COLOMBIA POTENCIA DE LA VIDA

TIC

GUÍA GENERAL

MAE.G.AS - DOMINIO DE ARQUITECTURA DE SEGURIDAD

Ministerio de Tecnologías de la Información y las Comunicaciones 2023

MAE

Ministerio de Tecnologías de la Información y las Comunicaciones

Viceministerio de Transformación Digital

Dirección de Gobierno Digital

Subdirección de Estándares y Arquitectura de Tecnologías de la Información

Equipo de trabajo

Óscar Mauricio Lizcano Arango - Ministro de Tecnologías de la Información y las Comunicaciones

Sindey Carolina Bernal Villamarín - Viceministra de Transformación Digital

Ana María Sterling Bastidas – Directora de Gobierno Digital

Luis Clímaco Córdoba Gómez - Subdirector de Estándares y Arquitectura de TI

Jairo Alberto Riascos Muñoz – Equipo de subdirección de Estándares y Arquitectura de TI

Claudia Milena Rodríguez Álvarez – Equipo Subdirección de Estándares y Arquitectura de TI

Julio César Anaya Esteves - Equipo de la Subdirección de Estándares y Arquitectura de TI

Empresa Consultora Yobiplex

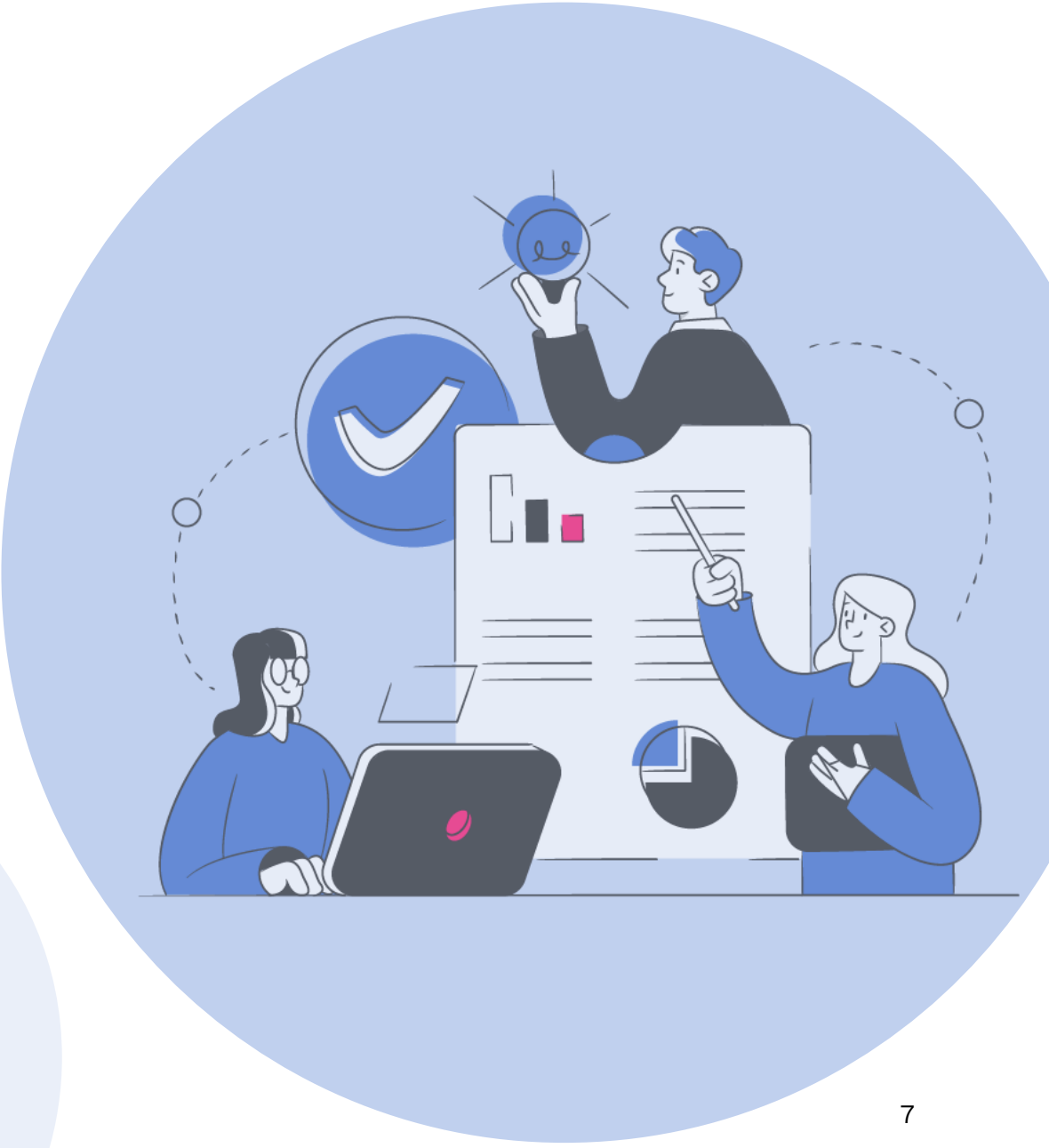
Versión	Observaciones
Versión 3.0 **Mayo 2023**	Guía General del Dominio de Arquitectura de Seguridad

Tabla de contenido

Listado de ilustraciones

Listado de tablas

1. Introducción



La arquitectura empresarial incluida la arquitectura de seguridad tiene que ver con la alineación de los sistemas institucionales y los sistemas de información de apoyo para lograr los objetivos institucionales de una manera eficaz y eficiente, recordemos que los sistemas son la combinación de procesos, personas y tecnología.

La arquitectura de seguridad contiene una visión equilibrada del riesgo, consecuencias negativas se mantienen a un nivel aceptable y se aprovechan al máximo las oportunidades. El enfoque impulsado por la institución es clave para la arquitectura de seguridad, ya que, los motivadores institucionales ofrecen el contexto para evaluaciones de riesgo; definen si es necesario el cumplimiento de algún marco de control y justifican la necesidad de medidas de seguridad.

Es la experiencia común de muchas entidades que las soluciones de seguridad de la información, a menudo se diseñan, adquieren e instalan sobre una base táctica. Se identifica un requisito, se desarrolla una especificación y se busca una solución para satisfacer esa situación. En este proceso no hay oportunidad de considerar la dimensión estratégica, y el resultado es que la organización construye una mezcla de soluciones técnicas para un fin concreto, cada una diseñada y especificada de manera independiente y sin garantía de que serán compatibles e interoperables. A menudo no hay un análisis de los costos a largo plazo, especialmente los costos operativos que constituyen una gran proporción del costo total, y no existe una estrategia que pueda identificarse para respaldar los objetivos de la organización.

Un enfoque que evita estos problemas parciales es el desarrollo de una arquitectura de seguridad impulsada por la institución y que describe una interrelación estructurada entre las soluciones técnicas y de procedimiento para respaldar las necesidades a largo plazo de la institución.

Una arquitectura de seguridad no existe de forma aislada. Es parte de la organización. Se basa en la información institucional, que ya está disponible en la arquitectura empresarial y también produce información que debería ser utilizada por la arquitectura empresarial. Ésta es la razón por la que resulta beneficiosa una estrecha integración de la arquitectura de seguridad en la arquitectura empresarial.

1.1. Usted Está Aquí

Ilustración 1. Dominio de Arquitectura de Seguridad, como parte del Modelo de Arquitectura Empresarial. Fuente: Propia

Esta guía muestra cómo debe definirse una arquitectura de Seguridad dentro de un ejercicio de arquitectura empresarial, es una guía general que presenta de manera metodológica como abordarla.

La arquitectura de Seguridad se debe definir en base a la arquitectura institucional, de información, de sistemas de información y de Tecnología deseadas durante la fase de diseño.

1.2. Propósito de esta guía

Objetivo general

- Definir la arquitectura de seguridad de la información y Ciberseguridad que se integre y fortalezca con los demás dominios del MAE dentro del alcance definido para el ejercicio de arquitectura empresarial.

Objetivos específicos

- Definir la arquitectura de seguridad actual
- Definir la arquitectura de seguridad objetivo
- Realizar el análisis de las brechas existentes entre la arquitectura deseada y la arquitectura actual

1.3. A quién va dirigida - Audiencia

Está guía va dirigida a las áreas y cargos que articulan e integran una visión completa de la entidad

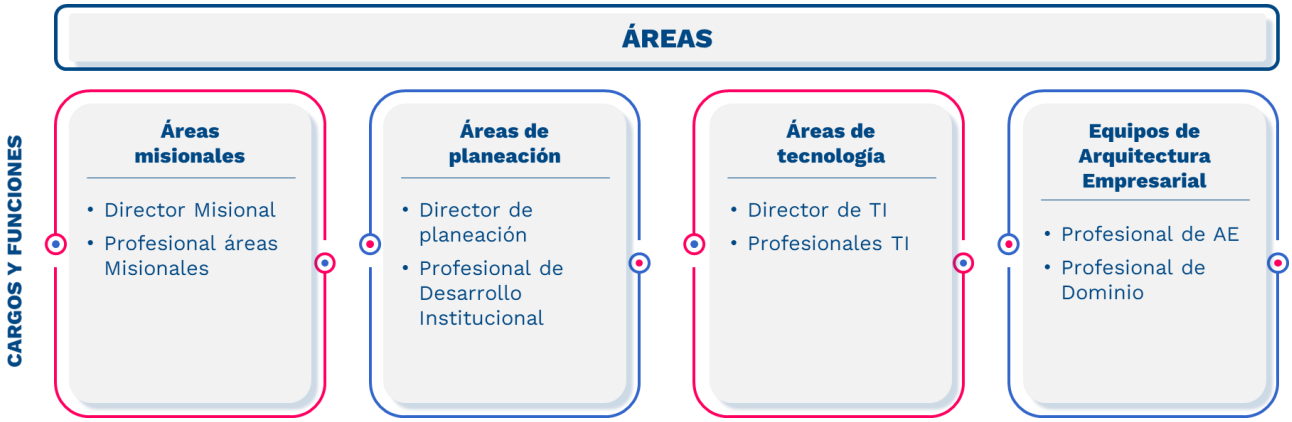


Ilustración 2. Audiencia
Fuente: Propia

2. Modelo conceptual

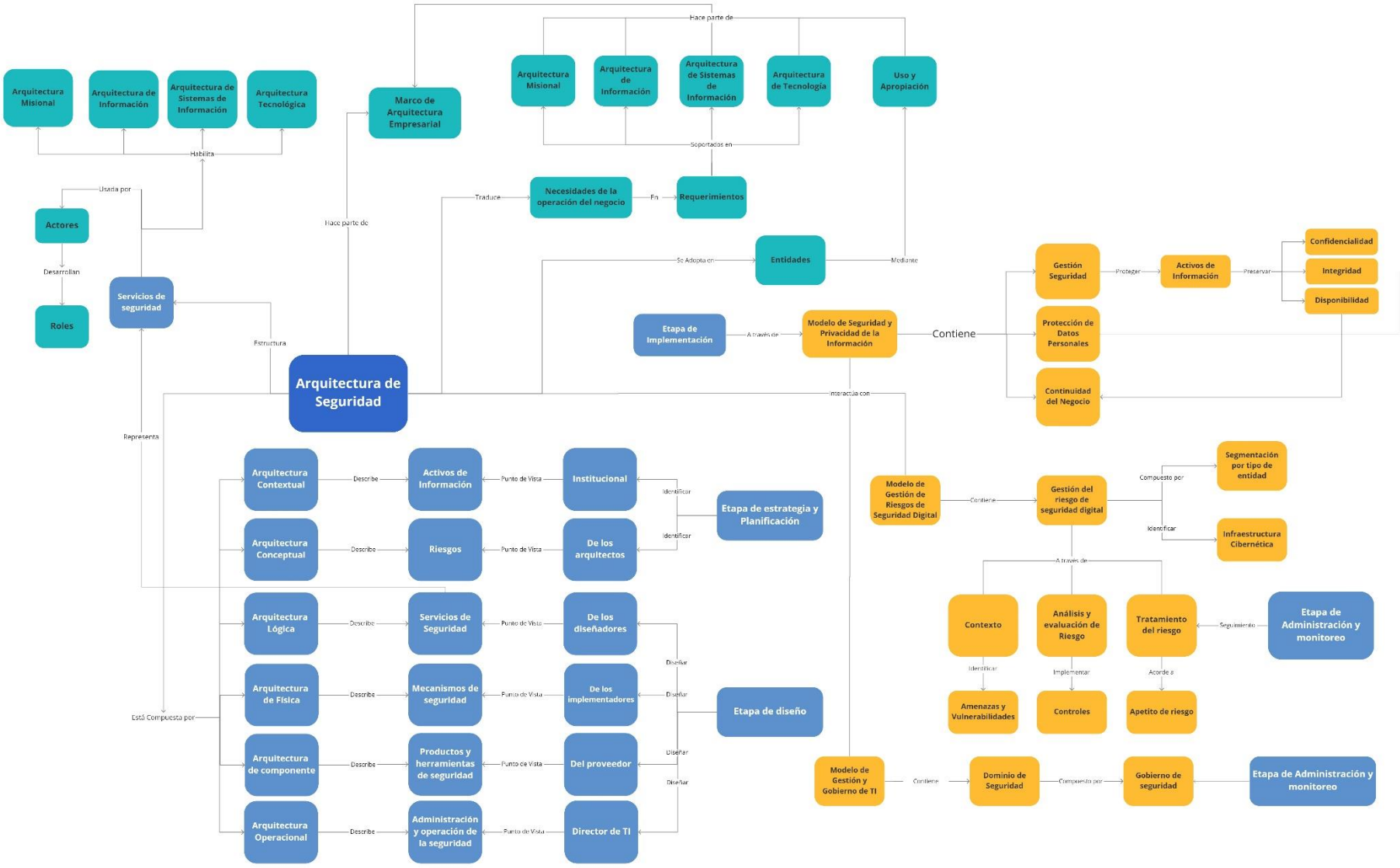


Ilustración 3. Modelo conceptual de Arquitectura de Seguridad. Fuente: Propia.

La arquitectura de seguridad establece servicios de seguridad que habilita las demás arquitecturas a través del aseguramiento y protección de la información misional y de apoyo implementando controles en los sistemas de información e infraestructura que la soportan, esta información es usada a su vez por actores que desarrollan un rol dentro de la entidad.[1]

Para la definición del modelo de Arquitectura de Seguridad se utilizó como base el marco de referencia SABSA (Sherwood Applied Business Security Architecture), SABSA es un modelo y una metodología para desarrollar arquitecturas de seguridad de la información impulsadas por el riesgo y para entregar soluciones de infraestructura de seguridad que respaldan iniciativas institucionales críticas. La característica principal del modelo SABSA es que todo debe derivarse de un análisis de los requisitos institucionales frente a seguridad, especialmente aquellos en los que la seguridad tiene una función habilitadora a través de la cual se pueden desarrollar y explotar nuevas oportunidades. SABSA no ofrece ningún control específico y se basa en otros, como la Organización Internacional para la Estandarización (ISO) o los procesos COBIT. Es puramente una metodología para asegurar la alineación institucional y un marco de "vida útil": se aplica a lo largo de todo el ciclo de vida, desde la ingeniería de requisitos hasta la gestión de las soluciones entregadas.

La metodología SABSA tiene seis arquitecturas de seguridad. Cada arquitectura tiene un propósito y vista diferente. A continuación, se presentan los puntos de vista de SABSA, su traducción en niveles de arquitectura y su descripción:

PUNTO DE VISTA	ARQUITECTURA	DESCRIPCIÓN
De la institución	Contextual	Describe los requerimientos institucionales
De los arquitectos	Conceptual	Describe la visión estratégica a alto nivel
De los diseñadores	Lógica	Describe los servicios de seguridad
De los implementadores	Física	Describe los mecanismos de seguridad
Del proveedor	De componente	Describe los productos y herramientas de seguridad
De los administradores de servicios (director de TI)	Operacional	Describe la administración y operación de la seguridad

Tabla 1. Puntos de vista SABSA. Fuente: SABSA White Paper Enterprise Security Architecture

Con estos puntos de vista, SABSA busca identificar y gestionar los riesgos de seguridad en los atributos institucionales, y convertirlos en oportunidades para el logro de la estrategia de seguridad.

Cada uno de estos puntos de vista responde a los interrogantes:

[1] En el modelo conceptual se cuenta con un código de colores que nos permite identificar los conceptos asociados al MAE (en color azul), los conceptos asociados al dominio que estamos desarrollando (en color verde) y los conceptos asociados a otros modelos (en color amarillo).

- ¿QUÉ es lo que se quiere proteger?
- ¿CÓMO se va a proteger?
- ¿DÓNDE se intentará asegurar?
- ¿QUIÉN está involucrado?
- ¿CUÁNDO se debe aplicar seguridad? Y
- ¿POR QUÉ tenemos que hacerlo?

A partir de la respuesta a estos interrogantes por cada nivel de arquitectura, se construye la matriz SABSA, que es el mapa de ruta que determina el ciclo de vida de la Arquitectura de Seguridad.

Para ello, SABSA sugiere dos vías de desarrollo:

1. Recorrer la matriz a partir de los requisitos institucionales hasta proveer una solución.

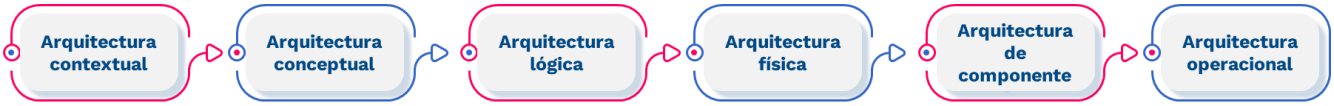


Ilustración 4.Recorrido de la matriz flujo 1.

2. Impulsar un requerimiento institucional a través de una solución específica.

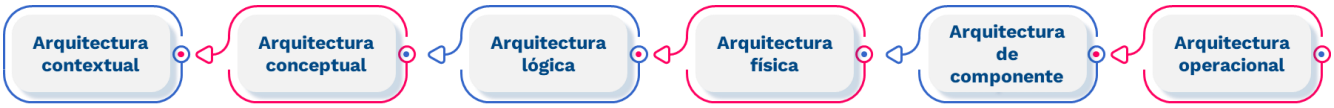


Ilustración 5.Tabla 3. Recorrido de la matriz flujo 2.

Se sugiere se desarrolle como la entidad lo encuentre pertinente de acuerdo con sus necesidades y su situación actual.

A continuación, se describe cada una de las arquitecturas de seguridad y su descripción

Arquitectura Operacional	Arquitectura Contextual
	Arquitectura Conceptual
	Arquitectura Lógica
	Arquitectura Física
	Arquitectura de Componente

Tabla 2.Modelo de SABSA para la Arquitectura de Seguridad. Fuente: SABSA White Paper Enterprise Security Architecture.

La arquitectura contextual está en la parte superior e incluye los requisitos y objetivos institucionales, se identifican los activos de la institución principales de la entidad en materia de seguridad.

La segunda es la arquitectura conceptual, que es la vista de arquitectura, en ella encontramos los atributos específicos en seguridad que quiere lograr la entidad en materia de seguridad y que deben ser aplicables a todos los activos identificados.

La tercera es la arquitectura lógica la cual se desarrolla desde la perspectiva de las dependencias claves de la entidad. A partir de esta vista se desarrollan los servicios de seguridad, a través de la definición de los procesos de seguridad y los controles requeridos para mitigar los riesgos identificados sobre los activos de la institución, para asegurar así que se cumpla con los atributos o principios de seguridad establecidos.

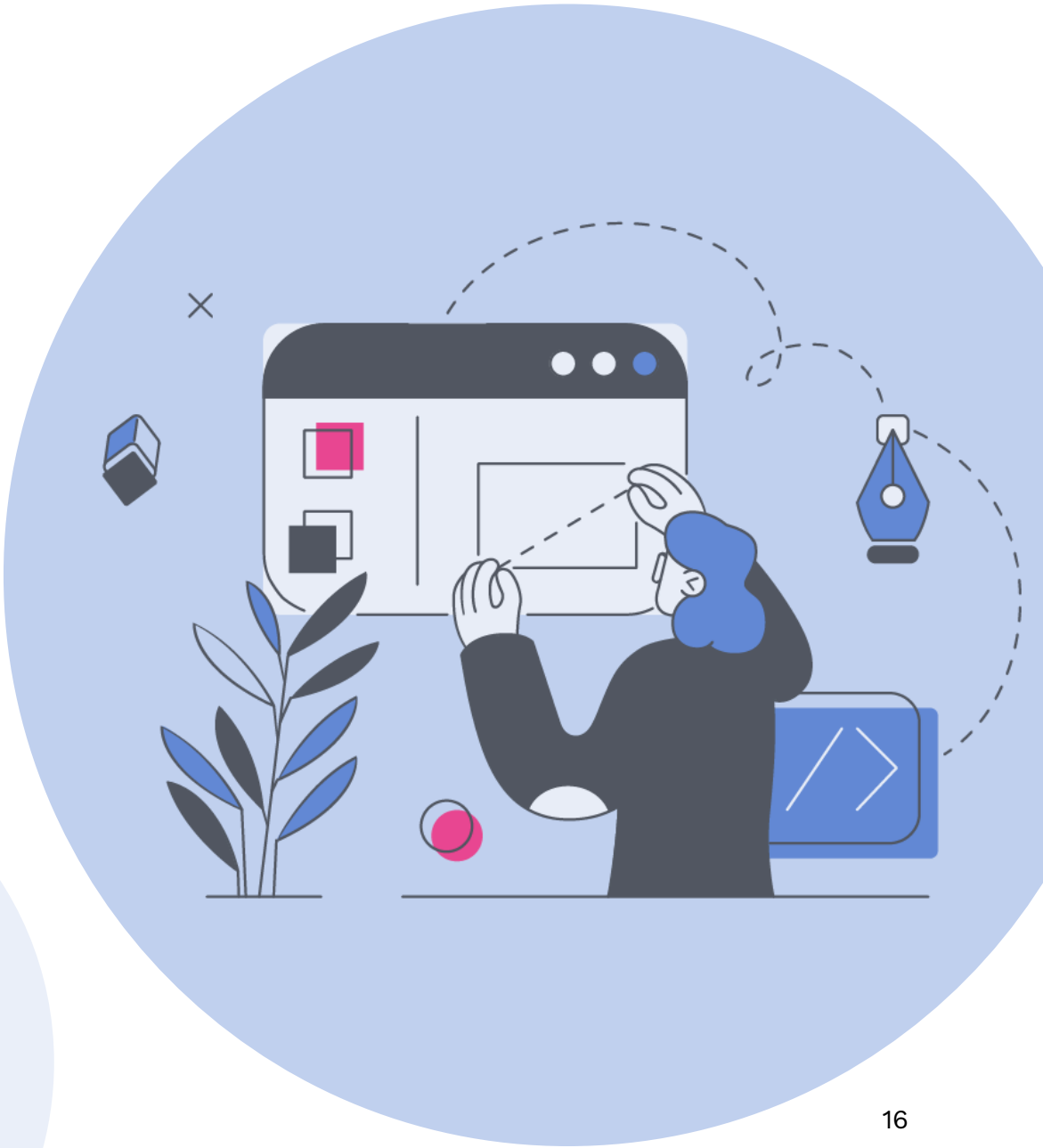
La cuarta es la arquitectura física a partir de la cual se relacionan los mecanismos de seguridad con los que cuenta la entidad para la protección de los activos a nivel de infraestructura tecnológica.

La quinta es la arquitectura de componente en donde se identifican los estándares, protocolos y herramientas de seguridad que apalanquen la administración y monitoreo de la arquitectura de seguridad implementada.

Y por último la capa operativa cruza las cinco capas restantes y describe la seguridad en el funcionamiento diario de la organización.

Por otro lado, esta arquitectura de seguridad a su vez se articula con el modelo de seguridad y privacidad de la información, con el modelo de gestión de riesgos de seguridad digital y con el modelo de gobierno y gestión de TI del MRAE, con sus respectivas asociaciones tal como se evidencia en el modelo conceptual.

3. Lineamientos

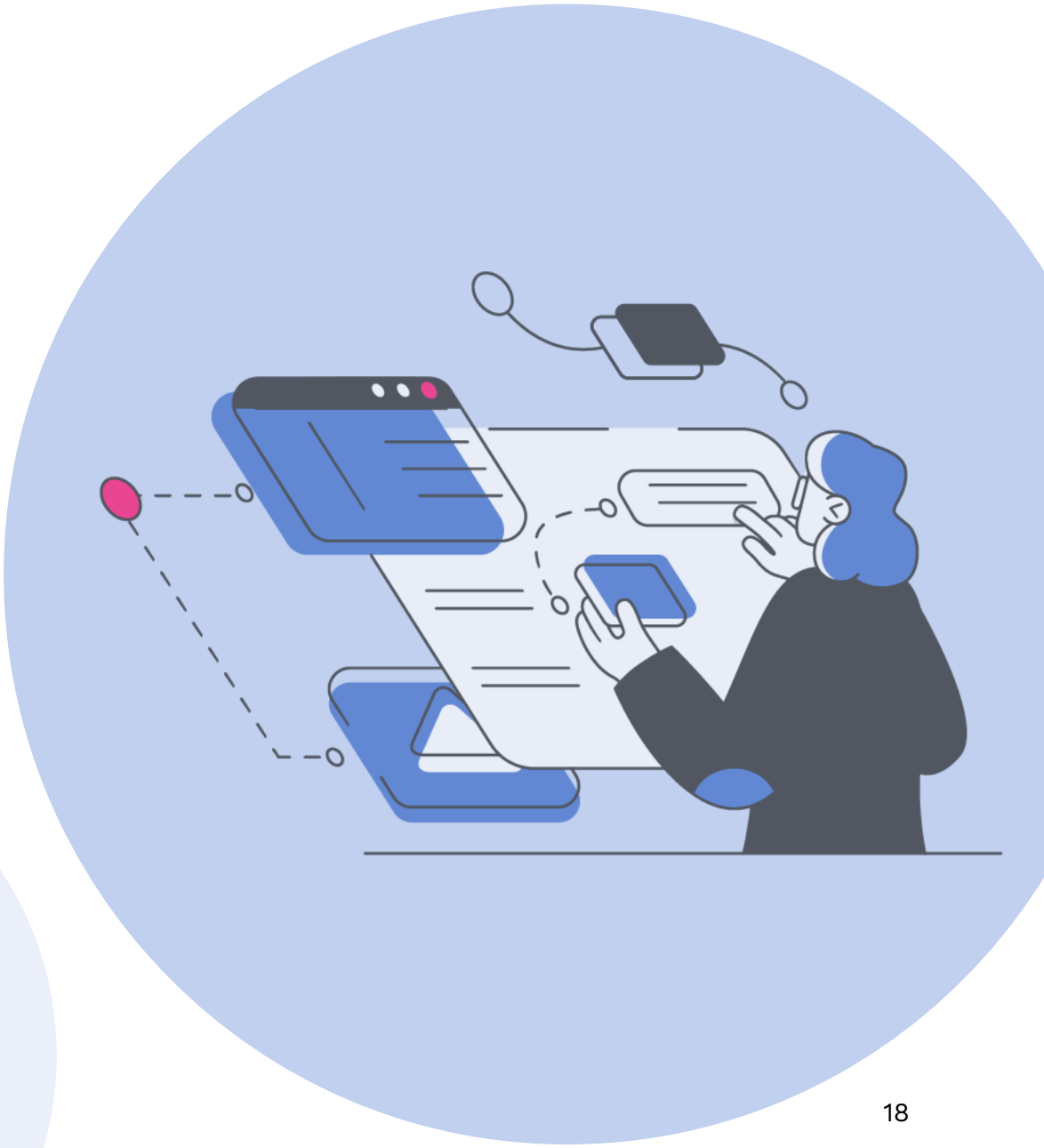


A continuación, encontraremos los lineamientos asociados a la arquitectura de seguridad y una breve descripción de los mismos para dar cumplimiento.

CÓDIGO	NOMBRE	DESCRIPCIÓN
MAE.LI.AS.01	Catálogo de servicios de seguridad de la información y ciberseguridad	Las entidades de la administración pública deben contar con un catálogo de servicios de seguridad que comprende una lista de servicios que proporcionan e identifican funciones específicas de seguridad para los sistemas de información y una lista de servicios institucionales relacionados con seguridad de la información y ciberseguridad.
MAE.LI.AS.02	Análisis de impacto del negocio	Las entidades de la administración pública deben realizar el análisis de impacto de negocio para minimizar los riesgos de indisponibilidad de los servicios e infraestructuras de TI, que afecten las operaciones regulares de las organizaciones. Este análisis debe ser incorporado en el diseño de la o las arquitecturas de seguridad y formar parte del sistema de gestión de riesgos y ser utilizado como mecanismo de control para ejecutar tareas de monitoreo de crisis, planes de contingencia, capacidad de marcha atrás y prevención y atención de emergencias.
MAE.LI.AS.03	Arquitectura de Seguridad	Las entidades de la administración pública deben definir, evolucionar y aplicar una arquitectura de seguridad sobre la infraestructura tecnológica, los sistemas de información y los datos durante la ejecución de los ejercicios de arquitectura empresarial
MAE.LI.AS.04	Ciberseguridad	Las entidades de administración pública deben diseñar los controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la información identificados durante la ejecución de los ejercicios de arquitectura empresarial.

Tabla 3. Lineamientos Arquitectura de Seguridad. Fuente: Propia

4. Etapas



En esta sesión de la guía se describen las etapas que se desarrollan para definir la arquitectura de seguridad y se dan recomendaciones para afrontar el desarrollo del ejercicio como parte de la definición de la arquitectura empresarial.

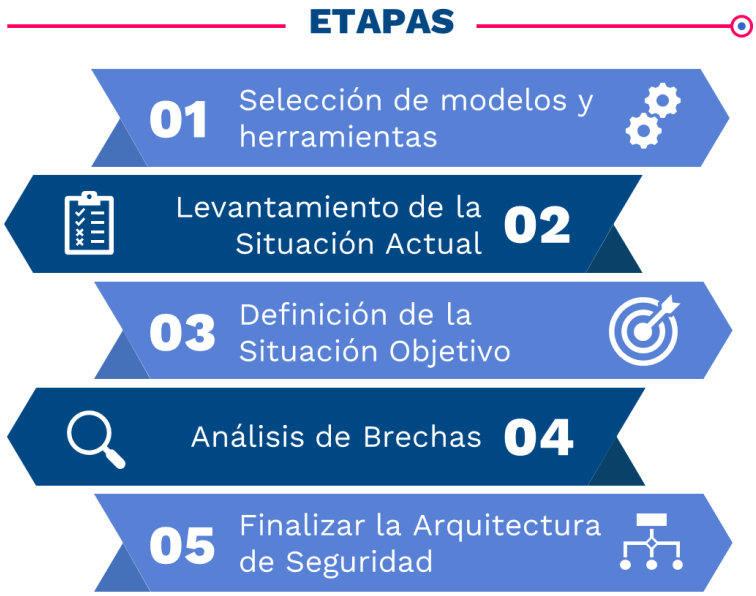


Ilustración 6. Etapas de definición de la Arquitectura de Seguridad. Fuente: Propia

4.1. Selección de Modelos y Herramientas

En esta etapa, se seleccionan los modelos de la industria, marcos de buenas prácticas, herramientas, artefactos, etc., que se usarán como parte de la definición de la arquitectura de seguridad.

Con base en las necesidades planteadas para el ejercicio de arquitectura empresarial, la arquitectura institucional definida y las preocupaciones de los interesados, se debe seleccionar todo lo que se considere útil y adecuado para apoyar o facilitar la correcta definición de la arquitectura; algunos ejemplos de listan a continuación.

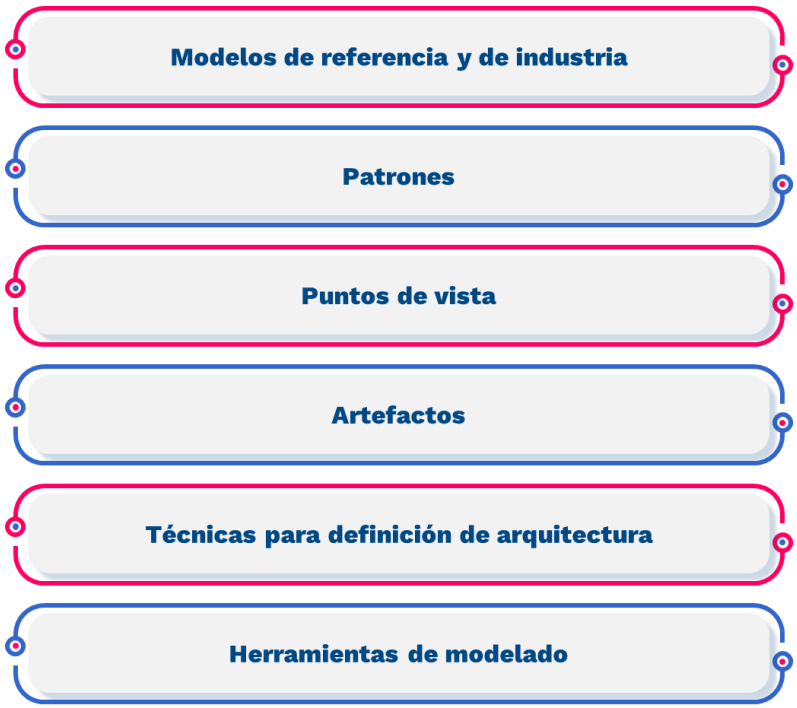


Ilustración 7. Ejemplos de modelos y herramientas. Fuente: Propia

Es clave en esta etapa consultar el repositorio de arquitectura empresarial de la entidad e identificar todos los artefactos, modelos o herramientas que se encuentren disponibles y que faciliten la definición de la arquitectura de seguridad. Si el repositorio de arquitectura empresarial es inicial, siempre debe indagarse por modelos probados, estándares o herramientas que puedan facilitar la definición de la arquitectura y mejorar su calidad.

Es posible que algunas vistas requeridas por los interesados no se encuentren en modelos existentes, en este caso, debería tomarse algún modelo o vista (según sea el caso) y complementarlo o simplemente definir uno desde cero, siempre pensando en que pueda cubrir la preocupación manifestada por el interesado o los interesados.

4.1.1. Estándares y mejores prácticas

En el Capítulo 8 de esta guía (Estándares y Mejores prácticas), se encuentran listadas una serie de marcos, prácticas probadas y estándares relacionados con la definición de arquitecturas de seguridad.

4.1.2. Herramientas

Existen gran cantidad de herramientas que facilitan la documentación y/o diagramación de la arquitectura de seguridad, ejemplos pueden ser: herramientas de modelado de componentes de seguridad y Caja de herramientas MinTIC.

4.2. Levantamiento de la Situación Actual

Para la situación actual se debe realizar el levantamiento de la arquitectura conceptual, lógica y física.

Vista conceptual de seguridad: en esta vista se define el contexto interno y externo regulatorio para los procesos clave identificados en una etapa previa al ejercicio, así como los activos de información más relevantes para cada proceso. Para esto definir:

a) **Catálogo de regulación:** el catálogo de regulación representa el consolidado de Leyes, Decretos y CONPES recopilados del análisis del contexto regulatorio de la entidad en materia de Seguridad y Privacidad de la Información.

b) **Catálogo de Políticas de Seguridad:** el catálogo de políticas de seguridad muestra el consolidado de directrices emitidas y aprobadas en materia de Seguridad de la Información.

c) **Catálogo de activos de información:** se relacionan los activos de información más relevantes para cada proceso en el alcance del ejercicio.

Vista lógica de seguridad: se identifican los servicios y componentes lógicos de seguridad para los procesos claves, así como el resultado del análisis de riesgos a los principales contenedores de información identificados en los procesos del alcance.

a) **Servicios de Seguridad:** se identifican los servicios de seguridad en aplicaciones e infraestructura tecnológica.

b) **Componentes de Seguridad:** en esta sección se representan los componentes de seguridad actuales en el contexto para los procesos que están involucrados en el alcance del ejercicio.

c) Matriz de Riesgos: la matriz de riesgos de seguridad representa una vista a alto nivel de los riesgos más críticos identificados para los sistemas de información de los procesos clave para el ejercicio.

Vista física de seguridad: en esta vista se presentan las tecnologías de seguridad que ofrecen servicios de seguridad informática a los sistemas de información identificados en el dominio de sistemas de información y la infraestructura tecnológica que utiliza.

a) **Catálogo de Tecnologías de Seguridad:** El catálogo de tecnologías de seguridad representa las tecnologías específicas por ámbito de seguridad con las cuales cuenta la entidad actualmente.

b) **Diagrama de zonas de seguridad y comunicaciones:** Esta vista de seguridad tiene como objetivo evidenciar los segmentos o zonas de red en una agrupación lógica funcional.

4.3. Definición de la Situación Objetivo

En la arquitectura de seguridad objetivo se definen los lineamientos, componentes y servicios que requiere la entidad para la gestión de la seguridad de la información y seguridad informática. Basados en las preocupaciones institucionales relacionadas con este ámbito, es necesario definir los requerimientos de seguridad para los sistemas de información (datos y aplicaciones) y la tecnología que soportarán los procesos de que claves identificados que requieran aseguramiento.

Desarrollo de la Arquitectura de Seguridad: Para el desarrollo de la Arquitectura de Seguridad iniciamos con el Perfil de Atributos de Negocio o Business Attribute Profile (BAP) en este caso atributos institucionales, identificando los principales motivadores de la entidad en materia de seguridad, descritos o esperados a través del Plan Estratégico Institucional, el Plan Estratégico de TI o el Plan de Transformación Digital de la entidad.

A continuación, se relacionan los atributos propuestos por SABSA con el fin de que la entidad defina con cuales se identifica.

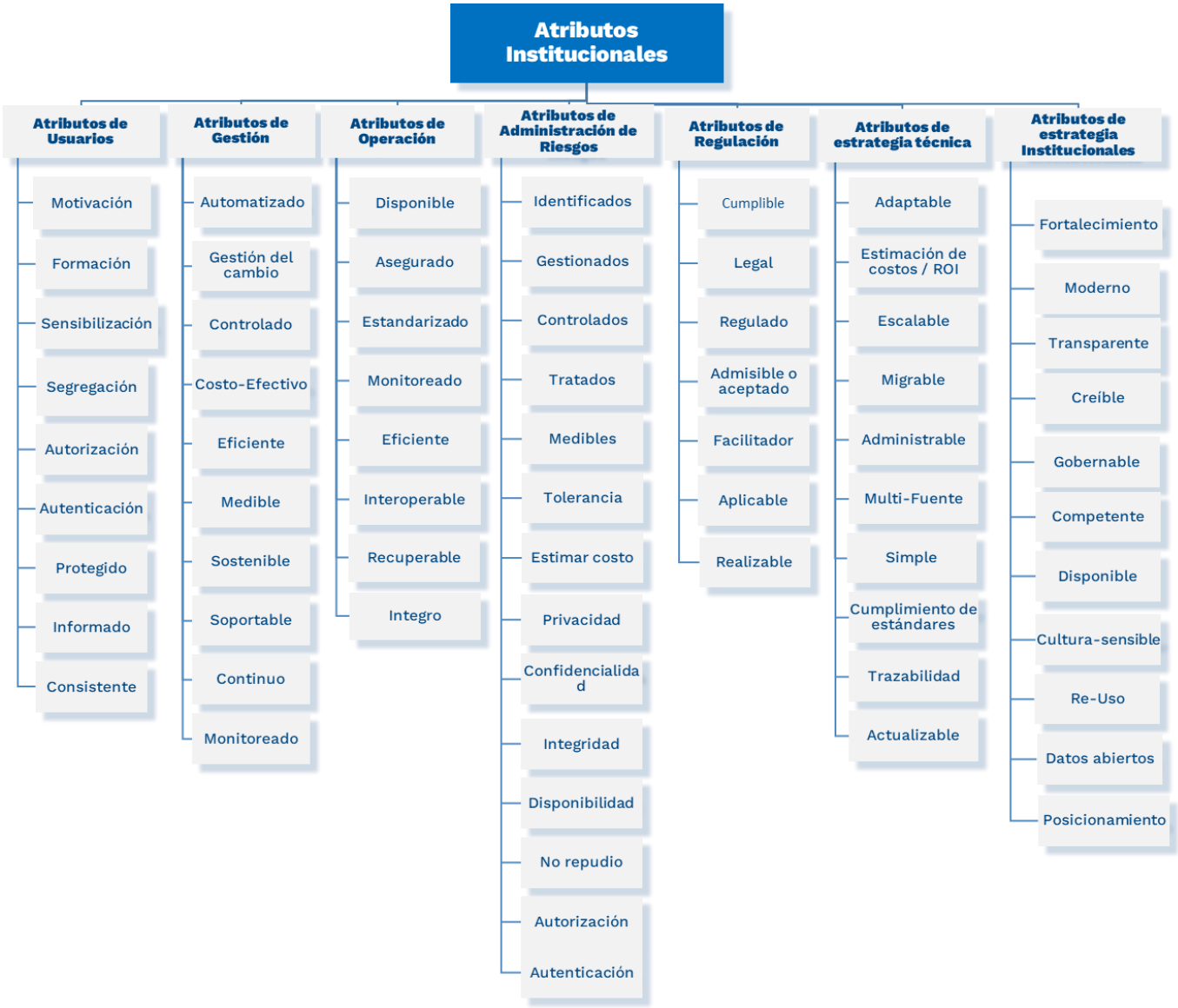


Ilustración 8. Diagrama de Atributos Institucionales. Fuente: SABSA

- Contextual = Vista de la capa empresarial. Comprender los requisitos institucionales (RI) de las partes interesadas
- Conceptual = Vista de capa de arquitectura. Diseño conceptual para cumplir con BR y estrategia de diseño.
- Lógica = Vista de capa de diseño. Entrega de “servicios” e “información” para cumplir con el concepto.
- Física = Vista de capa de construcción. Entrega de elementos tangibles para apoyar los servicios lógicos.
- Componente = Vista de comerciante. Hardware, herramientas y estándares para entregar el diseño físico.

- Gestión de servicios = vista Administrador de servicios. Cómo gestionamos la arquitectura.

4.3.1. Arquitectura contextual

Se deben identificar los activos de información institucionales más relevante para el o los procesos, tales como, información, software, hardware, personas, físicos, de la entidad en materia de seguridad, a partir de la declaración de:

- La misión y visión de la entidad
- La Estrategia Institucional actual
- Catálogo de requerimientos Regulatorios en materia de seguridad
- Motivadores institucionales o impulsores institucionales identificados en la entidad
- Programa de Fortalecimiento Institucional de la entidad
- Marco de arquitectura empresarial del MINTIC
- Modelo de Arquitectura empresarial

La arquitectura de seguridad contextual se ocupa de:

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
La institucional	Modelo de riesgo empresarial	Modelo de proceso empresarial	Organización y relaciones empresarial	Geografía empresarial	Dependencias del tiempo de la institución

Tabla 4. Vista contextual. Fuente: SABSA

4.3.2. Arquitectura conceptual

La vista de la arquitectura Conceptual se desarrolla desde la perspectiva de las dependencias claves identificadas previamente para abordar el ejercicio de arquitectura. En este nivel encontramos los atributos específicos en seguridad que quiere lograr la entidad en materia de seguridad y que deben ser aplicables a todos los activos identificados.

Una vez identificados estos atributos, se definieron los dominios de control que debe adoptar la entidad para mitigar los riesgos identificados, y se establecieron los ciclos de vida o plazos y los recursos involucrados. La arquitectura de seguridad conceptual se ocupa de:

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Perfil de atributos institucionales	Objetivos de control	Estrategias de seguridad y estratificación arquitectónica	Modelo de entidad de seguridad y marco de confianza	Modelo de dominio de seguridad	Duración y plazos relacionados con la seguridad

Tabla 5. Vista conceptual. Fuente: SABSA.

4.3.3. Arquitectura lógica

La vista de la arquitectura Lógica se desarrolla desde la perspectiva de las Gerencias y Coordinaciones de la entidad. Como fuentes para el análisis se cuenta con los principios de seguridad establecidos dentro del marco de Arquitectura empresarial y los requerimientos mandatorios para la implementación del Modelo de seguridad y privacidad de la información. La arquitectura de seguridad lógica se ocupa de:

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Modelo de información de la institución	Políticas de seguridad	Servicios de seguridad	Esquema de entidad y perfiles de privilegios	Asociaciones y definiciones de dominio de seguridad	Ciclo de procesamiento de seguridad

Tabla 6. Vista lógica. Fuente: SABSA.

4.3.4. Arquitectura física

La vista de la arquitectura física contempla al implementador, que hace referencia al profesional que puede tomar las descripciones lógicas y los diagramas y convertirlos en un modelo tecnológico que se puede utilizar para la infraestructura tecnológica. El papel del implementador es elegir y ensamblar los elementos físicos que harán que el diseño lógico cobre vida. Por lo tanto, esta vista también se conoce como arquitectura de seguridad física. En el mundo de los sistemas de información institucional, el diseñador produce un conjunto de abstracciones lógicas que describen el sistema que se va a construir. Estos deben convertirse en un modelo de arquitectura de seguridad física que describa el modelo de tecnología real y especifique el diseño detallado de los diversos componentes del sistema. Los servicios de seguridad lógica se expresan ahora en términos de los mecanismos de seguridad física y los servidores que se utilizarán para prestar estos servicios. La arquitectura de seguridad física se ocupa de:

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Modelo de datos institucional	Normas, prácticas y procedimientos de seguridad	Mecanismos de seguridad	Usuarios, aplicaciones e interfaz de usuario	Infraestructura de red y plataforma	Ejecución de la estructura de control

Tabla 7. Vista física. Fuente: SABSA.

4.3.5. Arquitectura de componente

El implementador necesita ensamblar e instalar una serie de productos de proveedores especializados y un equipo con las habilidades de integración para unir estos productos durante la implementación del diseño.

Cada uno de los instaladores e integradores es el equivalente a un proveedor, que trabaja con productos especializados y componentes del sistema. Algunas de estas "operaciones" están relacionadas con el hardware, otras con el software y otras con el servicio. Los proveedores trabajan con una serie de componentes que son elementos de hardware, elementos de software y especificaciones y estándares de interfaz. Por lo tanto, esta capa del modelo arquitectónico también se denomina arquitectura de seguridad de componentes. La arquitectura de seguridad de componente se ocupa de:

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Estructuras de datos detalladas	Estándares de seguridad	Productos y herramientas de seguridad	Identidades, funciones, acciones y ACL	Procesos, nodos, direcciones y protocolos	Cronograma y secuenciación de los pasos de seguridad

Tabla 8. Vista de componente. Fuente: SABSA.

4.3.6. Arquitectura operacional

En el ámbito de los sistemas de información, la arquitectura de gestión de servicios se ocupa de las operaciones de sistemas clásicos y el trabajo de gestión de servicios. Aquí, el foco de atención está solo en las partes de ese trabajo relacionadas con la seguridad. La arquitectura de gestión de servicios de seguridad se ocupa de lo siguiente:

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Garantía de continuidad operativa	Gestión de riesgo operacional	Gestión y soporte de servicios de seguridad	Gestión y soporte de aplicaciones y usuarios	Seguridad de sitios y plataformas	Programa de operaciones de seguridad

Tabla 9. Vista operacional. Fuente: SABSA.

4.4.Análisis de Brechas

Es necesario realizar para cada dominio de arquitectura un análisis de las capacidades actuales frente a las de la arquitectura objetivo con el fin de determinar las brechas requeridas para alcanzar la arquitectura destino. Se genera una propuesta de componentes candidatos que permiten ir cubriendo las brechas a través de procesos, servicios, componentes de aplicación, de tecnología y seguridad que responden en igual medida a las capacidades y requerimientos de arquitectura objetivo descrito.

Desde el punto de vista de seguridad se deben plantear componentes para la gestión de la continuidad del servicio, monitoreo de infraestructura, aplicaciones y seguridad, así como, componentes de gestión de accesos y cifrado y establecimiento de las políticas de seguridad y privacidad de la información.

4.4.1. Pasos para desarrollar el análisis de brechas

- **Paso 1:** Emplear la herramienta del análisis de brecha que tiene en cuenta los procesos, actividades o tareas. (diseñar una matriz que lo contenga
- **Paso 2:** Insertar los procesos, actividades o tareas que se deben eliminar y las nuevas que la entidad debe adoptar.
- **Paso 3:** Indicar qué procesos, actividades o tareas deben mantenerse o modificarse.
- **Paso 4:** Por cada decisión que se ha tomado en el análisis se debe identificar como una brecha.
- **Paso 5:** Documentar las brechas identificadas teniendo en cuenta el nombre, descripción y el motivador misional que soporta.
- **Paso 6:** Asociar los componentes de solución de la arquitectura objetivo con las brechas que se cierran con la implementación del componente respectivo.
- **Paso 7:** Estimar el esfuerzo, la duración y los recursos financieros para cada componente de solución.
- **Paso 8:** Priorizar los componentes de solución a partir de criterios establecidos por la institución.
- **Paso 9:** Actualizar el repositorio de Arquitectura Empresarial.

A continuación, se muestra un ejemplo de cómo debería verse la matriz:

Arquitectura Objetivo / Arquitectura Actual	Componente de Seguridad 3: Gestión de riesgos	Componente de Seguridad 2: Gestión de activos de información	Componente de Seguridad 4: tratamiento de documentación electrónica	Componente de Seguridad Eliminado
Componente de Seguridad 1: controles de acceso débiles				Eliminar
Componente de Seguridad 2: Gestión de activos de información		Modificar		
Componente de Seguridad 3: Gestión de riesgos	Mantener			
Componente de Seguridad Nuevo			Crear	

Tabla 10. Matriz – Análisis de brechas. Fuente: propia.

En el ejemplo de la matriz podemos ver que el componente de seguridad 1 se elimina, el componente de seguridad 2 se modifica ya que hay una brecha entre la situación y objetivo, el componente de seguridad 3 se mantiene quiere decir que no sufre cambios y por el componente de seguridad 4 se crea.

4.4.2. Consolidación de brechas (catálogo de brechas)

Una vez construida la matriz, se deben caracterizar las brechas encontradas como parte del análisis; este catálogo de brechas puede ser compartido para toda la definición de arquitectura y entrará a hacer parte del Repositorio de Arquitectura Empresarial; debe incluir como mínimo los siguientes campos:

Campo	Descripción
Código de la brecha	Identificador de la brecha (se recomienda usar codificación que permita identificar las brechas por dominio)
Dominio	dominio de arquitectura empresarial a la que pertenece la brecha
Tipo de Intervención	Debe seleccionar entre: crear, modificar o eliminar
Nombre	nombre que se le da a la brecha
Descripción	descripción de la brecha

Tabla 11. Caracterización de las brechas.

A continuación, se relaciona un ejemplo de las brechas consolidadas en los componentes de seguridad.

Código de la brecha	Dominio	Tipo de intervención	Nombre	Descripción
BS1	Seguridad	Eliminar	Brecha de seguridad1	
BS2	Seguridad	Modificar	Brecha de seguridad2	
BS3	Seguridad	Mantener	Brecha de seguridad3	
BS4	Seguridad	Crear	Brecha de seguridad4	

Tabla 12. Ejemplo catálogo de brechas.

4.5. Finalizar la arquitectura de seguridad

Antes de finalizar la definición de la arquitectura de seguridad, es importante realizar una serie de pasos que garanticen la correcta definición de la arquitectura, se espera que se desarrollen estas actividades conscientemente y se documenten de forma sencilla.

4.5.1. Definir Componentes Candidatos de Seguridad para el Mapa de Ruta

Finalizado el análisis de brechas, debe definirse una propuesta inicial de los componentes que harán parte del mapa de ruta de la arquitectura empresarial; con la construcción de este mapa de ruta (enfocado solamente a la arquitectura de seguridad), se busca cerrar las brechas identificadas en la etapa anterior. Esta definición inicial (borrador), será útil para cuando se empiece a construir un mapa de ruta consolidado.

ID	Nombre de Componente	Descripción	Brechas asociadas	Motivador
CS1	Componente de seguridad1		BS1- BS4	
CS2	Componente de seguridad2		BS2	
CS3	Componente de seguridad3		BS3	
CS4	Componente de seguridad4		BS2- BS4	

Tabla 13. Matriz de componentes candidatos de seguridad.

4.5.2. Validar el impacto sobre la arquitectura empresarial

Definida la situación objetivo, es importante validar como la arquitectura de seguridad impacta a la arquitectura empresarial y viceversa, esto incluye, entre otros:

- Impacto de la arquitectura de seguridad sobre otros proyectos de la entidad.
- Impacto de la arquitectura de seguridad a la hora de elegir un producto de un proveedor respecto a otro.
- Impacto de la arquitectura de seguridad sobre otras arquitecturas previamente definidas (sea que se encuentren implementadas o en proceso de implementación).
- Impacto la arquitectura de seguridad al momento de implementar un componente de seguridad de acuerdo al caso y necesidades de la entidad si decide comprarlo, o adquirir un servicio on-premise o infraestructura como servicio (IaaS) o Plataforma como servicio (PaaS), entre otros.
- Impacto de otras arquitecturas o proyectos sobre la arquitectura de seguridad definida.
- Posibilidad de que la entidad implemente efectivamente la arquitectura de seguridad definida.
- Factores externos que puedan afectar la implementación de la arquitectura.
- Restricciones de la arquitectura tecnológica para implementar la arquitectura de seguridad.

4.5.3. Realizar una revisión formal con los interesados

Deben realizarse sesiones de trabajo donde se explique a los interesados cómo fueron abordadas sus preocupaciones relacionadas con la arquitectura de seguridad. Es muy importante que todos los interesados tengan clara la situación objetivo, las decisiones que se tomaron y por qué se tomaron; porque una vez inicie la implementación de los proyectos definidos en el mapa de ruta de la arquitectura empresarial, el conocimiento por parte de los interesados de la propuesta puede conllevar al fracaso en la implementación de la arquitectura de seguridad definida.

5. Roles

En el desarrollo de las actividades para definir y gestionar la Arquitectura de Seguridad participan los siguientes roles:

Rol	Responsabilidades
Alta dirección	- La arquitectura de seguridad no se puede lograr a menos que los principales responsables de la toma de decisiones estén de su lado.
Arquitecto Empresarial	- Proporcionar orientación a la entidad sobre los modelos y herramientas más apropiados para desarrollar su ejercicio de Arquitectura Empresarial. - Mantener la arquitectura alineada al Marco de Referencia de Arquitectura Empresarial. - Gestionar el ejercicio de Arquitectura Empresarial, garantizando que se mantenga una coherencia al avanzar sobre la integración de los demás dominios con el de seguridad.
Arquitecto de Seguridad	- Adquirir una comprensión completa de la tecnología y los sistemas de información de la entidad. - Planificación, investigación y diseño de arquitecturas de seguridad robustas para cada proyecto de TI que enfrenta la entidad. - Realizar pruebas de vulnerabilidad, análisis de riesgo y evaluaciones de seguridad. - Responsable de estándares de seguridad, sistemas de seguridad y protocolos de autenticación. -Preparación para estimaciones de costos e identificación de problemas de integración con sistemas.

Tabla 14. Roles en Arquitectura de Seguridad.

6. Caso práctico

Esta sección de la guía hará parte del anexo de casos de estudio de AE del MAE. En este caso de estudio se abordará un municipio, es una organización fundamental para el desarrollo de la comunidad. Su finalidad es brindar servicios que aseguren la participación en el progreso económico, social y cultural de los ciudadanos. Para favorecer estas tareas y apoyar su gestión, en los últimos años, los municipios han incorporado controles de seguridad en las tecnologías de la información y comunicación como una estrategia eficaz. Sin embargo, el nivel de adopción de estas herramientas no es homogéneo entre municipios, lo que puede implicar grandes diferencias en la forma en que éstos entregan sus servicios a la ciudadanía. Para lograr una visión integral es necesario adoptar la arquitectura empresarial como instrumento para la identificación de esos requerimientos.

6.1. Contexto de Arquitectura Institucional.

Durante el ejercicio desarrollo de la situación actual del dominio de arquitectura institucional se identificó que el acalde del Municipio de San Marcos junto que el secretario de Cultura, Recreación y Deporte han definido que uno de los pilares fundamentales del plan de desarrollo es la promoción y gestión de las actividades culturales y deportivas que contribuyan al esparcimiento, convivencia, integración de los próximos años. Sin embargo, aunque cuentan con un plan de cultura, recreación y deporte en el que se contemplan actividades para diferentes intereses, han notado que no se logra la participación y cobertura planeadas y que no cuentan con la información suficiente para tomar decisiones e implementar acciones de mejora. Además de esto, los ciudadanos manifiestan que el proceso de inscripción a las actividades es engorroso, ya que se lleva a cabo de manera presencial en las instalaciones de la alcaldía. Por otro lado, los instructores responsables del desarrollo de las actividades no cuentan con herramientas eficientes para registrar la participación de manera efectiva de los beneficiarios.

Por lo anterior, se identifica que la Alcaldía del Municipio de San Marcos tiene como motivador institucional para el alcance de este ejercicio de arquitectura: “Incrementar la participación de los ciudadanos en actividades culturales, recreativas y deportivas”.

En la definición de la arquitectura institucional se determinó que el proceso a abordar es el de Gestión de cultura, recreación y deporte, en el cual requieren contar ejecutar las siguientes actividades:

- Gestionar las actividades culturales, recreativas o deportivas.
- Publicar calendario de actividades culturales, recreativas y deportivas.
- Registrar instructores.
- Registrar inscripción y participación a actividades culturales, recreativas y deportivas.

6.2. Levantamiento de la situación actual

Vista conceptual de seguridad: en esta vista se define el contexto interno y externo regulatorio para los procesos clave identificados en una etapa previa al ejercicio, así como los activos de información más relevantes para cada proceso. Para esto definir:
Catálogo de regulación: el catálogo de regulación representa el consolidado de Leyes, Decretos y CONPES recopilados del análisis del contexto regulatorio de la entidad en materia de Seguridad y Privacidad de la Información.

Año	ID del documento	Nombre	Descripción
1997	Ley 397 de 1997	Ley General de Cultura	"Por la cual se desarrollan los artículos 70, 71 y 72 y demás artículos concordantes de la Constitución Política y se dictan normas sobre patrimonio cultural, fomentos y estímulos a la cultura, se crea el Ministerio de la Cultura y se trasladan algunas dependencias"
2012	Ley Estatutaria 1581 de 2012	Protección De Datos Personales	Es una ley que complementa la regulación vigente para la protección del derecho fundamental que tienen todas las personas naturales a autorizar la información personal que es almacenada en bases de datos o archivos, así como su posterior actualización y rectificación. Esta ley se aplica a las bases de datos o archivos que contengan datos personales de personas naturales.
2019	CONPES 02 de 2019	CONPES 02 de 2019	Generar un entorno propicio para el desarrollo cultural, social y económico de la ciudad, a través del fomento, la promoción y el incentivo de la Economía Cultural y Creativa, en el marco del reconocimiento, el respeto y la promoción de los derechos y libertades culturales, y de la Agenda Bogotá Cultural 2038.
2015	Decreto XXXX de 2015(ejemplo)		Por el cual se adopta la Política Pública de Deporte, Recreación, Actividad Física, Parques y Escenarios para el municipio

Tabla 15. Catálogo de regulación.

Catálogo de Políticas de Seguridad: el catálogo de políticas de seguridad muestra el consolidado de directrices emitidas y aprobadas en materia de Seguridad de la Información.

Identificador	Nombre	Descripción/Alcance
SGSI –XXX- XXX	Política de Seguridad y Privacidad de la Información	Declaración de la Política de Seguridad y Privacidad de la Información de la Alcaldía Municipal de San Marcos
SGSI-XXX-XXX-XXX	Política de tratamiento de datos personales	Declaración de la Política de tratamiento de datos personales de la de la Alcaldía Municipal de San Marcos • Principios para el Tratamiento • Responsables del Tratamiento • Encargados del Tratamiento
SGSI-XXX-XXX	Manual de políticas específicas de seguridad de la información	Declaración de las políticas específicas de seguridad de la información de la de la Alcaldía Municipal de San Marcos • Políticas de dispositivos móviles y teletrabajo • Políticas de seguridad de los recursos humanos • Políticas gestión de activos • Políticas gestión de medios de almacenamiento • Políticas control de acceso • Políticas seguridad física y del entorno • Políticas seguridad en las operaciones • Políticas seguridad de las comunicaciones • Políticas adquisición, desarrollo y mantenimiento de sistemas • Políticas relaciones con los proveedores • Políticas gestión de incidentes • Políticas cumplimiento

Tabla 16. Catálogo de Políticas de Seguridad.

Catálogo de activos de información: se relacionan los activos de información más relevantes para el o los procesos.

Identificador	Nombre activo de información	Proceso	Nombre del activo contenedor de la información (hardware-software –físico)
XX	Actas del Comité Primario	Gestión de Cultura, Recreación y Turismo	Documento físico Repositorio Digital

Tabla 17. Catálogo de activos de información.

Vista lógica de seguridad: se identifican los servicios y componentes lógicos de seguridad para los procesos claves, así como el resultado del análisis de riesgos a los principales contenedores de información identificados en los procesos del alcance.

a) Servicios de Seguridad: se identifican los servicios de seguridad en aplicaciones e infraestructura tecnológica.
b) Componentes de Seguridad: en esta sección se representan los componentes de seguridad actuales en el contexto para el o los procesos claves para el ejercicio.
c) Matriz de Riesgos: la matriz de riesgos de seguridad representa una vista a alto nivel de los riesgos más críticos identificados para los sistemas de información de los procesos clave para el ejercicio.

Identificador	Servicio	Descripción	Responsable
ST_XX	Configurar políticas de seguridad de Firewall	Configurar políticas de seguridad de Firewall	Técnico de TI
ST_XX	Configurar antivirus en equipos terminales	Configurar antivirus en equipos terminales	Técnico de TI

Tabla 18. Servicios de seguridad.

De los anteriores servicios, el proceso de Gestión de Cultura, Recreación y Turismo consume directamente los servicios relacionados con Filtrado Web y Antivirus, los cuales están activos por defecto en las estaciones de trabajo y portátiles para minimizar riesgos relacionados con la navegación en internet e infección de virus y/o malware.

No se encontró un catálogo de servicios documentado o formalizado relacionado con seguridad de la información en la de la Alcaldía Municipal de San Marcos, se encontraron servicios de TI.

Componentes de Seguridad: en esta sección se representan los componentes de seguridad actuales en el contexto para el o los procesos claves para el ejercicio.

IDENTIFICADOR	COMPONENTE	DESCRIPCIÓN	ÁREA DE SEGURIDAD	SERVICIOS/ RESPONSABLE
XXXX	Política de Seguridad	Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y reglamentos pertinentes.	Autenticación Autorización Auditoría Aseguramiento Disponibilidad Protección de Activos Administración Gestión del Riesgo Cumplimiento Administración de los Datos	TI

Tabla 19. Componentes de seguridad.

Matriz de Riesgos: la matriz de riesgos de seguridad representa una vista a alto nivel de los riesgos más críticos identificados para los sistemas de información del proceso analizado.

*Relacionar la matriz de riesgos de la entidad en donde se asocian riesgos de seguridad al proceso analizado, de acuerdo con la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas del DAFP.
Vista física de seguridad: en esta vista se presentan las tecnologías de seguridad que ofrecen servicios de seguridad informática a los sistemas de información identificados en el dominio de aplicaciones y su infraestructura tecnológica.

a) Catálogo de Tecnologías de Seguridad: El catálogo de tecnologías de seguridad representa las tecnologías específicas por ámbito de seguridad con las cuales cuenta la entidad actualmente.

CATEGORÍA	GRUPO FUNCIONAL	TECNOLOGÍA	¿ Cuenta con la Tecnología?
Protección Perimetral	Navegación	Antivirus	SI
		Filtrado de contenido	NO
	Correo	Antivirus y protección anti-spam	SI
	Detección y prevención de Intrusiones	IPS en línea	NO
		IDS	NO
	VPN	IPSec Site to Site	NO
		SSL y IPSec acceso puestos	SI
		IPSec acceso dispositivos	NO
	Firewall	Firewall de Red	SI
		Firewall de Aplicaciones - WAF	NO

Tabla 20. Catálogo de Tecnologías de Seguridad.

b) Diagrama de zonas de seguridad y comunicaciones: Esta vista de seguridad tiene como objetivo evidenciar los segmentos o zonas de red en una agrupación lógica funcional.

- INTERNET: En esta zona se encuentran los accesos y servicios de clientes VPN, conexiones virtuales, aplicaciones móviles o servicios en la nube.
- WAN: En esta zona se encuentra la segmentación por dependencias y la red inalámbrica.

Ilustración 9. Diagrama de zonas de seguridad y comunicaciones.

6.3. Levantamiento de la situación Objetivo

A continuación, se presenta el resultado de la vista Contextual de la Alcaldía Municipal de San Marcos

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Imagen y Reputación **Innovación** **Accesibilidad y cobertura**	Riesgo reputacional Riesgo Tecnológico Riesgo Operativo Descentralización de la información Ausencia de lineamientos o buenas prácticas de seguridad	Gestión de riesgos de seguridad Plan estratégico de seguridad	Ciudadanía Funcionarios y contratistas	Colombia Zona en la que se encuentra ubicado el municipio	Plan estratégico versión vigente Plan de Fortalecimiento Institucional

Tabla 21.Vista Contextual.

A continuación, se presenta el resultado de la vista Conceptual de la Alcaldía Municipal de San Marcos

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Confidencialidad de la información **Integridad de la información** **Disponibilidad de la Información**	MSPI Gestión de activos Ciclo de vida aplicativo y tecnológico Gestión de Seguridad Física Gestión de la continuidad de Negocio Cumplimiento Regulatorio	Estrategia de seguridad (Plan estratégico) Estrategia de seguridad tecnológica	Dependencias Propietarios y custodios de Activos Entes de control	Funcionarios Clientes Gobierno nacional Proveedores Entes de control	Marco de Arquitectura Empresarial Regulación Nacional en materia de seguridad vigente

Tabla 22.Vista conceptual.

A continuación, se presenta la vista lógica del marco de referencia para Alcaldía Municipal de San Marcos

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Gobierno de Datos **Gestión de la Innovación** **Gestión de la Tecnología**	Política de seguridad y privacidad Política Organización de la Seguridad Política Clasificación y responsabilidad de activos de información Política Ciclo de vida aplicativo y desarrollo seguro Políticas de Intercambio de información Política protección de datos personales Metodología de gestión de riesgos Plan de continuidad de Negocio	Conciencia y formación en seguridad Ciclos de vida de la información Gestión de roles e identidades Servicios de seguridad Autorización	Dependencias Responsable de seguridad de la información	Seguridad perimetral Seguridad en desarrollo Seguridad en Centro de cómputo principal Seguridad en portal Web	Ciclo de vida de los datos Ciclo de vida del aplicativo Ciclo de vida tecnológico

Tabla 23.Vista lógica.

A continuación, se presenta el resultado de la vista física para la Alcaldía del municipio de San Marcos.

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Modelamiento de Datos **Metadatos** **Gestión de información** **Estructurada y No estructurada** **Normalización** **Clasificación** **Seguridad y privacidad** **Áreas seguras** **Tecnologías de seguridad**	Sistema de gestión de seguridad (ISO 27000) Buenas prácticas en seguridad (NIST, SANS) Ley Estatutaria 1581 de 2012 Protección de datos personales Ley Estatutaria 1712 de 2014 Transparencia y del Derecho de Acceso a la Información Pública Nacional CONPES Ciberseguridad CONPES Seguridad Digital	Protección de Datos Personales Metodología de gestión de riesgos Arquitectura Orientada a Servicios Metodología de desarrollo seguro	Responsable de Seguridad Sistema de gestión de incidentes	Sistemas de información de la Alcaldía del Municipio de San Marcos Centro de datos	Definición de los controles Establecimiento del marco de gobierno Implantación de tecnologías de seguridad Definición de procedimientos y guías

Tabla 24.Vista física.

A continuación, se presenta el resultado de la vista de componente para la Alcaldía del Municipio de San Marcos

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Información confidencial **Información restringida** **Información Interna** **Información Pública**	Herramientas de gestión de riesgo Herramientas de control de riesgo Herramientas de análisis de riesgo Herramientas de control de cumplimiento Herramientas de auditoría	COBIT - Control Objectives for Information and related Technology ITIL - Information Technology Infrastructure Library COSO - Marco de control interno empresarial ISO/IEC 27000-series – Estándares de seguridad ISO 22301 – Continuidad de Negocio	Gestor de Identidades Listas de acceso – ACLs Firmas digitales Responsable de seguridad de la información	USATI OSEI Centro de monitoreo Mesa de Soporte técnico	Soporte 7x24x365 Centro de datos principal Centro de datos

		BSIMM - Building Security In Maturity Model OWASP - Open Web Application Security Project SOA - Service-Oriented Architecture RBAC - Control de acceso basado en funciones			

Tabla 25.Vista de componente.

A continuación, se presenta el resultado de la vista operativa para la Alcaldía del Municipio de San Marcos

ACTIVOS (QUÉ)	MOTIVACIÓN (PORQUÉ)	PROCESO (CÓMO)	GENTE (QUIÉN)	UBICACIÓN (DÓNDE)	TIEMPO (CUÁNDO)
Sistemas de Monitoreo y alarma **Copias de respaldo**	Errores humanos intencionales y no intencionales Ingeniería social Accesos no autorizados Modificaciones intencionales y no intencionales de la información Fuga de información intencional y no intencional Caída o falla de servicios	Administración del control de acceso físico y lógico Planes de respaldo de la información Planes de contingencia y continuidad tecnológica Administración de los sistemas de seguridad perimetral Autorización transferencia de información Gestión de la Continuidad y Disponibilidad	Responsable de la información Custodio de la información Desarrolladores Administradores de Tecnología Mesa de ayuda Proveedores Administradores de sistemas de información Usuarios finales	Alcaldía del Municipio de San Marcos Portales Web de la Alcaldía	Durante todo el ciclo de vida de los procesos, datos, aplicaciones, tecnología y personas.

Tabla 26.Vista operativa.

6.4. Análisis de brechas

Se identifica que la entidad debe crear, modificar, mantener y eliminar los siguientes componentes de seguridad de la información y de ciberseguridad.

Arquitectura Objetivo	Gestión de riesgos de Seguridad	Sistema de gestión de seguridad	Concienciación y formación en seguridad	Componente de Seguridad Eliminado

Arquitectura Actual				
Concienciación y formación en seguridad			Mantener	
Gestión de riesgos de Seguridad	Modificar			
Política de copia de respaldo para servidores y equipos terminales críticos		Crear		
Política de copia de respaldo solo a equipos terminales				Eliminar

Tabla 27.Análisis de brechas.

7. Artefactos

A continuación, se relacionan los artefactos a desarrollar en el dominio de arquitectura de seguridad.

TIPO	NOMBRE	DESCRIPCIÓN
Catálogo	Catálogo de servicios de seguridad	El Catálogo de servicios de seguridad de servicios destinados a desarrollar las soluciones necesarias que lleven a conseguir un nivel de seguridad adecuado.
Catálogo	Catálogo de normatividad	El catálogo del entorno regulatorio representa el consolidado de Leyes, Decretos y CONPES recopilados del análisis del entorno regulatorio de la entidad en materia de Seguridad y Privacidad de la Información
Catálogo	Catálogo de políticas de seguridad	El catálogo de políticas representa el consolidado de directrices emitidas y aprobadas por la Dirección General en materia de Seguridad de la Información.
Catálogo	Catálogo de infraestructura de seguridad	El catálogo de infraestructura de seguridad representa el consolidado de controles de seguridad informática con los que cuenta la entidad
Matriz	Matriz de Roles y responsabilidades de ciberseguridad	Matriz en donde se identifican los roles y funciones definidos que intervienen las acciones encaminadas a proteger los activos.
Matriz	Matriz de riesgos de seguridad de la información	La matriz de riesgos de seguridad representa los riesgos más críticos a alto nivel, identificados para los componentes de información y sistemas de información.
Matriz	Matriz de roles y responsabilidades de protección de datos personales	Matriz en donde se identifican los roles y funciones definidos que intervienen las acciones encaminadas a proteger los datos personales consignados en una BD estructurada y no estructurada.
Matriz	Matriz de roles y responsabilidades de continuidad del negocio	Matriz en donde se identifican los roles y funciones definidos que intervienen las acciones encaminadas a la continuidad del negocio y recuperación tecnológica.
Diagrama	Diagrama de redes y comunicaciones	Esta vista de seguridad tiene como objetivo evidenciar los segmentos o zonas de red en una agrupación lógica funcional.
Diagrama	Diagrama de redes y comunicaciones asociadas a continuidad	Esta vista de seguridad tiene como objetivo evidenciar los segmentos o zonas de red de alta disponibilidad y redundancia en una agrupación lógica funcional
Diagrama	Diagrama de atributos institucionales	El diagrama de atributos institucionales tiene como fin definir y descomponer un conductor o motivador institucional de la entidad, en requisitos o atributos de seguridad, utilizando un enfoque basado en riesgos
Diagrama	Diagrama de componentes lógicos de seguridad	El diagrama de componentes lógicos de la institución, de datos y aplicaciones y de tecnología.

Tabla 28. Artefactos de Arquitectura de Seguridad.

8. Estándares y Mejores prácticas

TEMA	NOMBRE	DESCRIPCIÓN
Modelo	Modelo de seguridad y privacidad de la información y sus anexos.	La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos.
Seguridad de la información	ISO 27001:2013	Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI)
Seguridad de la información	NIST 800-53	Proporciona un catálogo de controles de seguridad y privacidad para todos los sistemas de información federales de EE. UU., excepto los relacionados con la seguridad nacional.
Ciberseguridad	ISO/IEC 27032_2012	Es una norma internacional de gestión de continuidad de negocio. ISO 22301 identifica los fundamentos de un Sistema de Gestión de la Continuidad de negocio, estableciendo el proceso, los principios y la terminología de gestión de continuidad de negocio.
Ciberseguridad	NIST 8259	El programa de ciberseguridad para IoT del NIST respalda la desarrollo y aplicación de estándares, pautas y herramientas relacionadas para mejorar la ciberseguridad de los dispositivos y los entornos en los que se implementan.
Ciberseguridad	Scaled Agile framework	Es un marco de para implementar prácticas ágiles que constituye un cúmulo de conocimientos que incluye instrucciones estructuradas sobre las funciones y responsabilidades, la forma de planificar y gestionar el trabajo, y los valores que hay que defender.
Protección de datos personales	ISO 27701:2019	Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Información de Privacidad (PIMS). Esta normativa se basa en los requisitos, controles y objetivos de la norma ISO 27001: Requisitos de Sistemas de Gestión de Seguridad de la Información (SGSI).
Protección de datos personales	The OECD Privacy Framework	Un enfoque en la implementación práctica de la protección de la privacidad a través de un enfoque basado en la gestión de riesgos, y la necesidad de abordar la dimensión global de la privacidad mediante una mejor interoperabilidad .
Protección de datos personales	Estándares de Protección de Datos Personales para los Estados Iberoamericanos 2017	Responde a las necesidades y exigencias nacionales e internacionales que demanda el derecho a la protección de datos personales, en una sociedad donde las tecnologías de la in-formación y del conocimiento cobran cada vez

		mayor relevancia en todos los quehaceres de la vida cotidiana
Continuidad	ISO 22301:2019	Es la última versión de la norma internacional para sistemas de gestión de la continuidad de negocio (SGCN) y proporciona un marco de buenas prácticas para ayudar a las organizaciones a gestionar eficazmente el impacto de una interrupción en su funcionamiento

Tabla 29. Estándares y Mejores Prácticas.