales estén en su custodia, deberá velar por el buen uso de estos dispositivos, así como garantizar la seguridad de la información contenida en ellos y el buen estado físico de los mismos.

- Los funcionarios del IBAL no deben usar los dispositivos de propiedad de la empresa los cuales estén en su custodia, en sitio o zonas de la ciudad identificadas como no seguras, o que no brinden seguridad física para evitar riesgos sobre estos dispositivos y a la información contenida en ellos.

- El proceso de Gestión Tecnológica deberá garantizar la administración y gestión de los dispositivos móviles de propiedad de la empresa, con el fin de evitar instalar o desinstalar software o aplicaciones, que no estén autorizadas por la empresa.

- Los funcionarios del IBAL que tengan a cargo dispositivos móviles de propiedad de la empresa los cuales estén en su custodia, no está permitido el uso de los dispositivos para el almacenamiento de información personal.

Política de respaldo de la información.

- El proceso de Gestión Tecnológica garantizará el suministro de las herramientas de software y hardware necesarias, para realizar el proceso de copias de seguridad, de todos los sistemas de información como aplicativos, bases de datos y archivos digitales con información corporativa que contengan información del IBAL. Así mismo deberá propender por tener lugar externo al data center principal, para el almacenamiento de estas copias.

- Los funcionarios del IBAL, contratistas y demás partes interesadas, deberán realizar los procedimientos definidos por el proceso de gestión tecnológica relacionados con las copias de seguridad, con las herramientas y medios diseñados para este fin. Deberá ser responsabilidad de cada uno garantizar la integridad y confidencialidad de esta información. Está totalmente prohibido el uso de estos procedimientos o medios para almacenar información personal del funcionario, contratista o parte interesada.

Política de uso de internet.

- El proceso de Gestión Tecnológica garantizará la disponibilidad del acceso a internet a los funcionarios del IBAL, para que desarrollen el cumplimiento de sus actividades laborales, en las cuales tengan que necesitar el servicio de internet.

- Los funcionarios del IBAL que utilizan el servicio de internet no deberán consultar paginas no seguras. Así como les es prohibido descargar material de origen desconocido. Se resalta que el uso de internet es exclusivamente para la ejecución de las actividades laborales y no para realizar actividades de índole personal ni recreativo.

- El proceso de Gestión Tecnológica deberá implementar los mecanismos necesarios para garantizar la seguridad perimetral en la red de comunicaciones del IBAL, con el fin de gestionar el acceso seguro a internet de los funcionarios, con el fin de bloquear o restringir las páginas, puertos, servicios y aplicaciones que no son necesarias para el desarrollo sus actividades laborales.

- Los funcionarios del IBAL, no deberán utilizar herramientas de software o hardware para incumplir las restricciones relacionadas con la seguridad perimetral en la red de comunicaciones de la empresa, está totalmente prohibido el uso de alguna de ellas.

9 ELABORAR UN PROCEDIMIENTO EN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, BASADO EN UN DOMINIO CRÍTICO IDENTIFICADO EN LA HERRAMIENTA DE EVALUACIÓN DE EFECTIVIDAD DE LOS CONTROLES ESTABLECIDOS EN LA NORMA ISO/IEC 27001:2013, CON EL FIN DE DOCUMENTAR EL PROCEDIMIENTO QUE SE AJUSTE AL PROCESO DE GESTIÓN TECNOLÓGICA.

Para la elaboración del presente procedimiento de seguridad, se tomó referencia la guía 3 de MinTic llamada Procedimientos de seguridad de la información versión 1.0 de fecha 25/04/2016; así mismo, se tuvo en cuenta el siguiente activo y control correspondiente:

Activo: GT-002 Base de datos SOLIN ERP - Probabilidad: Media (60%) - Impacto: Catastrófico (100%) - Zona de Riesgo: Extremo

Control: A.12.3.1 Respaldo de información.

Nombre del procedimiento**:** Procedimiento para la realización de las copias de respaldo y su restauración.

Objetivo**:** Garantizar el almacenamiento y restauración de las copias de seguridad de la base de datos del software SOLIN CLOUD ERP, con el fin de asegurar la disponibilidad de los datos en caso que se materialice un riesgo relacionado con la seguridad de la información.

Alcance**:** Este procedimiento abarca las actividades para la realización, almacenamiento y restauración de las copias de seguridad de la base de datos del software SOLIN CLOUD ERP; así mismo, se establecerán los roles y responsabilidades del personal del proceso de gestión tecnológica encargado de desarrollar estas actividades.

Definiciones**:**

- **Base de datos.** Conjunto de datos estructurados, almacenados en tablas relacionadas, que en su conjunto componen información organizada de la empresa.

- **Copia de seguridad.** Conjunto de actividades cuya finalidad es duplicar los datos almacenados en una instancia principal, almacenarlos en un sitio distinto al principal de donde se aloja la base, con el fin de poder recuperarlos en caso de presentarse un fallo con esta.

- **Data center principal.** Infraestructura física que aloja el rack de comunicaciones, rack de servidores, sistemas de alimentación de energía, ups y protección perimetral en la sede principal del IBAL.

- **Data center respaldo.** Infraestructura física en otra sede de la empresa o remota, que aloja el rack de comunicaciones de la sede, rack de servidores de respaldo, sistemas de alimentación de energía y ups.

- **Motor de base de datos MS Sql Server.** Sistema de gestión de bases de datos relacionales de Microsoft, que permite el almacenamiento y gestión de los datos de forma rápida y estructurada.

- **Plan de mantenimiento.** Conjunto de actividades que se desarrolla en el motor de base de datos **MS Sql Server,** para ejecutar una tarea específica en él.

- **Restauración copia de seguridad.** Actividades para reestablecer una copia de seguridad en un motor de base de datos diferente al principal, con el fin de preservar la disponibilidad de los datos.

- **Tarea programada.** Secuencia de comando programados desde el sistema operativo Windows server, para ejecutarse en una hora determinada con el fin de realizar alguna acción con archivos.

- **Cifrado de Windows.** Método para proteger un directorio y los archivos que en él se encuentran, por medio de una contraseña para evitar el acceso no autorizado a esta información.

- **Copia de seguridad completa.** Copia de todos los datos contenidos en una base de datos, la cual se realiza para generar una copia idéntica a la principal en un periodo de tiempo.

- **Copia de seguridad diferencial.** Copia de los datos que se han modificado desde la copia de seguridad completa generada con anterioridad.

Normatividad: Con relación al marco legal para el desarrollo de este procedimiento, se va a tener en cuenta el procedimiento del sistema integrado de gestión (SIG) del IBAL GT-P-001 PROCEDIMIENTO PROCESO GESTIÓN TECNOLÓGICA, el cual define las directrices del proceso de gestión tecnológica.

Consideraciones generales**:**

- Es responsabilidad del líder del proceso de gestión tecnológica o quien sea delegado por él, la realización de las actividades enunciadas dentro del procedimiento. El funcionario del proceso de gestión tecnológica que realice la actividad de ejecución de las copias de respaldo, no deberá ser el mismo funcionario que realice su restauración.
- El horario de las actividades de ejecución y restauración de las copias de respaldo, será definida por el líder del proceso de gestión tecnológica, de

acuerdo con el nivel de procesamiento de los usuarios en el sistema de información, esto con el fin de no interrumpir las actividades laborales.

- Los directorios donde se almacenan las copias de respaldo en el servidor principal y en el servidor de respaldo, deberán estar cifrados y la contraseña será responsabilidad el líder del proceso de gestión tecnológica.
- La realización de las actividades enunciadas en el procedimiento, se realizarán de lunes a sábado.
- No se podrá almacenar copias de respaldo en otro medio diferente al servidor principal y de respaldo.

Desarrollo**:**

Nro.	Actividad	Tarea	Punto de control	Responsable
1	Revisión copia de respaldo en el servidor de base de datos en el data center principal	Verificar la ejecución del plan de mantenimiento en el visor de archivos de registros de SQL SERVER.	SQL Server Management Studio (SSMS), opción registros de SQL Server	Líder del proceso de Gestión tecnológica o su delegado
		Verificar espacio en el disco duro	Explorador de archivos de Windows del servidor	Líder del proceso de Gestión tecnológica o su delegado
		Verificar archivos .bak (última fecha de creación el archivo más reciente)	Unidad seleccionada para el almacenamiento de las copias de seguridad	Líder del proceso de Gestión tecnológica o su delegado
		Revisión de la ejecución de tarea programada.	Historial Programador de tareas de Windows server	Líder del proceso de Gestión tecnológica o su delegado
		Diligenciar el registro del SIG	GT-R-003 Seguimiento Copias de respaldo	Líder del proceso de Gestión tecnológica o su delegado
2	Revisión copia de respaldo en el servidor de base de datos en el data center respaldo	Verificar archivos .bak en el directorio en el servidor de respaldo.	Explorador de archivos de Windows del servidor	Líder del proceso de Gestión tecnológica o su delegado
		Verificar espacio en el disco duro	Explorador de archivos de Windows del servidor	Líder del proceso de Gestión tecnológica o su delegado
3	Restauración copias de respaldo	Restaurar el archivo .bak (última fecha de creación el archivo más reciente) a la base de datos en el servidor de respaldo.	SQL Server Management Studio (SSMS), sobre escribiendo la base de datos actual y cerrando sus conexiones.	Líder del proceso de Gestión tecnológica o su delegado
		Diligenciar el formato donde se registre la evidencia de la restauración de las copias de seguridad. La información deberá ser extraída del visor de registros de SQL Server.	Formato: Restauración Copias de respaldo	Líder del proceso de Gestión tecnológica o su delegado

4	Limpieza de mantenimiento	Eliminar los archivos .bak, de las copias de respaldo que tengan más de 5 días de antigüedad.	SQL Server Management Studio (SSMS) y explorador de archivos de Windows.	Líder del proceso de Gestión tecnológica o su delegado

Registros

Restauración Copias de respaldo

Fecha y Hora restauración	Nombre de Funcionario	Instancia del servidor de respaldo	Nombre de la base de datos	Tiempo de restauración (minutos)	Observaciones

Control de cambios.

Fecha	Cambio	Versión

Elaboró

Adriana Díaz Lenis

Gerardo Campos Molina

Revisó y Aprobó

CONCLUSIONES

La Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, de acuerdo con el instrumento de evaluación, no alcanza el nivel inicial en la implementación del MSPI, motivo por el cual deberá incrementar sus esfuerzos en desarrollar una estrategia que le permita avanzar en la implementación de la política. Este trabajo deberá articularse los controles propuestos y determinar cuáles de ellos se pueden ejecutar, sin necesidad de realizar grandes inversiones.

Es importante que el IBAL desarrolle de manera integral el MSPI, ya que este le permite identificar fallas o vulnerabilidades que se puedan tener en los procesos relacionados con la seguridad de la información, y que pueden llegar a generar en un futuro grandes consecuencias que pueden afectar las finanzas de la empresa.

El IBAL debe tomar conciencia sobre de la importancia de contar con una estrategia relacionada con la seguridad de la información, ya que muchos procesos que se gestionan en la actualidad, tienen un algo componente de tecnología, el cual debe ser gestionado adecuadamente para evitar pérdidas en la información.

La política de seguridad y privacidad de la información debe ser un documento vivo, que genere una cultura entre los funcionarios del IBAL, que brinde herramientas para realizar sus actividades de manera ágil y segura, generando confianza entre las partes interesadas de la empresa y así garantizar la mejora en la prestación de los servicios de acueducto y alcantarillado que presta el IBAL.

La correcta identificación de los activos de información, inicia con el conocimiento exacto del concepto de activo, los tipos de activos que maneja el IBAL y la importancia que tienen estos durante el desarrollo de las actividades del grupo de Gestión Comercial y el grupo de Gestión Tecnológica, siendo este último, pieza fundamental para gestionar la seguridad de la información.

El procedimiento diseñado para la realización y restauración de las copias de respaldo del activo con alto nivel de criticidad: Base de datos del Software SOLIN CLOUD, ayudará a salvaguardar los datos relevantes para el desarrollo de los procesos dentro de la dirección Comercial. Así mismo, este documento le indicará al personal de TI del IBAL las actividades que se deben desarrollar para la restauración de estas copias en ambientes de respaldo. Todo esto con el propósito de preparar a la empresa en caso de que se presente algún incidente de seguridad y éste atente contra la continuidad del negocio.

RECOMENDACIONES

- Es importante que el IBAL revise su política de seguridad y privacidad de la información para que incluya aspectos como: esté alineada con los objetivos del SIG, identificar los responsables con roles definidos con relación a la seguridad de la información, la política debe tener revisiones periódicas que le permitan validar su efectividad en la empresa.

- Es importante que el IBAL participe activamente en grupos de interés relacionados con la seguridad informática, ya que a través de estos se pueden encontrar experiencias que enriquezcan el proceso al interior de la empresa, como también se puede generar conocimiento a través de la enseñanza de los mecanismos utilizados en el IBAL, que han brindado un desempeño positivo.

- El IBAL deberá implementar una política específica relacionada con el uso de dispositivos móviles, ya que la información que se procesa en estos dispositivos, son críticos para la gestión de la empresa.

- El IBAL deberá implementar una política específica relacionada con el teletrabajo o trabajo en casa, con el fin de garantizar seguridad en las conexiones de los funcionarios y la información que se genera en medio digital, la cual es gestionada de manera remota.

- El IBAL deberá realizar una gestión de activos de información, que le permita identificar activos críticos y así brindarles el tratamiento adecuado, con el fin de minimizar el impacto que pueda generar un incidente de seguridad sobre ellos.

- El IBAL deberá realizar e implementar un plan de continuidad del negocio o plan de recuperación de desastres, con el objetivo de tener un instrumento que le

permita recuperarse en el menor tiempo posible de un incidente que impacte la empresa.

- El IBAL deberá implementar una arquitectura redundante en un centro de cómputo externo al principal, que permita tener contar con una alternativa inmediata ante un incidente que se pueda generar en el principal. Así mismo este centro de cómputo alterno puede ser utilizado como pruebas de las copias de seguridad.

- El IBAL deberá implementar un procedimiento que le permita detectar vulnerabilidades en sus sistemas críticos de información, con el fin de garantizar continuidad en la prestación de los servicios y la seguridad en los procesos.

- El IBAL deberá implementar una política específica para los proveedores de la empresa o terceros que ejerzan funciones a nombre de la empresa, con el fin de garantizar la seguridad y privacidad de la información.

BIBLIOGRAFÍA

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: DAFP, Micrositio MIPG. Instructivo. 2021. [Consulta: 02 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/web/mipg/inicio

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. [Sitio web]. Bogotá: DAFP, Ley 489 de 1998. [Consulta: 02 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186

ESCUELA SUPERIOR DE ADMINISTRACIÓN PÚBLICA. [Sitio web]. Bogotá: ESAP, Plan de continuidad del negocio BCP. [Consulta: 15 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=186

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Diagnostico Seguridad y Privacidad de la Información. [Consulta: 02 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/Plan%20de%20seguridad%20y%20privacidad%20de%20la%20informacion%20-%20(DIAGNOSTICO)%20%20IBAL.pdf

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Modelo de seguridad y privacidad de la información MSPI. [Consulta: 02 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/Plan%20de%20seguridad%20y%20privacidad%20de%20la%20informaci%C3%B3n.pdf

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Matriz de caracterización gestión tecnológica del SIG. 2021. [Consulta: 03 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/CARACTERIZACI%C3%93N%20GESTI%C3%93N%20TECNOLOGICA%20v14.pdf

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Matriz de caracterización proceso gestión jurídica y contractual. 2021. Instructivo 2021. [Consulta: 03 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/CARACTERIZACI%C3%93N%20GESTI%C3%93N%20JURIDICA%20INTEGRAL%20VERSION%2022_1.pdf

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Manual específico de funciones y competencias laborales. Manual 2018. [Consulta: 03 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/MANUAL-DE-FUNCIONES-RESOLUCION-0755-DEL-03-DE-AGOSTO-DE-2018_0.pdf

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. Resolución. 2019.. [Consulta: 02 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/Politica%20de%20seguridad%20de%20la%20infromaci%C3%B3n.pdf

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Procedimiento auditorias de gestión, Instructivo

2020. [Consulta: 02 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/EI-P-001%20PROCEDIMIENTO%20AUDITORIAS%20INTERNAS%20DE%20GESTI%C3%93N%20v11_0.pdf

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL [sitio web]. Ibagué: IBAL. Política de Administración de Riesgos. SIG 2019. [Consulta: 03 de mayo de 2021]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/POLITICA%20RIESGOS%202019_1.pdf

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. [sitio web]. Bogotá: ICONTEC. NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. Norma Técnica 2006. [Consulta: 03 de mayo de 2021]. Disponible en: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

INTERNACIONAL ORGANIZATION FOR STANDARDIZATION.[sitio web]. Bogotá: ISO. Guía ISO/IEC 73. 2002. [Consulta: 03 de mayo de 2021]. Disponible en: https://iso.cat/wp-content/uploads/2019/09/Cap-1-8-2-a-6-Guia_ISO-IEC-73.pdf

INTERNACIONAL ORGANIZATION FOR STANDARDIZATION. [sitio web]. Bogotá: ISO2700.ES, Relación con los proveedores. Norma Técnica. [Consulta: 15 de mayo de 2021]. Disponible en internet: https://www.iso27000.es/iso27002_15.html

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Resolución 0500 de marzo de 10 de 2021. Resolución 2021. [Consulta: 18 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162624_recurso_1.pdf

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Guía para la Implementación de Seguridad de la Información en una MIPYME. Instructivo 2016. Resolución 2021. [Consulta: 03 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150522_Guia_Seguridad_informacion_Mypimes.pdf

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Elaboración De La Política General De Seguridad Y Privacidad De La Información. Resolución 2021. [Consulta: 30 de septiembre de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-5482_G2_Politica_General.pdf

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Guía para la gestión y clasificación de activos de información. [Consulta: 30 de septiembre de 2021]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Modelo de Seguridad y Privacidad de la Información. Instructivo. Febrero 2021. [Consulta: 03 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Instrumento de Evaluación MSPI. Archivo digital. [Consulta: 03 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150507_Instrumento_Evaluacion_MSPI.xlsx

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [Sitio web]. Bogotá: MINTIC, Instructivo instrumento Evaluación MSPI. Instructivo 2017. [Consulta: 03 de mayo de 2021]. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-150519_Instructivo_instrumento_Evaluacion_MSPI.pdf

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. [Sitio web]. Bogotá: CONPES 3854 de 2016, Política Nacional De Seguridad Digital. Documento 2016. [Consulta: 03 de mayo de 2021]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

SECRETARIA DEL SENADO DE LA REPÚBLICA DE COLOMBIA. [Sitio web]. Bogotá: Ley de Servicios Públicos Domiciliarios. Ley 142 de 1994. [Consulta: 03 de mayo de 2021]. Disponible en http://www.secretariasenado.gov.co/senado/basedoc/ley_0142_1994.html

UTP. NTC 5411-1:2006. Términos y Definiciones. [Consulta: 03 de mayo de 2021]. Disponible en: https://www.utp.edu.co/gestioncalidad/sin-categoria/277/terminos-y-definiciones/pdf

ANEXOS

Anexo A. AUTORIZACIÓN PROYECTO APLICADO

V0.1

Ibagué, mayo 5 de 2021

Doctor:
FELIPE ANDRES CALDERON QUIROGA
Director Administrativo
IBAL SA ESP OFICIAL

Asunto: Autorización para la ejecución del proyecto titulado: ***IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ESTABLECIDO POR MINTIC, PARA LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, EN CUMPLIMIENTO DE LA POLÍTICA DE GOBIERNO DIGITAL.***

Cordial saludo,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia "UNAD". Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto título: ***IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ESTABLECIDO POR MINTIC, PARA LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, EN CUMPLIMIENTO DE LA POLÍTICA DE GOBIERNO DIGITAL*** el cual se encuentra avalado por parte la Institución de educación superior "UNAD".

El proyecto en su objetivo general describe lo siguiente: "*Diseñar un plan de seguridad y privacidad de la información para la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, basado en el marco de referencia del ministerio de las Tecnologías de la información y las comunicaciones, que apoye la implementación de la política de gobierno digital*"; al mismo tiempo será apoyado por los objetivos específicos: "1. Determinar el estado actual de la adopción de la política de seguridad de la información, a partir de la elaboración del autodiagnóstico que permita identificar el nivel de madurez en la implementación del modelo MSPI del MINTIC; 2. Proponer la actualización de la política de la seguridad de la información, con base los lineamientos de la fase de planificación, del MSPI de MINTIC, alineado con los objetivos misionales de la empresa; 3. Elaborar el plan de seguridad y privacidad de la información, de acuerdo con las guías metodológicas establecidas por MINTIC en el MSPI; 4. Generar recomendaciones para la implementación del MSPI de acuerdo con los lineamientos de la política de Gobierno Digital." para obtener como resultado un alto impacto en la seguridad de la empresa *Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL*.

V0.1

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transaparencia de la ejecución del proyecto:

- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por la *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL*.
- La *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL* deberá establecer qué tipo de información es privada y cuál es pública para delimintar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de prubas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El documento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrerar profesional.

Firman en Ibagué., a los 5 días del mes de mayo de 2021

Cordialmente,

ADRIANA DÍAZ LENIS
Estudiante UNAD.

GERARDO CAMPOS MOLINA
Estudiante UNAD

Anexo B. ACUERDO DE CONFIDENCIALIDAD

V 0.1

ACUERDO DE CONFIDENCIALIDAD ENTRE ADRIANA DÍAZ LENIS, GERARDO CAMPOS MOLINA Y LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

Por la **parte reveladora**

Nombre: Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL
Dirección: K 3 1 04
Teléfono: 2756000
E-mail: sistemas@ibal.gov.co

Por la parte **receptora de la información**

Nombre: Adriana Díaz Lenis
Dirección: Calle 11 4 46
Teléfono: 3142664150
E-mail: adrianadiazlenis@gmail.com

Nombre: Gerardo Campos Molina
Dirección: Parque Residencial Altagracia Torre 5 Apartamento 206
Teléfono: 3002385187
E-mail: gcamposm@unadvirtual.edu.co

IDENTIFICACIÓN DEL PROYECTO

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES:**

1. Que la información compartida en virtud del presente acuerdo pertenece a la *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL*, y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del *Proyecto aplicado con el título: IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ESTABLECIDO POR MINTIC, PARA LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, EN CUMPLIMIENTO DE LA POLÍTICA DE GOBIERNO DIGITAL.*
2. Que la información de propiedad de *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL* ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto aplicado *IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ESTABLECIDO POR MINTIC, PARA LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, EN CUMPLIMIENTO DE LA POLÍTICA DE GOBIERNO DIGITAL, Adriana Díaz Lenis y Gerardo Campos Molina* que para el presente caso actual como **revelador, guarda y administrados** de la información de propiedad de *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL.*

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente a la *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL*, así como también a no utilizar dicha información en beneficio propio ni de terceros, sólo con fines estadisticos y de mejoramiento de la *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL*.

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales, modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto *IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN ESTABLECIDO POR MINTIC, PARA LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL, EN CUMPLIMIENTO DE LA POLÍTICA DE GOBIERNO DIGITAL,* lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba

guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL*, restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**

7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la **información confidencial** sin el previo consentimiento por escrito por parte de la *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL*.

9. La **parte receptora** se compromete a establecer que los datos a utilizar son: *Información de los procesos del sistema integrado de gestión, la información del proceso de gestión tecnológica, el inventario de activos de información relacionados con el proyecto, información de los controles de seguridad que se tienen adoptados en la empresa, Cargos de los funcionarios responsables del proceso de gestión tecnológica y cargos de los funcionarios asociados al proyecto, los cuales están amparados por la ley 1581 de 2012 y no pueden ser revelados en el documento final del proyecto.*

10. La información capturada por la **parte receptora** se observará como *cifras para estudio comparativo e información cuantitativa y cualitativa*, y no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad de todo el personal de la *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL* no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de la *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL*, ni violentará la ley de delitos informáticos Colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. Los estudiantes *Adriana Días Lenis y Gerardo Campos Molina* se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la *Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL* para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el respositorio institucional y de acceso público.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de sus alcances, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes *Adriana Díaz Lenis, Gerardo Campos Molina y LA Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL* se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de

las clausulas del presente acuerdo de confidencialidad por parte de *Adriana Díaz Lenis y Gerardo Campos Molina*.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Ibagué, a los 5 días del mes de mayo de 2021.

Como Parte Receptora:

ADRIANA DÍAZ LENIS
Estudiante UNAD
CC. 65.775.349 de Ibagué

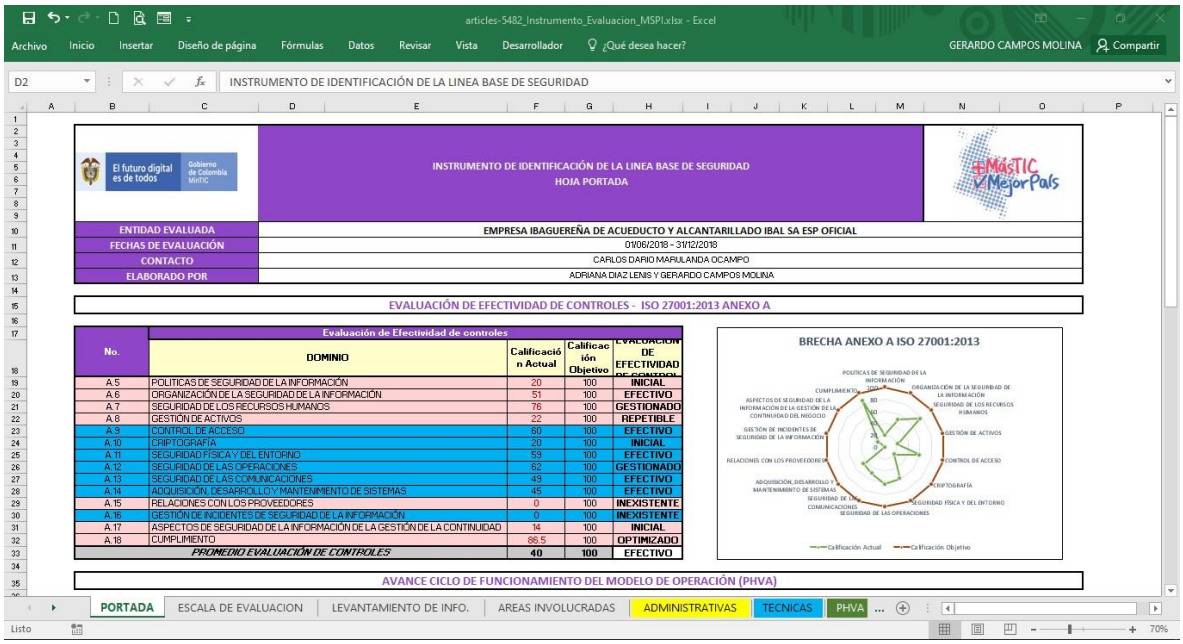
GERARDO CAMPOS MOLINA
Estudiante UNAD.
cc. 93.402.185 de Ibagué

Por la parte reveladora:

FELIPE ANDRES CALDERON QUIROGA
Director Administrativo
Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL
Nit. 800.089.809-6

Anexo C. INSTRUMENTO DE EVALUACIÓN

Evaluación de Efectividad de controles



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA PORTADA

ENTIDAD EVALUADA	EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL
FECHAS DE EVALUACIÓN	01/06/2018 - 31/12/2018
CONTACTO	CARLOS DARIO MARULANDA OCAMPO
ELABORADO POR	ADRIANA DIAZ LENIS Y GERARDO CAMPOS MOLINA

EVALUACIÓN DE EFECTIVIDAD DE CONTROLES - ISO 27001:2013 ANEXO A

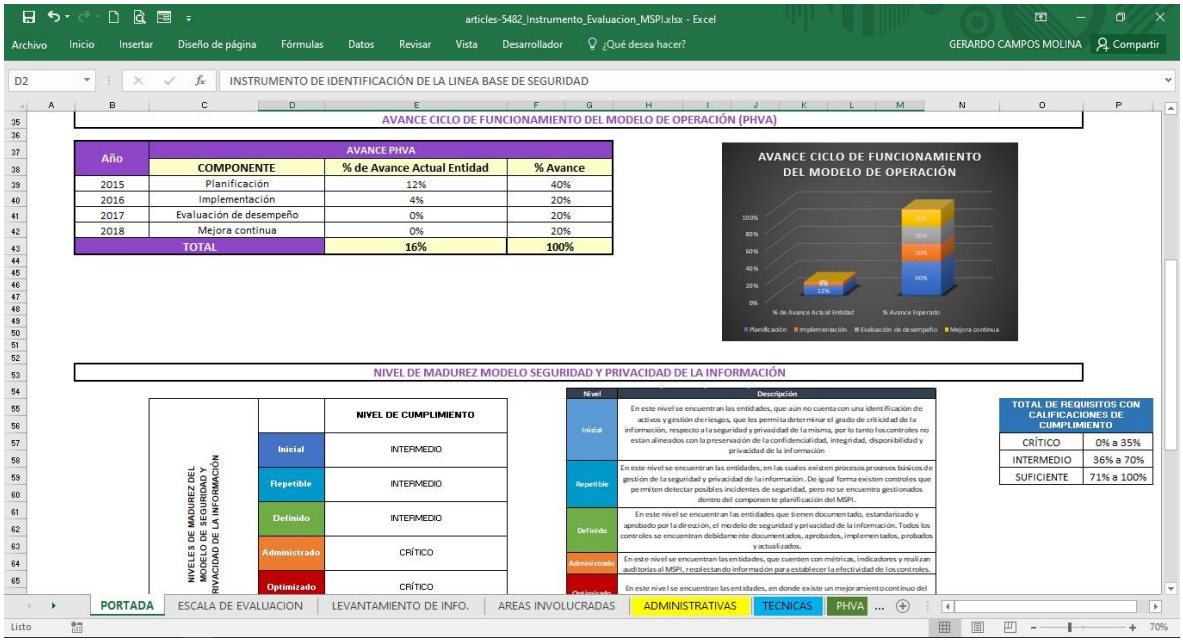
No.	Evaluación de Efectividad de controles DOMINIO	Calificación Actual	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	INICIAL
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	51	100	EFECTIVO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	76	100	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	22	100	REPETIBLE
A.9	CONTROL DE ACCESO	60	100	EFECTIVO
A.10	CRIPTOGRAFÍA	20	100	INICIAL
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	53	100	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	52	100	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	48	100	EFECTIVO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	45	100	EFECTIVO
A.15	RELACIONES CON LOS PROVEEDORES	0	100	INEXISTENTE
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD	14	100	INICIAL
A.18	CUMPLIMIENTO	86.5	100	OPTIMIZADO
	PROMEDIO EVALUACIÓN DE CONTROLES	40	100	EFECTIVO

BRECHA ANEXO A ISO 27001:2013

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

PORTADA | ESCALA DE EVALUACION | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA

Avance ciclo de funcionamiento del modelo de operación (phva)



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN (PHVA)

Año	AVANCE PHVA COMPONENTE	% de Avance Actual Entidad	% Avance
2015	Planificación	12%	40%
2016	Implementación	4%	20%
2017	Evaluación de desempeño	0%	20%
2018	Mejora continua	0%	20%
TOTAL		16%	100%

AVANCE CICLO DE FUNCIONAMIENTO DEL MODELO DE OPERACIÓN

NIVEL DE MADUREZ MODELO SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

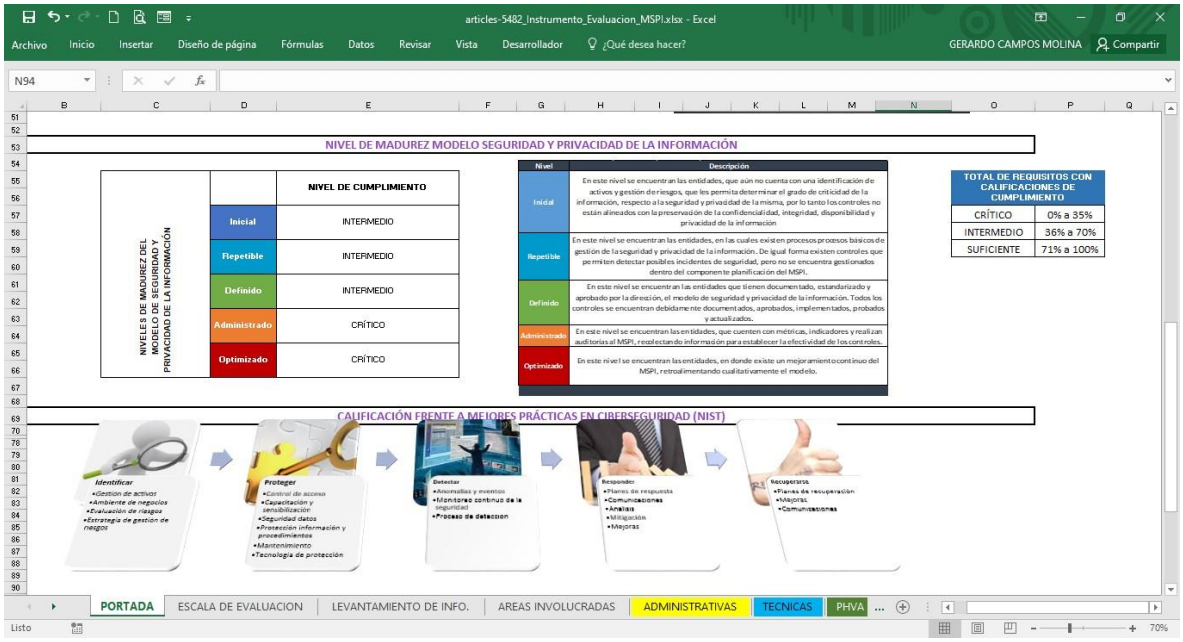
NIVELES DE MADUREZ DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	NIVEL DE CUMPLIMIENTO
Inicial	INTERMEDIO
Repetible	INTERMEDIO
Definido	INTERMEDIO
Administrado	CRÍTICO
Optimizado	CRÍTICO

Nivel	Descripción
Inicial	En este nivel se encuentran las entidades, que aún no cuenta con una identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto los controles no están alineados con la preservación de la confidencialidad, integridad, disponibilidad y privacidad de la información
Repetible	En este nivel se encuentran las entidades, en las cuales existen procesos básicos de gestión de la seguridad y privacidad de la información. De igual forma existen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentra gestionados dentro del componente planificación del MSPI.
Definido	En este nivel se encuentran las entidades que tienen documentado, estandarizado y aprobado por la dirección, el modelo de seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Administrado	En este nivel se encuentran las entidades, que cuenten con métricas, indicadores y realizan auditorias al MSPI, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las entidades, en donde existe un mejoramiento continuo del

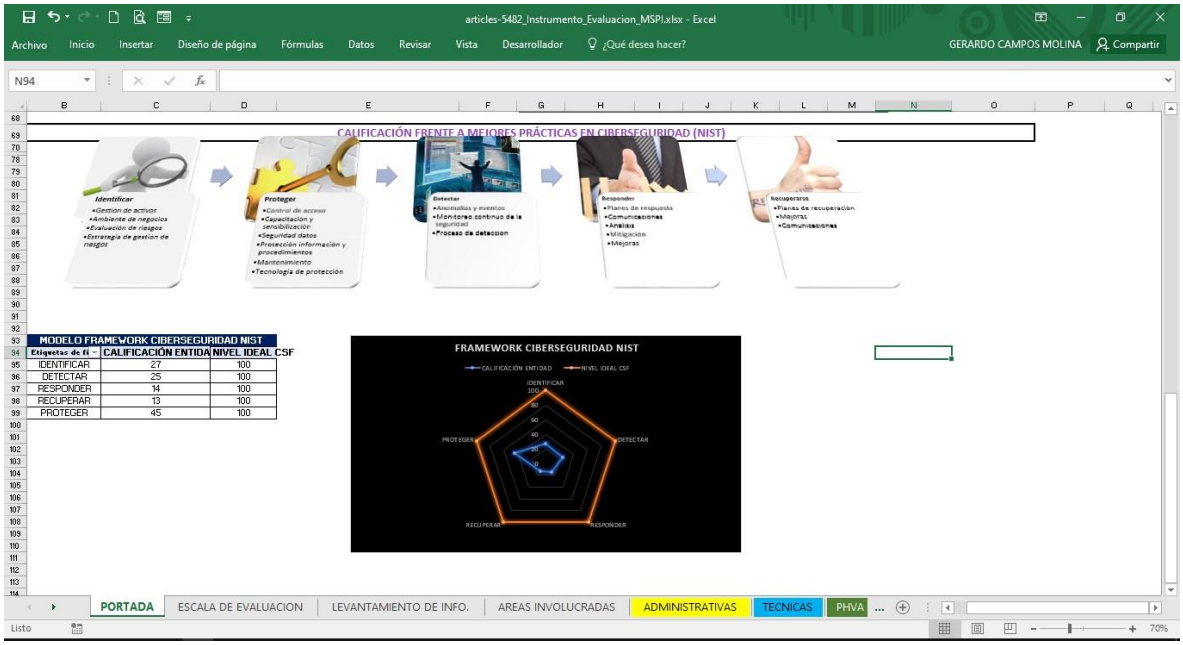
TOTAL DE REQUISITOS CON CALIFICACIONES DE CUMPLIMIENTO	
CRÍTICO	0% a 35%
INTERMEDIO	36% a 70%
SUFICIENTE	71% a 100%

PORTADA | ESCALA DE EVALUACION | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA

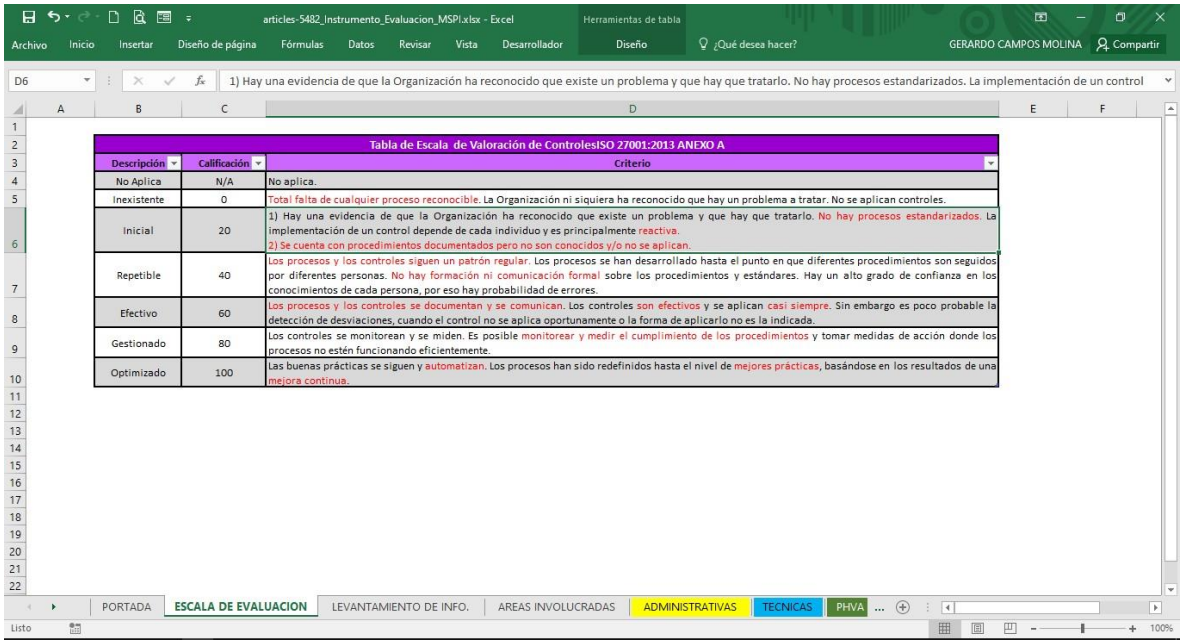
Nivel de madurez modelo seguridad y privacidad de la información



Calificación frente a mejores prácticas en ciberseguridad (NIST)



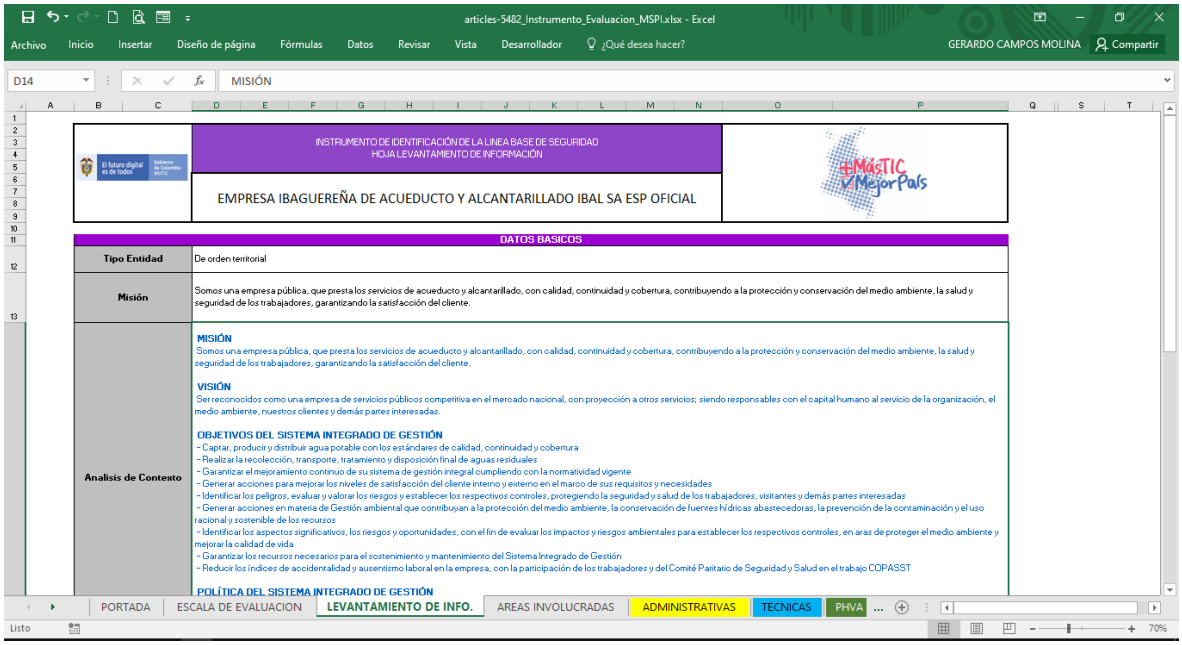
Escala de evaluación



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

Tabla de Escala de Valoración de ControlesISO 27001:2013 ANEXO A		
Descripción	Calificación	Criterio
No Aplica	N/A	No aplica.
Inexistente	0	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.
Inicial	20	1) Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva. 2) Se cuenta con procedimientos documentados pero no son conocidos y/o no se aplican.
Repetible	40	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.
Efectivo	60	Los procesos y los controles se documentan y se comunican. Los controles son efectivos y se aplican casi siempre. Sin embargo es poco probable la detección de desviaciones, cuando el control no se aplica oportunamente o la forma de aplicarlo no es la indicada.
Gestionado	80	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.
Optimizado	100	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.

Levantamiento de información



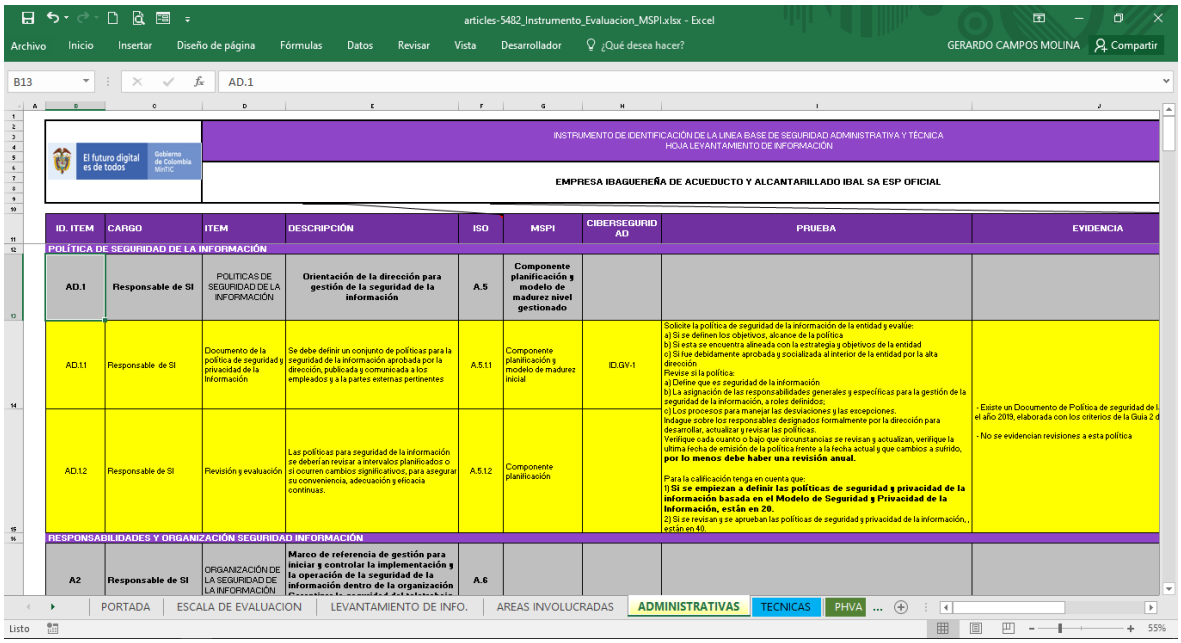
articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD
HOJA LEVANTAMIENTO DE INFORMACIÓN

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

DATOS BASICOS	
Tipo Entidad	De orden territorial
Misión	Somos una empresa pública, que presta los servicios de acueducto y alcantarillado, con calidad, continuidad y cobertura, contribuyendo a la protección y conservación del medio ambiente, la salud y seguridad de los trabajadores, garantizando la satisfacción del cliente.
Analisis de Contexto	**MISIÓN** Somos una empresa pública, que presta los servicios de acueducto y alcantarillado, con calidad, continuidad y cobertura, contribuyendo a la protección y conservación del medio ambiente, la salud y seguridad de los trabajadores, garantizando la satisfacción del cliente. **VISIÓN** Ser reconocidos como una empresa de servicios públicos competitiva en el mercado nacional, con proyección a otros servicios; siendo responsables con el capital humano al servicio de la organización, el medio ambiente, nuestros clientes y demás partes interesadas. **OBJETIVOS DEL SISTEMA INTEGRADO DE GESTIÓN** - Captar, producir y distribuir agua potable con los estándares de calidad, continuidad y cobertura - Realizar la recolección, transporte, tratamiento y disposición final de aguas residuales - Garantizar el mejoramiento continuo de su sistema de gestión integral cumpliendo con la normatividad vigente - Generar acciones para mejorar los niveles de satisfacción del cliente interno y externo en el marco de sus requisitos y necesidades - Identificar los peligros, evaluar y valorar los riesgos y establecer los respectivos controles, protegiendo la seguridad y salud de los trabajadores, visitantes y demás partes interesadas - Generar acciones en materia de Gestión ambiental que contribuyan a la protección del medio ambiente, la conservación de fuentes hídricas abastecedoras, la prevención de la contaminación y el uso racional y sostenible de los recursos - Identificar los aspectos significativos, los riesgos y oportunidades, con el fin de evaluar los impactos y riesgos ambientales para establecer los respectivos controles, en aras de proteger el medio ambiente y mejorar la calidad de vida - Garantizar los recursos necesarios para el sostenimiento y mantenimiento del Sistema Integrado de Gestión - Reducir los índices de accidentalidad y ausentismo laboral en la empresa, con la participación de los trabajadores y del Comité Paritario de Seguridad y Salud en el trabajo COPASST **POLÍTICA DEL SISTEMA INTEGRADO DE GESTIÓN**

Pruebas administrativas



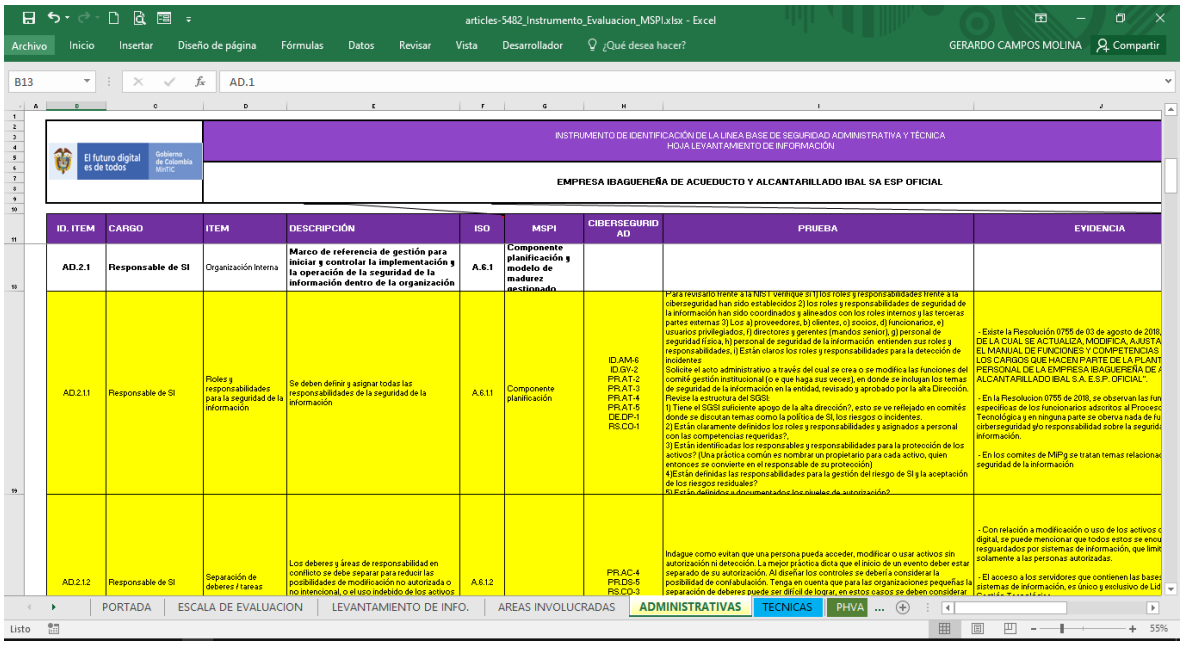
articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN								
AD.1	Responsable de SI	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	Orientación de la dirección para gestión de la seguridad de la información	A.5	Componente planificación y modelo de madurez nivel gestionado			
AD.1.1	Responsable de SI	Documento de la política de seguridad y privacidad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes	A.5.1.1	Componente planificación y modelo de madurez inicial	ID.GV-1	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a) Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones.	- Existe un Documento de Política de seguridad de l... el año 2019, elaborada con los criterios de la Guia 2 d... - No se evidencian revisiones a esta política
AD.1.2	Responsable de SI	Revisión y evaluación	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	A.5.1.2	Componente planificación		Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo que circunstancias se revisan y actualizan, verifique la ultima fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, **por lo menos debe haber una revisión anual.** Para la calificación tenga en cuenta que: 1) **Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20.** 2) Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, , están en 40.	
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN								
A2	Responsable de SI	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización	A.6				

PORTADA | ESCALA DE EVALUACION | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

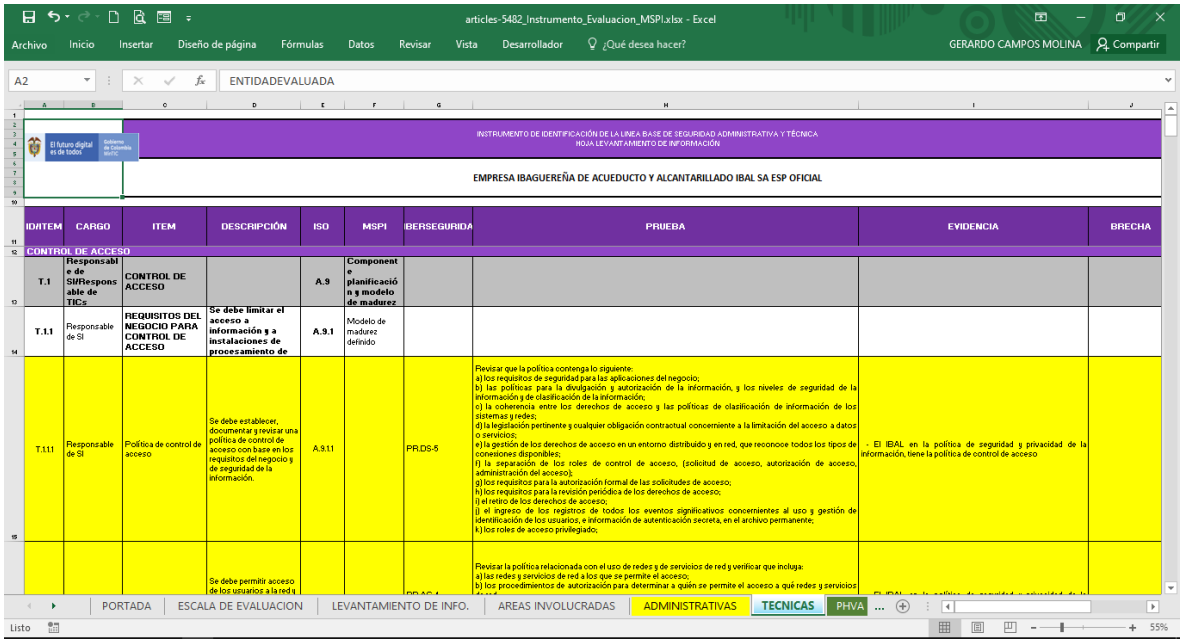
INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

ID. ITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	CIBERSEGURIDAD	PRUEBA	EVIDENCIA
AD.2.1	Responsable de SI	Organización Interna	Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización	A.6.1	Componente planificación y modelo de madurez gestionado			
AD.2.1.1	Responsable de SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	A.6.1.1	Componente planificación	ID.AM-6 ID.GV-2 PR.AT-2 PR.AT-3 PR.AT-4 PR.AT-5 DE.DP-1 RS.CO-1	Para revisarlo frente a la NIST verifique si 1) los roles y responsabilidades frente a la ciberseguridad han sido establecidos 2) los roles y responsabilidades de seguridad de la información han sido coordinados y alineados con los roles internos y las terceras partes externas 3) Los a) proveedores, b) clientes, c) socios, d) funcionarios, e) usuarios privilegiados, f) directores y gerentes (mandos senior), g) personal de seguridad física, h) personal de seguridad de la información entienden sus roles y responsabilidades, i) Están claros los roles y responsabilidades para la detección de incidentes Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto ze ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes. 2) Están claramente definidos los roles y responsabilidades y asignados a personal con las competencias requeridas?, 3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección) 4)Están definidas las responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales? 5)Están definidos y documentados los niveles de autorización?	- Existe la Resolución 0755 de 03 de agosto de 2018,... DE LA CUAL SE ACTUALIZA, MODIFICA, AJUSTA... EL MANUAL DE FUNCIONES Y COMPETENCIAS... LOS CARGOS QUE HACEN PARTE DE LA PLANT... PERSONAL DE LA EMPRESA IBAGUEREÑA DE A... ALCANTARILLADO IBAL S.A. E.S.P. OFICIAL". - En la Resolucion 0755 de 2018, se observan las fun... especificas de los funcionarios adscritos al Proceso... Tecnológica y en ninguna parte se observa nada de fu... cirberseguridad y/o responsabilidad sobre la seguridad... información. - En los comites de MIPg se tratan temas relacionad... seguridad de la información
AD.2.1.2	Responsable de SI	Separación de deberes / tareas	Los deberes y áreas de responsabilidad en conflicto se debe separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos	A.6.1.2		PR.AC-4 PR.DS-5 RS.CO-3	Indague como evitan que una persona pueda acceder, modificar o usar activos sin autorización ni detección. La mejor práctica dicta que el inicio de un evento deber estar separado de su autorización. Al diseñar los controles se deberá considerar la posibilidad de confabulación. Tenga en cuenta que para las organizaciones pequeñas la separación de deberes puede ser difícil de lograr, en estos casos se deben considerar	- Con relación a modificación o uso de los activos d... digital, se puede mencionar que todos estos se encu... resguardados por sistemas de información, que limit... solamente a las personas autorizadas. - El acceso a los servidores que contienen las bases... sistemas de información, es único y exclusivo de Lid...

PORTADA | ESCALA DE EVALUACION | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA

Pruebas técnicas



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista Desarrollador ¿Qué desea hacer? GERARDO CAMPOS MOLINA Compartir

A2 ENTIDADEVALUADA

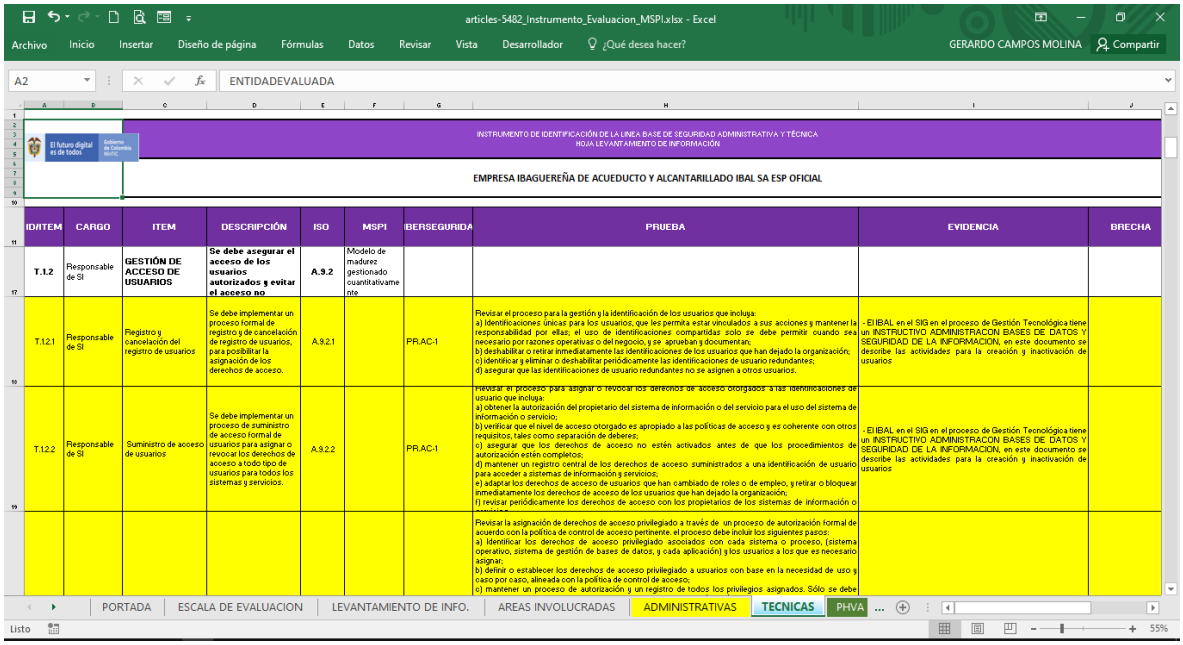
INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

IDITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	IBERSEGURIDA	PRUEBA	EVIDENCIA	BRECHA
CONTROL DE ACCESO									
T.1	Responsable de SI/Responsable de TICs	CONTROL DE ACCESO		A.9	Componente planificación y modelo de madurez				
T.1.1	Responsable de SI	REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	Se debe limitar el acceso a información y a instalaciones de procesamiento de	A.9.1	Modelo de madurez definido				
T.1.1.1	Responsable de SI	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	A.9.1.1		PR.DS-5	Revisar que la política contenga lo siguiente: a) los requisitos de seguridad para las aplicaciones del negocio; b) las políticas para la divulgación y autorización de la información, y los niveles de seguridad de la información y de clasificación de la información; c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes; d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios; e) la gestión de los derechos de acceso en un entorno distribuido y en red, que reconoce todos los tipos de conexiones disponibles; f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso); g) los requisitos para la autorización formal de las solicitudes de acceso; h) los requisitos para la revisión periódica de los derechos de acceso; i) el retiro de los derechos de acceso; j) el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente; k) los roles de acceso privilegiado;	- El IBAL en la política de seguridad y privacidad de la información, tiene la política de control de acceso	
			Se debe permitir acceso de los usuarios a la red			PR.AC-4	Revisar la política relacionada con el uso de redes y de servicios de red y verificar que incluya: a) las redes y servicios de red a los que se permite el acceso; b) los procedimientos de autorización para determinar a quién se permite el acceso a qué redes y servicios		

PORTADA ESCALA DE EVALUACION LEVANTAMIENTO DE INFO. AREAS INVOLUCRADAS ADMINISTRATIVAS TECNICAS PHVA

Listo 55%



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista Desarrollador ¿Qué desea hacer? GERARDO CAMPOS MOLINA Compartir

A2 ENTIDADEVALUADA

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

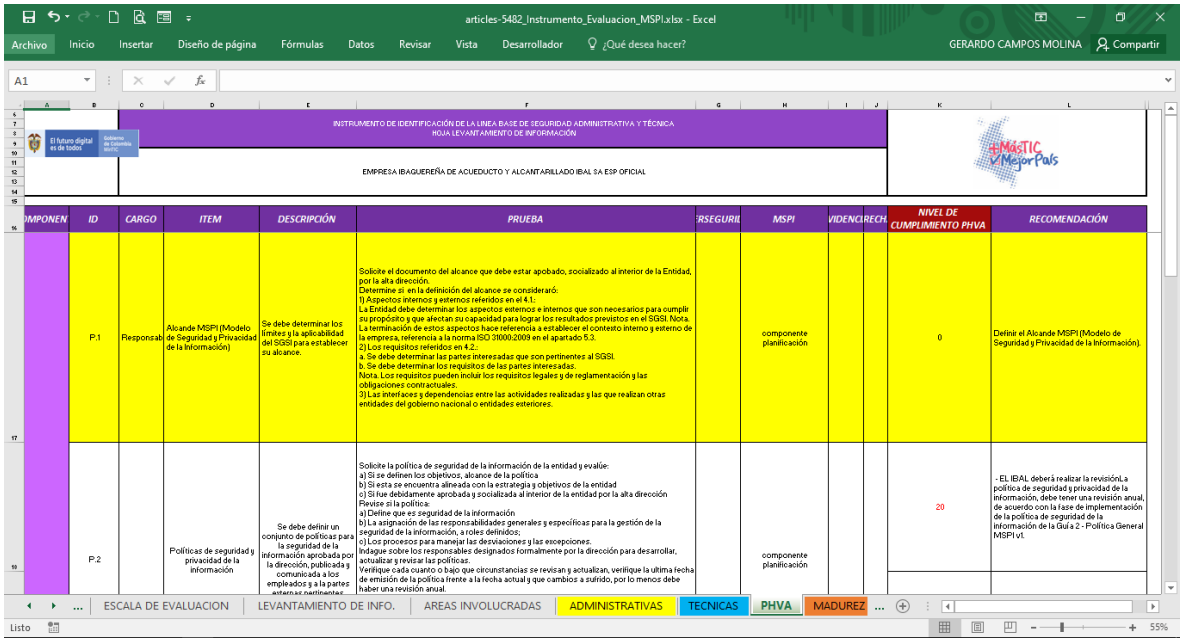
EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

IDITEM	CARGO	ITEM	DESCRIPCIÓN	ISO	MSPI	IBERSEGURIDA	PRUEBA	EVIDENCIA	BRECHA
T.1.2	Responsable de SI	GESTIÓN DE ACCESO DE USUARIOS	Se debe asegurar el acceso de los usuarios autorizados y evitar el acceso no	A.9.2	Modelo de madurez gestionado cuantitativamente				
T.1.2.1	Responsable de SI	Registro y cancelación del registro de usuarios	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	A.9.2.1		PR.AC-1	Revisar el proceso para la gestión y la identificación de los usuarios que incluya: a) identificaciones únicas para los usuarios, que les permita estar vinculados a sus acciones y mantener la responsabilidad por ellas; el uso de identificaciones compartidas solo se debe permitir cuando sea necesario por razones operativas o del negocio, y se aprueban y documentan; b) deshabilitar o retirar inmediatamente las identificaciones de los usuarios que han dejado la organización; c) identificar y eliminar o deshabilitar periódicamente las identificaciones de usuario redundantes; d) asegurar que las identificaciones de usuario redundantes no se asignen a otros usuarios.	- El IBAL en el SIG en el proceso de Gestión Tecnológica tiene un INSTRUCTIVO ADMINISTRACON BASES DE DATOS Y SEGURIDAD DE LA INFORMACION, en este documento se describe las actividades para la creación y inactivación de usuarios	
T.1.2.2	Responsable de SI	Suministro de acceso de usuarios	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	A.9.2.2		PR.AC-1	Revisar el proceso para asignar o revocar los derechos de acceso otorgados a las identificaciones de usuario que incluya: a) obtener la autorización del propietario del sistema de información o del servicio para el uso del sistema de información o servicio; b) verificar que el nivel de acceso otorgado es apropiado a las políticas de acceso y es coherente con otros requisitos, tales como separación de deberes; c) asegurar que los derechos de acceso no estén activados antes de que los procedimientos de autorización estén completos; d) mantener un registro central de los derechos de acceso suministrados a una identificación de usuario para acceder a sistemas de información y servicios; e) adaptar los derechos de acceso de usuarios que han cambiado de roles o de empleo, y retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han dejado la organización; f) revisar periódicamente los derechos de acceso con los propietarios de los sistemas de información o	- El IBAL en el SIG en el proceso de Gestión Tecnológica tiene un INSTRUCTIVO ADMINISTRACON BASES DE DATOS Y SEGURIDAD DE LA INFORMACION, en este documento se describe las actividades para la creación y inactivación de usuarios	
							Revisar la asignación de derechos de acceso privilegiado a través de un proceso de autorización formal de acuerdo con la política de control de acceso pertinente. el proceso debe incluir los siguientes pasos: a) Identificar los derechos de acceso privilegiado asociados con cada sistema o proceso, (sistema operativo, sistema de gestión de bases de datos, y cada aplicación) y los usuarios a los que es necesario asignar; b) definir o establecer los derechos de acceso privilegiado a usuarios con base en la necesidad de uso y caso por caso, alineada con la política de control de acceso; c) mantener un proceso de autorización y un registro de todos los privilegios asignados. Sólo se debe		

PORTADA ESCALA DE EVALUACION LEVANTAMIENTO DE INFO. AREAS INVOLUCRADAS ADMINISTRATIVAS TECNICAS PHVA

Listo 55%

Avance del ciclo PHVA



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

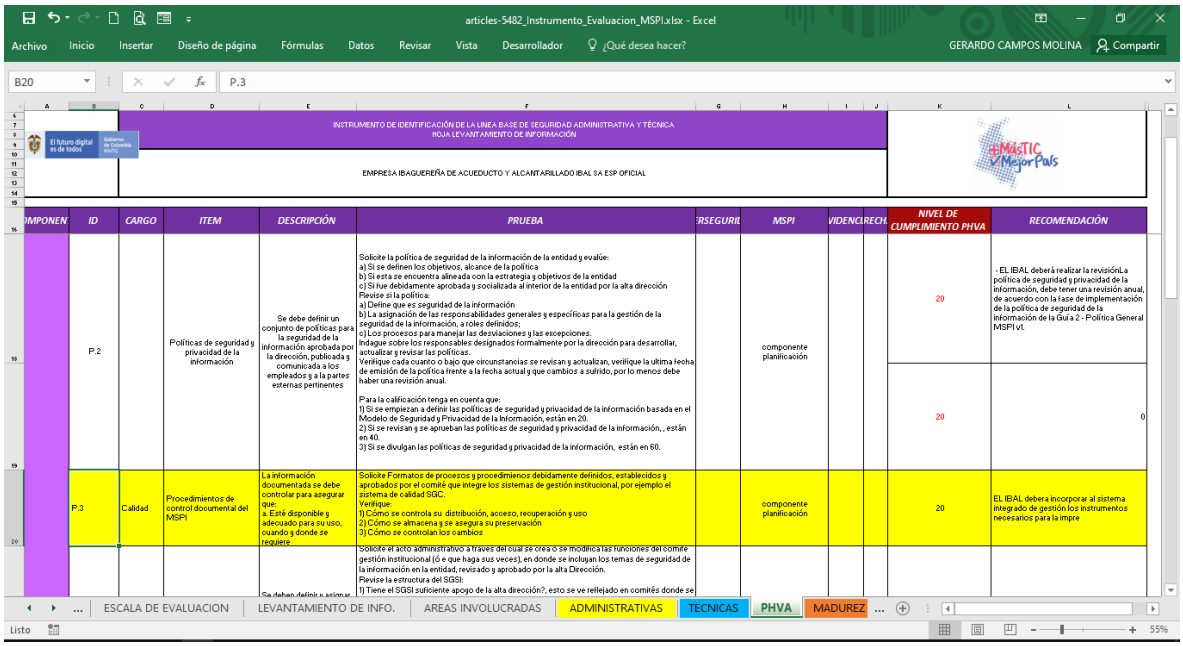
INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

COMPONEN	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	ERSEGURI	MSPI	VIDENCI	RECH	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
	P.1	Responsab	Alcande MSPI (Modelo de Seguridad y Privacidad de la Información)	Se debe determinar los límites y la aplicabilidad del SGSI para establecer su alcance.	Solicite el documento del alcance que debe estar aprobado, socializado al interior de la Entidad, por la alta dirección. Determine si en la definición del alcance se consideró: 1) Aspectos internos y externos referidos en el 4.1: La Entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el SGSI. Nota. La terminación de estos aspectos hace referencia a establecer el contexto interno y externo de la empresa, referencia a la norma ISO 31000:2009 en el apartado 5.3. 2) Los requisitos referidos en 4.2.: a. Se debe determinar las partes interesadas que son pertinentes al SGSI. b. Se debe determinar los requisitos de las partes interesadas. Nota. Los requisitos pueden incluir los requisitos legales y de reglamentación y las obligaciones contractuales. 3) Las interfaces y dependencias entre las actividades realizadas y las que realizan otras entidades del gobierno nacional o entidades exteriores.		componente planificación			0	Definir el Alcande MSPI (Modelo de Seguridad y Privacidad de la Información).
	P.2		Políticas de seguridad y privacidad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a) Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo que circunstancias se revisan y actualizan, verifique la ultima fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual.		componente planificación			20	- EL IBAL deberá realizar la revisiónLa política de seguridad y privacidad de la información, debe tener una revisión anual, de acuerdo con la fase de implementación de la política de seguridad de la información de la Guí a 2 - Política General MSPI v1.

ESCALA DE EVALUACION | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA | MADUREZ

Listo



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

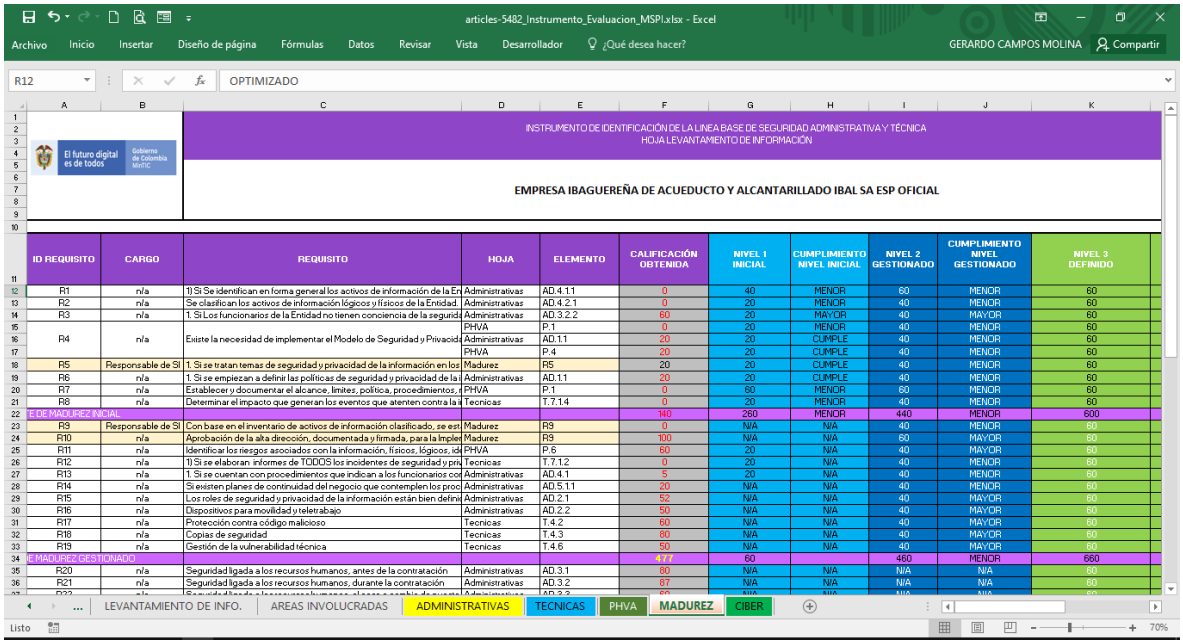
EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

COMPONEN	ID	CARGO	ITEM	DESCRIPCIÓN	PRUEBA	ERSEGURI	MSPI	VIDENCI	RECH	NIVEL DE CUMPLIMIENTO PHVA	RECOMENDACIÓN
	P.2		Políticas de seguridad y privacidad de la información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a la partes externas pertinentes	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a) Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo que circunstancias se revisan y actualizan, verifique la ultima fecha de emisión de la política frente a la fecha actual y que cambios a sufrido, por lo menos debe haber una revisión anual. Para la calificación tenga en cuenta que: 1) Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2) Si se revisan y se aprueban las políticas de seguridad y privacidad de la información, , están en 40. 3) Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.		componente planificación			20	- EL IBAL deberá realizar la revisiónLa política de seguridad y privacidad de la información, debe tener una revisión anual, de acuerdo con la fase de implementación de la política de seguridad de la información de la Guí a 2 - Política General MSPI v1.
										20	0
	P.3	Calidad	Procedimientos de control documental del MSPI	La información documentada se debe controlar para asegurar que: a. Esté disponible y adecuado para su uso, cuando y donde se requiere	Solicite Formatos de procesos y procedimienos debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional, por ejemplo el sistema de calidad SGC. Verifique: 1) Cómo se controla su distribución, acceso, recuperación y uso 2) Cómo se almacena y se asegura su preservación 3) Cómo se controlan los cambios		componente planificación			20	EL IBAL debera incorporar al sistema integrado de gestión los instrumentos necesarios para la impre
					Solicite el acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó e que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección. Revise la estructura del SGSI: 1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se						

ESCALA DE EVALUACION | LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA | MADUREZ

Listo

Nivel de madurez del MSPI



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista Desarrollador ¿Qué desea hacer? GERARDO CAMPOS MOLINA Compartir

R12 OPTIMIZADO

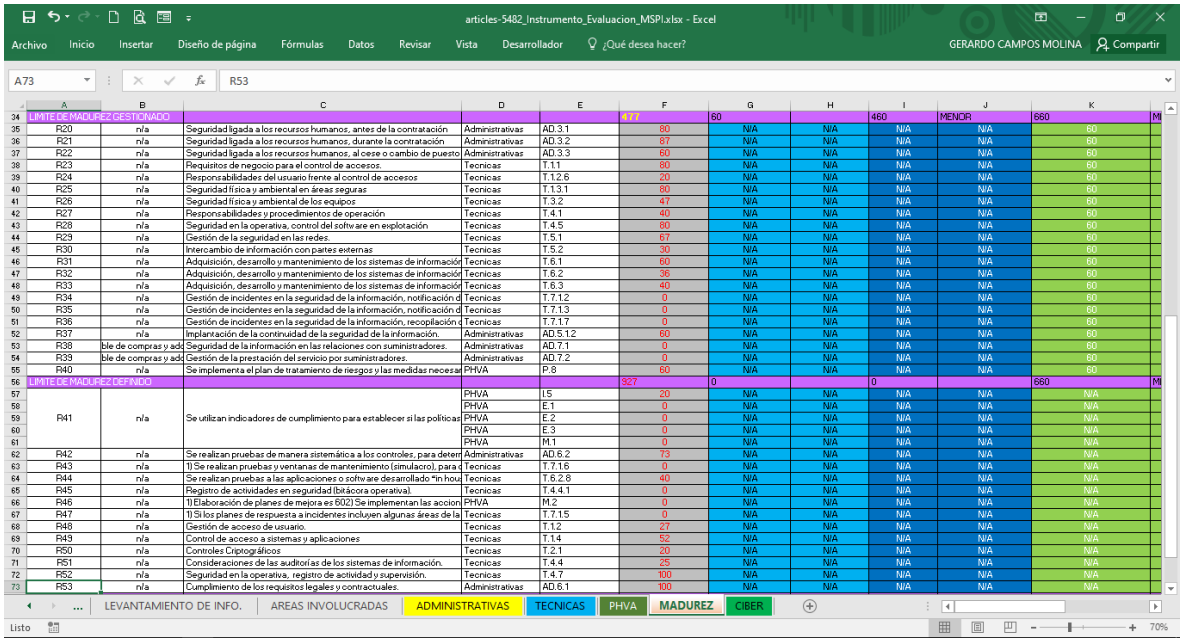
INSTRUMENTO DE IDENTIFICACIÓN DE LA LÍNEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

ID REQUISITO	CARGO	REQUISITO	HOJA	ELEMENTO	CALIFICACIÓN OBTENIDA	NIVEL 1 INICIAL	CUMPLIMIENTO NIVEL INICIAL	NIVEL 2 GESTIONADO	CUMPLIMIENTO NIVEL GESTIONADO	NIVEL 3 DEFINIDO
R1	n/a	1) Si Se identifican en forma general los activos de información de la En	Administrativas	AD.4.1.1	0	40	MENOR	80	MENOR	60
R2	n/a	Se clasifican los activos de información lógicos y físicos de la Entidad.	Administrativas	AD.4.2.1	0	20	MENOR	40	MENOR	60
R3	n/a	1. Si Los funcionarios de la Entidad no tienen conciencia de la seguridad	Administrativas	AD.3.2.2	60	20	MAYOR	40	MAYOR	60
R4	n/a	Existe la necesidad de implementar el Modelo de Seguridad y Privacidad	PHVA	P.1	0	20	MENOR	40	MENOR	60
			Administrativas	AD.1.1	20	20	CUMPLE	40	MENOR	60
			PHVA	P.4	20	20	CUMPLE	40	MENOR	60
R5	Responsable de SI	1. Si se tratan temas de seguridad y privacidad de la información en los	Madurez	R5	20	20	CUMPLE	40	MENOR	60
R6	n/a	1. Si se empiezan a definir las políticas de seguridad y privacidad de la	Administrativas	AD.1.1	20	20	CUMPLE	40	MENOR	60
R7	n/a	Establecer y documentar el alcance, límites, política, procedimientos, r	PHVA	P.1	0	60	MENOR	60	MENOR	60
R8	n/a	Determinar el impacto que generan los eventos que atenten contra la i	Tecnicas	T.7.1.4	0	20	MENOR	40	MENOR	60
E DE MADUREZ INICIAL					140	260	MENOR	440	MENOR	600
R9	Responsable de SI	Con base en el inventario de activos de información clasificado, se est	Madurez	R9	0	N/A	N/A	40	MENOR	60
R10	n/a	Aprobación de la alta dirección, documentada y firmada, para la Imple	Madurez	R9	100	N/A	N/A	60	MAYOR	60
R11	n/a	Identificar los riesgos asociados con la información, físicos, lógicos, id	PHVA	P.6	60	20	N/A	40	MAYOR	60
R12	n/a	1) Si se elaboran informes de TODOS los incidentes de seguridad y pro	Tecnicas	T.7.1.2	0	20	N/A	40	MENOR	60
R13	n/a	1. Si se cuentan con procedimientos que indican a los funcionarios cor	Administrativas	AD.4.1	5	20	N/A	40	MENOR	60
R14	n/a	Si existen planes de continuidad del negocio que contemplen los proc	Administrativas	AD.5.1.1	20	N/A	N/A	40	MENOR	60
R15	n/a	Los roles de seguridad y privacidad de la información están bien defini	Administrativas	AD.2.1	52	N/A	N/A	40	MAYOR	60
R16	n/a	Dispositivos para movilidad y teletrabajo	Administrativas	AD.2.2	50	N/A	N/A	40	MAYOR	60
R17	n/a	Protección contra código malicioso	Tecnicas	T.4.2	60	N/A	N/A	40	MAYOR	60
R18	n/a	Copias de seguridad	Tecnicas	T.4.3	80	N/A	N/A	40	MAYOR	60
R19	n/a	Gestión de la vulnerabilidad técnica	Tecnicas	T.4.6	50	N/A	N/A	40	MAYOR	60
E MADUREZ GESTIONADO					477	60		460	MENOR	660
R20	n/a	Seguridad ligada a los recursos humanos, antes de la contratación	Administrativas	AD.3.1	80	N/A	N/A	N/A	N/A	60
R21	n/a	Seguridad ligada a los recursos humanos, durante la contratación	Administrativas	AD.3.2	87	N/A	N/A	N/A	N/A	60

LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA | MADUREZ | CIBER

Listo 70%



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista Desarrollador ¿Qué desea hacer? GERARDO CAMPOS MOLINA Compartir

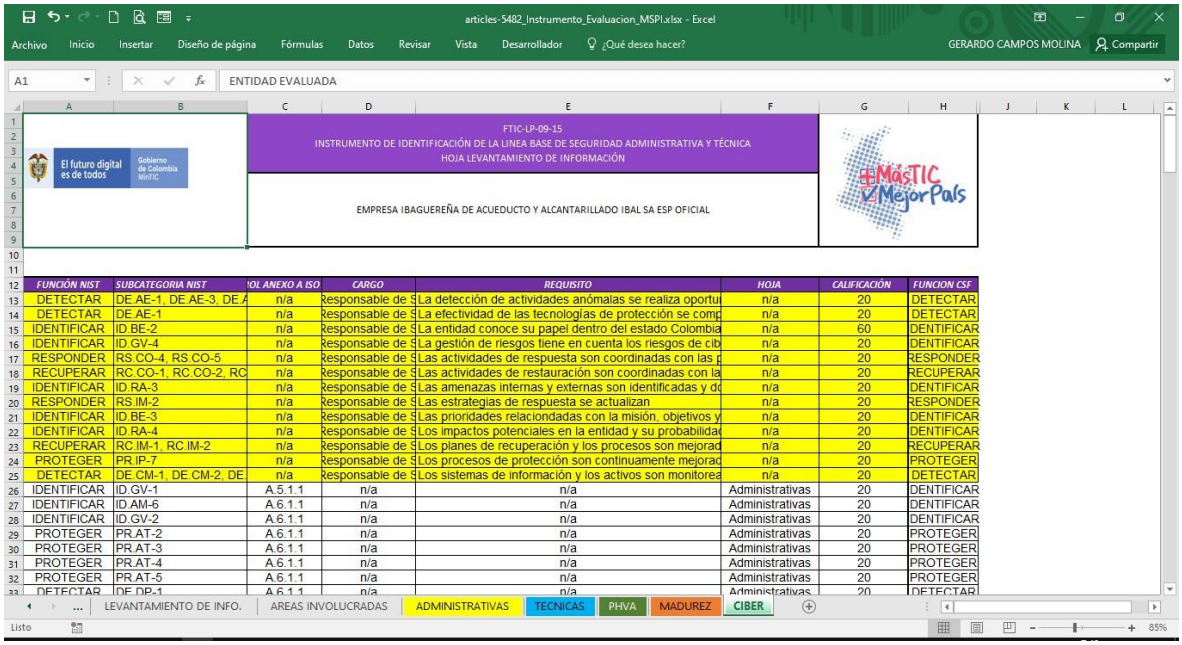
A73 R53

LIMITE DE MADUREZ GESTIONADO					477	60		460	MENOR	660	M
R20	n/a	Seguridad ligada a los recursos humanos, antes de la contratación	Administrativas	AD.3.1	80	N/A	N/A	N/A	N/A	60	
R21	n/a	Seguridad ligada a los recursos humanos, durante la contratación	Administrativas	AD.3.2	87	N/A	N/A	N/A	N/A	60	
R22	n/a	Seguridad ligada a los recursos humanos, al cese o cambio de puesto	Administrativas	AD.3.3	60	N/A	N/A	N/A	N/A	60	
R23	n/a	Requisitos de negocio para el control de accesos.	Tecnicas	T.1.1	80	N/A	N/A	N/A	N/A	60	
R24	n/a	Responsabilidades del usuario frente al control de accesos	Tecnicas	T.1.2.6	20	N/A	N/A	N/A	N/A	60	
R25	n/a	Seguridad física y ambiental en áreas seguras	Tecnicas	T.1.3.1	80	N/A	N/A	N/A	N/A	60	
R26	n/a	Seguridad física y ambiental de los equipos	Tecnicas	T.3.2	47	N/A	N/A	N/A	N/A	60	
R27	n/a	Responsabilidades y procedimientos de operación	Tecnicas	T.4.1	40	N/A	N/A	N/A	N/A	60	
R28	n/a	Seguridad en la operativa, control del software en explotación	Tecnicas	T.4.5	80	N/A	N/A	N/A	N/A	60	
R29	n/a	Gestión de la seguridad en las redes.	Tecnicas	T.5.1	67	N/A	N/A	N/A	N/A	60	
R30	n/a	Intercambio de información con partes externas	Tecnicas	T.5.2	30	N/A	N/A	N/A	N/A	60	
R31	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información	Tecnicas	T.6.1	60	N/A	N/A	N/A	N/A	60	
R32	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información	Tecnicas	T.6.2	36	N/A	N/A	N/A	N/A	60	
R33	n/a	Adquisición, desarrollo y mantenimiento de los sistemas de información	Tecnicas	T.6.3	40	N/A	N/A	N/A	N/A	60	
R34	n/a	Gestión de incidentes en la seguridad de la información, notificación d	Tecnicas	T.7.1.2	0	N/A	N/A	N/A	N/A	60	
R35	n/a	Gestión de incidentes en la seguridad de la información, notificación d	Tecnicas	T.7.1.3	0	N/A	N/A	N/A	N/A	60	
R36	n/a	Gestión de incidentes en la seguridad de la información, recopilación d	Tecnicas	T.7.1.7	0	N/A	N/A	N/A	N/A	60	
R37	n/a	Implantación de la continuidad de la seguridad de la información.	Administrativas	AD.5.1.2	60	N/A	N/A	N/A	N/A	60	
R38	ble de compras y ad	Seguridad de la información en las relaciones con suministradores.	Administrativas	AD.7.1	0	N/A	N/A	N/A	N/A	60	
R39	ble de compras y ad	Gestión de la prestación del servicio por suministradores.	Administrativas	AD.7.2	0	N/A	N/A	N/A	N/A	60	
R40	n/a	Se implementa el plan de tratamiento de riesgos y las medidas necesar	PHVA	P.8	60	N/A	N/A	N/A	N/A	60	
LIMITE DE MADUREZ DEFINIDO					327	0		0		660	M
			PHVA	I.5	20	N/A	N/A	N/A	N/A	N/A	
			PHVA	E.1	0	N/A	N/A	N/A	N/A	N/A	
R41	n/a	Se utilizan indicadores de cumplimiento para establecer si las políticas	PHVA	E.2	0	N/A	N/A	N/A	N/A	N/A	
			PHVA	E.3	0	N/A	N/A	N/A	N/A	N/A	
			PHVA	M.1	0	N/A	N/A	N/A	N/A	N/A	
R42	n/a	Se realizan pruebas de manera sistemática a los controles, para deter	Administrativas	AD.6.2	73	N/A	N/A	N/A	N/A	N/A	
R43	n/a	1) Se realizan pruebas y ventanas de mantenimiento (simulacro), para c	Tecnicas	T.7.1.6	0	N/A	N/A	N/A	N/A	N/A	
R44	n/a	Se realizan pruebas a las aplicaciones o software desarrollado *in hou	Tecnicas	T.6.2.8	40	N/A	N/A	N/A	N/A	N/A	
R45	n/a	Registro de actividades en seguridad (bitácora operativa).	Tecnicas	T.4.4.1	0	N/A	N/A	N/A	N/A	N/A	
R46	n/a	1) Elaboración de planes de mejora ej: 6D2) Se implementan las accion	PHVA	M.2	0	N/A	N/A	N/A	N/A	N/A	
R47	n/a	1) Si los planes de respuesta a incidentes incluyen algunas áreas de la	Tecnicas	T.7.1.5	0	N/A	N/A	N/A	N/A	N/A	
R48	n/a	Gestión de acceso de usuario.	Tecnicas	T.1.2	27	N/A	N/A	N/A	N/A	N/A	
R49	n/a	Control de acceso a sistemas y aplicaciones	Tecnicas	T.1.4	52	N/A	N/A	N/A	N/A	N/A	
R50	n/a	Controles Criptográficos	Tecnicas	T.2.1	20	N/A	N/A	N/A	N/A	N/A	
R51	n/a	Consideraciones de las auditorías de los sistemas de información.	Tecnicas	T.4.4	25	N/A	N/A	N/A	N/A	N/A	
R52	n/a	Seguridad en la operativa, registro de actividad y supervisión.	Tecnicas	T.4.7	100	N/A	N/A	N/A	N/A	N/A	
R53	n/a	Cumplimiento de los requisitos legales y contractuales.	Administrativas	AD.6.1	100	N/A	N/A	N/A	N/A	N/A	

LEVANTAMIENTO DE INFO. | AREAS INVOLUCRADAS | ADMINISTRATIVAS | TECNICAS | PHVA | MADUREZ | CIBER

Listo 70%

CSF NIST



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista Desarrollador ¿Qué desea hacer? GERARDO CAMPOS MOLINA Compartir

A1 ENTIDAD EVALUADA

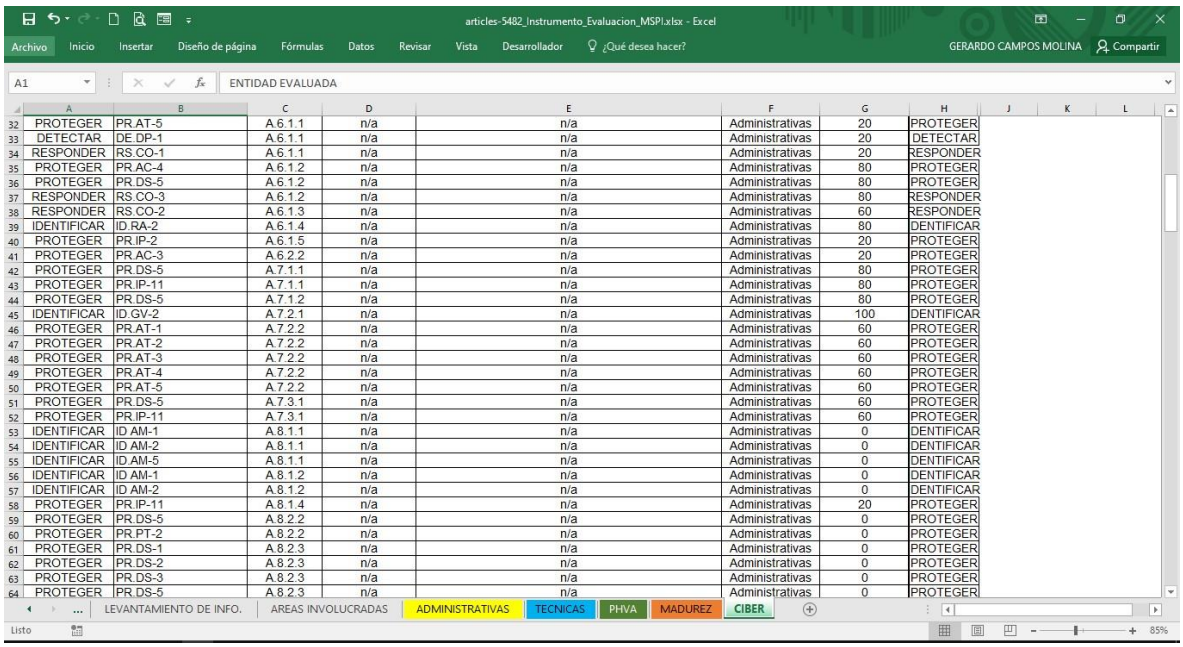
FTIC-LP-09-15
INSTRUMENTO DE IDENTIFICACIÓN DE LA LINEA BASE DE SEGURIDAD ADMINISTRATIVA Y TÉCNICA
HOJA LEVANTAMIENTO DE INFORMACIÓN

EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL

FUNCIÓN NIST	SUBCATEGORIA NIST	!OL ANEXO A ISO	CARGO	REQUISITO	HOJA	CALIFICACIÓN	FUNCION CSF
DETECTAR	DE.AE-1, DE.AE-3, DE.A	n/a	Responsable de S	La detección de actividades anómalas se realiza oportu	n/a	20	DETECTAR
DETECTAR	DE.AE-1	n/a	Responsable de S	La efectividad de las tecnologías de protección se comp	n/a	20	DETECTAR
IDENTIFICAR	ID.BE-2	n/a	Responsable de S	La entidad conoce su papel dentro del estado Colombia	n/a	60	DENTIFICAR
IDENTIFICAR	ID.GV-4	n/a	Responsable de S	La gestión de riesgos tiene en cuenta los riesgos de cib	n/a	20	DENTIFICAR
RESPONDER	RS.CO-4, RS.CO-5	n/a	Responsable de S	Las actividades de respuesta son coordinadas con las p	n/a	20	RESPONDER
RECUPERAR	RC.CO-1, RC.CO-2, RC	n/a	Responsable de S	Las actividades de restauración son coordinadas con la	n/a	20	RECUPERAR
IDENTIFICAR	ID.RA-3	n/a	Responsable de S	Las amenazas internas y externas son identificadas y do	n/a	20	DENTIFICAR
RESPONDER	RS.IM-2	n/a	Responsable de S	Las estrategias de respuesta se actualizan	n/a	20	RESPONDER
IDENTIFICAR	ID.BE-3	n/a	Responsable de S	Las prioridades relacionadas con la misión, objetivos y	n/a	20	DENTIFICAR
IDENTIFICAR	ID.RA-4	n/a	Responsable de S	Los impactos potenciales en la entidad y su probabilidad	n/a	20	DENTIFICAR
RECUPERAR	RC.IM-1, RC.IM-2	n/a	Responsable de S	Los planes de recuperación y los procesos son mejorad	n/a	20	RECUPERAR
PROTEGER	PR.IP-7	n/a	Responsable de S	Los procesos de protección son continuamente mejorad	n/a	20	PROTEGER
DETECTAR	DE.CM-1, DE.CM-2, DE	n/a	Responsable de S	Los sistemas de información y los activos son monitorea	n/a	20	DETECTAR
IDENTIFICAR	ID.GV-1	A.5.1.1	n/a	n/a	Administrativas	20	DENTIFICAR
IDENTIFICAR	ID.AM-6	A.6.1.1	n/a	n/a	Administrativas	20	DENTIFICAR
IDENTIFICAR	ID.GV-2	A.6.1.1	n/a	n/a	Administrativas	20	DENTIFICAR
PROTEGER	PR.AT-2	A.6.1.1	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.AT-3	A.6.1.1	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.AT-4	A.6.1.1	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.AT-5	A.6.1.1	n/a	n/a	Administrativas	20	PROTEGER
DETECTAR	DE.DP-1	A.6.1.1	n/a	n/a	Administrativas	20	DETECTAR

... LEVANTAMIENTO DE INFO. AREAS INVOLUCRADAS ADMINISTRATIVAS TECNICAS PHVA MADUREZ CIBER

Listo 85%



articles-5482_Instrumento_Evaluacion_MSPI.xlsx - Excel

Archivo Inicio Insertar Diseño de página Fórmulas Datos Revisar Vista Desarrollador ¿Qué desea hacer? GERARDO CAMPOS MOLINA Compartir

A1 ENTIDAD EVALUADA

PROTEGER	PR.AT-5	A.6.1.1	n/a	n/a	Administrativas	20	PROTEGER
DETECTAR	DE.DP-1	A.6.1.1	n/a	n/a	Administrativas	20	DETECTAR
RESPONDER	RS.CO-1	A.6.1.1	n/a	n/a	Administrativas	20	RESPONDER
PROTEGER	PR.AC-4	A.6.1.2	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.DS-5	A.6.1.2	n/a	n/a	Administrativas	80	PROTEGER
RESPONDER	RS.CO-3	A.6.1.2	n/a	n/a	Administrativas	80	RESPONDER
RESPONDER	RS.CO-2	A.6.1.3	n/a	n/a	Administrativas	60	RESPONDER
IDENTIFICAR	ID.RA-2	A.6.1.4	n/a	n/a	Administrativas	80	DENTIFICAR
PROTEGER	PR.IP-2	A.6.1.5	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.AC-3	A.6.2.2	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.DS-5	A.7.1.1	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.IP-11	A.7.1.1	n/a	n/a	Administrativas	80	PROTEGER
PROTEGER	PR.DS-5	A.7.1.2	n/a	n/a	Administrativas	80	PROTEGER
IDENTIFICAR	ID.GV-2	A.7.2.1	n/a	n/a	Administrativas	100	DENTIFICAR
PROTEGER	PR.AT-1	A.7.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.AT-2	A.7.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.AT-3	A.7.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.AT-4	A.7.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.AT-5	A.7.2.2	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.DS-5	A.7.3.1	n/a	n/a	Administrativas	60	PROTEGER
PROTEGER	PR.IP-11	A.7.3.1	n/a	n/a	Administrativas	60	PROTEGER
IDENTIFICAR	ID.AM-1	A.8.1.1	n/a	n/a	Administrativas	0	DENTIFICAR
IDENTIFICAR	ID.AM-2	A.8.1.1	n/a	n/a	Administrativas	0	DENTIFICAR
IDENTIFICAR	ID.AM-5	A.8.1.1	n/a	n/a	Administrativas	0	DENTIFICAR
IDENTIFICAR	ID.AM-1	A.8.1.2	n/a	n/a	Administrativas	0	DENTIFICAR
IDENTIFICAR	ID.AM-2	A.8.1.2	n/a	n/a	Administrativas	0	DENTIFICAR
PROTEGER	PR.IP-11	A.8.1.4	n/a	n/a	Administrativas	20	PROTEGER
PROTEGER	PR.DS-5	A.8.2.2	n/a	n/a	Administrativas	0	PROTEGER
PROTEGER	PR.PT-2	A.8.2.2	n/a	n/a	Administrativas	0	PROTEGER
PROTEGER	PR.DS-1	A.8.2.3	n/a	n/a	Administrativas	0	PROTEGER
PROTEGER	PR.DS-2	A.8.2.3	n/a	n/a	Administrativas	0	PROTEGER
PROTEGER	PR.DS-3	A.8.2.3	n/a	n/a	Administrativas	0	PROTEGER
PROTEGER	PR.DS-5	A.8.2.3	n/a	n/a	Administrativas	0	PROTEGER

... LEVANTAMIENTO DE INFO. AREAS INVOLUCRADAS ADMINISTRATIVAS TECNICAS PHVA MADUREZ CIBER

Listo 85%

Anexo D. FORMATO CORRESPONDIENTE A LA ALTERNATIVA DE GRADO

https://docs.google.com/document/d/1QSBX6qN18DLKicu9OTm6dTwNXQomIOgc/edit?usp=sharing&ouid=114717429178189539476&rtpof=true&sd=true

Anexo E. RESUMEN ANALÍTIO ESPECIALIZADO RAE

Fecha de Realización:	01/11/2021
Programa:	Especialización en seguridad informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	ETAPA DE PLANIFICACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN, PARA LA EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL
Autor(es):	ADRIANA DIAZ LENIS Y GERARDO CAMPOS MOLINA
Palabras Claves:	MSPI, MINTIC, MIPG, ISO/IEC 27001:2013, DAFP
Descripción: (250 palabras)	Con el desarrollo de este proyecto aplicado, se busca establecer las bases para la implementación del MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN (MSPI) en la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, a través del desarrollo de la FASE DE PLANIFICACIÓN DEL MODELO, basados en las guías y directrices que estableció el ministerio de las TIC para las entidades del estado, con el fin de apoyar el cumplimiento de la política de gobierno digital anteriormente llamada gobierno en línea.

Fuentes bibliográficas destacadas:

COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Manual para la Implementación de la Política de Gobierno Digital. Versión 7 de abril de 2019. [Consultado: 15 de mayo de 2021].

Disponible en: https://gobiernodigital.mintic.gov.co/692/channels-594_manual_gd.pdf COLOMBIA. MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Modelo de Seguridad y Privacidad de la Información. 2021. Disponible en: https://gobiernodigital.mintic.gov.co/692/articles-162623_recurso_1.pdf COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA FUNCION PÚBLICA. Guía para la administración del riesgo y el diseño de controles en entidades pública. Versión 5 diciembre de 2020 [en línea]. Bogotá D.C.: p. 1-87. [Consultado: 18 de mayo de 2021]. Disponible en: https://www.funcionpublica.gov.co/documents/418548/34150781/Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controles+en+entidades+p%C3%BAblicas+-+Versi%C3%B3n+5+-+Diciembre+de+2020.pdf/68d324dd-55c5-11e0-9f37-2e5516b48a87?t=1611247032238&download=true EMPRESA IBAGUEREÑA DE ACUEDUCTO Y ALCANTARILLADO IBAL SA ESP OFICIAL. Matriz de caracterización gestión tecnológica del SIG. 2021. Instructivo 2021. [Consultado el: 2021-05-03]. [En línea]. Disponible en: https://www.ibal.gov.co/sites/default/files/ibal/sites/default/files/images/stories/CARACTERIZACI%C3%93N%20GESTI%C3%93N%20TECNOLOGICA%20v14.pdf	
Contenido del documento:	Primero se realizó un contexto de los aspectos, características y lineamientos relacionados con la implementación de la política de gobierno digital, el modelo de seguridad y privacidad de la información (MSPI) y su articulación con el Formulario Único de

	Reporte de Avances de la Gestión - Furag (MiPg y MECI) en la Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL. Identificados los aspectos de la política y el modelo, se realizó el recolección y análisis de la información del IBAL, con el fin de elaborar el autodiagnóstico definido en el MSPI e identificar el estado actual de la empresa con relación a la implementación de la política y el modelo. Basados en los resultados del estado actual de la empresa, se elaboraron los objetivos para la planificación del MSPI para él IBAL, con base en los lineamientos de Ministerio de las Tecnologías de la Información y Comunicaciones (MINTIC). Para el desarrollo de los objetivos, se realizó la identificación y gestión de activos de información de acuerdo con la guía del Departamento Administrativo de la Función Pública (DAFP), con el fin de gestionar los riesgos asociados a estos activos por medio de su clasificación en información pública, pública clasificada y pública reservada, si contiene o no datos personales, determinar el nivel de criticidad del activo con relación a la integridad, disponibilidad, confidencialidad y se identificación si existen o no infraestructuras críticas cibernéticas.

	Lo anterior se desarrolló con el fin de identificar los controles asociados a la seguridad de la información, los cuales se van a planificar en el IBAL, con el fin de reducir o eliminar el riesgo asociados a los activos de información. Por último, en la fase de planificación, se elaboraron los aspectos normativos y las características funcionales para que el IBAL pueda implementar el MSPI y le permita asegurar la seguridad de la información.
Marco Metodológico:	El proyecto aplicado se desarrolló de acuerdo con los lineamientos del ministerio de tecnologías de información y las comunicaciones – MINTIC, relacionados con el MSPI, realizando las fases de diagnóstico y planificación, las cuales son previas en el ciclo PHVA por el cual se opera este modelo.
Conceptos adquiridos :	Articulación de un modelo de seguridad a los fines de la seguridad informática en una organización *con el fin de mantener la integridad, disponibilidad y privacidad de la información*. Desarrollo de la planificación de un MSPI para una organización. Gestión del riesgo y diseño de controles con base en la ISO/IEC 27001:2013. Infraestructuras críticas cibernéticas.
Conclusiones:	Es importante la socialización de la fase de planificación del MSPI en los directivos de La Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL, con el fin de establecer estrategias a corto, mediano y largo plazo, que propendan por la implementación del MSPI.

	Ya que La Empresa Ibaguereña de Acueducto y Alcantarillado IBAL SA ESP OFICIAL tiene un sistema integrado de gestión con las normas ISO 45001:2018, ISO 14001 Y ISO 9001:2015, deberá aprovechar esta coyuntura para realizar todos los esfuerzos necesarios para implementar y operar de acuerdo con el ciclo PHVA, el modelo de seguridad y privacidad de la información (MSPI) de acuerdo con los lineamientos de MINTIC, con el objetivo implementar y gestionar los controles necesarios en el proceso de gestión tecnológica, que le permitan una adecuada gestión del riesgo y así garanticen la seguridad de la información, con el fin de contribuir con la continuidad del negocio.