LOS LIBERTADORES
FUNDACIÓN UNIVERSITARIA

# PROPUESTA ARQUITECTURA DE SEGURIDAD PARA ORGANIZACIONES QUE UTILICEN LOS PRINCIPALES MODELOS DE SERVICIOS DE INFORMÁTICA EN LA NUBE

# SECURITY ARCHITECTURE PROPOSAL FOR ORGANIZATIONS THAT USE THE MAIN MODELS OF CLOUD COMPUTING SERVICES

**Evelin Pilar Díaz Rodríguez**

Ingeniera de Telecomunicaciones, Universidad Cooperativa de Colombia

epdiazr01@libertadores.edu.co

**John Alexander Pachón Pinzón**

Especialista de seguridad de la información e informática, Universidad Sergio Arboleda

John.pachon@escuelaing.edu.co

**Yenny Isabel Serrato Rodriguez**

Especialista en Seguridad de la Información, Universidad Sergio Arboleda

yiserrator@libertadores.edu.co

## Resumen

La finalidad de este artículo es mostrar al lector la identificación de diferentes dominios y artefactos que componen una arquitectura de seguridad de la información considerados por el autor, y que a su vez son esenciales para lograr una arquitectura robusta, que apalanque y logre una cultura y madurez de seguridad, especialmente en organizaciones donde el CORE de negocio utiliza modelos de servicio desplegados en la nube. La metodología utilizada partió de una

investigación de tipo exploratoria y método cualitativo enfocado en establecer una visión general del tema que sirva para una posterior investigación más profunda y detallada, con base a opiniones y experiencias vividas relacionadas, principalmente con los temas de seguridad de la información, se realizó el análisis obteniendo como resultado buenas prácticas expresadas en palabras (no datos numéricos). Como resultado se proponen en este documento 7 dominios que deberían conforma la arquitectura de seguridad planteada, integrando en cada uno de ellos los respectivos artefactos. En conclusión, el presente documento pretende evidenciar la importancia de contar con una arquitectura de seguridad a nivel empresarial, que permita establecer una articulación en los diferentes frentes y procesos de cualquier organización.

***Palabras clave:*** Gobierno, Planificación, Arquitectura, Seguridad, sinergia, organizaciones, Cloud, artefacto, dominio, apetito de riesgo

## Abstract

The purpose of this article is to show to the reader, the identification of different domains and artifacts that make up an information security architecture considered by the author, and at the same time, are essential to achieve a robust architecture that leverages and achieves a security culture and maturity, especially in organizations where the business CORE uses service models deployed in the cloud. The methodology used was based on an exploratory type of research and qualitative method focused on establishing an overview of the subject that will serve for a subsequent more in-depth and detailed research, based on opinions and experiences related mainly to information security issues, the analysis was carried out obtaining as a result good practices expressed in words (not numerical data). As a result, this document proposes 7 domains that should conform the proposed security architecture, integrating in each of them the respective artifacts. In conclusion, this document aims to demonstrate the importance of having a security architecture at the enterprise level, which allows to establish an articulation in the different fronts and processes of any organization.

***Keywords:*** Governance, Planning, Architecture, Security, synergy, organizations, Cloud, artifact, domain, risk appetite.

## I. Introducción

En la actualidad la seguridad de la información es considerada un conjunto de mecanismos cuyo objetivo es proteger y garantizar la confidencialidad, integridad y disponibilidad de la información, comúnmente mencionada como la Triada de seguridad. La mayoría de las organizaciones busca establecer medidas y controles tanto preventivos, como reactivos, con el objetivo de resguardar sus activos, sin proporcionar la adecuada importancia y sin definir metodologías claras, alcanzables y concretas, evitando materializar amenazas latentes.

Por otra parte, dentro de las diferentes estrategias que aplican las compañías para gestionar la Seguridad de la información se encuentra crear políticas y procedimientos, adquirir herramientas de monitoreo y realizar aseguramiento de su infraestructura, sin embargo, es importante que exista una Arquitectura de Seguridad que permita articular a toda la organización, integrando la misión y visión, macroprocesos, áreas consideradas críticas, herramientas, recursos, entre otros.

Al mismo tiempo, entre los errores más habituales de las organizaciones, está considerar que con migrar infraestructura o utilizar entornos y servicios Cloud se eliminarán todos los riesgos que afecten directa o indirectamente la seguridad de la información y es por ello que incurren en migraciones precipitadas, improvisadas, y sin enfocarse en la seguridad de sus activos y los datos que allí se almacenan. Lo anterior sin desconocer que los proveedores de servicio en nube ofrecen bastantes beneficios para las organizaciones, pero son enfáticos en tener en cuenta el modelo de responsabilidad compartida, que es donde principalmente se delegan las funciones entre cliente y proveedor.

Teniendo en cuenta la importancia y los beneficios que produce establecer un modelo de arquitectura de seguridad en las organizaciones que migran a entornos en nube, surge el siguiente

cuestionamiento: ¿Cuáles son los componentes esenciales que una arquitectura de seguridad de la información debería contemplar, para lograr una cultura y plan de madurez de seguridad aceptable en cualquier organización que utilice los modelos de servicio en la nube (IaaS, SaaS PaaS) como su *Core* de negocio?

El alcance del documento contempla desde identificación de los artefactos considerados esenciales de una arquitectura de seguridad de la información, hasta sugerir cuales son los principales elementos aplicables para lograr una cultura y plan de madurez de seguridad en organizaciones que utilicen los modelos de servicio en la nube (IaaS, SaaS PaaS) como su *Core* de negocio.

## II. Referencias Metodológicas

**ISO/IEC 27001:2013**

Es una norma y/o estándar internacional enfocado al sistema de gestión de seguridad de la información que permite el aseguramiento de la confidencialidad integridad y disponibilidad de los datos, asimismo permite a las organizaciones la evaluación de riesgo y aplicación de controles (NTC-ISO-IEC 27001:2013, 2013)

**NIST-SP 800-53**

Publicación de la NIST, la cual proporciona un catálogo de controles de seguridad y privacidad para sistemas y activos de información (NIST, 2020)

**NIST.SP.800-181**

Publicación de la NIST específicamente de la NICE (National Initiative for Cybersecurity Education) enfocada a describir los roles, funciones, conocimientos y habilidades en Ciberseguridad (NIST, y otros, 2020)

**CIS CONTROLS V7 CLOUD**

Guía de controles de CIS para la Nube enfocado a la aplicación de buenas prácticas (CIS, 2022).

**SABSA**

Marco de arquitectura de dominio optimizado para arquitecturas de seguridad (SABSA Institute, 2016)

## III. Referentes Teóricos

### ¿Qué es Seguridad de la Información?

Seguridad de la información hace referencia a proteger la información ante riesgos y amenazas que pueden afectarla, de igual manera se enfoca en salvaguardar y garantizar sus tres principales propiedades: la confidencialidad, integridad y disponibilidad.

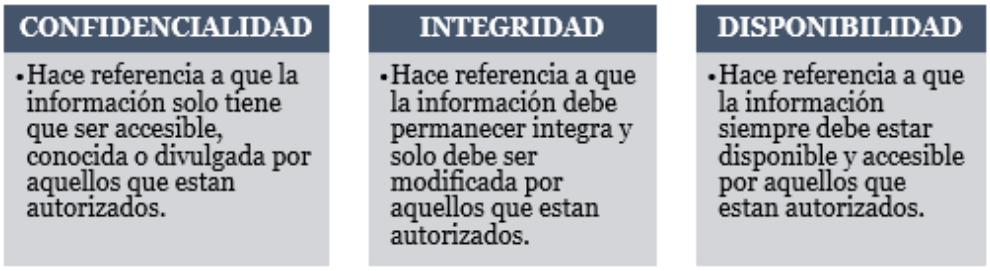


*Ilustración 1. Propiedades de la información*

### ¿Qué es Informática en la Nube?

Ofrecer y/o acceder bajo demanda a recursos tecnológicos como Servidores, Base de datos, Aplicaciones, Análisis, Networking, Almacenamiento, herramientas específicas para desarrolladores, entre otros, a través de internet, y pagar únicamente por uso.

**¿Cuáles son los Principales Modelos de Servicio de Informática en Nube?**

Entre los principales y más reconocidos modelos de servicio de informática en la nube se encuentra el IaaS, SaaS y PaaS, los cuales se describen continuación:


*Ilustración 2. Principales Modelos de Servicios de Informática en la Nube*

En relación con infraestructura como servicio (IaaS), tenemos que (NIST, Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, 2011) lo define como: la capacidad que se ofrece al consumidor donde se suministra procesamiento, almacenamiento, redes y otros recursos informáticos fundamentales donde el consumidor puede implementar y ejecutar software, que puede incluir sistemas operativos y aplicaciones. El consumidor no administra ni controla la infraestructura de la nube, pero tiene control sobre los sistemas operativos, el almacenamiento y las aplicaciones implementadas; y posiblemente control limitado de componentes de red selectos (por ejemplo, servidores de seguridad de host).

En relación con Plataforma como servicio (PaaS), tenemos que (NIST, Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, 2011) lo define como: La capacidad que se ofrece al consumidor para desplegar en la infraestructura de la nube aplicaciones creadas o adquiridas por el usuario usando lenguajes de programación, bibliotecas, servicios y herramientas compatibles con el proveedor. El consumidor no administra ni controla la infraestructura de la nube, incluidos red, servidores, sistemas operativos o el almacenamiento, pero tiene control sobre

las aplicaciones implementadas y los posibles ajustes de configuración para el entorno de alojamiento de aplicaciones.

En relación con Software como servicio (SaaS) tenemos que (NIST, Peter Mell, Timothy Grance, The NIST Definition of Cloud Computing, 2011) lo define como: La capacidad que se ofrece al consumidor, es la de utilizar las aplicaciones del proveedor que se ejecutan en una infraestructura en la nube. Las aplicaciones son accesibles desde varios dispositivos clientes a través de una interfaz ligera, como un navegador web (por ejemplo, correo electrónico basado en la web), o una interfaz de programa. El consumidor no gestiona ni controla la infraestructura de la nube, incluyendo la red, los servidores, los sistemas operativos, el almacenamiento o incluso las capacidades individuales de las aplicaciones, con la posible excepción de los ajustes de configuración limitados de las aplicaciones específicas del usuario.

**Modelo de Responsabilidad Compartida**

El modelo de responsabilidad compartida determina los límites, como su nombre lo indica de las responsabilidades que tienen los proveedores de servicio en nube, así como el cliente y compartida entre ambos entes, de acuerdo con los Modelos de Servicios de Informática en la Nube. Para ejemplificar el Modelo de Responsabilidad Compartida se relaciona a continuación algunos de los modelos ofrecidos por dos proveedores de servicio en la nube (Azure y AWS):

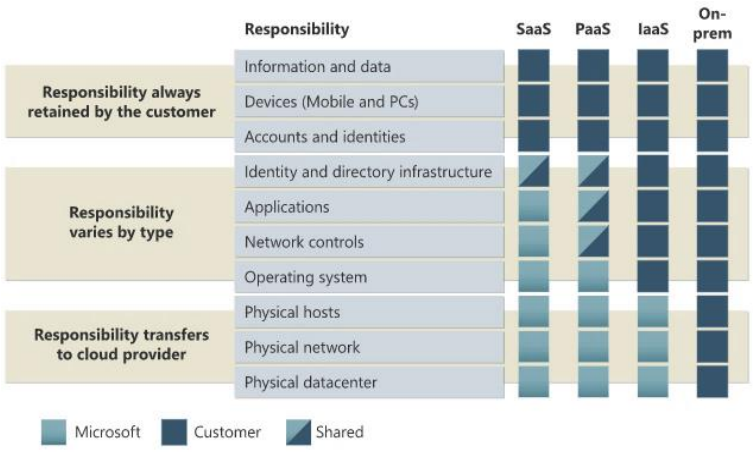


*Ilustración 3. Tomado de División de responsabilidad Microsoft (Microsoft, 2022)*

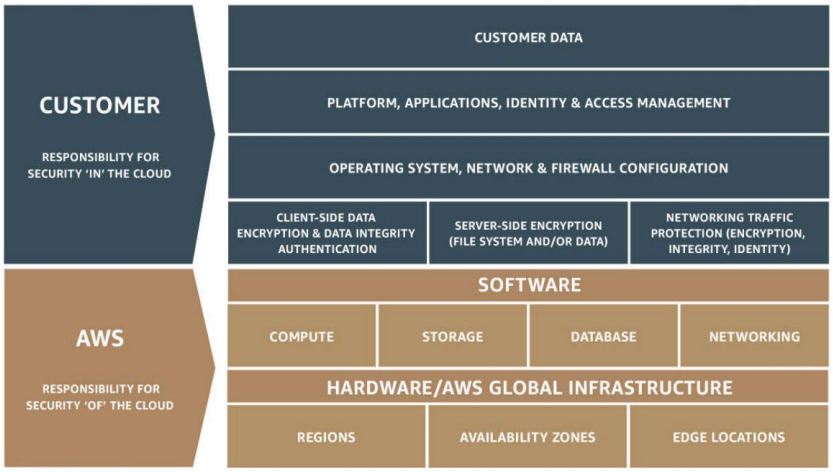


*Ilustración 4. Tomado de Modelo de responsabilidad compartida AWS (AWS, 2022)*

**¿Qué es una Arquitectura de Seguridad?**

En efecto SABSA define una arquitectura de seguridad como una estructura de componentes organizacionales, conceptuales, lógicos y físicos que interactúan de manera coherente para lograr y mantener un estado de riesgo administrado (SABSA Institute, 2016)

Actualmente en las diferentes organizaciones los datos son el activo más críticos e importantes, por lo cual implementar una arquitectura de seguridad se convierte en una excelente alternativa para garantizar la confidencialidad integridad y disponibilidad de la información, en tal sentido, a continuación, se relaciona algunos beneficios de inherentes que permite:

- ✓ Gestionar adecuadamente la seguridad de la información
- ✓ Guiar a las organizaciones a implementar un sistema de gestión de seguridad
- ✓ Aumentar los niveles de madurez de seguridad de las organizaciones
- ✓ Implementar controles de manera eficiente
- ✓ Ejecutar procesos y procedimientos de manera apropiada

## IV. Metodología

El presente artículo académico es una investigación de tipo exploratoria que "*busca establecer las bases para una investigación más profunda*" y *"no necesariamente se espera obtener conclusiones o recomendaciones determinantes"* (Investigadores, 2020), pretendiendo obtener una "*visión general acerca de una determinada realidad* (Investigación exploratoria: qué es, características y ejemplos, 2022).

Por otra parte, el método de investigación aplicado en el documento es cualitativo el cual según (Santander Universidades, 2021) indica que "*La investigación cualitativa implica recopilar y analizar datos no numéricos para comprender conceptos, opiniones o experiencias, así como datos sobre experiencias vividas, emociones o comportamientos, con los significados que las personas les atribuyen. Por esta razón, los resultados se expresan en palabras".*

Entre los objetivos específicos del artículo se encuentra:

- ✓ Identificar los dominios y artefactos esenciales de una arquitectura de seguridad de la información
- ✓ Explicar la importancia de implementar arquitecturas de seguridad de la información y cómo se articulan con diferentes áreas de una organización.
- ✓ Sugerir los principales componentes de una arquitectura de seguridad de la información aplicables en organizaciones que utilicen los tres modelos de servicios en nube (IaaS, SaaS, PaaS).

## V. Resultados

En la fase inicial del análisis se identificaron los dominios que coincidían en diferentes metodologías, estándares y buenas prácticas de seguridad, en la siguiente tabla se relaciona dicha exploración, con las respectivas cláusulas y/o controles aplicables:

| DOMINIO | REFERENCIAS METODOLÒGICAS | | | |
|---|---|---|---|---|
| | NIST-SP 800-53 | ISO/IEC 27001:2013 | NIST.SP. 800-181 | CIS CONTROLS V7 CLOUD |
| **ESTRATEGIA ORGANIZACIONAL Y TI** | Program Manager (PM)<br>Planning (PL)<br>Personnel Security (PS)<br>System and Services Acquisition (SA) | Cláusula (5, 6, 8, 9.3)<br>Anexo (A.6, A.9.3, A.12, A.13.2.1, A.15, A.18.2.2) | | [19] |
| **GOBIERNO DE SEGURIDAD** | Program Manager (PM)<br>Planning (PL)<br>Personnel Security (PS)<br>System and Services Acquisition (SA) | Cláusula (5.3, 6, 7.1, 7.2, 9.1)<br>Anexo (A.6.1, A.7.1) | | |
| **PERSONAS** | Awareness and Training (AT)<br>Threat Awareness Program PM-16 | Cláusula (7.2, 7.3)<br>Anexo (A.7.2.2) | X | [17] |
| **MODELOS DE SERVICIO (IAAS – SAAS - PAAS)** | CA-3 Information Exchange | Anexo (A.15) | | [4-6-9-10-16-17-18-19-20] |
| **GESTIÒN DE INCIDENTES** | Incident Response (IR) | Anexo (A.16) | | [19 - 20] |
| **AUDITORIA / NORMATIVIDAD / CUMPLIMIENTO** | Audit and Accountability (AU)<br>AC-2 Account Management<br>CM-5 Access Restrictions for Change<br>RA-5 Vulnerability Monitoring and Scanning<br>CA-9 Internal System Connections<br>CM-1 Policy and Procedures | Cláusula (9.2)<br>Anexo (A.12.7, A.18) | | [3,6,16] |

*Ilustración 5. Referentes Teóricos*

La siguiente imagen expone los artefactos identificados como esenciales en seguridad y los cuales apalancan los principales dominios propuestos para lograr una arquitectura de seguridad de la información aplicable en organizaciones que utilicen los tres principales modelos de servicios en nube:


*Ilustración 6. Artefactos esenciales en una Arquitectura de Seguridad de la Información*

Como resultado final, la propuesta de arquitectura de seguridad de la información está compuesta por 7 dominios principales que representan la alineación y articulación entre las diferentes áreas, recursos, personas y herramientas aplicables en organizaciones que adoptan su infraestructura con modelos de servicios en nube (IaaS, SaaS, PaaS).

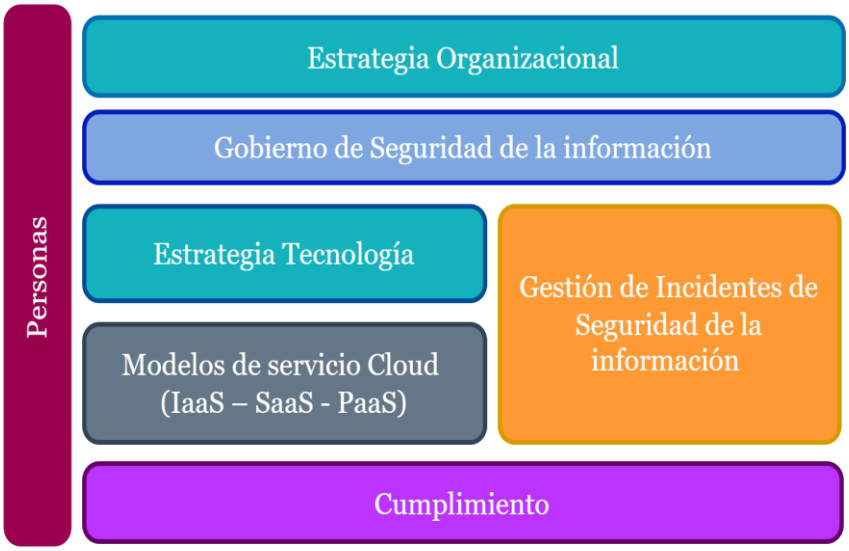


*Ilustración 7. Dominios Propuestos Arquitectura de Seguridad*

**Dominio Estrategia Organizacional**

En este dominio es importante disponer con el compromiso de la alta gerencia, articulándose con la visión, misión y decisiones empresariales, de esta manera se podrán integrar mucho más fácil los requisitos de seguridad y se aseguran los recursos necesarios para implementar una arquitectura de seguridad de la información. Del mismo modo en este dominio se debe incluir el apetito de riesgo, el cual permite tener claro cuál es el nivel de riesgo y los límites aceptados, permitiendo así una mayor planificación adhiriendo control táctico y estratégico.

**Dominio Estrategia de Tecnología**

En este dominio debe destacar la integración entre las herramientas (Software y Hardware), recurso humano, procedimientos y aplicación de buenas prácticas en cada artefacto son fundamentales para establecer las bases de la estrategia de tecnología y debe estar alineada con la estrategia organizacional (Primer Dominio) y con el Dominio de Gobierno de Seguridad.

**Dominio Gobierno de Seguridad de la Información**

En este dominio debe prevalecer la soberanía y autonomía de arquitectura de seguridad de la información, la cual no debe ser opacada por la alta gerencia en las organizaciones, sin embargo se debe tener claro que no es la máxima autoridad y su mayor reto es tener credibilidad, (lo cual en la opinión del autor es uno de los retos más difíciles de conseguir), El máximo líder y equipo de trabajo en este dominio debe tener claro su plan de gobierno de seguridad de la información, el cual debe identificar, interiorizar, proceder a su aprobación de la alta gerencia, divulgar y socializar y por último debe buscar maneras de protegerlo, esto ayuda a construir la credibilidad de la cual se hablaba anteriormente, El plan de gobierno debe involucrar las Políticas, Normativas, Estándares, Leyes, Roles, Controles, y estos deben ser claros y sencillos, aterrizados a la realidad de la organización, medibles con objetivos y metas alcanzables. Como en cualquier

gobierno, el establecimiento de Políticas y normativas debe ser su cimiento, basado en el contexto organizacional y alineado a los dos Dominios ya presentados, se debe tener claro cuáles son los límites y el apetito de riesgo, las Políticas y Normativas no deberían ser copiadas de una organización a otra, lo cual es un error muy común en seguridad, sin embargo pueden ser una guía pero cada organización es un "mundo diferente" y deben convertirse en el ADN de la Seguridad y tomarle la importancia que se merece. Otro de los artefactos que se incluye en este dominio es la adquisición de servicios y herramientas de seguridad considerando la relación con proveedores y clientes, adhiriendo y resaltando el plan de Gobierno contemplado.

**Dominio Personas, Cultura y Capacitación**

Una de las mayores afirmaciones que se suelen escuchar en seguridad de la información es que las personas son el "Talón de Aquiles" de la seguridad y no hay que sobrevalorar esas afirmaciones, debido a que dentro de las organizaciones se pueden aplicar todas las capas de seguridad (defensa en profundidad) que el músculo financiero nos ofrezca, sin embargo quien manipula la información al final siempre es el ser humano y basta tan solo un error, desconocimiento o una falta de interés para que la seguridad de la información en una organización se vea afectada. Es la razón por la cual en el presente artículo se generó un dominio para las personas, buscando precisamente resaltar la importancia que tiene educarlas y sacarlas de la falta de comprensión frente a la seguridad de la información. Solo si educamos a las personas se puede generar un cambio cultural y podemos reducir costos importantes dentro de las mismas organizaciones, la educación en seguridad debe ser sencilla, evitando terminología técnica, empatizando y buscando similitudes entre la organización y vida que hay fuera de ella (Familia (hijos, padres), amigos, animales, finanzas, economía), cuando logramos incluir la seguridad de la información en estos ámbitos se facilita captar el interés de las personas y logramos reducir las amenazas relacionadas con el factor humano en nuestras organizaciones.

**Dominio Modelos De Servicio Cloud (IaaS – SaaS - PaaS)**

El presente artículo está enfocado a las organizaciones que migran o que utilizan servicios en la nube, sin embargo, el presente dominio no se enfoca en describir dichos servicios, por el contrario, busca precisar los artefactos de seguridad que se recomienda tomar en consideración para integrarse en la arquitectura de seguridad de la información y lograr un nivel de madurez sólido.

En este dominio, en primer lugar se sugiere tomar en consideración que toda la organización debe entender y conocer cómo funciona los modelos de servicio Cloud que se adquieren, en segundo lugar, ser conscientes de la existencia de los modelos de responsabilidad compartida y de su titánica importancia con relación a la protección de datos, la privacidad de la información y su relación con el gobierno de datos, en donde el factor humano es determinante, para dar cumplimiento normativo y legislativo (en este ámbito el autor recomienda empaparse de la ley de protección de datos personales - GPDR). En tercer lugar, cabe resaltar en este dominio que los controles son aplicables según el modelo de servicio contratado, es decir si usted contrata un servicio SaaS, IaaS, o PaaS puede aplicar controles frente a los datos, pero no puede aplicar controles a nivel hardware. Por último, en este dominio se sugiere un articulación y apoyo constante de las áreas legales de cada organización, con el fin de clarificar los límites entre el ofrecimiento de servicios a clientes y la responsabilidad compartida que se adquiere con los proveedores de servicio y terceros.

**Dominio de Gestión de Incidentes**

La gestión de incidentes de seguridad de la información es uno de los procesos considerados fundamentales en las organizaciones, lamentablemente solo se da la verdadera importancia cuando la organización ha sido afectada por un ataque cibernético. Por lo anterior este dominio aspira a resaltar la trascendencia que tiene la gestión de Incidentes de Seguridad de la Información. En primer lugar, debemos poder tener una adecuada identificación de los activos

de la información su clasificación y su evaluación, si se conoce que activo es crítico también se conoce que se debe priorizar y monitorear, idealmente se podría monitorear todos los activos, sin embargo, aterrizado a la realidad puede resultar poco productivo y con costos elevados. Segundo, se debe tener claro el proceso, los roles y responsabilidades ante un incidente de Seguridad de la Información, debido a que los incidentes pueden generar según su afectación pánico generalizado y no todos deben ni pueden ser partícipes en una posible contención y/o mitigación, de aquí nace la importancia de contemplar un equipo de gestión y respuesta de incidentes, preparado y con un nivel de experiencia tanto técnico como táctico y estratégico, por último se propone el uso de elementos como CSIRT (equipo de respuesta a incidentes de seguridad), SOC (Centro de Operaciones de Seguridad), Pruebas de Ethical Hacking continuo, así como revisar a fondo los temas de informática forense sobre todo cuando actualmente este campo tiene poca documentación y exploración en servicios contratados en nube.

**Dominio Auditoría / Normatividad / Cumplimiento**

Finalmente se presenta el Dominio de cumplimiento, enfocando principalmente a infraestructuras en nube, centralizándose en las auditorías y posteriormente enfocándose en lo reglamentario, normativo y cumplimiento. En cuanto al artefacto de Auditorías se sugiere que cree un plan de auditoría avanzado donde se identifique ítems auditables frente a la base de los dominios y artefactos mencionados durante este documento, con el objetivo de brindar un alcance apropiado, pertinente, receptivo, basado en riesgos documentados, reconocimiento de la estrategia corporativa; es muy aconsejable que el auditor tenga conocimientos en infraestructura en Cloud lo cual permitirá que el plan de auditoría genere valor y realmente mejore la articulación de la arquitectura de seguridad propuesta. Continuando con los artefactos normativos y cumplimiento, es conveniente que exista una articulación sólida entre las áreas de Legal, Protección de Datos y financiero, recursos humanos y el gobierno de seguridad , debido que dependiendo del tipo de organización y su naturaleza pueden aplicar o no, normas y regulaciones

específicas, así mismo se debe conocer las sanciones y multas a las cuales se encuentra expuesta la organización, adicionalmente debe existir transparencia en lo ofrecido y/o adquirido de los terceros (ej. Clientes externos y proveedores).

La siguiente imagen muestra el resultado final y es la arquitectura de seguridad integrando todos los componentes descritos anteriormente:

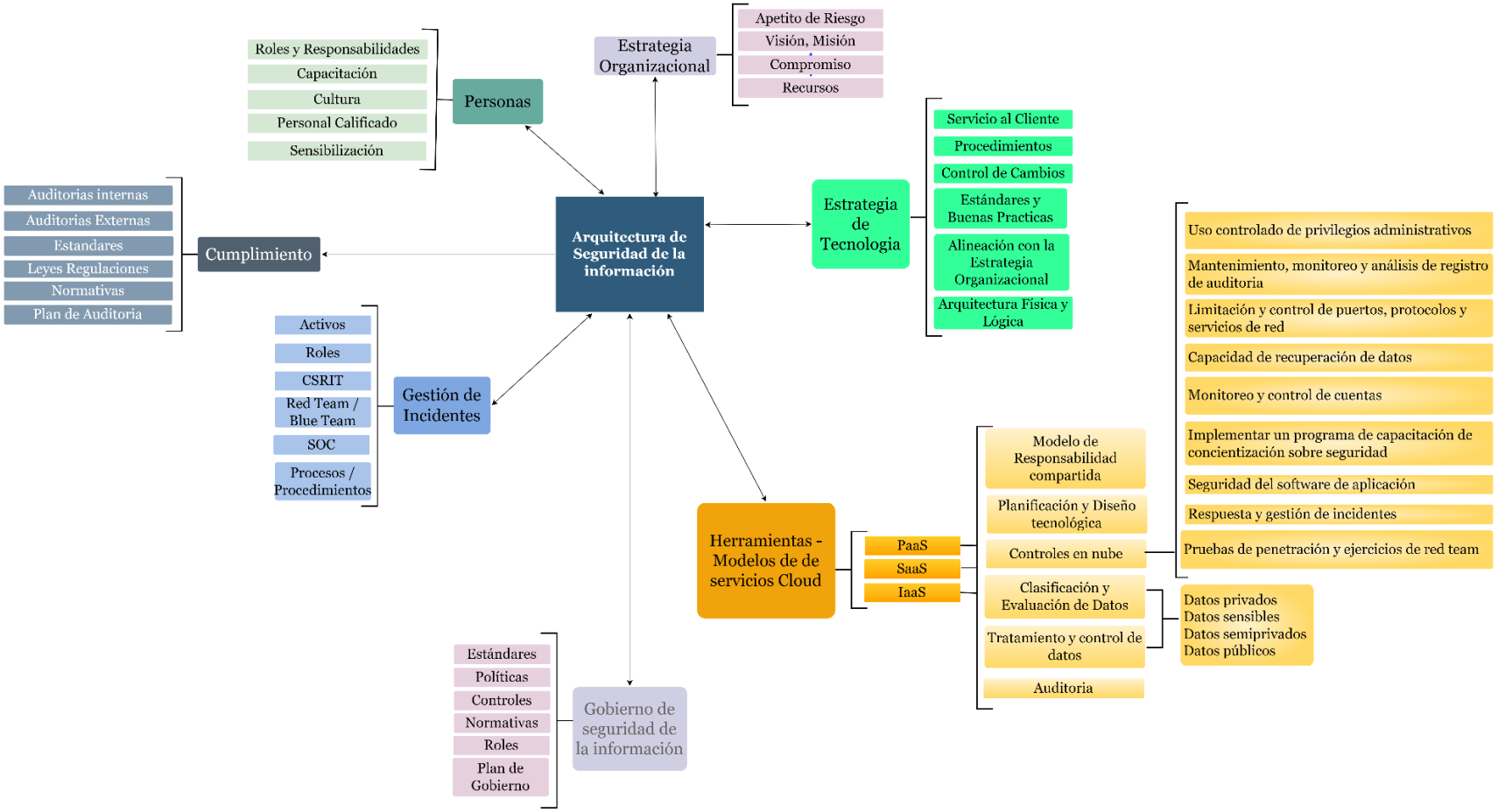


*Ilustración 8. Propuesta Arquitectura de Seguridad de la Información*

## VI. Conclusiones

- En organizaciones que utilicen los modelos de servicio en la nube (IaaS, SaaS PaaS) como su Core de negocio, es muy importante tener claro los modelos de responsabilidad compartida ofrecidas por el proveedor de servicio en Nube, lo cual permite determinar los límites de las responsabilidades que se tienen al momento de adquirir estos servicios.
- Implementar una arquitectura de seguridad de la información permite:
    - ✓ Gestionar de manera adecuada la seguridad de la información
    - ✓ Guiar a las organizaciones al momento de adoptar un sistema de gestión de seguridad
    - ✓ Aumentar los niveles de madurez y su cultura organizacional
    - ✓ Gestionar riesgos eficazmente
    - ✓ Implementar de controles apropiados
    - ✓ Ejecutar procesos y procedimientos de manera oportuna
    - ✓ Gestionar monitoreo y auditorías.
- Los Dominios descritos cuentan a su vez con artefactos sugeridos como básicos y elementales en la creación e implementación de una Arquitectura de seguridad de la información, no pretenden ser impositivos, pero si bajo la experiencia del autor son elementales.
- Se plantea la existencia de una adecuada capacitación frente a infraestructuras en nube para que la arquitectura genere un valor agregado a la organización y facilite los procesos internos integrándose con la estrategia organizacional y correlacionando todos los dominios descritos.

**Acerca del Autor**

Candidata a Especialista en Seguridad de la información de la Fundación Universitaria Los Libertadores e Ingeniera de Telecomunicaciones de la Universidad Cooperativa de Colombia. Certificada en: Auditor Interno ISO/IEC 27001, Scrum Foundation Profesional, AWS Professional Services: Best Practices (Training), Security Gobernance at Scale (Training), Interpretación de la Norma ISO/IEC 27018:2019 Técnicas de Seguridad, Diplomado de Ciberseguridad, Evidencias Digitales, CEH V.9 (Training), Desarrollo de Aplicaciones Web Seguras Basado en Guia OWASP. Se ha desempeñado en sector privado como Analista de Seguridad de la información y Ciberseguridad y como Especialista de Seguridad. WebSite: linkedin.com/in/evelin-díaz

**Acerca del Asesor Externo**

John Alexander Pachón Pinzón, Especialista de seguridad de la información e informática de la Universidad Sergio Árboleda e ingeniero de sistemas de la Universidad Escuela Colombiana de Ingeniería Julio Garavito. Certificado en: Cyber Security foundation professional, scrum foundation professional, NSE2 network security associate, nse1 network security associate, auditor interno Iso 22301:2012, ITIL. Diplomado en Gerencia de Proyectos. Con conocimientos en seguridad de la información, ciberseguridad, técnicas anti forenses de la seguridad informática, seguridad en marketing digital y manejo de proyectos. Se ha desempeñado como ingeniero de desarrollo, ingeniero senior y coordinador de infraestructura y telecomunicaciones para empresas del sector financiero, analista de seguridad de la información y especialista de seguridad TI, además como docente de la Universidad Escuela Colombiana de Ingeniería Julio Garavito.

**Acerca del Docente**

Yenny Isabel Serrato Rodriguez, Especialista en Seguridad de la Información de la Universidad Sergio Arboleda e Ingeniera en Telemática de la Universidad Distrital Francisco José de Caldas. Email: yiserrator@gmail.com. Es certificada como: CEH, Auditor Líder e interno ISO 27001:2012, Auditor interno ISO 22301:2019, ITIL, Cobit, Scrum Foundations, entre otros. Adicional, posee conocimientos en informática forense, ciberseguridad, auditoría interna y manejo de proyectos. Se ha desempeñado como Oficial de seguridad de la información para empresas multinacionales, consultor para empresas públicas y privadas liderando equipos de trabajo multidisciplinarios, además docente universitario en varias universidades.

## VII. Referencias

AWS. (2022). *shared-responsibility-model.* Obtenido de shared-responsibility-model: https://aws.amazon.com/es/compliance/shared-responsibility-model/

CIS. (2022). *CIS Critical Security Controls*. Obtenido de https://www.cisecurity.org/insights/white-papers/cis-controls-cloud-companion-guide

*Investigación exploratoria: qué es, características y ejemplos*. (2022). Obtenido de tiposdeinvestigacion.org: https://tiposdeinvestigacion.org/exploratoria/#:~:text=Caracter%C3%ADsticas%20de%20la%20investigaci%C3%B3n%20exploratoria,-Busca%20informaci%C3%B3n%20sobre&text=Se%20plantea%20el%20tema%20de,no%20se%20formula%20la%20pregunta.&text=Esta%20investigaci%C3%B3

Investigadores. (27 de febrero de 2020). *Tecnicasdeinvestigacion.com*. Obtenido de Tecnicasdeinvestigacion.com: https://tecnicasdeinvestigacion.com/investigacion-exploratoria/

Microsoft. (2022). *Shared responsibility in the cloud.* Obtenido de Shared responsibility in the cloud: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

NIST. (Septiembre de 2020). *NIST-SP 800-53.* Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

NIST, Peter Mell, Timothy Grance. (Septiembre de 2011). *The NIST Definition of Cloud Computing*. Obtenido de https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

NIST, Petersen, R., Santos, D., Smith, M., Wetzel, K., & Witte, G. (Noviembre de 2020). *NIST.SP.800-181r1.* Obtenido de https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

NTC-ISO-IEC 27001:2013, I. (2013).

SABSA Institute. (Enero de 2016). Integrating Risk and Security within a TOGAF® Enterprise Architecture. *Integrating Risk and Security within a TOGAF® Enterprise Architecture*.

Santander Universidades. (10 de 12 de 2021). *www.becas-santander.com/*. Obtenido de www.becas-santander.com/: https://www.becas-santander.com/content/becasmicrosites/es/blog/cualitativa-y-cuantitativa.html