Elaboración de un plan de proyecto que permita implementar, en Centrales Eléctricas de Norte de Santander S.A. E.S.P., mecanismos de autenticación digital según la política de gobierno digital del Ministerio de Tecnologías de la Información y las Comunicaciones

GABRIEL LEONARDO ÁVILA BUSTOS

GREGORIO ANTONIO SUÁREZ VERA

Universidad EAN

Facultad de Ingeniería

Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Bogotá, Colombia

2021

Elaboración de un plan de proyecto que permita implementar, en Centrales Eléctricas de Norte de Santander S.A. E.S.P., mecanismos de autenticación digital según la política de gobierno digital del Ministerio de Tecnologías de la Información y las Comunicaciones

GABRIEL LEONARDO ÁVILA BUSTOS

GREGORIO ANTONIO SUÁREZ VERA

Trabajo de grado presentado como requisito para optar al título de:

Magister en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Director (a):

Luis Armando Cobo Campo

Modalidad:

Trabajo Dirigido

Universidad EAN

Facultad de Ingeniería

Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Bogotá, Colombia

2021

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma del jurado

_____

Firma del jurado

_____

Firma del director del trabajo de grado

Bogotá D.C. Día - mes – año

Dedicatoria de Gregorio

A DIOS por sobre todas las cosas, por disponerlo todo para la obtención de este gran logro.

A mis padres, hermanos y demás familia, por creer en mí y acompañarme en cada paso.

A mi amada esposa, por su apoyo y comprensión inagotables.

A mi hija y sobrinas, por ser mi inspiración.

Dedicatoria de Gabriel

A mi difunto padre por enseñarme la importancia de la educación.

A mi madre por su abnegación, perseverancia y tenacidad para impulsarme a salir adelante.

A mis hermanos y sobrina por apoyarme para cumplir mis metas.

A mi esposa por acompañarme en el camino de la vida y apoyarme para la obtención de este logro.

Agradecimientos

A DIOS por proveernos de todo lo requerido para hacer realidad nuestro logro.

A los profesores por su motivación, guía e invaluables aportes para nuestra formación personal y profesional.

A cada integrante de la familia CENS que nos brindó su apoyo a lo largo de este programa de maestría.

Resumen

Pese a que, en 2017, Anteliz & Toloza hicieron un diagnóstico y propuesta para la implementación de la estrategia de gobierno en línea en Centrales Eléctricas de Norte de Santander S.A. E.S.P. (CENS), el presente trabajo constituye el primer estudio e intento de la organización dirigido a cumplir con lo definido puntualmente para la autenticación y firma digital, más aún, dado lo reciente de la documentación que el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) ha publicado sobre el tema.

El presente trabajo busca responder al interrogante que tiene la organización respecto a si los mecanismos de autenticación digital de los servicios de Tecnología de Información expuestos a sus grupos de interés externos cumplen con los diversos lineamientos y pautas definidas por MINTIC desde el Servicio Ciudadano Digital Base de Autenticación Digital, al tiempo que esboza el plan de acción a seguir para la implementación de dichos mecanismos de manera alineada con las pautas y recomendaciones del estándar de la National Institute of Standards and Technology (NIST), marco de ciberseguridad adoptado por MINTIC.

A lo largo del documento y en el orden descrito, se realiza el diagnóstico de los mecanismos actuales de autenticación digital de CENS, con base en el estándar NIST 800-63B, como lo establece MINTIC; se evalúa la integración de los Servicios Ciudadanos Digitales en la Arquitectura Empresarial de CENS; se analiza el impacto de la planeación estratégica y la Arquitectura Empresarial de CENS, sobre el proyecto de implementación de los mecanismos de autenticación digital; se diseña el plan de proyecto según la metodología de gestión de proyectos del PMI, para la implementación de los mecanismos de autenticación digital en CENS; se presenta el plan de divulgación y se anexa la evidencia de la estrategia de comunicación ejecutada para la promoción y adopción del plan de proyecto definido.

El trabajo realizado permitió evidenciar el bajo cumplimiento de los mecanismos de autenticación digital de los servicios de T.I. de CENS expuestos a sus grupos de interés externos, respecto a lo definido por MINTIC con base en los lineamientos y pautas del estándar SP 800-63B de NIST. Asimismo, permitió conocer la favorabilidad que tiene CENS para hacer realidad lo definido en el proyecto de implementación de mecanismos de autenticación digital y dar cumplimiento satisfactorio lo definido en dicho campo de la seguridad digital.

Palabras clave: Autenticación digital, NIST, MINTIC, CENS, proyecto.

Abstract

Despite the fact that, in 2017, Anteliz & Toloza made a diagnosis and proposal for the implementation of the online government strategy at Centrales Eléctricas de Norte de Santander S.A. E.S.P. (CENS), this work constitutes the first study and attempt of the organization aimed at complying with what is specifically defined for authentication and digital signature, even more so, given the recent documentation that the Ministry of Information Technologies and Communications (MINTIC) has published on the subject.

This work seeks to answer the question that the organization has regarding whether the digital authentication mechanisms of the Information Technologies services exposed to its external stakeholders comply with the various guidelines defined by MINTIC from the Digital Citizen Service Base of Digital Authentication , while outlining the action plan to follow for the implementation of such mechanisms in line with the guidelines and recommendations of the National Institute of Standards and Technology (NIST) standard, the cybersecurity framework adopted by MINTIC.

Throughout the document and in the order described, the current CENS digital authentication mechanisms are diagnosed, based on the NIST 800-63B standard, as established by MINTIC; the integration of the Digital Citizen Services in the CENS Business Architecture is evaluated; the impact of the strategic planning and the Business Architecture of CENS on the project of implementation of digital authentication mechanisms is analyzed; the project plan is designed according to the PMI project management methodology, for the implementation of digital authentication mechanisms in CENS; the dissemination plan is presented and the evidence of the communication strategy implemented for the promotion and adoption of the defined project plan is attached.

The work carried out made it possible to demonstrate the low compliance of the digital authentication mechanisms of CENS IT services exposed to its external stakeholders, with respect to what is defined by MINTIC based on the guidelines and guidelines of the NIST SP 800-63B standard . Likewise, it allowed to know the favorability that CENS has to make what is

defined in the project for the implementation of digital authentication mechanisms a reality and to satisfactorily comply with what is defined in such field of digital security.

Keywords: Digital authentication, NIST, MINTIC, CENS, project

Tabla de contenido

Lista de figuras

Lista de tablas

1. INTRODUCCIÓN

La necesidad del Estado, de abrirse a sus ciudadanos, tiene en la desconfianza hacia la política y sus instituciones, una de sus causas. La redefinición de la relación entre individuo e institución constituye la opción de acercar a ciudadanos con gobiernos y ese acceso requerido, en términos de visibilidad a la gestión y toma de decisiones puede ser proporcionado por las Tecnologías de la Información y las Comunicaciones. (Pirni et al, 2019, p.477).

De acuerdo con la Organización de los Estados Americanos, "El Gobierno Electrónico es la aplicación de las tecnologías de la información y la comunicación (TIC) al funcionamiento del sector público, con el objetivo de brindar mejores servicios al ciudadano e incrementar la eficiencia, la transparencia y la participación ciudadana" (OEA,s.f).

En Colombia, la estrategia de gobierno electrónico fue conocida inicialmente con el nombre de Gobierno en Línea (GEL), que evolucionó en 2018 a política de Gobierno Digital, siendo el objetivo de esta última "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital" (MINTIC, 2018a).

La obligatoriedad de cumplimiento de esta política por parte de las entidades del Estado ha llevado a que en Centrales Eléctricas de Norte de Santander S.A. E.S.P. (CENS), por ser una empresa de origen público territorial, previamente se haya presentado un estudio en aras de hacer realidad dicha implementación.

En ese sentido, Toloza & Anteliz (2017), trabajadores de CENS, a través de su proyecto de grado: "Diagnóstico y propuesta para la implementación de la estrategia de gobierno en línea en Centrales Eléctricas de Norte de Santander S.A. E.S.P. (CENS)", se enfocaron en:

- Analizar la conceptualización y normatividad asociada a la estrategia de gobierno en línea en la República de Colombia.
- Diagnosticar el estado actual de cumplimiento de CENS, respecto a los lineamientos de la estrategia de gobierno en línea.
- Identificar las brechas que posee CENS, para el cumplimiento de los lineamientos de la estrategia de gobierno en línea.

- Proponer un plan de acción que le permita a CENS, cubrir las brechas identificadas y cumplir con los lineamientos de implementación estipulados, para los componentes de TIC para servicios y TIC para gobierno abierto.
- Diseñar y realizar el prototipo de una aplicación en CENS que ofrezca servicios de TIC, además de permitir la transparencia y participación de los usuarios del servicio de energía.

El estudio de Toloza & Anteliz (2017) estimó un cumplimiento de CENS del 54,4% en el componente de TIC para Servicios, del 29,7% en el componente TIC para Gobierno Abierto, del 64,1% para el componente de TIC para la Gestión y del 62,7% para el componente de Seguridad y Privacidad de la Información; resultados que, sin ser satisfactorios, se acercan al cumplimiento del 80% exigido por la estrategia GEL, concluyendo que se debe continuar trabajando en la adopción e implementación de la estrategia de Gobierno en Línea al interior de la organización.

Pese a la evolución de estrategia de Gobierno en Línea (GEL) a política de Gobierno Digital, el trabajo de Toloza y Anteliz constituye una fuente de información base para la propuesta de implementar en CENS, mecanismos de autenticación digital, que se desea construir con el trabajo que enmarca el presente proyecto.

El acercamiento de las instituciones a sus usuarios ha conllevado a la digitalización de sus servicios al tiempo que los mismos se han migrado a Internet. “A partir del hecho de que los datos están expuestos en Internet, la vulnerabilidad de éstos crece ya que pueden sufrir ataques cibernéticos. Cualquiera que fuera la tecnología usada, los sistemas de e-gobierno tienen que ser seguros debido a la sensibilidad de los datos que manipulan” (Baquerizo y Guevara, 2016, p.74).

CENS no escapa al riesgo de sufrir este tipo de ataques y por ello, el presente trabajo busca responder al interrogante que tiene la organización respecto a si los mecanismos de autenticación digital de los servicios de T.I. expuestos a sus grupos de interés externos cumplen con los diversos lineamientos y pautas definidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) desde el Servicio Ciudadano Digital Base de Autenticación Digital.

La autenticación digital que, según lo define la guía de lineamientos de los Servicios Ciudadanos Digital del MINTIC en su página 27, “es el procedimiento que, utilizando mecanismos de autenticación, permite verificar los atributos digitales de una persona cuando adelanten trámites y servicios a través de medios digitales “. Además, en caso de requerirse, permite tener certeza sobre la persona que ha firmado un mensaje de datos, o la persona a la que

se atribuya el mismo en los términos de la Ley 527 de 1999 y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen, y sin perjuicio de la autenticación notarial", ha sido objeto de estudio de múltiples trabajos formales que han encontrado, en la implementación de mecanismos de autenticación biométrica y firma digital, solución a la necesidad que se tiene en cuanto a minimizar la vulnerabilidad de bienes y recursos.

Si bien, CENS ha construido una línea base de seguridad con lineamientos para sus aplicaciones web con la que busca garantizar la provisión de trámites y servicios digitales seguros a sus grupos de interés, el presente trabajo constituye el primer estudio e intento de la organización dirigido a cumplir con lo definido para la autenticación y firma digital, más aún, dado lo reciente de la documentación que MINTIC ha publicado sobre el tema.

El presente trabajo, inicia con el diagnóstico de los mecanismos actuales de autenticación digital de CENS, con base en las pautas definidas por el estándar NIST 800-63B, como lo establece MINTIC; a continuación, se evalúa la integración de los Servicios Ciudadanos Digitales en la Arquitectura Empresarial de CENS; luego, se analiza el impacto de la planeación estratégica y la Arquitectura Empresarial de CENS, sobre el proyecto de implementación de los mecanismos de autenticación digital; posteriormente y partiendo de los resultados obtenidos del desarrollo de los puntos anteriores, se expone el detalle de la propuesta del plan de proyecto según la metodología de gestión de proyectos del PMI, para la implementación de los mecanismos de autenticación digital en CENS; finalmente, se presenta el plan de divulgación y se anexa la evidencia de la estrategia de comunicación ejecutada para la promoción y adopción del plan de proyecto definido.

2. OBJETIVOS

2.1. Objetivo general

Elaborar y divulgar un plan de proyecto que permita implementar, en Centrales Eléctricas de Norte de Santander S.A. E.S.P., mecanismos de autenticación digital según la política de gobierno digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

2.2. Objetivos específicos

- Realizar el diagnóstico de los mecanismos actuales de autenticación digital de CENS S.A. E.S.P., según la Política de Gobierno Digital.
- Evaluar la integración de los Servicios Ciudadanos Digitales en la Arquitectura Empresarial de CENS S.A. E.S.P.
- Analizar el impacto de la planeación estratégica y la Arquitectura Empresarial de CENS S.A. E.S.P., sobre el proyecto de implementación de los mecanismos de autenticación digital.
- Diseñar el plan de proyecto según la metodología de gestión de proyectos del PMI, para la implementación de los mecanismos de autenticación digital en CENS S.A. E.S.P.
- Ejecutar una estrategia de comunicación para la promoción y adopción del plan de proyecto definido.

3. JUSTIFICACIÓN

A nivel mundial, el impacto e influencia de las TIC en diversos ámbitos es tal, que se puede decir que "pasaron de ser un progreso científico en un campo específico, a convertirse en una revolución de la vida humana, que afecta desde la comunicación cotidiana hasta tareas de alta complejidad relacionadas con la salud, la educación, la política y la economía" (Chacón, Ordoñez y Anichiarico, 2017, p. 4)

Colombia no escapa a dicha realidad y es por ello que el gobierno nacional, a través del MINTIC-, definió, en el año 2008, la estrategia para la implementación del Gobierno en Línea (GEL), la cual, "desde sus inicios, centró sus esfuerzos en introducir las TIC en los procesos y procedimientos de las entidades del Estado, con el objetivo de mejorarlos, automatizarlos y volverlos más eficientes, para mejorar la gestión pública y la relación del Estado con los ciudadanos" (MINTIC, 2018d) ; estrategia que Centrales Eléctricas de Norte de Santander S.A. E.S.P. – CENS S.A. E.S.P.- debe implementar de acuerdo a lo reglamentado en el decreto 1413 de 2017, dada su condición de entidad pública del orden territorial.

El relacionamiento planteado por la implementación del gobierno electrónico ha generado el acercamiento de las entidades a los ciudadanos, lo cual, ha traído consigo riesgos a los que CENS S.A. E.S.P. no es ajena, lo que le ha hecho necesario orientar sus esfuerzos a descubrir vulnerabilidades de bienes y recursos, "donde un bien se define como algo de valor y la vulnerabilidad se define como la debilidad que se puede explotar para violar un sistema o la información que contiene".ISO-7498(1994)

Al evaluar sus bienes y recursos, CENS ha determinado que sus Servicios Ciudadanos Digitales requieren prioridad de estudio y el presente proyecto le permitirá analizar los riesgos de suplantación a los que se ve expuesta en virtud del uso frecuente de estos por parte de usuarios externos; diagnosticar su capacidad actual de respuesta a los mismos e identificar las brechas con relación a lo definido por la política de Gobierno Digital, para construir un plan de proyecto enfocado a superar dichas brechas; estudio que constituirá un punto de partida y referencia para la implementación de mecanismos de autenticación digital en otros sistemas de la organización, puesto que suministrará información detallada en cuanto a tiempo, recursos (humanos, financieros y tecnológicos), acciones, lecciones aprendidas y gestión de riesgos, necesarias para hacer realidad dicha implementación, aplicando la metodología de gestión de proyectos del PMI.

Cabe señalar que el entregable del presente proyecto apuntará a la protección de bienes y recursos de la organización que, a su vez, favorece la normal operación de sus procesos, en pro de la continuidad del servicio público esencial que CENS S.A .E.S.P presta con fines de apalancar el desarrollo económico y productivo de las comunidades que integran su zona de cobertura en todo Norte de Santander, sur de Cesar y sur de Bolívar, al tiempo que buscará garantizar a los usuarios del servicio de energía eléctrica, la integridad, disponibilidad y confidencialidad de su información.

4. MARCO DE REFERENCIA

Las tecnologías de información y comunicaciones TIC han permitido la cercanía de las organizaciones - tanto corporaciones privadas como entidades públicas- con las personas, a través de herramientas como la internet, que "fundamentalmente persigue acortar las distancias de comunicación, en el caso de las actividades gubernamentales, entre gobierno y ciudadanos" (Riascos, Martínez y Solano, 2008, p. 2).

En una sociedad en donde la individualidad, la libertad y el derecho a elegir se han vuelto los bienes más preciados, en la que los grupos sociales a pesar de ser cada vez más pequeños son al mismo tiempo cada vez más numerosos y más activos de lo que eran antes (Belil, 2003); "el Internet adquiere un papel relevante, pues es una herramienta, que bien utilizada, puede ser de gran utilidad en la construcción de procesos participativos más efectivos e incluyentes" (Villa, 2008, p. 3)

No se pretende que el Internet venga a reemplazar los mecanismos de participación ciudadana tradicionales, sino de reforzarlos y ofrecer nuevas formas y medios que sean más acordes con los tiempos actuales. El Internet puede ser un medio para que los ciudadanos se impliquen de manera mucho más activa en los procesos de construcción de los planes; pues permite que la información se vuelva mucho más accesible; ya no es necesario, por ejemplo, desplazarse a un sitio concreto en una hora determinada para poder ser escuchado. (Villa, 2008, p. 4)

Esta tendencia de utilizar las tecnologías de información y comunicaciones por parte del gobierno para acercarse a los ciudadanos se conoce como gobierno electrónico o gobierno digital.

La Gobernabilidad Electrónica (eGovernance) se refiere al uso de las tecnologías de la información y la comunicación por parte del sector público con el objetivo de mejorar el suministro de información y el servicio proporcionado. De esta manera, se trata de estimular la participación ciudadana en el proceso de toma de decisiones, haciendo que el gobierno sea más responsable, transparente y eficaz (Unesco, s.f, p. 2).

Según la Organización de Estados Americanos (OEA, s.f.) el gobierno digital, utiliza las tecnologías de información y comunicación para ayudar a los gobiernos a ser más accesibles a los electores, mejorar los servicios y a ser más eficientes, y a estar cada vez más conectados con otras partes de la sociedad.

En Colombia, esta corriente inició en el año 2000 a través del documento CONPES 3072 con la agenda de conectividad diseñada para el desarrollo de la estrategia de gobierno electrónico con el fin de "construir un gobierno eficiente y transparente al garantizar la calidad, prontitud y confianza en la información y servicios institucionales ofrecidos por este medio" (Departamento Nacional de Planeación, 2000, p.15). Para ello se definieron los 3 sectores en los que se debían concentrar los esfuerzos: Comunidad, sector productivo y estado; además se definieron 6 estrategias de las cuales la de Gobierno en Línea se considera la más importante, la cual se impulsó posteriormente y evolucionó a lo que ahora se conoce como Política de Gobierno Digital,

El Gobierno Electrónico entrega beneficios directos a la comunidad en general, tales como la eliminación de las barreras de tiempo y espacio, la facilidad en las comunicaciones, el acceso igualitario a la información, [...] en suma, una mayor calidad de vida de la ciudadanía. Por su parte, la utilización de estas tecnologías en la gestión pública puede traer grandes beneficios, pues constituyen pilares fundamentales para la modernización y eficacia del Estado, ayudan al control interno y externo aportando transparencia al sector público, disminuye costos del sector público al compartir recursos, ayuda a la descentralización acercando el Gobierno a los ciudadanos y facilita la participación ciudadana en los procesos de tomas de decisiones, entre otros (Concha y Naser,2012,p.14).

Implementar un Gobierno Electrónico implica, entre otras actividades, replantear, agregar y/o eliminar procesos, definir políticas de calidad y seguridad, analizar los procesos de negocio en cada uno de los servicios públicos, todo esto en vías de lograr la integración e interoperabilidad de estos servicios (Concha y Naser, 2012, p.14).

La Estrategia de Gobierno en Línea, buscando cercanía entre las entidades y los ciudadanos, estableció cuatro componentes: TIC para Gobierno Abierto, TIC para Servicio, TIC para la Gestión, y Seguridad y Privacidad de la Información.

El componente de TIC para Servicios comprende la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los usuarios y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo. Si bien es cierto que en el artículo 5 del Decreto 1 de 1984, se estableció que las personas ya podían hacer peticiones ante autoridades de forma verbal o escrita, y a través de cualquier medio, solamente a partir de la expedición de la Ley 1437 de 2011 se dio la opción a la ciudadanía en

general, que, para realizar cualquier trámite relacionado con una petición, queja, reclamo o solicitud, podía utilizar cualquier medio tecnológico que tuviera la entidad disponible para dicho procedimiento.

Del mismo modo, de acuerdo con lo establecido en el artículo 14 del Decreto 19 de 2012, se confirma la opción que tiene el ciudadano en el momento de interponer su petición, queja, reclamo y/o solicitud (PQRS), de usar los medios electrónicos, es decir, sin necesidad de acercarse a la oficina obligatoriamente. (Campo, 2017, p. 13)

Fueron evidentes los beneficios de la tecnología frente a la interposición y/o notificación de las peticiones, quejas, reclamos y solicitudes (PQRS), una vez se expidió el código de procedimiento administrativo y de lo contencioso administrativo (Ley 1437 de 2011)

Éste acercamiento entre las entidades públicas y los ciudadanos ha generado riesgos en la seguridad de los datos para las dos partes, lo que hace importante que la comunicación entre el estado y los ciudadanos se realice de forma segura, y que los datos que se intercambian estén protegidos de ataques informáticos a los que están expuestos en la red, como lo afirma Zapata (2012), "las redes teleinformáticas están expuestas a ataques e intrusiones que pueden dejar inoperativos los recursos y causar pérdidas de la imagen, productividad, credibilidad y competitividad, provocando perjuicios económicos que podrían comprometer la continuidad del negocio". Esta situación pareciera estar empeorando "pues continúan apareciendo diversas amenazas, vulnerabilidades y ataques; perjudicando directamente a los negocios que son altamente dependientes de sus sistemas y redes de información." (Zapata, 2012, p. 2)

Lo anterior, crea la necesidad de aplicar seguridad informática que consiste en asegurar que los recursos del sistema de información de una organización sean utilizados de la manera que se decidió y que el acceso a la información, su respectiva modificación, sólo sea posible a las personas que se encuentren autorizadas y dentro de los límites de su autorización. (Costas,2014, citado por citado por Tirado, et al. 2017, p.4), o, como lo indica la norma ISO-7498(1994), son "mecanismos que minimizan la vulnerabilidad de bienes y recursos, donde un bien se define como algo de valor y la vulnerabilidad se define como la debilidad que se puede explotar para violar un sistema o la información que contiene.".

Como parte de la política de Gobierno Digital de Colombia definida por el MINTIC, se establecieron los servicios ciudadanos digitales como habilitadores, "los cuales buscan facilitar y brindar un adecuado acceso a los servicios de la administración pública haciendo uso de medios

digitales, para lograr la autenticación electrónica" (MINTIC, 2018c) y es que, debido al incremento de los delitos informáticos, "se está buscando mejorar la seguridad con el fin de disminuir las probabilidades de que un delincuente pueda acceder a un dispositivo. En especial, se pretende mejorar la primera y más importante barrera de seguridad, la autenticación" (Garrido, 2016, p. 3).

La autenticación es la forma de acreditar la identidad del emisor del mensaje, a través de métodos que combinen 3 factores: conocimiento (contraseña), posesión (dispositivo) e inherencia (biometría).

En cuanto al repudio de la información transmitida electrónicamente el mecanismo utilizado para garantizarse es la firma digital, que es "el conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor del documento" (Ministerio de Ciencia y Tecnología de Costa Rica, 2006, citado por Romero, 2016, p. 7), la cual debe estar respaldada por una entidad de certificación.

Lo anterior lleva a que se preste atención al servicio de autenticación electrónica, que es un servicio ciudadano digital básico que "permite validar a los usuarios por medios electrónicos [...] y provee los mecanismos necesarios para firmarlos electrónicamente, en los términos de la Ley 527 de 1999" (MinTIC, 2017, p. 6). Trabajos previos subrayaron la necesidad de adoptar un marco de referencia general sobre teoría de la identificación personal para los procesos de autenticación. (Gabaldón y Pereira, 2008) y MinTIC ha dado respuesta a dicha necesidad al adoptar el estándar SP 800-63B del marco de ciberseguridad NIST.

En el decreto 1413 de 2017, se define que el uso de los servicios ciudadanos digitales, "será obligatorio para los organismos y entidades públicas, así como para los particulares que desempeñen funciones públicas" (MinTIC, 2017, p. 9); por tanto, es pertinente implementar en CENS, mecanismos de autenticación digital que den cumplimiento a los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

Implementar un Gobierno Electrónico implica, entre otras actividades, replantear, agregar y/o eliminar procesos, definir políticas de calidad y seguridad, analizar los procesos de negocio en cada uno de los servicios públicos, todo esto en vías de lograr la integración e interoperabilidad de estos servicios (Concha y Naser,2012, p.14). El concepto de Arquitectura Empresarial surge como respuesta a este desafío.

MINTIC ha desarrollado el documento maestro del Modelo de Arquitectura Empresarial (MAE), el cual se convierte en un instrumento para implementar el habilitador de Arquitectura de la Política de Gobierno Digital del Estado Colombiano que establece el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

La Arquitectura Empresarial permite superar el desafío que representa alinear las áreas estratégicas y los procesos de negocios con las áreas de T.I., con lo que "es posible generar mayor valor, mejorar el desempeño, la comunicación y la integración en las empresas, que finalmente llevarán a la creación de ventaja competitiva mediante el apoyo efectivo para el cumplimiento de las estrategias y objetivos establecidos en el negocio" (Arango et al, 2010, p.111)

La inadecuada planeación de un proyecto causa pérdidas económicas, retrasos en la entrega de los proyectos y debilita la imagen institucional, por lo que debe planearse de tal forma que garantice las expectativas de calidad, costo y tiempo asegurando de esta manera el éxito del mismo (Romero, 2014), por tanto el plan de proyecto se elaborará para que sea desarrollado aplicando la metodología de gestión propuesta por el Project Management Institute (PMI), la cual es la metodología más acogida a nivel global en el desarrollo de proyectos.

El PMI ha desarrollado el PMBOK y esta guía identifica lo que constituye el cuerpo de conocimiento en gerencia de proyectos generalmente reconocido como buenas prácticas, cuyo conocimiento es aplicable a la mayoría de los proyectos y cuyos lineamientos y prácticas pueden mejorar el éxito de los proyectos. (Guerrero, 2013).

5. MARCO INSTITUCIONAL

5.1. Reseña histórica.

La historia de la compañía inicia el 16 de junio de 1896 con la protocolización de la escritura pública 121 que crea la "Compañía de Alumbrado Eléctrico de Cúcuta"; posteriormente, el 16 de octubre de 1952 se constituye la empresa "Centrales Eléctricas de Cúcuta S.A." que inició operaciones el 3 de enero de 1953 y posteriormente en 1955 cambió su razón social por "Centrales Eléctricas del Norte de Santander S.A.".

En el marco de la ley 142 de 1994, se constituyó como Empresa de Servicios Públicos, siendo en ese entonces la nación a través de los ministerios de Hacienda y de Minas y Energía, el principal accionista de la empresa con el 78,98% de las acciones y quedando a partir de esa fecha bajo la vigilancia y control de la Superintendencia de Servicios Públicos Domiciliarios.

En el primer trimestre de 2009 y mediante un proceso de enajenación, la nación efectuó la venta de las acciones de su propiedad a las Empresas Públicas de Medellín que pasó a ser el accionista mayoritario, convirtiendo a Centrales Eléctricas del Norte de Santander (CENS) en una filial del grupo empresarial EPM. Centrales Eléctricas del Norte de Santander (CENS, 2020)

5.2. Presentación

Centrales Eléctricas del Norte de Santander S.A. E.S.P es una empresa de servicios públicos mixta, de nacionalidad colombiana, constituida como sociedad por acciones, del tipo de las anónimas, sometida al régimen general de los servicios públicos domiciliarios, que presta sus servicios en 47 municipios de los departamentos Norte de Santander, sur del departamento de Bolívar y sur del Cesar, y que ejerce sus actividades dentro del ámbito del derecho privado como empresario mercantil.(CENS, 2020).

5.3. Misión

Centrales Eléctricas del Norte de Santander S.A. E.S.P es una empresa del Grupo Empresarial EPM que presta los servicios de Transmisión, Distribución y Comercialización de energía eléctrica, contribuyendo a la construcción de territorios competitivos y sostenibles en donde

participa, mediante la prestación responsable e integral de soluciones de energía eléctrica. (CENS, 2020).

5.4. Visión

En el año 2022, CENS será reconocida entre sus grupos de interés como una empresa socialmente responsable; referente en estándares de excelencia, con modelos de gestión, reputación y transparencia que impulsen la productividad de los negocios en que participa; ofreciendo un portafolio integral de soluciones competitivas de energía eléctrica que contribuya al cumplimiento de la MEGA y al posicionamiento multilatino del Grupo Empresarial EPM. (CENS, 2020).

5.5. Sector y mercado

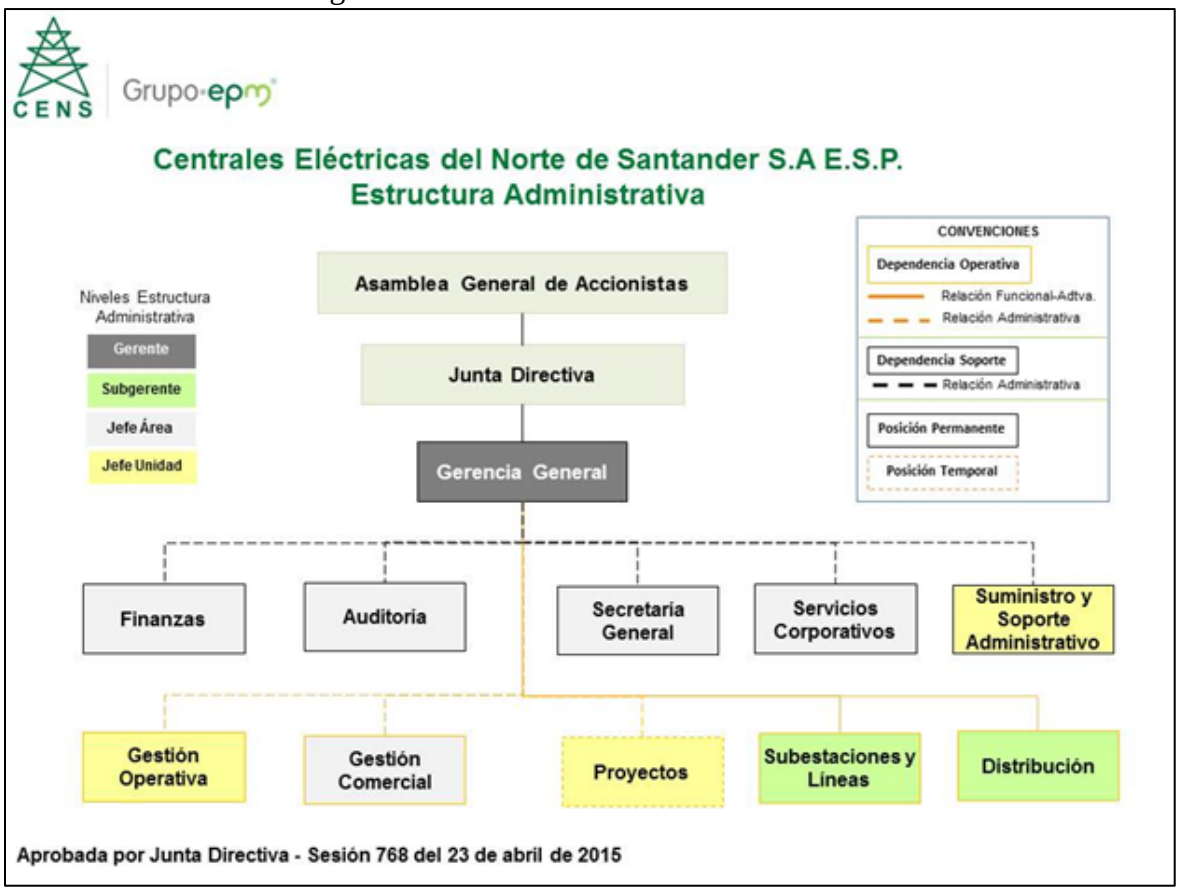
CENS se ubica en el sector económico terciario o de servicios, presta además del servicio de energía eléctrica, los servicios de estudio de análisis de redes eléctricas; prueba de PCB; servicios de tomografía; calibración de medidores de energía; mantenimiento predictivo y preventivo de subestaciones eléctricas; energía temporal; línea energizada; alquiler temporal de transformadores y trabajo a potencial (CENS, 2020).

Debido a la naturaleza del servicio, CENS ocupa una posición dominante en el mercado de servicio de energía eléctrica en el departamento Norte de Santander, sur del departamento del Cesar y sur del departamento de Bolívar; sin embargo, compite con empresas comercializadoras de energía principalmente en el mercado de energía no residencial.

5.6. Estructura organizacional

CENS está estructurada en 10 dependencias (2 subgerencias, 5 áreas y 3 unidades) que dependen de la gerencia general. Éstas, a su vez, contienen equipos de trabajo a los cuales están adscritos los trabajadores. A continuación, se presenta la estructura administrativa:

Figura 1. Estructura administrativa de CENS



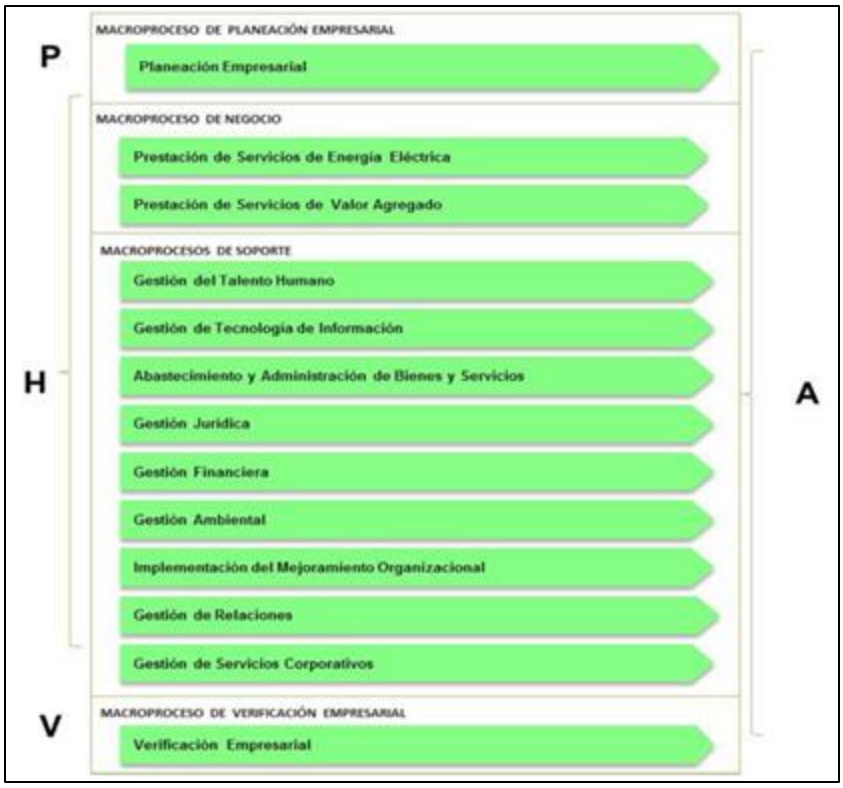
Fuente. CENS

5.7. Procesos

El modelo de procesos de Centrales Eléctricas del Norte de Santander S.A. E.S.P. es el principal elemento organizador de la gestión, a través del que se establece, implementa y mejora continuamente la eficacia, eficiencia y efectividad del Sistema de Gestión de Calidad y del Sistema de Gestión de Activos. Utilizando el ciclo PHVA busca la visión transversal de la empresa y no la de cada una de sus áreas, facilita el flujo de información, el pensamiento basado en riesgos y el desarrollo de modelos de mejoramiento. (CENS, s.f.).

El modelo de gobierno de Centrales Eléctricas del Norte de Santander S.A. E.S.P., está compuesto por 13 macroprocesos mencionados a continuación:

Figura 2. Mapa de procesos de CENS



Fuente. CENS

5.8. Análisis del sector

Centrales Eléctricas del Norte de Santander S.A. E.S.P. pertenece al sector del servicio público de energía eléctrica.

El sector energético en Colombia está organizado en mercados de generación, transmisión, distribución y comercialización de energía, y en el cual participan diversas entidades tanto públicas como privadas. Grupo Energía Bogotá (GEB, 2018).

Según GEB, en la organización del sector energético, la actividad de generación consiste en la producción de la energía eléctrica a partir de la transformación de una fuente de energía natural como agua, carbón o gas, los cuales son inyectados al sistema eléctrico nacional; la actividad de transmisión consiste en la distribución de la energía producida por los generadores a nivel nacional a través de redes eléctricas (líneas), del sistema interconectado de transmisión de energía eléctrica en Colombia denomina Sistema de Transmisión Nacional (STN), que operan a tensiones superiores a 220 kilovoltios (kV); la actividad de distribución consiste en transportar

energía a través de líneas y subestaciones hasta los inmuebles, operan a tensiones inferiores a 220 kV y están asociadas a la distribución municipal, distrital o local; la actividad de comercialización es la compra y venta de energía eléctrica, incluyendo la facturación del servicio, recaudo del pago y atención de los clientes (GEB, 2018).

Además, el mercado clasifica a los usuarios en regulados para los cuales las tarifas son establecidas por el ente regulador, y no regulados cuyas tarifas son acordadas entre las partes.

En el sector de la energía eléctrica en Colombia participan entidades que ejercen funciones de regulación, supervisión, planeación y control del sistema eléctrico, entre las cuales se destacan las que mencionamos a continuación.

- El ministerio de minas y energía: El ente encargado de definir los requisitos técnicos del servicio, los subsidios que otorga la nación, así como las políticas y lineamientos para el desarrollo del sector energético del país.
- Unidad de Planeación Minero-Energética (UPME): Adscrita al ministerio, define los requerimientos energéticos del país y es la encargada de elaborar el plan energético nacional y el plan de expansión del sector eléctrico. (GEB, 2018).
- Comisión de Regulación de Energía y Gas (CREG): Es la entidad encargada de regular la prestación de los servicios públicos de energía eléctrica, gas y combustibles, promover el desarrollo sostenido de estos sectores, atender oportunamente a los usuarios y las empresas. (CREG,2018)
- Superintendencia de Servicios Públicos Domiciliarios (SSPD): Encargada del control y vigilancia de las empresas prestadoras de servicios públicos en el país.
- Centro Nacional de Despacho (CND): Es una entidad de tipo técnico encargada de la planeación, supervisión y control de la operación integrada de los recursos de generación, interconexión y transmisión del Sistema Interconectado Nacional. (GEB,2018)
- Consejo Nacional de Operación (CNO): Entidad encargada de acordar los aspectos técnicos para garantizar que la operación integrada del Sistema Interconectado Nacional sea segura, confiable y económica. (GEB,2018).

6. DISEÑO METODOLÓGICO

6.1. Enfoque de investigación

Dado que, según Hernández, Fernández y Baptista (2010), "La investigación cualitativa proporciona profundidad a los datos, dispersión, riqueza interpretativa, contextualización del ambiente o entorno, detalles y experiencias únicas. Asimismo, aporta un punto de vista "fresco, natural y holístico" de los fenómenos, así como flexibilidad", el presente estudio aplica el enfoque de investigación cualitativo, en el que se determina la existencia y se evalúa la efectividad de los mecanismos de autenticación digital implementados en los servicios ciudadanos digitales de CENS, según la información tomada de diversas fuentes.

No obstante, al tratarse de un estudio de enfoque cualitativo, también se utilizarán instrumentos cuantitativos para analizar la información recopilada.

6.2. Tipo de estudio

Teniendo en cuenta que "Visualizar qué alcance tendrá nuestra investigación es importante para establecer sus límites conceptuales y metodológicos". (Hernández-Sampieri, 2014, p. 88), se tiene que el presente estudio es de tipo exploratorio, dado que, según exponen Hernández, Fernández y Baptista (2014), "busca examinar un tema o problema de investigación poco estudiado, del cual se tienen muchas dudas o no se ha abordado antes", tal como sucede en CENS, donde no se han evaluado los mecanismos de autenticación digital de los servicios ciudadanos con los que cuenta.

Por otra parte, el presente estudio también tiene un alcance de tipo descriptivo, puesto que, "con los estudios descriptivos se busca especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, procesos, objetos o cualquier otro fenómeno que se someta a un análisis" (Hernández, et al. 2014, p. 98), donde, los mecanismos de autenticación digital de los servicios ciudadanos digitales de CENS constituyen el objeto o fenómeno de estudio.

6.3. Población y muestra.

Según Hernández, et al. (2014), la población o universo se compone del conjunto de todos los casos que concuerdan con determinadas especificaciones, y la muestra como el subgrupo de la

población de interés sobre el cual se recolectan datos, y que tiene que definirse o delimitarse de antemano con precisión, debiendo ser representativo de dicha población.

Para el objeto de estudio del proyecto, la población se refiere a los 99 sistemas de información que constituyen la base de los servicios de Tecnología de Información de CENS y la muestra corresponde a los 6 servicios de Tecnología de Información expuestos a sus grupos de interés externos, objeto de estudio del presente trabajo, por considerar que en los mismos se tiene mayor riesgo de seguridad.

6.4. Instrumentos de la investigación

6.4.1. La observación estructurada

"La observación estructurada es una técnica usada en estudios diseñados para obtener una descripción sistemática de un fenómeno o para verificar una hipótesis" (Gallardo y Moreno, 1999, pp. 63).

La observación estructurada se aplicará para verificar el cumplimiento de lo definido, al momento del diligenciamiento de los diferentes instrumentos de diagnóstico construidos a partir de los lineamientos dados por MinTIC.

6.4.2. La entrevista

"La entrevista con fines de investigación puede ser entendida como la conversación que sostienen dos personas, celebrada por iniciativa del entrevistador con la finalidad específica de obtener alguna información importante para la indagación que realiza." (Ibid., p. 71).

Este instrumento resultará idóneo en su uso, en los momentos en que se proceda a diligenciar los diferentes instrumentos de diagnóstico construidos a partir de los lineamientos dados por MinTIC, para lo cual se conversará, según su temática, con:

- El profesional encargado de la seguridad de la información de CENS.
- Cada profesional de CENS encargado de la administración técnica y al personal designado por las respectivas firmas contratistas encargadas del soporte, actualización y mantenimiento de cada servicio de TI objeto de estudio.
- El profesional de estrategia y arquitectura de CENS

6.5. Instrumentos de diagnóstico a utilizar

Los diagnósticos se realizan con el fin de conocer el estado actual del elemento que está en estudio para de esta forma poder llevar a cabo las acciones de mejora. A continuación, se describen los instrumentos de diagnóstico construidos.

6.5.1. Orientados a evaluar la efectividad de los mecanismos de autenticación digital

El Decreto 620 del 2 de mayo de 2020 del Ministerio de Tecnologías de la Información y Comunicaciones, define el servicio de autenticación digital como el procedimiento que, utilizando mecanismos de autenticación, permite verificar los atributos digitales de una persona cuando adelanten trámites y servicios a través de medios digitales. Además, en caso de requerirse, permite tener certeza sobre la persona que ha firmado un mensaje de datos, o la persona a la que se atribuya el mismo en los términos de la Ley 527 de 1999 y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen, y sin perjuicio de la autenticación notarial.

Asimismo, define mecanismos de autenticación como las firmas digitales o electrónicas que, al ser utilizadas por su titular, permiten atribuirle la autoría de un mensaje de datos, lo anterior sin perjuicio de la autenticación notarial.

En ese orden de ideas, se tiene que la autenticación digital cubre los escenarios de verificación de atributos digitales de una persona y la firma digital de mensajes de datos.
Teniendo en cuenta que:

- El Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de las Tecnologías de la Información y las Comunicaciones, en el marco del Programa Gobierno Digital, tiene por propósito servir como guía para la mejora de los estándares de Seguridad de la Información de las entidades, toma como referencia las mejores prácticas en ciberseguridad definidas por el NIST (El Instituto Nacional de Estándares y Tecnología de Estados Unidos).
- NIST cuenta con un conjunto de documentos de cuatro volúmenes que contienen las directrices de identidad digital.
- La Organización Nacional de Acreditación de Colombia –ONAC- define los criterios para la acreditación de entidades de Certificación Digital.

Se construyeron tres instrumentos tipo cuestionario para realizar el diagnóstico de los mecanismos actuales de autenticación digital de CENS S.A. E.S.P., según la Política de Gobierno Digital, con base en:

- El documento SP 800-63-3 de NIST, el cual define el análisis de riesgo a efectuar ante un error de autenticación.
- El documento SP 800-63B de NIST, el cual define directrices referentes a la autenticación y gestión del ciclo de vida.
- El Anexo B del documento criterios específicos de acreditación de entidades de certificación digital CEA-4.1-10 de ONAC en lo que respecta al proceso de firma electrónica de mensajes de datos.

6.5.1.1. Orientados al análisis de riesgo ante un error de autenticación

NIST propone efectuar inicialmente un análisis de riesgo ante un eventual error de autenticación, para conocer su potencial impacto sobre las 6 categorías definidas por dicho ente, así:

- Categoría de riesgo 1: Inconveniencia, angustia o daño a la reputación o imagen.
- Categoría de riesgo 2: Pérdida financiera o responsabilidad de la agencia.
- Categoría de riesgo 3: Daño a programas de agencias o intereses públicos.
- Categoría de riesgo 4: Divulgación no autorizada de información confidencial.
- Categoría de riesgo 5: Seguridad personal.
- Categoría de riesgo 6: Violaciones civiles o penales.

Una vez determinado el potencial impacto sobre cada categoría, se podrá definir el Nivel de Garantía de Autenticación (AAL) requerido, siguiendo directrices de NIST.

Figura 3. Selección de AAL

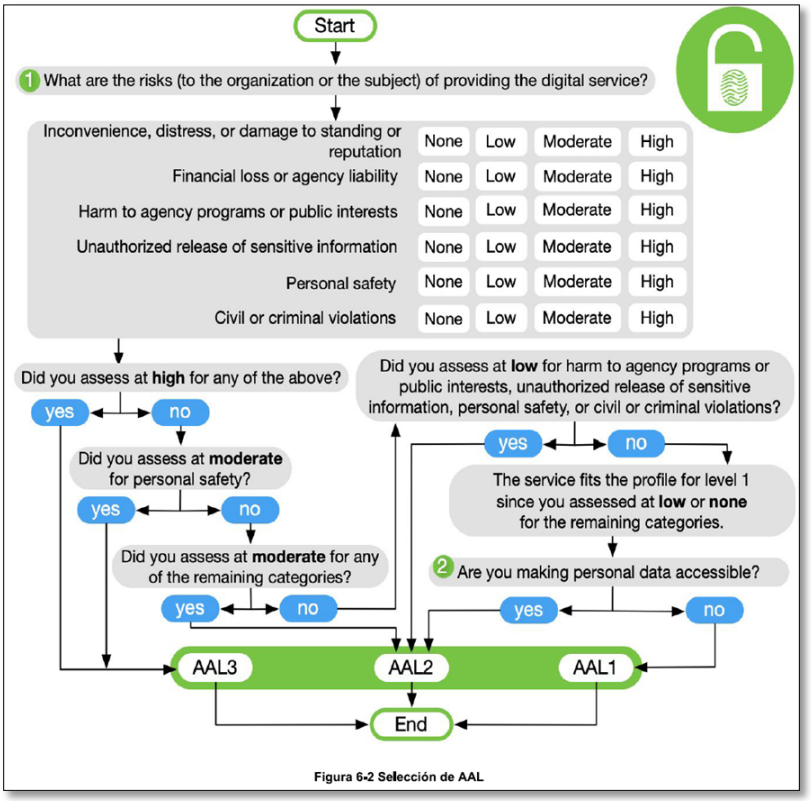


Figura 6-2 Selección de AAL

Fuente: NIST 800-63-3

6.5.1.2. Para el diagnóstico Nivel de Garantía de Autenticación (AAL) actual.

Una vez definido el Nivel de Garantía de Autenticación (AAL) requerido de cada servicio de Tecnología de Información evaluado, se procederá a diligenciar, mediante entrevista al respectivo administrador técnico de cada servicio, el instrumento tipo cuestionario construido con base en el documento SP 800-63B, el cual permitirá conocer el grado de cumplimiento de los mecanismos de autenticación de los servicios de T.I. analizados, respecto a lo establecido por NIST para verificar los atributos digitales de una persona.

6.5.1.3. Para el diagnóstico de Firma Digital.

El documento criterios específicos de acreditación de entidades de certificación digital CEA-4.1-10 de ONAC, en su anexo B reglamenta lo referente al proceso de firma electrónica de mensajes de datos, definiendo los estándares técnicos vigentes que constituyen los requisitos en cuanto a los formatos de firma digital, dispositivos criptográficos y la validación del estado del certificado.

El instrumento de diagnóstico a construirse apuntará a determinar el cumplimiento de los servicios digitales de CENS en cuanto a los requisitos definidos en el anexo B del documento CEA-4.1-10 de ONAC-y se diligenciará con el acompañamiento del respectivo administrador técnico de cada servicio, empleando la técnica de entrevista.

6.5.2. Orientados a evaluar la integración de los Servicios Ciudadanos Digitales en la Arquitectura Empresarial de CENS S.A. E.S.P.

El Decreto 620 de 2020 establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

El artículo 2.2.17.1.2 del mencionado decreto establece el ámbito de aplicación, por lo que serán sujetos obligados a la aplicación del presente título, todos los organismos y entidades que conforman las ramas del Poder Público en sus distintos órdenes, sectores y niveles, los órganos autónomos e independientes del Estado, y los particulares, cuando cumplan funciones administrativas o públicas, ubicándose CENS en este grupo.

Por su parte, el artículo 2.2.17.4.7 define las obligaciones de los sujetos obligados. Los sujetos a los que se refiere el artículo 2.2.17.1.2 del presente decreto tendrán a su cargo las siguientes obligaciones en cuanto a servicios ciudadanos digitales:

- Actualizar en el Sistema Único de Información de Trámites -SUIT-del Departamento Administrativo de la Función Pública -DAFP- los trámites u otros procedimientos administrativos en los cuales se haga uso de los servicios ciudadanos digitales. donde se informe claramente a los ciudadanos, usuarios o grupos de interés los pasos que deben adelantar para acceder a estos servicios.
- Analizar los riesgos inherentes a cada trámite de acuerdo con los lineamientos dados en la guía para la vinculación y uso de los servicios ciudadanos digitales.
- Definir las reglas y políticas que deben ser consideradas por el prestador de servicio en el intercambio y composición de la información de un servicio o trámite determinado. Lo anterior, atendiendo los lineamientos del Marco de Referencia de Arquitectura Empresarial para la Gestión de T.I. en el Estado, el Modelo de Seguridad y Privacidad de la Información (MSPI), así como del marco de interoperabilidad, para que las entidades que requieran esta información en sus procesos puedan exponer o consumir servicios según corresponda.

- Hacer uso de los servicios de intercambio de información publicados con el objeto de optimizar sus procesos, automatizar los trámites y servicios y recibir o acceder a la información que comparte el usuario de servicios ciudadanos digitales para integrarlos dentro de un trámite o actuación de la entidad.
- Firmar electrónicamente los documentos que así lo requieran, haciendo uso de los mecanismos otorgados para tal efecto, por el articulador o el prestador de servicios ciudadanos digitales, al funcionario respectivo.
- Concertar con el articulador los esquemas de soporte al usuario de servicios ciudadanos digitales de tal manera que los casos que competan a la prestación de servicios ciudadanos digitales sean escalados adecuadamente, sin perjuicio de los niveles de servicios y soporte que le competen a la entidad pública en el marco de la administración de sus sistemas de información.
- Presentar las peticiones, quejas, reclamos y solicitudes de información ante el articulador, cuando se presenten desviaciones en la calidad o anomalías en los servicios recibidos.
- Incluir los mecanismos de interoperabilidad necesarios que permitan hacer más ágiles y eficientes los trámites y servicios evitando solicitar información a ciudadanos y empresas a la que puedan acceder, consultar o solicitar a otra entidad. De igual forma, deberán usar el servicio de interoperabilidad para el intercambio de información con otras entidades.

Teniendo en cuenta lo planteado en la obligación 3 del artículo 2.2.17.4.7, se consideró idóneo evaluar la integración de los Servicios Ciudadanos Digitales en la Arquitectura Empresarial de CENS S.A. E.S.P., desde el cumplimiento de los lineamientos definidos en el Documento Maestro del Modelo de Arquitectura Empresarial.

Con base en estos lineamientos fue construido el instrumento tipo cuestionario orientado a establecer el cumplimiento de dichos lineamientos por parte de CENS S.A. E.S.P., información que se recopiló mediante la técnica de entrevista a quienes la manejan desde sus respectivos procesos.

6.5.2.1. Documento Maestro del Modelo de Arquitectura Empresarial

El MinTIC ha desarrollado el documento maestro del Modelo de Arquitectura Empresarial (MAE), el cual se convierte en un instrumento para implementar el habilitador de Arquitectura

de la Política de Gobierno Digital (PGD) del Estado Colombiano que establece el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos e innovadores, que generen valor público en un entorno de confianza digital.

Los propósitos de la PGD buscan que las entidades públicas impulsen y mejoren la provisión de servicios digitales de confianza y calidad, mediante procesos internos seguros y eficientes, la toma de decisiones basadas en datos, el empoderamiento ciudadano a través de un Estado Abierto y el desarrollo de Territorios y Ciudades Inteligentes para la solución de retos y problemáticas sociales.

El MAE permite que las entidades públicas apliquen un enfoque de arquitectura empresarial para fortalecer las capacidades institucionales requeridas para prestar servicios a los usuarios de cada entidad mediante el uso adecuado de las TIC. (MinTIC,2019, pp. 8-9)

El Modelo de Arquitectura Empresarial está compuesto por 7 dominios, así:

- Dominio de planeación de la arquitectura (DPA)
- Dominio de arquitectura misional
- Dominio de arquitectura de información
- Dominio de arquitectura de sistemas de información
- Dominio de arquitectura de infraestructura tecnológica
- Dominio de arquitectura de seguridad
- Dominio de uso y apropiación de la arquitectura

En cada dominio se establecen lineamientos, los cuales se definen como “orientaciones de carácter general y corresponden a disposiciones o directrices que deben ser ejecutadas en las entidades del Estado colombiano para implementar el Modelo de Arquitectura Empresarial” (MinTIC, 2019, p. 29)

El Documento Maestro del Modelo de Arquitectura Empresarial define, a su vez, para cada lineamiento, el respectivo entregable, insumo útil en nuestro estudio para determinar el nivel de cumplimiento desde la Arquitectura Empresarial de CENS.

La escala de calificación respecto al cumplimiento de cada lineamiento se definió de la siguiente manera:

- N=Nulo. Cuando no se tiene ningún tipo de avance respecto al entregable correspondiente al lineamiento.
- F=Formulado. Cuando se tiene una iniciativa enunciada en alguno de los instrumentos de planeación de la empresa (PETI, Planes de Mejoramiento), dirigida a cumplir con el entregable correspondiente al lineamiento.
- D=Desarrollándose. Cuando se tiene alguna iniciativa en marcha para cumplir con el entregable correspondiente al lineamiento.
- C=Cumplido. Cuando se cuenta con el entregable correspondiente al lineamiento.
- M=Mejorando. Cuando además de contar con el entregable correspondiente al lineamiento, éste se encuentra en mejora continua.

La información recolectada permitirá conocer el avance de CENS SA ESP en cada dominio del modelo.

6.5.3. Orientados a analizar el impacto de la planeación estratégica y la Arquitectura Empresarial de CENS S.A. E.S.P., sobre el proyecto de implementación de los mecanismos de autenticación digital.

La Guía para la Vinculación y Uso de los SCD (Versión 1.1 de mayo de 2020), presenta el modelo de los SCD, destinado a las autoridades referidas en el artículo 2.2.17.1.2 del Decreto 1078 de 2015, en el cual se indican cuáles son las condiciones necesarias y los pasos que deben realizar para la preparación, adecuación, integración, uso y apropiación de los SCD, a través de los cuales podrán integrar a sus sistemas de información los mecanismos de autenticación digital, interoperabilidad, carpeta ciudadana digital.

Por su parte, la Resolución número 002160 de 23 de octubre de 2020, "Por la cual se expide la Guía de lineamientos de los servicios ciudadanos digitales y la Guía para vinculación y uso de estos", define en su artículo No. 4, titulado *Estándares de implementación de los Servicios Ciudadanos Digitales contenidos en la Guía para vinculación y uso de los servicios ciudadanos digitales,* "Las autoridades señaladas en el artículo 2.2.17.1.2. del Decreto 1078 de 2015, deberán cumplir las condiciones y estándares establecidos en la Guía para vinculación y uso de los servicios ciudadanos digitales que se encuentran señaladas en el anexo 2 de la presente resolución, para la preparación, adecuación, integración, uso y apropiación de los servicios ciudadanos digitales, a través de los cuales podrán integrar a sus sistemas de información los

mecanismos de autenticación digital, interoperabilidad, carpeta ciudadana digital y vincularlos al Portal Único del Estado colombiano"

Para analizar el impacto de la planeación estratégica y la Arquitectura Empresarial de CENS S.A. E.S.P., sobre el proyecto de implementación de los mecanismos de autenticación digital, se diseñará un instrumento tipo lista de chequeo, basado en el capítulo 7 del anexo 2 de la resolución 002160 de 2020, en el cual se definen los requisitos a cumplir dentro del proceso de vinculación al Servicio de Autenticación Digital.

El instrumento de diagnóstico listará los requisitos definidos en el capítulo 7 del mencionado anexo 2 y permitirá enunciar, para cada requisito, la(s) iniciativa(s) y/o componente(s) con que CENS S.A. E.S.P., desde su planeación estratégica y/o arquitectura empresarial, estaría dando cumplimiento. La recopilación de la información se llevará a cabo mediante la técnica de entrevista al Profesional P2 Planeación y Gestión Operativa de CENS S.A. E.S.P.

La escala de calificación respecto al cumplimiento de cada requisito se definió de la siguiente manera:

- N=Nulo. Cuando no se tiene ningún tipo de avance respecto al entregable correspondiente al requisito.
- F=Formulado. Cuando se tiene una iniciativa enunciada en alguno de los instrumentos de planeación de la empresa (PETI, Planes de Mejoramiento) y/o componente propuesto en la Arquitectura Empresarial, dirigidos a cumplir con el entregable correspondiente al requisito.
- D=Desarrollándose. Cuando se tiene alguna iniciativa en marcha y/o componente de la Arquitectura Empresarial en construcción, para el cumplimiento del entregable correspondiente al requisito.
- C=Cumplido. Cuando se cuenta con el entregable correspondiente al requisito.
- M=Mejorando. Cuando además de contar con el entregable correspondiente al requisito, éste se encuentra en mejora continua.

La información recolectada permitirá conocer el avance de CENS S.A. E.S.P. en el cumplimiento de cada requisito.

7. DIAGNÓSTICO

7.1. Diagnóstico de los mecanismos actuales de autenticación digital de CENS S.A. E.S.P., según la Política de Gobierno Digital.

Este diagnóstico se hizo con base en lo definido por el estándar NIST, metodología descrita en una sección anterior del documento.

7.1.1. Instrumento para el análisis de riesgo

Siguiendo las directrices del documento SP 800-63-3 de NIST, se construyó un instrumento tipo cuestionario, el cual se aplicó a cada servicio de Tecnología de Información evaluado y se diligenció mediante entrevista al respectivo administrador técnico del servicio.

Al aplicar el instrumento de análisis de riesgo ante un acceso fraudulento en las aplicaciones objeto de estudio, originado por un error en la autenticación, se obtuvieron los resultados presentados en la tabla 1:

Tabla 1.Resultados diligenciamiento cuestionario análisis de riesgo según NIST 800-63-3

Nombre del servicio analizado	Categoría de riesgo 1 Inconveniencia, angustia o daño a la reputación	Categoría de riesgo 2: Pérdida financiera o responsabilidad de la agencia	Categoría de riesgo 3: Daño a programas de agencias o intereses públicos	Categoría de riesgo 4: Divulgación no autorizada de información confidencial	Categoría de riesgo 5: Seguridad personal	Categoría de riesgo 6: Violaciones civiles o penales
APP CENS	Bajo	Bajo	Bajo	Moderado	Bajo	Bajo
Asesor Virtual	Moderado	Bajo	Moderado	Moderado	Bajo	Bajo
Módulo Alumbrado Público	Moderado	Bajo	Bajo	Moderado	Bajo	Bajo
Módulo Junta Directiva	Moderado	Bajo	Bajo	Alto	Moderado	Bajo

Módulo Desconexiones Programadas	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
Módulo Radicación en línea de PQRS	Bajo	Bajo	Bajo	Moderado	Bajo	Bajo

Fuente. Elaboración propia con base en NIST 800-63-3

La información recolectada permitió conocer que:

- En ningún caso, una autenticación fraudulenta en alguna de las aplicaciones objeto de estudio podría generar pérdida financiera, ni violaciones civiles o penales.
- Una autenticación fraudulenta en el Módulo de Desconexiones Programadas tiene el mínimo impacto establecido por NIST sobre cada una de las 6 categorías de riesgo.
- La categoría de riesgo *Divulgación no autorizada de información confidencial* sería la más impactada por una autenticación fraudulenta en general para las aplicaciones objeto de estudio, seguida por la categoría de riesgo *Inconveniencia, angustia o daño a la reputación e imagen*.
- El Módulo de Junta Directiva representa el de mayor impacto potencial sobre las categorías de riesgo definidas por NIST, siendo la única en tener el mayor nivel de riesgo sobre una de las categorías como es el caso de *Divulgación no autorizada de información confidencial.*

Una vez determinado el potencial impacto sobre cada categoría, fue posible definir el Nivel de Garantía de Autenticación (AAL) requerido, siguiendo directrices de NIST, como se ilustra en la tabla 2.

Tabla 2. AAL definido para cada servicio objeto de estudio

Servicio objeto de estudio	**Nivel NIST**
APP CENS	AAL 2
Asesor virtual	AAL 2
Módulo Alumbrado Público	AAL 2

Servicio objeto de estudio	Nivel NIST
Módulo desconexiones programadas	AAL 1
Módulo Junta Directiva	AAL 3
Módulo Radicación de PQR'S	AAL 2

Fuente: Elaboración propia con base en NIST 800-63-3

En la tabla anterior se ilustra, como aspectos destacados, que el Módulo de Junta Directiva requiere el mayor Nivel de Garantía de Autenticación (AAL), mientras que el Módulo de Desconexiones Programadas el menor nivel.

7.1.2. Instrumento para el diagnóstico del Nivel de Garantía de Autenticación (AAL) actual.

Una vez definido el Nivel de Garantía de Autenticación (AAL) requerido de cada servicio de Tecnología de Información evaluado, se procedió a diligenciar, mediante entrevista al respectivo administrador técnico de cada servicio, el instrumento tipo cuestionario construido con base en el documento SP 800-63B, el cual permitió conocer el grado de cumplimiento de los mecanismos de autenticación de los servicios de T.I. analizados, respecto a lo establecido por NIST para verificar los atributos digitales de una persona.

Los resultados de este diagnóstico se resumen en la tabla 3.

Tabla 3. Resultados cumplimiento del nivel AAL definido para cada servicio

Servicio de T.I. evaluado	AAL definido	AAL1	AAL2	AAL3
APP CENS	AAL 2		Cumple	
Asesor Virtual	AAL 2		No cumple	
Módulo Alumbrado Publico	AAL 2		No cumple	
Módulo de radicación en línea de PQR's	AAL 2		No cumple	
Módulo desconexiones programadas	AAL 1	No cumple		
Módulo Junta Directiva	AAL 3			No cumple

Fuente. Elaboración propia con base en NIST 800-63B.

Por su parte, en la página 101 del anexo 2 de la resolución 002160 de 2020, se establecen: la relación de trámite, el grado de confianza y el mecanismo de consulta que se requiere de la Registraduría Nacional del Estado Civil (RNEC), tal como se define en la tabla 4.

Tabla 4. Relación grado de confianza – Consulta requerida RNEC

Tipo de trámite	**Grado de confianza**	**Requiere identificación con registraduría**	**Consulta requerida**
Riesgo de autenticación errónea nulo o mínimo	Bajo		N/A
Riesgo de autenticación errónea moderado	Medio	X	Consulta ANI y Sistema de Información de Registro Civil - SIRC
Riesgo de autenticación errónea considerable	Alto	X	Consulta bases de datos biométricas
Riesgo de autenticación errónea elevada	Muy Alto	X	Cédula digital

Fuente. Elaboración propia con base en el anexo 2 de la Resolución 002160 de 2020

En la página 7 del documento NIST 800-63-3, respecto al nivel de autenticación requerido (AAL), se establece lo siguiente:

- AAL1: Proporciona cierta seguridad
- AAL2: Proporciona una alta seguridad
- AAL3: Proporciona una muy alta seguridad

De acuerdo con lo anterior, se puede interpretar AAL1 como un nivel de seguridad bajo o medio, con lo cual es válida la homologación entre NIST y los grados de confianza establecidos por el anexo 2 de la resolución 002160 de 2020, como se ilustra en la tabla 5.

Tabla 5. Homologación Nivel de Autenticación NIST – Grado de Confianza RNEC.

NIST	**Resolución 002160**
AAL1	Bajo y Medio
AAL2	Alto
AAL3	Muy alto

Fuente. Elaboración propia.

En ese orden de ideas, la tabla 6 muestra el mecanismo de consulta requerido por cada servicio de T.I. analizado, según la citada resolución.

Tabla 6. Mecanismo de consulta definido para cada servicio objeto de estudio

Servicio objeto de estudio	**Consulta requerida**
APP CENS	Consulta bases de datos biométricas
Asesor virtual	Consulta bases de datos biométricas
Módulo Alumbrado Público	Consulta bases de datos biométricas
Módulo desconexiones programadas	Consulta ANI y Sistema de Información de Registró Civil – SIRC
Módulo Junta Directiva	Cédula Digital
Módulo Radicación de PQR'S	Consulta bases de datos biométricas

Fuente. Elaboración propia

La información recolectada con el instrumento para el diagnóstico del Nivel de Garantía de Autenticación (AAL) actual, permitió concluir que:

- En la gran mayoría de los casos, los mecanismos de autenticación de los servicios de T.I. objeto de estudio, no cumplen con lo definido por NIST 800-63B en el respectivo AAL requerido para los mismos.
- Solo la APP de CENS registra cumplimiento parcial en el AAL2.
- El escenario deseado de Nivel de Autenticación de cada servicio de TI analizado implicará emplear, como mínimo, uno de los mecanismos establecidos por la RNEC como servicio de tipo consulta requerida dentro de su portafolio.
- La propuesta para la implementación, en CENS, de mecanismos de autenticación digital según la política de gobierno digital del MinTIC, deberá abordar las acciones que permitan cumplir los requisitos para celebrar el convenio interinstitucional con la RNEC, según lo reglamenta la Resolución 5633 de 2016. Asimismo, buscará satisfacer lo definido por la resolución 002160 de 2020 en cuanto a la consulta requerida por cada servicio de T.I. analizado en el marco del presente proyecto.

7.1.3. Instrumento para el diagnóstico de los mecanismos de firma digital.

El instrumento de diagnóstico construido permitió conocer el cumplimiento de los servicios digitales de CENS en cuanto a los requisitos definidos en el anexo B del documento CEA-4.1-10 de ONAC y se diligenció con el acompañamiento del respectivo administrador técnico de cada servicio, empleando la técnica de entrevista. En la tabla 7 se muestran los resultados de la aplicación del cuestionario.

Tabla 7. Resultados cuestionario de diagnóstico firma digital

Servicio de T.I. evaluado	**Estándares técnicos vigentes de formatos de firma digital**	**Requisitos de seguridad**	**Requisitos de certificación de los productos o dispositivos criptográficos**	**CRL Validación estado de certificados**	**OCSP Protocolo estado de certificados**
APP CENS	Cumple	No cumple	No cumple	No cumple	No cumple
Asesor Virtual	No cumple	No cumple	No cumple	No cumple	No cumple
Módulo Alumbrado Publico	No cumple	No cumple	No cumple	No cumple	No cumple
Módulo de radicación en línea de PQR’s	No cumple	No cumple	No cumple	No cumple	No cumple
Módulo desconexiones programadas	No cumple	No cumple	No cumple	No cumple	No cumple
Módulo Junta Directiva	No cumple	No cumple	No cumple	No cumple	No cumple

Fuente. Elaboración propia con base en el documento CEA-4.1-10 de ONAC.

La información recolectada permitió conocer que:

- En la gran mayoría de los casos, los servicios de T.I. objeto de estudio, no cumplen con lo definido por el documento CEA-4.1-10 de ONAC en lo que respecta a la firma digital de mensajes de datos.
- Solo la APP de CENS registra cumplimiento respecto a los estándares técnicos vigentes de formatos de Firma Digital.

El diagnóstico de los mecanismos de autenticación digital y de firma digital a la luz de las pautas del estándar NIST 800-63, hizo evidente para CENS S.A. E.S.P. las necesidades de:

- Ajustar las interfaces de inicio de sesión de sus servicios de T.I.
- Definir y desarrollar integraciones entre sus sistemas de información, en favor de una mayor seguridad en los mecanismos de autenticación implementados en sus servicios de T.I.
- Integrar sus servicios de T.I. a las diferentes opciones de autenticación digital ofertadas por la RNEC, según el nivel de garantía requerido por cada uno de estos.

7.2. Evaluación de la integración de los Servicios Ciudadanos Digitales en la Arquitectura Empresarial de CENS S.A. E.S.P.

7.2.1. Arquitectura Empresarial de CENS

A nivel de grupo EPM los modelos de arquitectura empresarial, direccionamiento competitivo y modelo de sostenibilidad mostrados en la figura 4, se unificaron en un modelo de direccionamiento estratégico integrado con el propósito como eje central de la evolución organizacional, como se muestra en la figura 5

Figura 4. Modelos del grupo EPM

Fuente. Sistema de gestión integrado de CENS

Figura 5. Modelo de direccionamiento estratégico del grupo EPM

Fuente. Sistema de gestión integrado de CENS

A continuación, se define detalladamente cada uno de los componentes del modelo:

Propósito: Para qué existimos.

El Grupo EPM adopta el concepto de arquitectura para un mundo mejor para enfocar a los negocios en su aporte al desarrollo humano sostenible como factor de éxito.

Contribuir a la armonía de la vida para un mundo mejor.

Identidad: Lo que decidimos ser.

El Grupo EPM reconoce que debe alinear sus objetivos con los de la sociedad, para asegurar que sus actuaciones contribuyan efectivamente a hacer de ésta, el espacio propicio para la vida de todos sus integrantes. Para ello, declara cinco principios de acción a seguir y tres valores a compartir.

- Valores: Transparencia, Responsabilidad, Calidez.
- Principios de acción:
    - Cumplimos nuestros compromisos
    - Nuestro interés primordial es la sociedad
    - Brindamos un trato justo
    - Cuidamos el entorno y los recursos
    - Buscamos fundamentalmente servir.

La visión de sostenibilidad del grupo EPM concibe la protección y generación de valor para las empresas y la sociedad, desde las actividades nucleares de negocio, distante del enfoque filantrópico o asistencialista y sin suplantar competencias del estado ni de ningún otro actor.

Acción: Qué y cómo decidimos hacerlo.

El Grupo EPM reconoce la necesidad del enfoque territorial con el fin de hacer una gestión efectiva, pertinente y coherente, alineada con los objetivos empresariales y con su identidad, para integrarse e incidir sobre las estructuras del territorio.

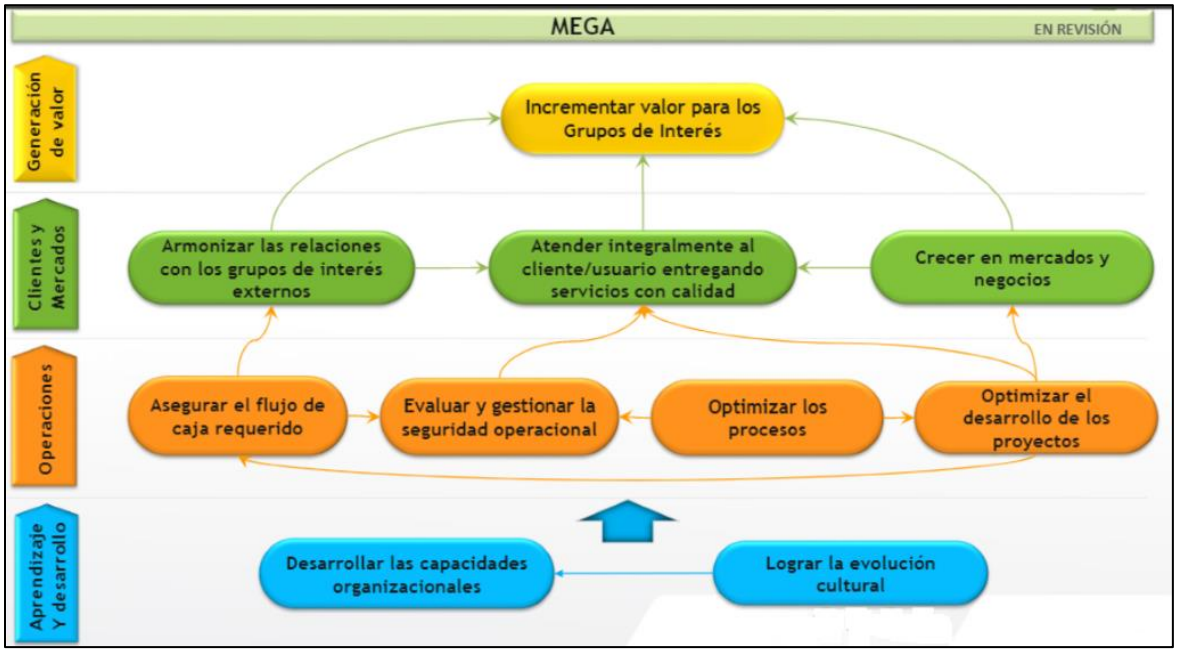
- Estrategia corporativa. Optimización de operaciones y crecimiento con criterios RSE
- Estrategia competitiva. Negocios generando valor para sus grupos de interés: Transmisión, Distribución, Comercialización.
- Estrategias de soporte
    - Estrategia de talento humano
    - Estrategia de innovación

- Estrategia de proveedores y servicios compartidos
- Estrategia de comunicaciones y relacionamiento
- Estrategia digital (T.I., TO, TC)
- Estrategia financiera
- Estrategia desarrollo de proyectos.

Resultados: Representa logros que se esperan alcanzar

- Contribución ODS.
- MEGA. En el 2025 el grupo EPM estará creciendo de manera eficiente, sostenible e innovadora; garantizando el acceso a los servicios que preste en los territorios donde esté presente, al 100% de la población; protegiendo 137 mil nuevas hectáreas de cuencas hídricas, además de las propias, con una operación carbono neutral y generando $12.6 billones de EBITDA.
- Objetivos estratégicos: Se detallan en la figura 6

Figura 6. Objetivos estratégicos de CENS



Fuente. Sistema de gestión integrado de CENS

7.2.2. Instrumento basado en el documento maestro del Modelo de Arquitectura Empresarial

Teniendo en cuenta lo planteado en la obligación 3 del artículo 2.2.17.4.7 del Decreto 620 de 2020, se consideró idóneo evaluar la integración de los Servicios Ciudadanos Digitales en la Arquitectura Empresarial de CENS S.A. E.S.P., desde el cumplimiento de los lineamientos definidos en el Documento Maestro del Modelo de Arquitectura Empresarial, el cual constituyó el punto de referencia clave en la comparación efectuada dentro del alcance de este segundo objetivo.

Con base en estos lineamientos fue construido el instrumento tipo cuestionario y se recopiló la información mediante la técnica de entrevista a quienes la manejan desde sus respectivos procesos.

El instrumento construido a partir del documento maestro de Modelo de Arquitectura Empresarial se presenta en el anexo A.

La información recolectada con este instrumento permitió conocer el avance de CENS en cada dominio del modelo, así:

- Dominio Planeación de la Arquitectura: Se cumple con el cronograma de ejercicios de Arquitectura Empresarial y al Documento de Arquitectura Empresarial en donde describa la arquitectura objetivo; se tiene avance en la construcción de la matriz de interesados de Arquitectura Empresarial. Se presenta incumplimiento respecto a los demás entregables del dominio.
- Dominio de Arquitectura Misional: Se presenta cumplimiento respecto al Modelo Estratégico de la entidad, Modelo financiero de la entidad, Modelo misional de la entidad, Portafolio de productos y servicios de la entidad, Marco normativo que rige la entidad, Documento con la definición de la Arquitectura Misional, Modelo de capacidades institucionales, Modelo de procesos, Modelo de recursos, Modelo Organizacional; no obstante, se tiene incumplimiento en cuanto al catálogo de hallazgos asociados a los procesos de la entidad.
- Dominio de Arquitectura de Información: No se tiene cumplimiento en ninguno de los entregables del dominio; no obstante, se presenta avance en cuanto a los entregables Catálogo de componentes de información, Documento con la definición de arquitectura de información, Vistas de la Arquitectura de Información, Vista de Gobierno de Arquitectura de Información y Hallazgos de componentes de información.

- Dominio de Arquitectura de Sistemas de Información: Se tiene cumplimiento respecto a todos los entregables del dominio: Documento con la definición de arquitectura de sistemas de información, Documentos de Arquitecturas de Referencia, Documentos de Arquitecturas de Solución, Documentos de Arquitecturas de Software y Catálogo de sistemas de información.
- Dominio de Arquitectura de Infraestructura Tecnológica: Se presenta cumplimiento en cuanto a los entregables correspondientes al Documento con la definición de arquitectura de infraestructura tecnológica, Catálogo de elementos de infraestructura, Vista de infraestructura tecnológica que evidencie el uso de servicios en la nube y Vista de infraestructura tecnológica que evidencia mecanismos que garanticen continuidad y disponibilidad. No obstante, se incumple con la Vista de interoperabilidad.
- Dominio de Arquitectura de Seguridad: Se cumple con los entregables correspondientes a Riesgos de componentes de información, Riesgos asociados a las aplicaciones y Mecanismos de auditoria y trazabilidad en las aplicaciones. Se tiene avance en los entregables de Riesgos de elementos de infraestructura y Controles de seguridad. No obstante, se tiene incumplimiento en cuanto al Documento con la definición de arquitectura de seguridad y Registros de auditoria y trazabilidad.
- Dominio de Uso y Apropiación de la Arquitectura: Solo se tiene cumplimiento en el entregable Hoja de ruta de Arquitectura Empresarial. Se tiene incumplimiento en cuanto a los demás entregables del dominio Plan de comunicaciones de la arquitectura empresarial, Proceso o procedimiento de arquitectura empresarial aprobado e implementado, Casos de negocio, Herramienta de AE implementada o Repositorio de AE con una estructura de carpetas acorde con los dominios abordados y ejercicios realizados.

La aplicación del instrumento de evaluación permitió descubrir la necesidad que tiene CENS en lo que respecta a enfocarse a brindar pronta atención al desarrollo de los entregables de los dominios de Arquitectura de Información y de Uso y Apropiación de la Arquitectura, para alinearse con el Modelo de Arquitectura Empresarial propuesto por MinTIC, dado que constituyen un factor clave para la integración e interoperabilidad de los servicios ciudadanos digitales con que cuenta, así como para la óptima implementación de nuevos servicios que le generen valor agregado a la organización y a sus diferentes grupos de interés.

7.3. Analizar el impacto de la planeación estratégica y la Arquitectura Empresarial de CENS S.A. E.S.P., sobre el proyecto de implementación de los mecanismos de autenticación digital.

El instrumento construido a partir del capítulo 7 del anexo 2 de la resolución 002160 de 2020, se presenta en el anexo A.

La información recolectada permitió conocer que el avance que CENS S.A. E.S.P. presenta en cuanto al cumplimiento de cada requisito, corresponde a la iniciativa a desarrollarse durante la vigencia 2021 y formulada desde su planeación estratégica, con la que se buscará desarrollar un diseño para la identificación biométrica de los clientes/usuarios en la atención de solicitudes y ejecución de trámites, en el marco del Plan de Atención al Ciudadano de la entidad.

Asimismo, en virtud del desarrollo del presente proyecto de grado, se puede afirmar que CENS S.A. E.S.P. presenta avances en lo que respecta a:

- El diagnóstico del riesgo, de acuerdo con lo definido por el estándar NIST SP 800-63B, en los mecanismos de autenticación de sus servicios de T.I. expuestos a sus grupos de interés externos.
- La determinación del grado de confianza requerido por cada servicio de T.I. expuesto a los grupos de interés externos, de acuerdo con lo definido por el estándar NIST SP 800-63B, en los mecanismos de autenticación de sus servicios de T.I. expuestos a sus grupos de interés externos.

El análisis efectuado en el desarrollo de este tercer objetivo permitió a CENS S.A. E.S.P., la necesidad de celebrar un contrato con un Operador Biométrico, el cual, lo guiará a CENS SA ESP en el cumplimiento de los requisitos de las fases de preparación, adecuación e integración, al tiempo que le permitirá satisfacer las necesidades de seguridad definidas en el capítulo 7 del anexo 2 de la resolución 002160 de 2020.

8. PLAN DE INTERVENCIÓN

El plan de intervención definido se detalla en el plan de dirección de proyecto desarrollado bajo metodología PMI descrito en el anexo B.

9. DESCRIPCIÓN DE LA ESTRATEGIA DE COMUNICACIÓN PARA LA PROMOCIÓN Y ADOPCIÓN DEL PLAN DE PROYECTO DEFINIDO.

Buscando cumplir con el quinto objetivo específico del presente trabajo y con el acompañamiento del equipo de trabajo de Comunicaciones de CENS, se elaboró el plan de comunicación dirigido a sus grupos de interés internos, el cual se ilustra en la figura 7.

Figura 7. Plan de comunicación para divulgación del plan de proyecto.

CENS Grupo epm	CENTRALES ELÉCTICAS DEL NORTE DE SANTANDER S.A. E.S.P. SISTEMA DE GESTIÓN PLAN DE LA COMUNICACIÓN										
AÑO DE PLANEACIÓN:	**2021**	**FECHA DE ELABORACIÓN:**	**ene-21**						**FECHA DE MODIFICACI**	**ene-21**	
ACTIVIDAD	**Plan de dirección de proyecto para la implementación, en CENS, de mecanismos de autenticación digital según la Política de Gobierno Digital del MINTIC**										
OBJETIVO GESTIÓN DE LA COMUNICACIÓN	Posicionar el proyecto de implementación de mecanismos de autenticación digital según la Política de Gobierno Digital del MINTIC										
OBJETIVO COMUNICACIÓN	Divulgar información del plan de proyecto de implementación de mecanismos de autenticación digital en los medios de la organización dirigidos a los grupos de interés internos										
OBJETIVO COMUNICACIÓN EXTERNA	Divulgar información de la iniciativa de proyecto de implementación de mecanismos de autenticación digital en los medios de la organización dirigidos a los grupos de interés externos										
OBJETIVOS MAPA ESTRATÉGICO	Gestionar las comunicaciones del proyecto										
ACCIONES	**INTERNA**	**DESCRIPCIÓN DE LA ACCIÓN**	**RESPONSABLE**	**DEPENDENCIAS DE APOYO**	**UNIDAD DE MEDIDA**	**META ANUAL**	**FECHA ESTIMADA**	**%AÑO**	**RECURSOS**	**DESCRIPCIÓN DE EJECUCIÓN**	**OBSERVACIONES**	**FUENTE**
Presentar iniciativa de proyecto en boletín semanal	X	Publicación de artículo informativo en el boletín semanal de CENS	Líder de comunicaciones de CENS	Gerencia	Artículo noticioso	1	15-feb-21	100%	Computador, cámara digital, conexión de red	Entrevistar a autores en Microsoft Teams Redactar la nota información Publicar en boletín		Bandeja de entrada de cuenta de e-mail corporativo
Presentar plan de proyecto a equipo de trabajo de Tecnología de Información de CENS	X	Solicitar espacio para presentar el plan de proyecto en grupo primario del equipo de trabajo	Profesional P1 Soluciones Informáticas	Área Servicios Corporativos	Hora	1	02-feb-21	100%	Computador Microsoft Teams Microsoft Word	Compartir en pantalla, el plan de proyecto elaborado para la implementación de mecanismos de autenticación digital en CENS		Listado de asistencia de participantes del evento
Presentar plan de proyecto a Área Servicios Corporativos	X	Solicitar espacio para presentar el plan de proyecto en grupo primario del área	Profesional P1 Soluciones Informáticas	Área Servicios Corporativos	Hora	1	19-feb-21	100%	Computador Microsoft Teams Microsoft Word	Compartir en pantalla, el plan de proyecto elaborado para la implementación de mecanismos de autenticación digital en CENS		Listado de asistencia de participantes del evento
Presentar plan de proyecto a Gerencia	X	Solicitar espacio para presentar el plan de proyecto en comité de gerencia	Profesional P1 Soluciones Informáticas	Gerencia	Hora	1	26-feb-21	100%	Computador Microsoft Teams Microsoft Word	Compartir en pantalla, el plan de proyecto elaborado para la implementación de mecanismos de autenticación		Listado de asistencia de participantes del evento

Fuente. Elaboración propia con base en la plantilla PT_309_GEC_001 del Sistema de Gestión Integrado de CENS

La divulgación hacia los grupos de interés externos deberá planearse y ejecutarse una vez la propuesta de proyecto cuyo plan de dirección se describe en el anexo B obtenga la debida aprobación y se incluya al plan operativo del equipo de trabajo de T.I. de CENS.

La evidencia recopilada a partir de la ejecución de las acciones enunciadas en el plan de comunicación anterior se ilustra en el anexo C.

10. RECOMENDACIONES Y CONCLUSIONES

A continuación, se presentan las recomendaciones para la implementación del plan de intervención propuesto y las conclusiones de cierre del trabajo.

10.1. Recomendaciones

- Propender por abordar toda la temática de la Política de Gobierno Digital bajo la figura de un proyecto organizacional que garantice la disposición de recursos para tal fin.
- Cubrir la brecha identificada como resultado del desarrollo del objetivo 2 como parte del alcance de la temática de la Política de Gobierno Digital.
- Determinar, en el corto plazo, el grado de cumplimiento de que tiene CENS respecto a los lineamientos definidos en el Marco de Interoperabilidad y el instrumento denominado Modelo de Seguridad para la Protección de la Información (MSPI), en procura de satisfacer, de manera transversal, las obligaciones definidas en el artículo 2.2.17.4.7 del Decreto 620 de 2020, para el aprovechamiento de los Servicios Ciudadanos Digitales Base de MINTIC.
- Crear un cargo en la estructura de la organización, sobre el que recaiga la responsabilidad de su transformación digital.
- Crear una línea base de seguridad que sirva como lista de verificación al evaluar los mecanismos de autenticación digital de los servicios de T.I. actuales y proyectados a adquirirse a futuro.
- Si bien, en el presente trabajo se abordaron los servicios de T.I. expuestos a los grupos de interés externos por considerar que en los mismos se tiene mayor riesgo de seguridad, es conveniente extender a la totalidad de los servicios de T.I. de CENS, en el corto plazo, los lineamientos definidos por MINTIC con base en el estándar NIST SP 800-63B.

10.2. Conclusiones

- El diagnóstico de los mecanismos de autenticación digital evidenció un nivel de riesgo entre moderado y bajo en las aplicaciones objeto de estudio, y que sólo una aplicación alcanzó el Nivel de Garantía de Autenticación (AAL) 3.
- En la evaluación de los lineamientos definidos en el Documento Maestro del Modelo de Arquitectura Empresarial, se determinó incumplimiento únicamente en el Dominio de Arquitectura de Información.

- La apertura de las instituciones a sus diferentes grupos de interés dejó de ser una opción para convertirse en una necesidad y las TIC'S constituyen un aliado para la transformación digital que les permite lograr esa cercanía en el relacionamiento con estos.
- El enfoque del estándar NIST SP 800-63, según el cual, el nivel de seguridad requerido se determina a partir del análisis de riesgo acarreado por un acceso fraudulento, resultó de gran ayuda y fácil aplicación, pues solo se requirió entrevistar a los respectivos administradores técnicos de los servicios de T.I. estudiados, quienes, desde su experticia, apoyaron el diligenciamiento del instrumento construido para tal fin.
- El análisis de riesgo bajo el estándar NIST 800-63 permitió conocer que, la *Divulgación no autorizada de información confidencial* y la i*nconveniencia, angustia o daño a la reputación e imagen*, constituyen, para CENS, las categorías de riesgo más impactadas del modelo, mientras que, en ningún caso, se tendría impacto en las categorías *pérdida financiera* y *violaciones civiles o penales*.
- Al indagar respecto a los lineamientos y pautas consideradas al implementar dichos mecanismos, los desarrolladores de los sistemas de información que constituyen la base de los servicios de T.I. informaron su desconocimiento de las especificaciones del estándar NIST SP 800-63B. Lo anterior, explica el que ninguno de los mecanismos de autenticación digital de los servicios de T.I. de CENS estudiados en el presente trabajo, haya cumplido con los lineamientos definidos por MINTIC para cada nivel de seguridad requerido.
- En la actualidad, el Servicio Ciudadano de Autenticación Digital se basa en los servicios prestados para tal efecto desde la RNEC, y la vinculación y uso de este depende del cumplimiento de las condiciones y procedimientos descritos en la Resolución 5633 de 2016, disposiciones que se refuerzan en la Resolución 2160 de 2020.
- Cumplir con los requisitos exigidos por la RNEC para la vinculación y uso de sus servicios, probablemente llevará a incurrir en altos costos, sobre todo si se tiene en cuenta la alta inversión que supone en términos de infraestructura de T.I. y seguridad; de ahí la importancia que tiene la contratación del operador biométrico, que facilita el cumplimiento de los requisitos y se constituye como el aliado estratégico para la firma del convenio con dicha entidad.
- La divulgación del plan de proyecto permitió sensibilizar al interior de la organización respecto a la importancia de propiciar las condiciones que garanticen trámites y servicios de TI seguros para las partes que intervienen, al tiempo que se contextualizó a los patrocinadores y, en general, al equipo del proyecto, respecto al alcance, tiempo, costo y requisitos de calidad del proyecto y su alineación con otras iniciativas definidas desde la planeación estratégica.

En el corto plazo, CENS buscará, desde su planeación estratégica, avanzar hacia su transformación digital desarrollando un diseño para la identificación biométrica de los clientes/usuarios en la atención de solicitudes y ejecución de trámites, en el marco del Plan de Atención al Ciudadano de la entidad, iniciativa afín a la propuesta de proyecto esbozada en el Anexo B del presente documento.

11. REFERENCIAS

Arango, M., Londoño, J., y Zapata, J. (2010). ARQUITECTURA EMPRESARIAL - VISIÓN GENERAL. Revista Ingenierías Universidad de Medellín, 9(16), 101-111. Recuperado de: https://revistas.udem.edu.co/index.php/ingenierias/article/view/46/32

Baquerizo M., y Guevara. C. (2016). "Análisis de la seguridad en los sistemas e-gobierno mediante el problema SAT," INGE CUC, vol. 12, no. 1, pp. 73-79, 2016. DOI: http://dx.doi.org/10.17981/ingecuc.12.1.2016.07

Campo, M. (2017). *Los beneficios de la tecnología frente a la interposición y/o notificación de las peticiones, quejas, reclamos y solicitudes (PQRS), una vez se expidió el código de procedimiento administrativo y de lo contencioso administrativo.* Recuperado de https://repository.unimilitar.edu.co/bitstream/handle/10654/17580/campobedoyamichaelaugusto2017.pdf

Centrales Eléctricas del Norte de Santander S.A. E.S.P. (2020). Recuperado de www.cens.com.co

Centrales Eléctricas del Norte de Santander S.A. E.S.P. (s.f) Sistema de Gestión de Calidad. Recuperado de https://sgi.almeraim.com/sgi/seguimiento/?nosgim

Chacón, A., Ordóñez, J., y Anichiarico, A. (2017). Hacia el reconocimiento de la inclusión digital como un derecho fundamental en Colombia. 134 Vniversitas, 139-168 (2017). doi: http://dx.doi.org/10.11144/Javeriana.vj134.hrid

Concha, G., Naser, A., (2012). *El desafío hacia el gobierno abierto en la hora de la igualdad.* Recuperado de http://iis7-e2.cepal.org/ddpe/publicaciones/xml/9/46119/W465.pdf.

Comisión de Regulación de Energía y Gas CREG (2018). Recuperado de http://www.creg.gov.co/index.php/es/creg/quienes-somos/mision-vision

De la Hoz, D,(2018). *Firma electrónica en la nube.* Recuperado de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81566/6/ddelahozTFM0618memoria.pdf

Departamento Nacional de Planeación. República de Colombia. (9 de febrero de 2000).Agenda de conectividad. Ministerio de Comunicaciones. Recuperado de https://www.mintic.gov.co/portal/604/articles-3498_documento.pdf

Gabaldón, L., Pereira, W., (2008). Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. Recuperado de: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1517-45222008000200008

Gallardo de Parada, Y., Moreno, A. (1999) *Recolección de la información.* Recuperado de http://www.unilibrebaq.edu.co/unilibrebaq/images/CEUL/mod3recoleccioninform.pdf

GEB (2018). Recuperado de

https://www.grupoenergiabogota.com/eeb/index.php/transmision-de-electricidad/sector-energetico-en-colombia

Guerrero, G. (2013). *Metodología para la gestión de proyectos bajo los lineamientos del Project Management Institute en una empresa del sector eléctrico* (Tesis de maestría). Recuperada de http://bdigital.unal.edu.co/11161/1/940429.2013.pdf

Hernández, R., Fernández, C., y Baptista, P. (2014). *Metodología de la investigación.* México: Mc Graw Hill.

MinTIC. (2017). *Decreto 1413*. Bogotá.

MinTIC. (2018a). *Manual de Gobierno en Línea*. Recuperado de http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-8011.html

MinTIC. (2018b). *Manual de Gobierno en Línea*. Recuperado de http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7650.html

MinTIC. (2018c). *Autenticación electrónica*. Recuperado de http://estrategia.gobiernoenlinea.gov.co/623/w3-article-9406.html

MinTIC. (2018d). *Manual de Gobierno Digital*. Recuperado de http://gobiernodigital.gov.co/623/articles-79394_recurso_1.pdf

MinTIC. (2019). *Documento Maestro del Modelo de Arquitectura Empresarial*. Recuperado de https://www.mintic.gov.co/arquitecturati/630/articles-144764_recurso_pdf.pdf

MinTIC (2020). Resolución número 002160. Recuperado de https://www.mintic.gov.co/portal/604/articles-152267_recurso_1.pdf

Norma Internacional ISO 7498 (2005). *Information technology -- Open Systems Interconnection.* Ginebra: Organización Internacional de Estándares.

OEA. e-Gobierno (s.f.). Recuperado de http://www.oas.org/es/temas/egovt.asp

OEA. Sobre e-Gobierno(s.f.). Recuperado de http://portal.oas.org/Portal/Sector/SAP/DptodeModernizacióndelEstadoyGobernabilidad/NPA/SobreProgramadeeGobierno/tabid/811/Default.aspx

Pirni, A., Giampellegrini, P. and Raffini, L. (2019) "Digital transformation and egovernment. For a research agenda on the Liguria Region". OBETS. Revista de Ciencias Sociales, 14(2): 471-490. doi: 10.14198/OBETS2019.14.2.07

Riascos, S., Martínez, G., y Solano, O. (2008). *El Gobierno Electrónico como estrategia de participación ciudadana en la Administración pública a nivel de Suramérica - Casos Colombia y Uruguay.* Recuperado de http://gyepro.univalle.edu.co/documentos/linc1.pdf

Romero, J., (2016). *Firma electrónica en el contexto del gobierno digital*. Recuperado de https://revistas.ucr.ac.cr/index.php/juridicas/article/download/29866/29877

Romero, S., (2014). Propuesta metodológica para la planificación de proyectos informáticos bajo el estándar PMI. *Revista Politécnica, 10* (18), 57-70. Recuperado el 13 de junio de 2020 de https://revistas.elpoli.edu.co/index.php/pol/article/view/376/542

Tirado, N., Ramos, D., Álvarez, E., Carreño, S. (2017). *Seguridad Informática, un mecanismo para salvaguardar la Información de las empresas*. *Revista Publicando, 4*(10 (2)), 462-473. Recuperado de https://www.rmlconsultores.com/revista/index.php/crv/article/view/367

Toloza, A., y Anteliz, R., (2017). *Diagnóstico y propuesta para la implementación de la estrategia de gobierno en línea en Centrales Eléctricas de Norte de Santander S.A. E.S.P. (CENS)*. (Trabajo de grado). Universidad EAN. Bogotá, Colombia.

UNESCO. (s.f).*Gobernabilidad electrónica Fortalecimiento de capacidades de la gobernabilidad electrónica.* Recuperado de http://biblioteca.udgvirtual.udg.mx:8080/jspui/bitstream/123456789/597/1/Gobernabilidad electrónica. fortalecimiento de capacidades de la gobernabilidad electrónica.pdf

Villa, A. (2008). *El papel de internet hacia un planeamiento territorial más participativo.* Recuperado de https://upcommons.upc.edu/bitstream/handle/2099/4496/9_AURIBEL.VILLA.pdf

Zapata Molina, L. (2012). *Evaluación y mitigación de ataques reales a redes IP utilizando tecnologías de virtualización de libre distribución*. Ingenius. Revista de Ciencia y Tecnología, (8), 11-19.

A. Anexo. Instrumentos de diagnóstico

- Instrumento para el análisis de riesgos. https://bit.ly/2Zw3aAM

- Instrumento para el diagnóstico AAL y firma digital https://bit.ly/2ZyTCoB

- Instrumento para el diagnóstico de cumplimiento de los lineamientos del Modelo Maestro de Arquitectura Empresarial. https://bit.ly/3aHkyZX

- Instrumento para el diagnóstico de cumplimiento de los requisitos para vinculación y uso del Servicio de Autenticación Digital. https://bit.ly/37xRqlM

B. Anexo. Plan de proyecto

Plan de dirección
de proyecto Implem

C. Anexo. Ejecución estrategia de comunicación

Ejecución estrategia de comur