**FORMATO PARA EL DESARROLLO DE COMPONENTE FORMATIVO**

| PROGRAMA DE FORMACIÓN | Implementación de auditoría técnica plataformas *cloud* |
| --- | --- |

| COMPETENCIA | 220601041- Implementar sistemas de gestión según normativa y requerimientos técnicos | RESULTADOS DE APRENDIZAJE | 220601041-4. Desarrollar proyectos de implementación de migración de información hacia entornos de nube de acuerdo con métodos y normativa. |
| --- | --- | --- | --- |

| NÚMERO DEL COMPONENTE FORMATIVO | 4 |
| --- | --- |
| NOMBRE DEL COMPONENTE FORMATIVO | Marcos de seguridad *cloud* |
| BREVE DESCRIPCIÓN | El presente componente formativo trabaja sobre tres de los marcos más importantes y de mayor adopción en cuanto a ciberseguridad; para lograr este objetivo, es necesario apropiar el tema del análisis de riesgos y las metodologías de aplicación, así como los estándares y los controles vigentes, que pueden ser utilizados para este fin. |
| PALABRAS CLAVE | amenaza, ciberseguridad, *cloud*, ISO, NIST |

| ÁREA OCUPACIONAL | 6 - Ventas y servicios |
| --- | --- |
| IDIOMA | Español |

1. **Tabla de contenidos**

**Introducción**

1. **Características de las metodologías de análisis y evaluación de riesgos**
   1. Objetivos de las metodologías de análisis y evaluación de activos
   2. Que es el análisis de riesgos
   3. Metodologías utilizadas en el análisis de riesgos
      1. *Metodología Magerit.*
      2. *Metodología OCTAVE (Evaluación de Vulnerabilidades y Amenazas en Activos Operacionalmente Críticos).*
      3. *Metodología CORAS (Construir una plataforma para el análisis de riesgos del sistema crítico de seguridad).*
      4. *Metodología MEHARI.*
      5. *NIST SP-830. ((Instituto Nacional de Estándares y Tecnología).*
2. **Controles de seguridad y marcos de referencia para servicios *cloud***
3. **Controles *Cloud Security Alliance* - *Security Guidance for Critical Areas of Focus in Cloud Computing* v4.0**
4. **Controles NIST Marco del Instituto Nacional de Estándares y Tecnología**
   1. Núcleo
   2. Niveles de Implementación ("*TIERs*")
   3. Perfil del marco
   4. Cómo utilizar el *framework* CSF

**Síntesis**

1. **Desarrollo de contenidos**

**Introducción**

Sea bienvenido al componente formativo “Marcos de seguridad *cloud*”. Para comenzar el recorrido por el mismo, visualice la información que se muestra a continuación:



Para la elaboración de este componente, se abordaron varios autores conocidos en **marcos de seguridad *cloud***, de quienes se han citado y referenciado conceptos y ejemplos para los fines educativos de esta materia, en el entendido de que el conocimiento es social y, por lo tanto, es para ser usado por quienes necesitan adquirirlo. Se espera que este documento sea útil para todos aquellos, aprendices y lectores en general, que estén interesados en acercarse a asuntos básicos de **implementación de auditoría técnica plataformas *cloud***.

1. **Características de las metodologías de análisis y evaluación de riesgos**

Analizar los riesgos informáticos es un proceso que comprende una serie de actividades que inician con la identificación y caracterización de los activos, la identificación de las amenazas y vulnerabilidades, y finalmente hacer una evaluación que permita determinar el riesgo en cada activo caracterizado. Este proceso permite la construcción de la matriz de riesgo, que es el insumo que nos lleva a definir un plan de tratamiento de riesgos que, de acuerdo a la norma ISO 27001, da la alternativa de poder mitigar o eliminar el riesgo, transferirlo, o aceptarlo, a partir de la implementación de controles de seguridad.

| Por esta razón, se hace imprescindible la utilización o adopción de una metodología que le permita al personal de tecnología realizar el proceso de una manera más ordenada, especializada y ajustada a las necesidades propias de cada organización. | Gestión de Riesgos - Controla la Incertidumbre para obtener el Éxito |
| --- | --- |

* 1. **Objetivos de las metodologías de análisis y evaluación de activos**

Todas las metodologías de análisis y evaluación de riesgos tienen por objetivo los siguientes puntos:

* La reducción de riesgos a un nivel aceptable.
* Preparar las estrategias que permitan prevenir incidentes de seguridad.
* Detectar las posibles debilidades existentes en los sistemas y servicios informáticos.
* Potenciar la correcta toma de decisiones en materia de seguridad de la información.
  1. **Qué es el análisis de riesgos**

Es poder determinar la probabilidad de un fallo en la seguridad de los activos caracterizados que pueda afectar cualquiera de los pilares de la seguridad, estos son: la integridad, la disponibilidad y la confidencialidad, afectando el *core* del negocio; e identificar cuáles serán las consecuencias o impactos producidos en la organización por dichos fallos.

Las siguientes son algunas de las metodologías más comunes o de mayor utilización en el mundo para este propósito.

* 1. **Metodologías utilizadas en el análisis de riesgos**

Desde el 2008, debido a la crisis financiera que se vivió en ese entonces, el análisis de riesgo ha tomado un papel importante al interior de las organizaciones, pues, antes de la crisis, este aspecto se trabajaba de forma sistemática y aislada de todas las entidades. Sin embargo, a partir de esa fecha, reforzar el control interno de las empresas fue asumido de manera más responsable, mediante el análisis y aplicación de la gestión del riesgo en todos los ámbitos y áreas.

Hoy en día, es posible ver diferentes métodos aplicados al análisis de riesgo y posibilitar su sistematicidad. A continuación, se revisan algunos de estos:

* + 1. ***Metodología Magerit.***

Esta metodología centra su funcionamiento en el hecho de poder caracterizar los activos en distintos grupos que faciliten la identificación de los riesgos y poder definir los controles o contramedidas necesarias que permitan evitar en un mayor porcentaje los incidentes de seguridad, lo que conlleva a generar un mayor grado de confianza para la organización, sus clientes y usuarios.

Desde el año 1997, cuando se publicó la primera versión de la metodología, hasta la actualidad, se ve cómo cada vez se consolida con mayor fuerza el análisis de riesgos como el primer gran proceso que lleva a poder gestionar la seguridad de la información.

Identificar los riesgos y evaluarlos es lo que permite definir los planes de tratamiento de riesgos; con la gestión realizada, se puede prevenir o disminuir la probabilidad de que se presenten ataques o incidentes de seguridad que afecten los datos, la información o los servicios que las organizaciones utilizan o prestan a sus clientes para el cumplimiento de su función misional.

En cuanto a losobjetivos de *Magerit*, esta metodologíaestablece unas metasde manera directa e indirecta, de acuerdo con el siguiente esquema:



* + 1. ***Metodología OCTAVE (Evaluación de Vulnerabilidades y Amenazas en Activos Operacionalmente Críticos).***

*OCTAVE* es una metodología que permite la identificación, evaluación y gestión de los riesgos informáticos desarrollada por la norma Internacional ISO 27001, su núcleo principal está determinado por un conjunto de criterios divididos en principios, atributos y resultados de dicha evaluación.



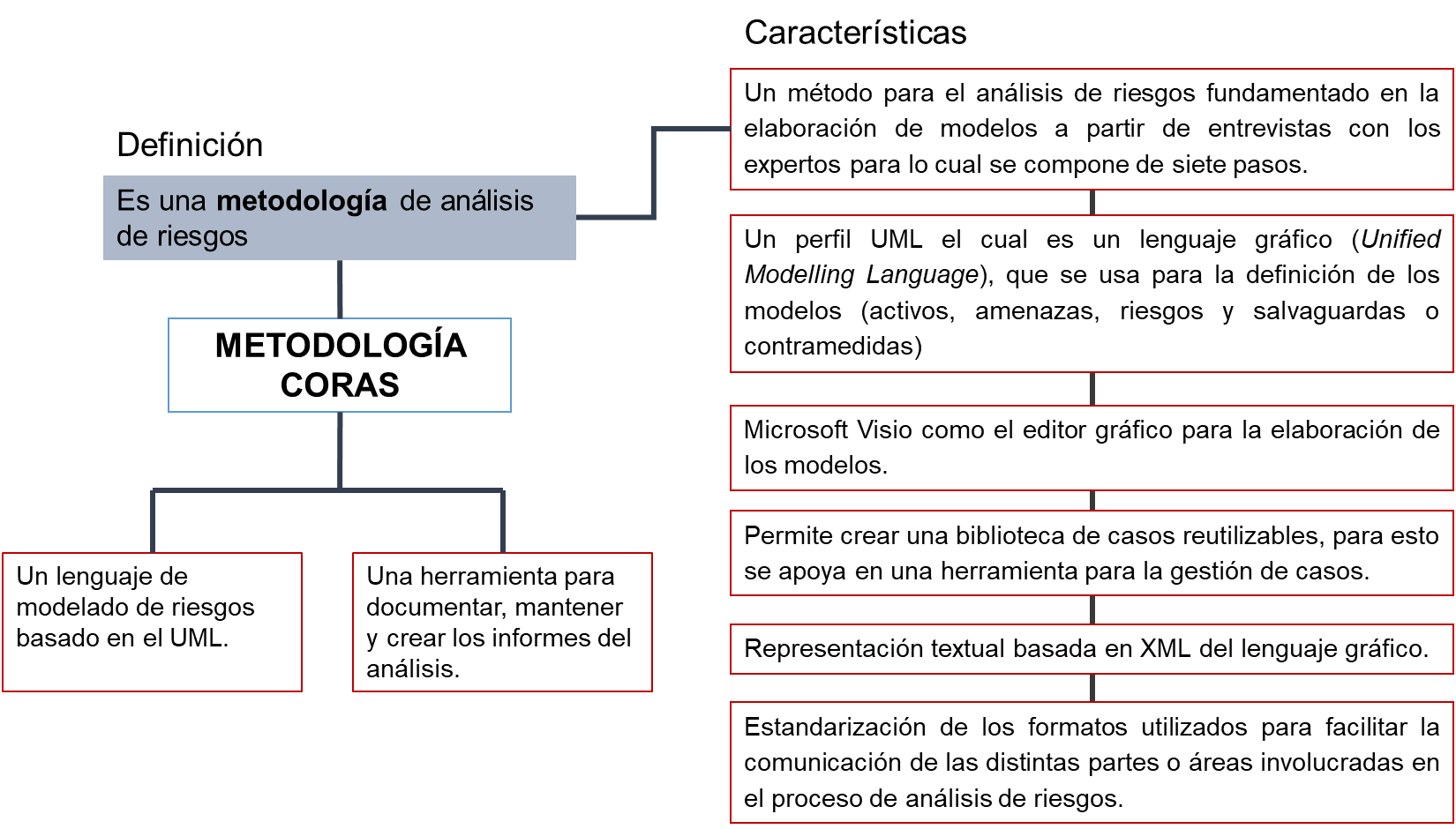
Esta metodología, en su proceso de caracterización de los activos, los divide en dos tipos:

* Sistemas (*hardware*, *software* y datos)
* Personal involucrado en los procesos de TI
  + 1. ***Metodología CORAS (Construir una plataforma para el análisis de riesgos del sistema crítico de seguridad).***

Fue construida en el año 2001 por SINTEF, la cual es una organización de investigación noruega que recibe financiamiento de organizaciones del sector público y privado. Su desarrollo fue financiado por la Unión Europea bajo el Proyecto CORAS (IST-2000-25031).

**Figura 1**

*Metodología CORAS*



La metodología **CORAS**, propone unos pasos para su consecución, estos son:



* + 1. ***Metodología MEHARI.***

Esta metodología fue desarrollada en el año 1998 por CUSIF (*Club de la Sécurité De L’information Français*); en el año 2007, pasó a ser *Open Source*. Tiene por objetivo permitir realizar un análisis individual o directo sobre las situaciones o escenarios de riesgo identificados, proporcionando un grupo de herramientas diseñadas específicamente para la gestión de la seguridad, adaptables a niveles distintos de madurez, que pueden ser a corto, mediano o largo plazo.

Su principal objetivo es la identificación, evaluación y reducción de riesgos. Para ello, se apoya en bases de datos de conocimiento propias, herramientas y mecanismos desarrollados para este propósito.



* + 1. ***NIST SP-830 (Instituto Nacional de Estándares y Tecnología).***

NIST SP-830 es desarrollado por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos de Norteamérica y proporciona una guía para la gestión del riesgo de los recursos y tecnologías de la información, entrega una serie de recomendaciones, actividades y procesos que permiten una adecuada gestión del riesgo y de la seguridad de la información.

En la siguiente figura, se pueden apreciar los nueve (9) pasos que sugiere esta metodología.

**Figura 2**

*Pasos de la metodología NIST SP-830*



En cuanto a los objetivos de la metodología NIST SP-830, se tienen los siguientes:

* El objetivo de desempeño de la gestión de riesgos es habilitar la organización para cumplir su misión.
* Mejorar el aseguramiento del sistema TI que almacena, procesa o transmite información organizacional.
* Permitir la gestión de riesgos para tomar decisiones bien fundamentadas de gestión y justificar los gastos que forman parte de un presupuesto de TI.
* Asistir a la administración en lo que se autoriza (o acredita) a los sistemas de TI, sobre la base de la documentación de soporte a partir de los resultados de la gestión de riesgos.

1. **Controles de seguridad y marcos de referencia para servicios *cloud***

Implantar medidas de seguridad y protección de los servicios ofertados y contratados en la nube requiere la utilización de lo que se denomina controles, que son una lista de buenas prácticas y recomendaciones dadas por diferentes organizaciones internacionales. A continuación, se presentan los controles de la norma **ISO 27002 – 27017,** que es la quecuenta con mayor reconocimiento y adopción en la industria.



Por su parte, la **ISO 27017** establece los controles de seguridad para servicios en la nube; está formada por 37 controles de seguridad en la nube que complementan la **ISO 27002,** y de igual manera, contiene 7 controles nuevos específicos para *cloud* que, al ser utilizados en conjunto con la norma **ISO 27001,** establecen controles específicos tanto para el proveedor de servicios *cloud* como para el cliente de servicios *cloud;* en ella se aclara cuáles son las responsabilidades y funciones tanto del proveedor como del cliente, a fin de lograr que los servicios ofrecidos y consumidos estén protegidos y se puedan incluir en un proceso de certificación **ISO 27001**.



De manera general, se clasifican los controles **ISO 27002** en 114 controles y 14 dominios globales, con 35 objetivos de control asociados, para que cada organización determine la cantidad y robustez de controles según las necesidades que se determinen. Es importante aclarar que para un proceso de certificación no se debe cumplir con la totalidad de estos, pues se utilizarán solo los que apliquen al ámbito de la organización.

A continuación, se aborda de manera muy general la estructura y cómo está diseñada la norma **ISO 27002:2013,** la cual en la actualidad se encuentra estandarizada, sin embargo, es importante mencionar que se encuentra en fase de revisión la nueva versión denominada **ISO/IEC 27.002:2021,** la cual se espera esté disponible a finales del año 2021 o principios del año 2022.

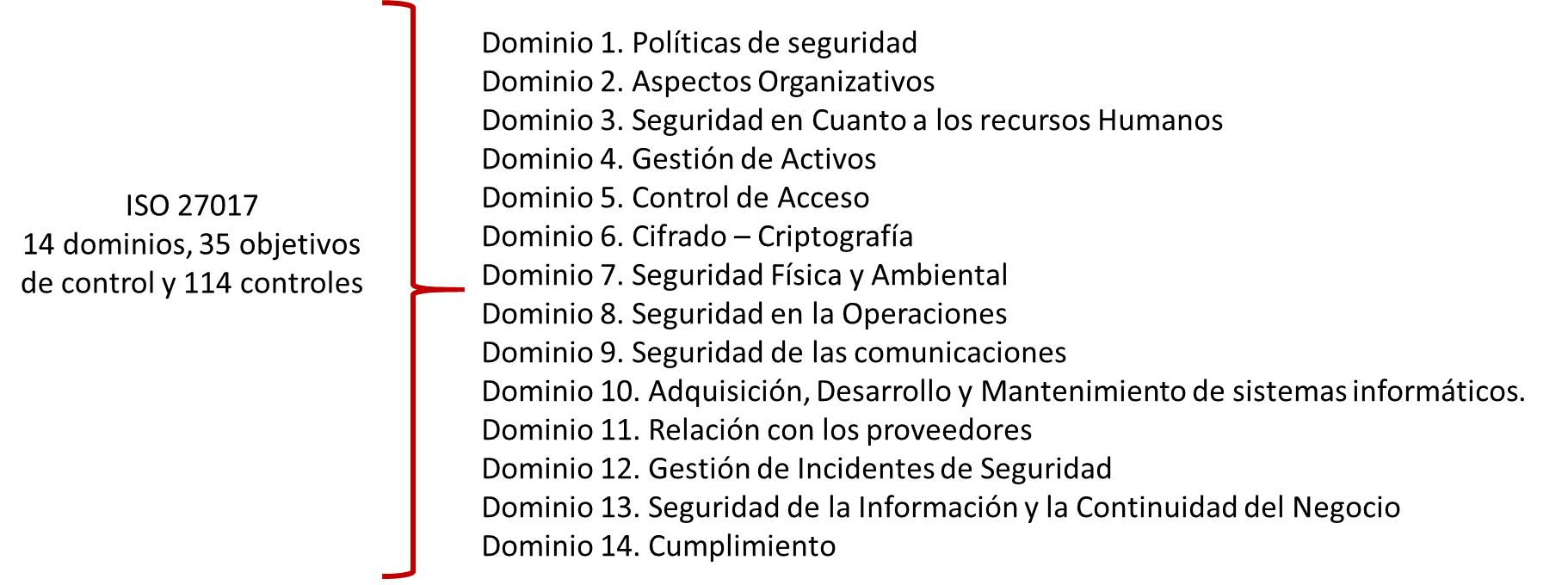
La implementación de una norma como **ISO 27017** trae múltiples beneficios tanto para el proveedor como para el cliente, los cuales se mencionan a continuación:



Como ya se ha indicado, la norma ISO 27017 tiene 114 controles y 14 dominios, los cuales se establecen en la siguiente figura:

**Figura 3**

*Dominios de la norma ISO 27017*



A continuación, se describen cada uno de estos dominios, teniendo en cuenta los objetivos propuestos para cada uno de ellos.

* **Dominio 1. Políticas de Seguridad**

Para este dominio, se establece la necesidad de que la organización cuente con un documento o política donde se exprese de manera general y clara la posición que frente a la seguridad establece la empresa. De igual manera, se crean las políticas complementarias, como una buena práctica de control a los diferentes procesos desarrollados por las organizaciones en la utilización de sistemas de información, plataformas, dispositivos lógicos y distintas ubicaciones de la empresa.

Se parte de la premisa típica en seguridad de la información: "*lo que no está permitido está prohibido*". Cada organización puede identificar sus propias necesidades específicas y, de esta manera, valorar los controles o salvaguardas necesarios que fundamenten las políticas de seguridad que le aplican, estructurando de esta manera una gestión más adecuada.



En la implementación de estos controles, según ISO 27017, se requiere, por parte del cliente de servicios en la nube, definir una política específica para la computación en nube, cuyo contenido sea consistente con los niveles de riesgo para los activos y la seguridad de la información considerados aceptables por la organización.

Por su parte, el proveedor de servicios *cloud* debería incrementar sus políticas de seguridad en relación con las actividades de provisión y uso de sus servicios de nube.

* **Dominio 2. Aspectos organizativos**

Este dominio centra su acción en establecer las estrategias administrativas de la gestión de la seguridad de la información, como factor fundamental para los objetivos y actividades propias de la organización.

La administración debe generar las condiciones necesarias que permitan la gestión de las actividades propias de la seguridad de la información como aprobación de las políticas de seguridad, la implementación de los controles, la asignación de tareas, segregación de funciones y designación de personas a cargo de la gestión de la seguridad de la información.

Este dominio cuenta con varios controles, tal como puede ser consultado en la siguiente gráfica:

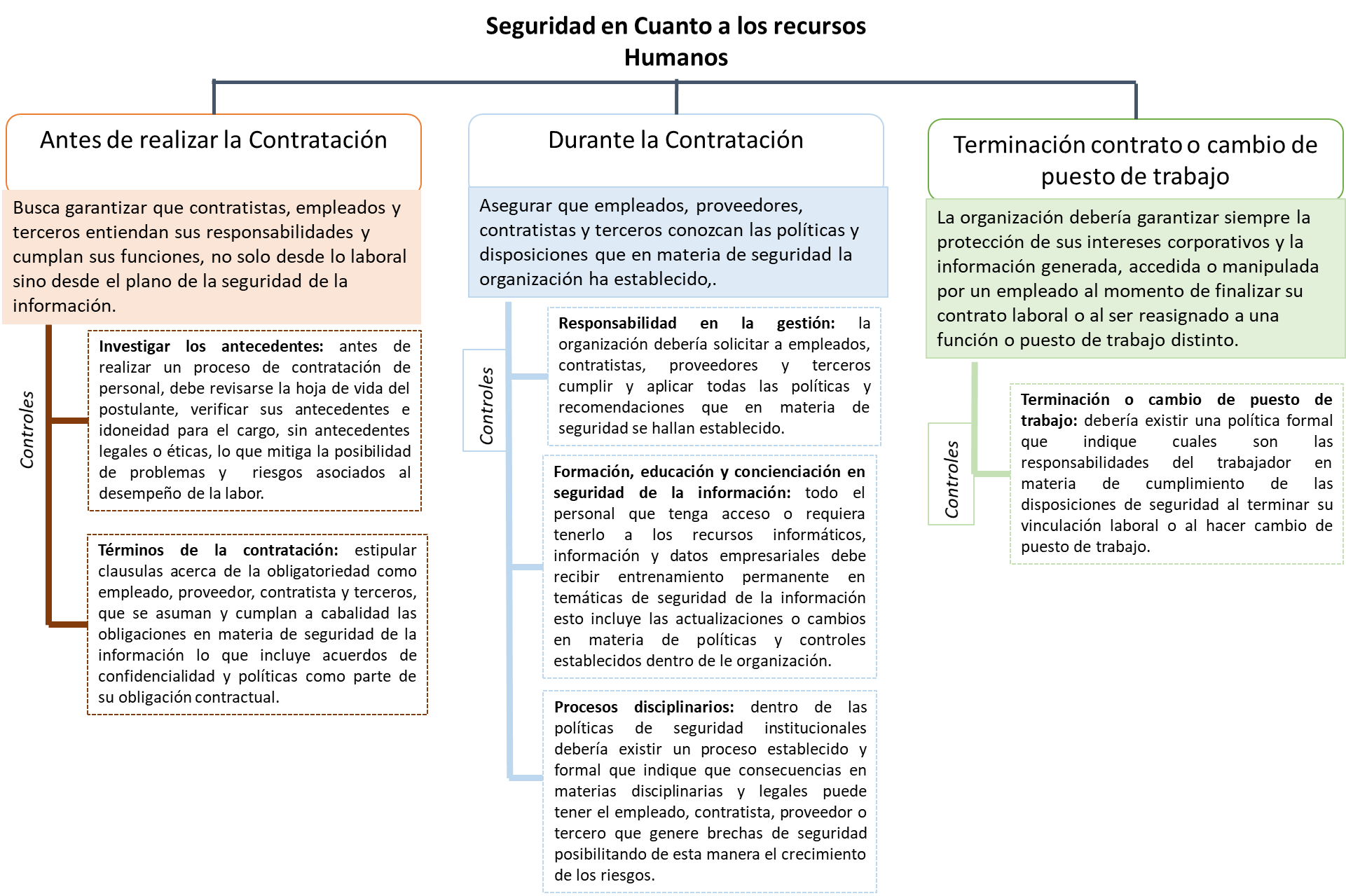


* **Dominio 3. Seguridad en cuanto a los recursos humanos**

Busca educar e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan el desarrollo de sus funciones y las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad. Este dominio cuenta con tres controles, los cuales se describen a continuación:

**Figura 4**

*Controles de la seguridad en cuanto a los recursos humanos*





* **Dominio 4. Gestión de activos**

Busca garantizar que las organizaciones tengan el conocimiento certero frente a los activos con que cuentan para el desarrollo de su *core* de negocio, como un factor diferencial y necesario para la gestión y administración del riesgo. Los activos pueden clasificarse y tener los controles correspondientes, como se puede observar en el siguiente recurso didáctico:



* **Dominio 5. Control de acceso**

Este dominio tiene por objetivo controlar el acceso a los recursos informáticos de la organización a partir de la implementación de restricciones y excepciones sobre quién y en qué nivel puede tener acceso a la información. El usuario es parte fundamental de este dominio, ya que se incluyen los mecanismos de autenticación, como nombres de usuario y contraseñas de acceso.

Para garantizar el cumplimiento de este objetivo, la norma establece los siguientes controles, que puede consultar a continuación:



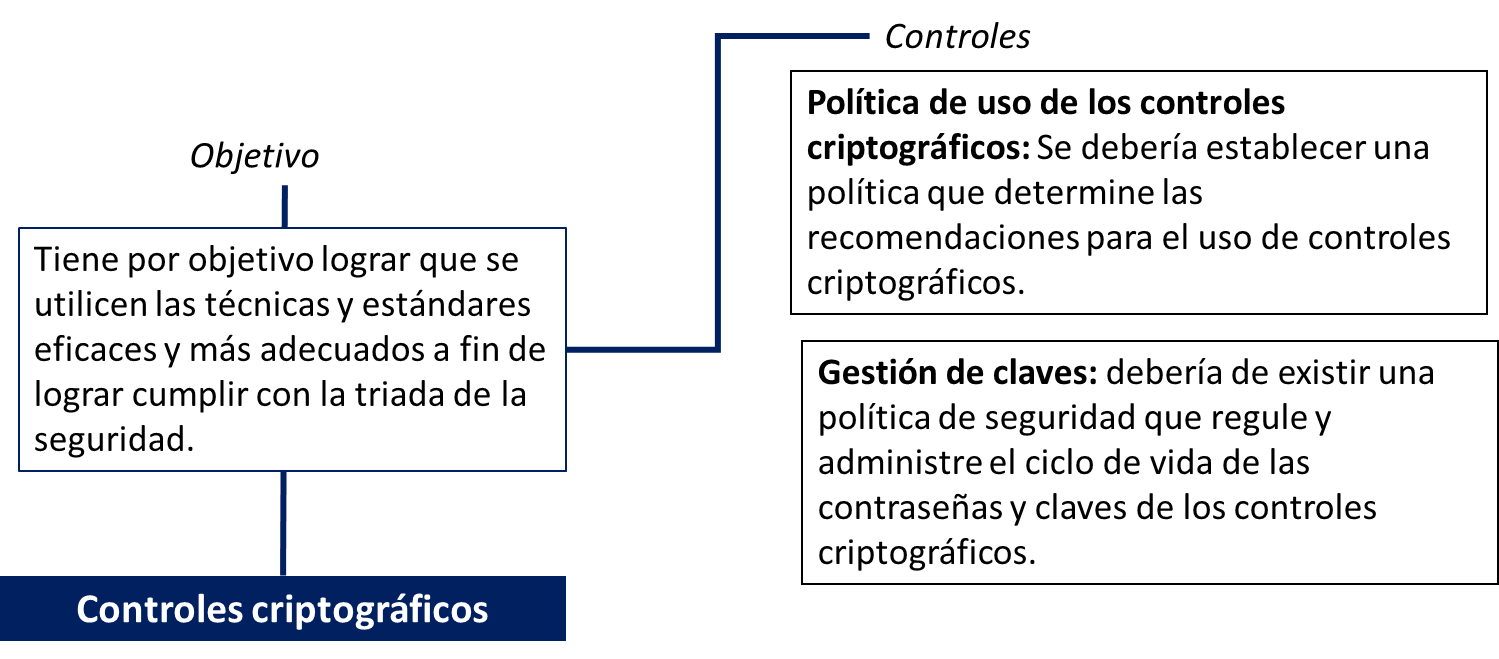
Para su implementación en ISO 27017 desde el lado del proveedor, se debe garantizar el proporcionar controles de acceso que permitan al cliente restringir el acceso a los servicios de nube contratados. Y por el lado del cliente, debería asegurarse que el acceso a la información de los servicios de nube puede y es restringido tal y como se especifica en su política de control de accesos, incluyendo la restricción de acceso a los servicios, a las funcionalidades de los servicios, además de los datos del cliente que se mantienen en el servicio.

* **Dominio 6. Cifrado – Criptografía**

Este es un control que busca el uso de herramientas y estándares criptográficos en la protección de la información que es transportada a través de redes, a partir de un análisis de riesgos hecho a los recursos y servicios, en busca de lograr la protección de la integridad, confidencialidad y disponibilidad de la información. Para ello, cuenta con los siguientes controles:

**Figura 5**

*Controles de cifrado y criptografía*

****

* **Dominio 7. Seguridad física**

Busca minimizar el riesgo en cuanto a las interferencias y fallas en la prestación de los servicios, mediante la definición de perímetros de seguridad y de áreas a proteger, facilitando la implementación de controles de seguridad y protección de las instalaciones donde se realice procesamiento de información contra accesos físicos no autorizados, tal como se observa en el siguiente recurso didáctico:



* **Dominio 8. Seguridad en las operaciones**

Se debe controlar la realización, actualización y mantenimiento de los procedimientos de operación de la organización; cuando se presenten cambios o actualizaciones previstos o imprevistos, se debe evaluar cuál es el impacto que esto generará sobre los recursos; de igual manera, se deben asignar los responsables dentro de dichos procesos, a fin de minimizar al máximo su impacto en la operación.

**Tabla 1**

*Controles para la seguridad en las operaciones*

| **CONTROL DE LA NORMA** | **OBJETIVO** | **APLICACIÓN DE CONTROLES** |
| --- | --- | --- |
| **Responsabilidades y procedimientos de operación** | Garantizar siempre la disponibilidad y adecuado funcionamiento de los recursos, evitando el acceso físico no autorizado, las interferencias o daños e interferencias a la información de la organización. | **Documentación de procedimientos de operación.** Todos los procesos operativos dentro de la organización deben estar debidamente documentados y a disposición cuando sean requeridos. |
| **Gestión de cambios.** Cualquier tipo de cambio, actualización o modificación debería contar con una política de control de cambios, para evitar afectaciones en la seguridad o en los procesos de negocio. |
| **Gestión de capacidades.** Se debería monitorear el uso de los recursos junto a las proyecciones futuras, en cuanto a requerimientos de capacidad, para garantizar el rendimiento adecuado en los sistemas. |
| **Separación de entornos de desarrollo, prueba y producción.** Los tres entornos deberían permanecer separados, para reducir los riesgos de acceso no autorizado o de cambios no autorizados en los sistemas en operación. |
| **Seguridad operacional del administrador.** Este control extendido en ISO/IEC 27017 indica que se deberían definir, documentar y monitorear procedimientos para las operaciones administrativas de un entorno de computación en la nube. |
| **Protección contra código malicioso** | Proveer de políticas, estrategias y herramientas de protección, a fin de evitar la presencia de *malware*. | **Controles contra *software* malicioso:** Deberían de implementarse controles con herramientas que permitan detectar, prevenir y recuperar ante afectaciones ocasionadas por *malware* y combinar con la concientización adecuada de los usuarios. |
| **Copias de seguridad** | Establecer estrategias que garanticen el respaldo en caso de pérdida o daño de la información. | **Copias de seguridad de la información**. Deberían de establecerse políticas y procedimientos que obliguen a realizar pruebas regulares de las copias de seguridad realizadas al *software*, los datos y a las imágenes de sistema operativo. |
| **Registro de actividad y supervisión** | Registrar los eventos provocados por incidentes de seguridad de la información y generar y conservar las evidencias. | **Registro y gestión de eventos de actividad**: Se deberían revisar periódicamente los registros relacionados con incidentes de seguridad producidos. |
| **Protección de los registros de información.** Los registros de incidentes de seguridad deberían ser protegidos contra accesos no autorizados. |
| **Registros de actividad del administrador y los usuarios de los sistemas.** Deberían establecerse estrategias y procedimientos que registren las acciones y el resultado de las mismas hechas por todos los usuarios sobre las aplicaciones, para luego revisar y proteger periódicamente. |
| **Sincronización de relojes.** Se deberían establecer políticas y procesos de actualización y sincronización única en los relojes de los equipos de la organización. |
| **Monitorización de los servicios de nube.** Este control extendido en ISO/IEC 27017 indica que el cliente debería disponer de la capacidad de monitorear aspectos específicos de la operación de los servicios de nube que el cliente utiliza. |
| **Gestión del *software* que se encuentra en producción** | Cuando las aplicaciones y servicios están en producción, se debe garantizar la integridad y disponibilidad de los sistemas operacionales de la organización. | **Instalación del *software* en sistemas en producción.** Se deberían implementar procedimientos y políticas de control para evitar la instalación de *software* en aplicaciones y sistemas que se encuentren en producción. |
| **Gestión de la vulnerabilidad técnica** | Preparar los servicios y activos para evitar la existencia de vulnerabilidades técnicas que puedan ser explotadas, poniendo en riesgo la organización. | **Gestión de las vulnerabilidades.** Se deberían desarrollar estrategias de análisis de vulnerabilidades sobre los sistemas de información, de manera oportuna y periódica, para evaluar qué tan alta es la exposición y, con este insumo, implementar medidas para mitigar los riesgos. |
| **Restricciones en la instalación de *software*.** Se deberían establecer e implementar las políticas y reglas que determinan el proceso de instalación de *software* por parte de los usuarios. |
| **Consideraciones de las auditorías a los sistemas informáticos** | Disminuir el impacto que podría generar el realizar actividades de auditoría en los sistemas en producción. | **Controles de auditoría.** Se deberían establecer estrategias de coordinación y planificación de las actividades de auditoría cuando estas involucren la verificación de los aplicativos, servicios y sistemas en producción. |

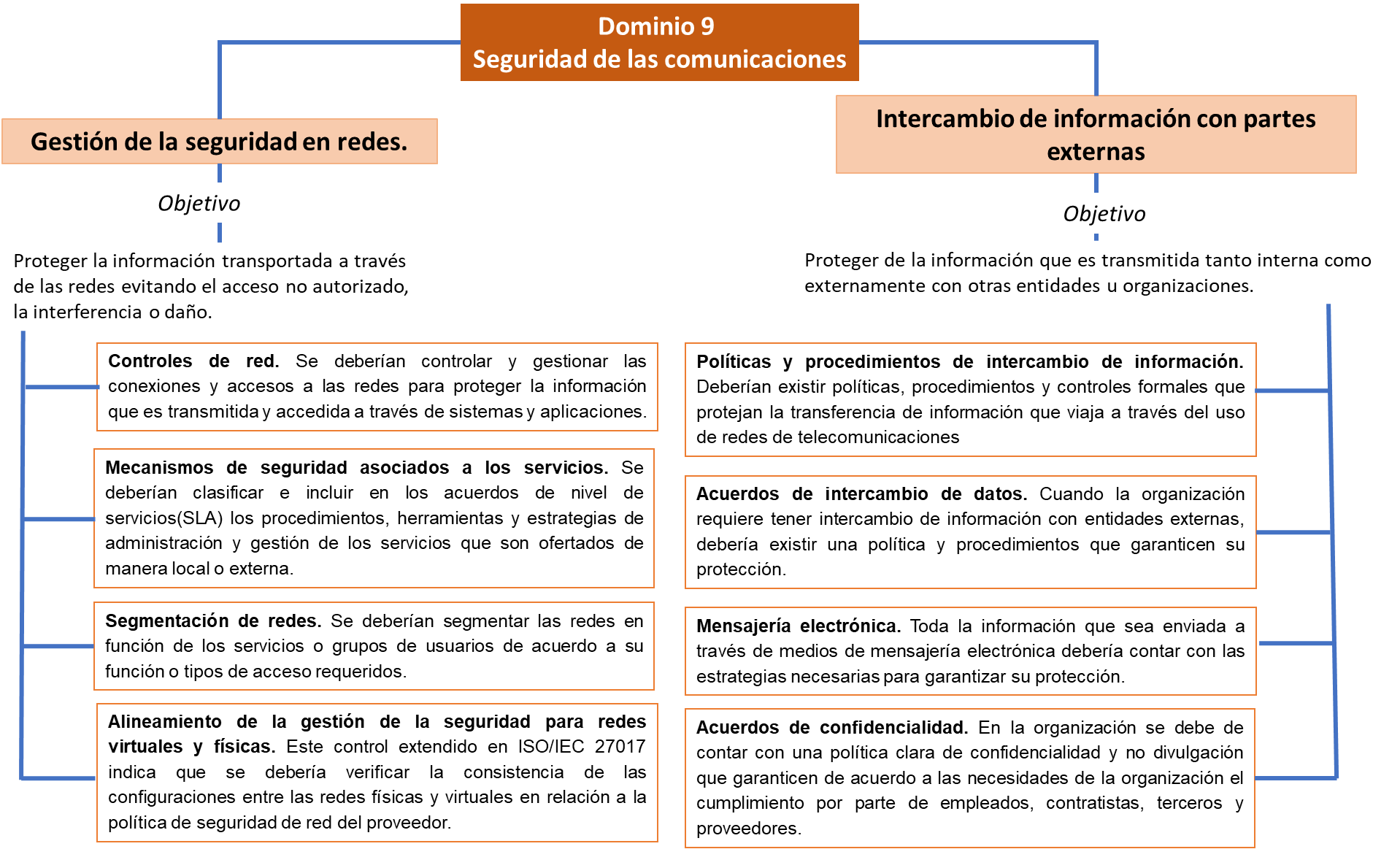
* **Dominio 9. Seguridad de las comunicaciones**

Este es un control que busca la protección de la información que es transportada a través de las redes telemáticas, al igual que la infraestructura que la soporta.

Cuando existe intercambio con otras organizaciones, deberían establecerse acuerdos y políticas que regulen el intercambio y el cumplimiento de la legislación vigente.

**Figura 6**

*Controles de la seguridad de las comunicaciones*



* **Dominio 10. Adquisición, desarrollo y mantenimiento de sistemas informáticos.**

Este es un dominio que busca el establecimiento de políticas y procesos formales en todas las fases del ciclo de desarrollo de *software* y en los procesos de adquisición de aplicaciones. Para este objetivo, se requiere:

* + Asegurar la inclusión de controles para la validación de datos en los procesos de adquisición y el desarrollo de los sistemas informáticos.
  + Definir e implementar las normas y procedimientos que serán aplicados durante el ciclo de vida de los aplicativos informáticos y de la infraestructura de base que los soporta.
  + Definir los métodos para proteger la información sensible o crítica.
  + Deben de establecerse medidas de protección especiales sobre los aplicativos o servicios que soportan la operación de la empresa.

En el siguiente recurso didáctico, se especifican los controles relacionados con el dominio de adquisición, desarrollo y mantenimiento de sistemas informáticos:



* **Dominio 11. Relación con los proveedores**

El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.

La organización debe chequear la implementación de los acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios, para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados con terceras personas.

Los controles aplicados en el dominio 11, relación con los proveedores, se encuentran descritos en la siguiente tabla:

**Tabla 2**

*Controles de la relación con los proveedores*

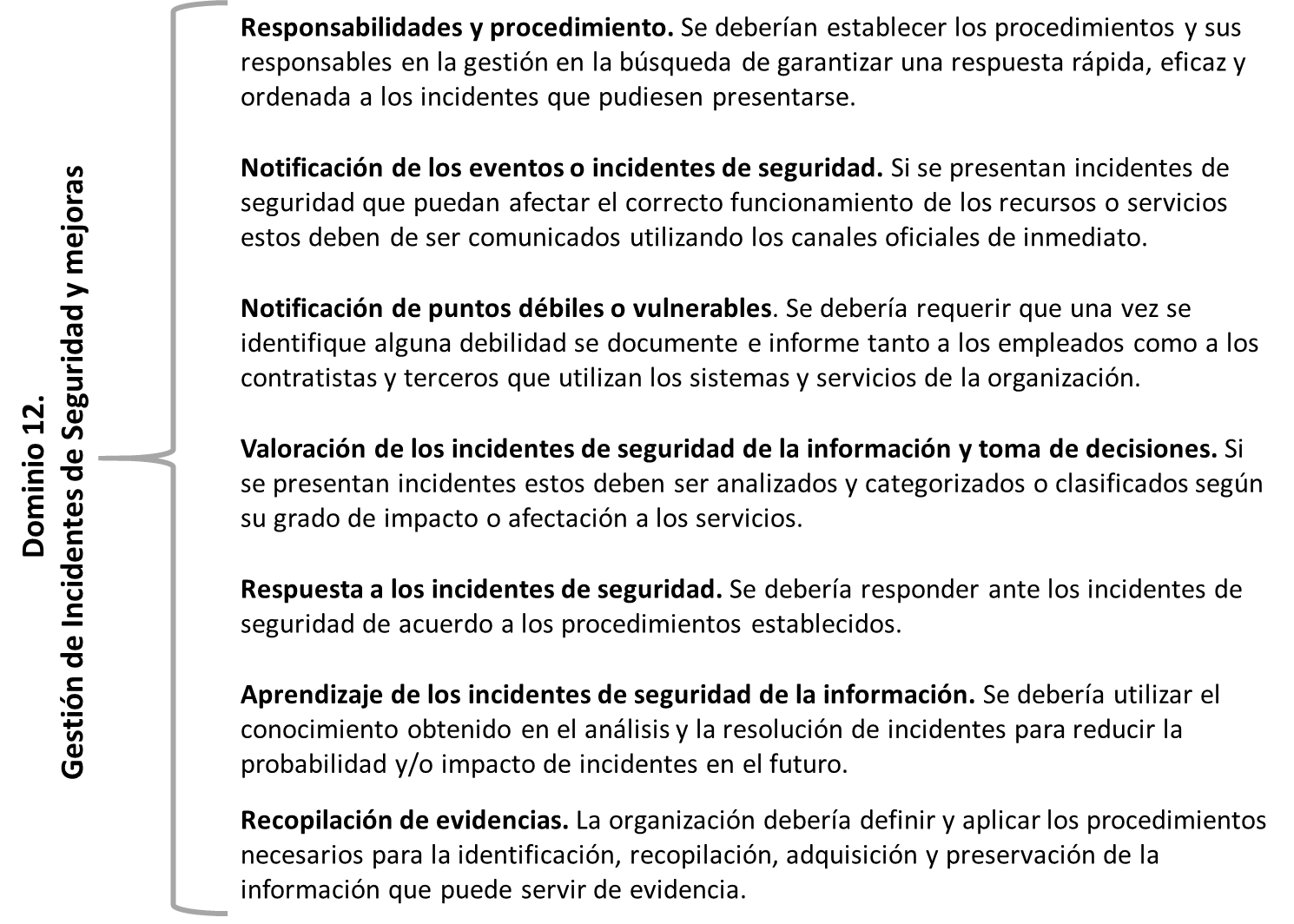
| **CONTROL DE LA NORMA** | **OBJETIVO/CONDICIÓN** | **APLICACIÓN DE CONTROLES** |
| --- | --- | --- |
| **Seguridad de la información en las relaciones con proveedores** | Se deberían proteger los datos e información que por su particularidad requieran ser utilizados por proveedores o terceros con quien se tenga algún tipo de contrato o vínculo. | **Política de seguridad de la información para proveedores.**  Se deberían establecer y firmar acuerdos y políticas de confidencialidad y seguridad que incluyan requisitos de seguridad de la información, con el objetivo de mitigar los riesgos asociados al acceso por parte de proveedores y terceras personas. |
| **Tratamiento del riesgo dentro de acuerdos de suministro.** Se deberían establecer y acordar los requerimientos de seguridad pertinentes y ajustados a cada proveedor que requiera acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura que soportan la información de la organización. |
| **Gestión de la prestación del servicio por proveedores** | Establecer acuerdos de nivel de seguridad ajustados a cada proveedor que permitan mantener una provisión adecuada y alineada de los servicios con estos acuerdos. | **Supervisión y revisión de los servicios prestados por externos.**  Las organizaciones deberían de establecer rutinas regulares de revisión, monitoreo y auditoría de los servicios ofrecidos por el proveedor. |
| **Gestión de cambios en los servicios** **prestados** **por externos.**  Se deberían establecer las políticas y procedimientos necesarios para la gestión de cambios en los servicios que realizan los proveedores, manteniendo y mejorando las políticas de seguridad de la información, los procedimientos y controles específicos. |

* **Dominio 12. Gestión de incidentes de seguridad**

Busca garantizar que los incidentes relacionados con la seguridad de la información y las vulnerabilidades que permiten su ejecución sean comunicados de manera oportuna y formal, para que se apliquen las acciones correctivas necesarias y en el tiempo adecuado.

**Figura 7**

*Controles de la gestión de incidentes de seguridad*



* **Dominio 13. Seguridad de la información y la continuidad del negocio**

El objetivo es garantizar el cumplimiento de la seguridad de la información durante las fases de activación, desarrollo y puesta en producción o reactivación de un servicio o aplicación posteriormente a una caída o interferencia, para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos, sin perder la seguridad de la información.



* **Dominio 14. Cumplimiento**

Las administraciones de los sistemas de información están reguladas por disposiciones legales y contractuales, por lo que cada servicio o recurso debe tener claridad en cuanto a sus requisitos normativos y contractuales a cumplir, a fin de evitar sanciones de cualquier tipo como consecuencia del no cumplimiento.

En la siguiente tabla, podrá encontrar, de manera general, los controles aplicados a este dominio.

**Tabla 3**

*Controles de cumplimiento*

| **CONTROL DE LA NORMA** | **OBJETIVO/CONDICIÓN** | **APLICACIÓN DE CONTROLES** |
| --- | --- | --- |
| **Cumplimiento de los requisitos legales y contractuales** | No presenta | **Identificación de la legislación aplicable.** Se debería identificar, documentar y mantener en constante actualización la información explícita de cada sistema de información, a fin de cumplir con la legislación y normativa de cada servicio o recurso. |
| **Derechos de propiedad intelectual.** Se deberían establecer políticas de seguridad que obliguen a la utilización de *software* legal y al respeto por la propiedad intelectual de los fabricantes y proveedores. |
| **Protección de los registros de la organización.** Según los requerimientos legales, contractuales o legislativos, se debe buscar la protección por pérdidas, destrucción, falsificación, accesos y publicaciones no autorizadas de los registros de los sistemas de información. |
| **Protección de datos y privacidad de la información personal.** Según corresponda, se debería garantizar el derecho a la privacidad y protección de los datos personales, de acuerdo con la legislación y el cumplimiento legal requerido. |
| **Regulación de los controles criptográficos.** Se deberían utilizar controles de cifrado de datos, en cumplimiento con la legislación, las normativas y los acuerdos establecidos. |
| **Revisiones a la seguridad de la información** | Garantizar que la seguridad de la información se implemente y gestione de acuerdo con las políticas y los procedimientos establecidos por la organización. | **Revisión independiente de la seguridad.** Se deberían revisar los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información, de manera regular e independiente, planificada o cuando se presenten cambios significativos en la organización. |
| **Cumplimiento de las políticas y normas establecidas para la seguridad.** Los gerentes deberían revisar periódicamente el cumplimiento de los procedimientos de seguridad dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad establecido por la organización. |
| **Verificación del cumplimiento.** Los sistemas de información se deberían revisar periódicamente para verificar su cumplimiento con las políticas, normas y estrategias de seguridad dispuestas por la organización. |

1. **Controles *Cloud Security Alliance - Security Guidance for Critical Areas of Focus in Cloud Computing* v4.0.**

Las buenas prácticas que generan seguridad en el escenario de la computación en la nube son uno de los propósitos de Cloud Security Alliance (CSA), por esta razón, han elaborado una hoja de ruta práctica y ejecutable, con el fin de que las organizaciones puedan afrontar el reto que significa el almacenaje en la nube.

Esto no quiere decir que esta organización (CSA) desee crear una nueva clasificación de referencia, por el contrario, se trata de un modelo en armonía con los ya existentes, especialmente el modelo de trabajo **NIST** *Special Publication* 800-145, **ISO/IEC** 17788 e **ISO/IEC** 17789, solo que hay mayor concentración en aspectos de seguridad requeridos por profesionales en el ramo. En esta versión 4.0, hay una serie de dominios que deben tenerse en cuenta, estos son:

* DOMINIO 1 - Conceptos y arquitecturas de la computación en la nube
* DOMINIO 2 - Gobierno y gestión del riesgo corporativo
* DOMINIO 3 - Cuestiones legales, contratos y descubrimiento electrónico
* DOMINIO 4 - Cumplimiento y gestión de auditoría
* DOMINIO 5 - Gobierno de la información
* DOMINIO 6 - Plano de gestión y continuidad del negocio
* DOMINIO 7 - Seguridad de la infraestructura
* DOMINIO 8 - Virtualización y contenedores
* DOMINIO 9 - Respuesta ante incidentes
* DOMINIO 10 – Seguridad de aplicaciones
* DOMINIO 11 - Seguridad y cifrado de datos
* DOMINIO 12 - Gestión de identidades, derechos y accesos
* DOMINIO 13 - Seguridad como servicio

De manera general, se abordará cada uno de los dominios antes mencionados:

* **Dominio 1. Conceptos y arquitecturas de la computación en la nube.**

En este dominio, se describe y define la computación en la nube, se referencia una terminología básica, y se detalla la lógica general y el marco arquitectónico utilizados en el resto del documento. (ISMS Forum, 2021)



* **Dominio 2. Gobierno y gestión del riesgo corporativo.**

La gobernanza o el gobierno de la gestión del riesgo es un tema muy extenso, por lo que este recurso se centrará en cómo afecta o se focaliza desde la nube, y esto se ve en 4 aspectos fundamentales, así:



|  | Recuerde que la tarea principal de la seguridad de la información es la de proveer de procesos y controles para proteger la información electrónica y los sistemas que se usan para acceder a ella. Es decir, en una estructura jerárquica simple, la seguridad de la información es una herramienta para la gestión del riesgo de la información, que a su vez es un instrumento para la gestión del riesgo empresarial, y éste se convierte en una herramienta de gobernanza. Los cuatro conceptos están estrechamente relacionados, pero requieren de un enfoque, de procesos, y de herramientas individuales. |
| --- | --- |

* **Dominio 3. Cuestiones legales, contratos y descubrimiento electrónico.**

En este dominio, se hace referencia a algunas de las dificultades legales más comunes que pueden surgir al mover datos o servicios a la nube y al operar las solicitudes de descubrimiento electrónico emanadas de los procesos judiciales. Este dominio cubre los siguientes aspectos, como puede observarse en el siguiente recurso didáctico:



* **Dominio 4. Cumplimiento y gestión de auditoría.**

Migrar servicios tradicionales a la nube requiere que las organizaciones estén al tanto legal sobre la entrega, medición y comunicación del cumplimiento legislativo de varias regulaciones en cada jurisdicción (país), este es uno de los muchos desafíos que se debe afrontar, y tanto cliente como proveedores deben entender y valorar las diferencias territoriales y las implicaciones que acarrea su no cumplimiento, entre las que se encuentran:



Algunos temas adicionales, específicos de la nube, a los se debe prestar especial atención, se pueden ver a continuación:



* **Dominio 5. Gobierno de la información.**

La seguridad de la información tiene por objetivo principal la protección de los datos que son utilizados en las aplicaciones y sistemas informáticos de las organizaciones. Al migrar servicios a la nube, se vienen nuevos desafíos debido a la elasticidad y entornos multipropietarios, ya que estos datos pueden ser transferidos a entornos externos o públicos.

El gobierno de la información/gobierno del dato se define como la garantía ofrecida respecto al uso adecuado de los datos e información, de acuerdo con las políticas, estándares y estrategias organizacionales, donde también se tienen en cuenta los objetivos de regulación (hasta dónde va el alcance de dicha regulación), los objetivos contractuales (cuál es la meta del contrato establecido) y los de negocio (qué y cómo se permite la transacción entre las partes).

En cuanto al gobierno de la información y de los datos, hay una serie de características del uso de la nube y de almacenamiento de información que pueden afectar (ISMS Forum, 2021), entre los cuales están:



* **Dominio 6. Plano de gestión y continuidad del negocio.**

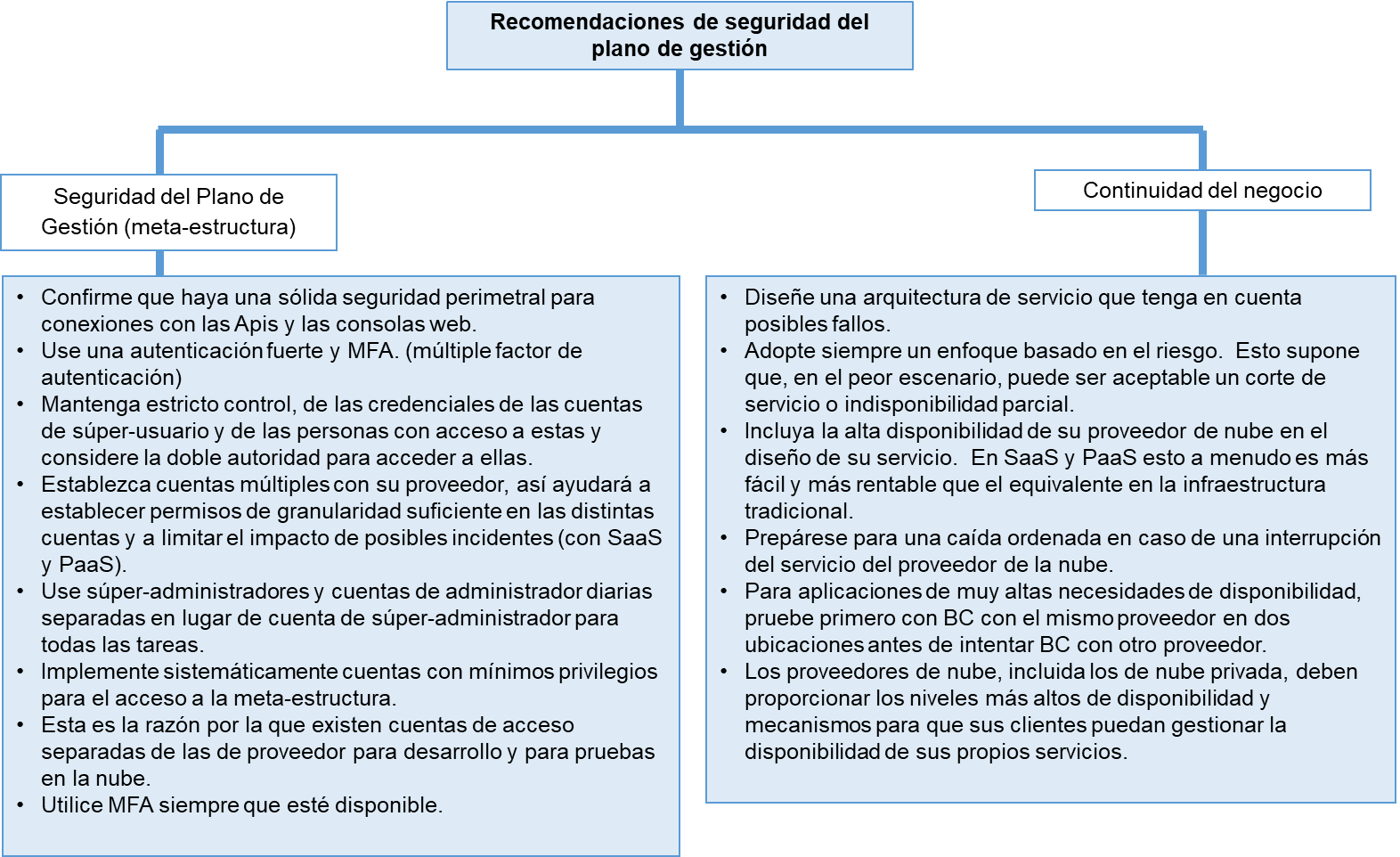
El plano de gestión está compuesto por herramientas e interfaces que permiten la administración de la infraestructura, las plataformas y las aplicaciones. Sin embargo, la nube permite desglosar y centralizar la administración de estos recursos. La tecnología ha permitido que en el presente se haga control mediante API y consolas web, lo que antes se llevaba a cabo mediante la configuración del centro de datos con servidores y cables.

Es así que el acceso al plano de gestión equivale al acceso sin restricciones al centro de datos, si no hay aplicación de otros controles de seguridad que limiten dicho acceso o trabajen dentro de este.

En este dominio, se deben tener en cuenta, entre otras, las siguientes recomendaciones:

**Figura 8**

*Recomendaciones de seguridad del plano de gestión*



Nota*.* Adaptada de laGuía de seguridad de áreas críticas para la computación en la nube V4.0

<https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf>

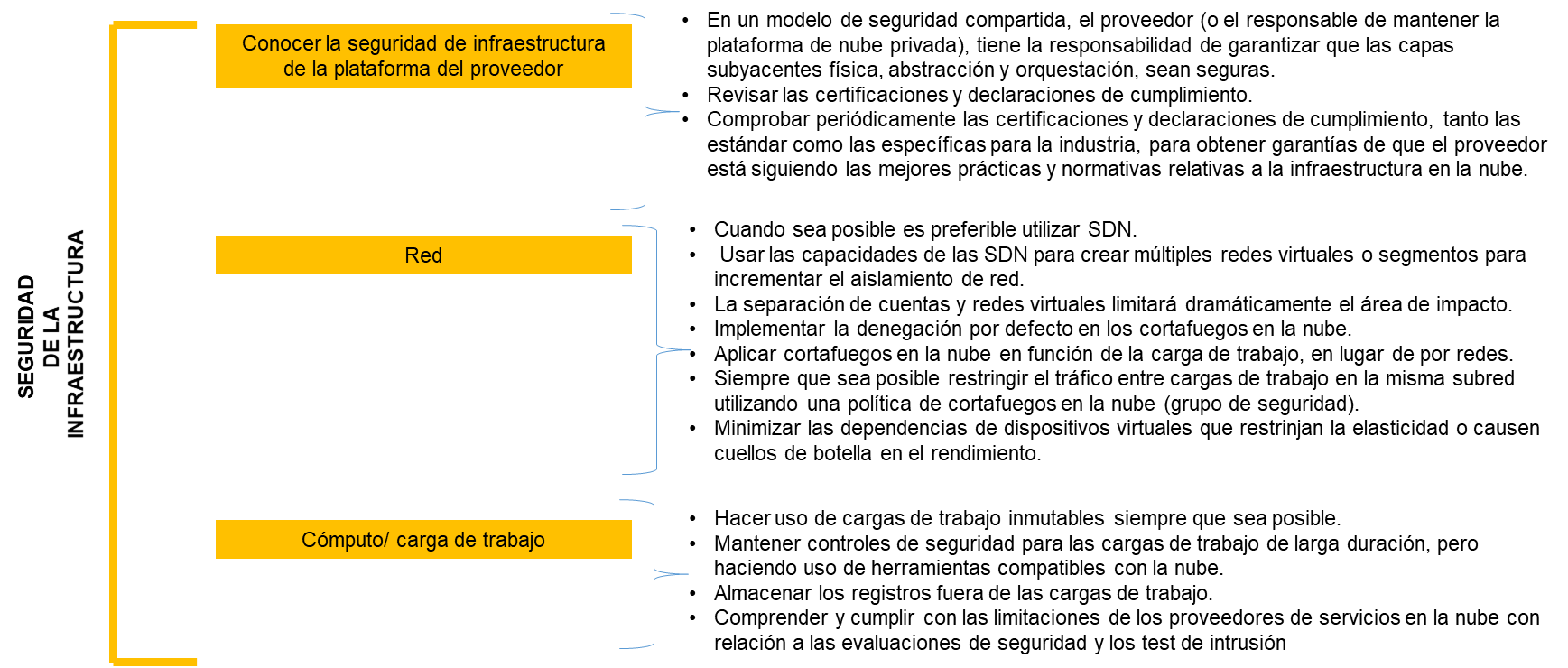
* **Dominio 7. Seguridad de la infraestructura**

La seguridad en la nube es un factor diferencial y clave, este involucra las redes de datos, de telecomunicaciones y de servidores sobre las cuales se construyen las nubes. Comprende las capas más inferiores de la seguridad, incluyendo desde las instalaciones físicas hasta la configuración e implementación de los componentes de la infraestructura sobre la cual está construida la nube; además de tener presente la seguridad de computación (carga de trabajo), las artes y el almacenamiento.

Para este dominio, se deben tener en cuenta las siguientes recomendaciones:

**Figura 9**

*Seguridad de la infraestructura*



Nota*.* Adaptada de laGuía de seguridad de áreas críticas para la computación en la nube V4.0

<https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf>

* **Dominio 8. Virtualización y contenedores**

La virtualización es la tecnología fundamental que permite la computación en la nube; no es solo una herramienta para crear máquinas virtuales, siendo la computación en la nube una tecnología que agrupa una gran cantidad de recursos; es ahí donde la virtualización permite el agrupamiento de estos recursos, que posteriormente serán administrados a través de la orquestación.

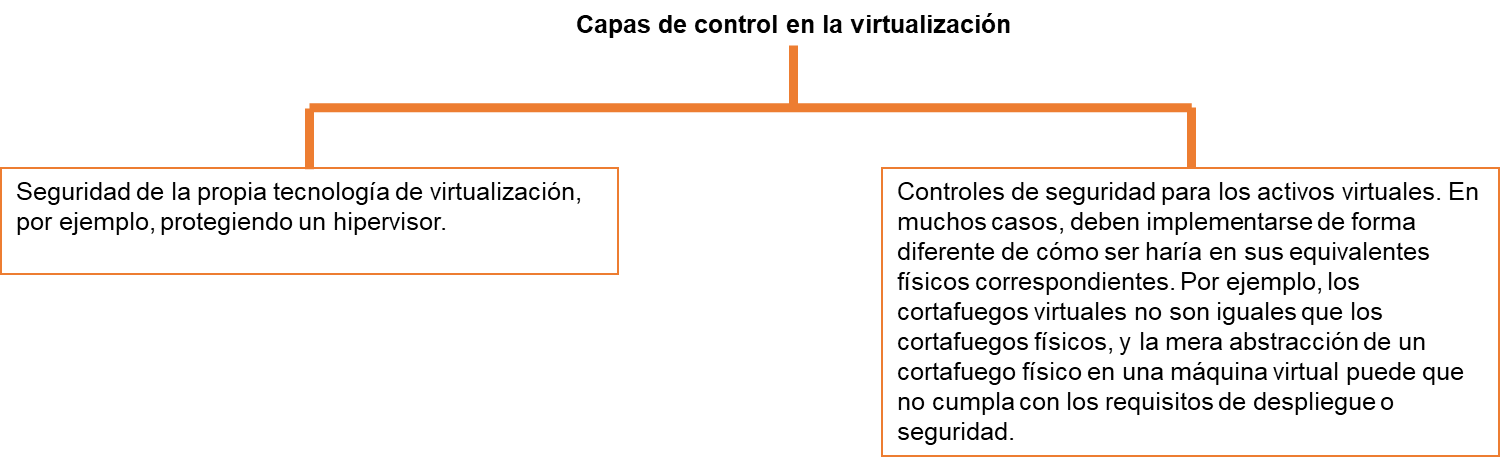
Los recursos que esencialmente son utilizados para grupos virtualizados son:

* Computación
* Red
* Almacenamiento
* Contenedores

La virtualización agrega dos nuevas capas a los controles de seguridad:

**Figura 10**

*Capas de control en la virtualización*



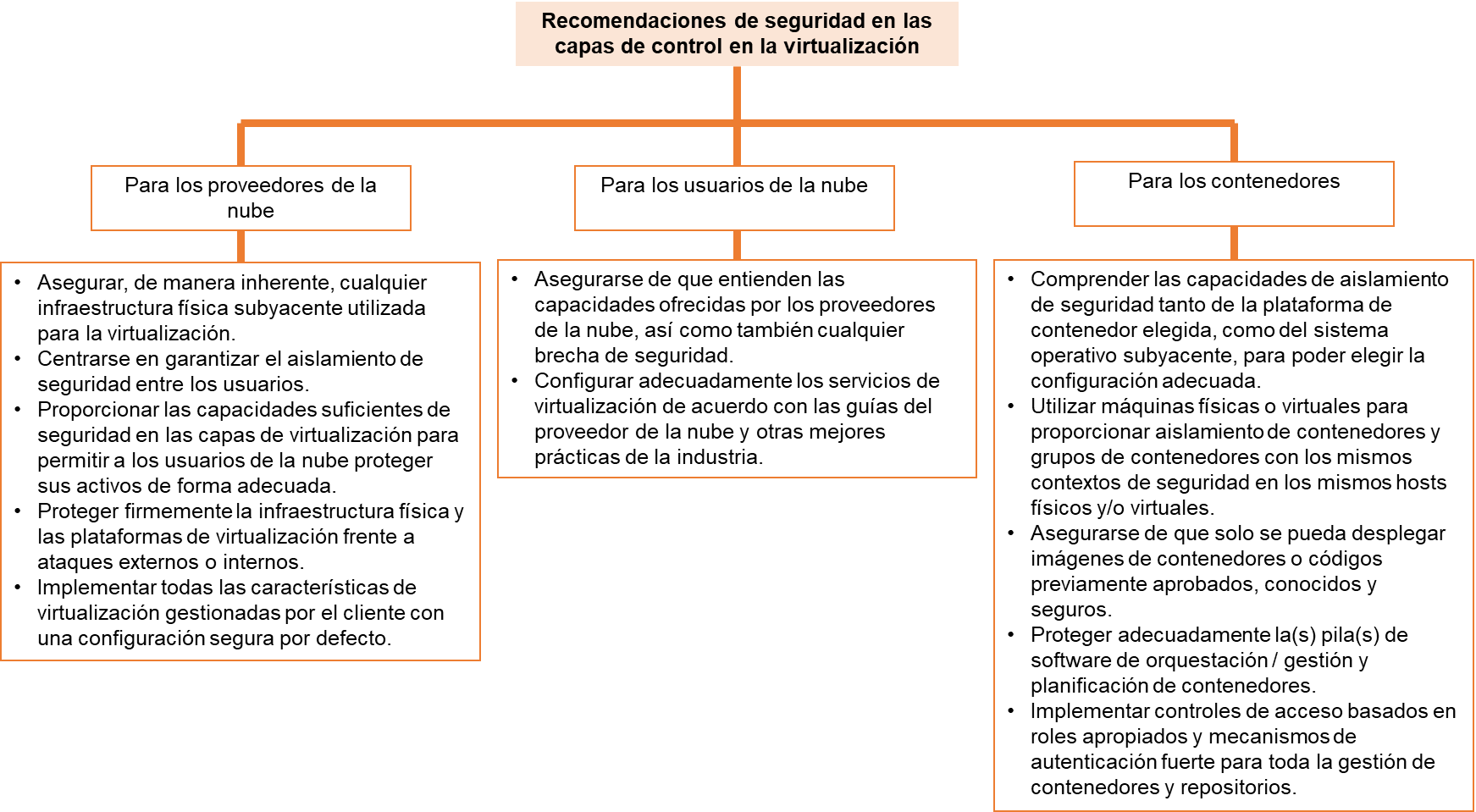
Nota*.* Adaptada de laGuía de seguridad de áreas críticas para la computación en la nube V4.0

<https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf>

Las siguientes son algunas de las recomendaciones a tener en cuenta para este dominio.

**Figura 11**

*Recomendaciones de seguridad en las capas de control*



Nota*.* Adaptada de laGuía de seguridad de áreas críticas para la computación en la nube V4.0

<https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf>

* **Dominio 9. Respuesta ante incidentes**

Este es un aspecto fundamental en cualquier programa de seguridad. Si bien los controles preventivos ayudan a mitigar en gran parte los riesgos, no siempre son efectivos, por lo que las organizaciones deben contar con un plan de respuesta a incidentes, que les permita establecer cómo actuar frente a un ataque, toda vez que los procesos de la nube son distintos, así que se deben adaptar a esta nueva realidad.

A continuación, se muestra cómo es el ciclo de vida de respuestas a incidentes, según la recomendación de la norma NIST 800-61 rev2.

**Figura 12**

*Ciclo de vida de una respuesta a incidentes*



Nota. Guía de seguridad de áreas críticas para la computación en la nube V4.0

[*https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf*](https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf)

A continuación, encontrará algunas recomendaciones del dominio:



* **Dominio 10. Seguridad de aplicaciones**

El dominio correspondiente a la seguridad de la aplicación está destinado a los equipos de desarrollo de *software* y TI que busquen el desarrollo de aplicaciones seguras en entornos de computación en la nube, en especial, *PaaS* e *IaaS* (varias de las técnicas en esta sección son usadas para respaldar aplicaciones de *SaaS* seguras). (CSA, 2018).

En este dominio, usted se centrará en:

* Cómo difiere la seguridad de la aplicación en la nube.
* Revisar los aspectos básicos de desarrollo de *software* seguro y cómo estos cambian en la nube.
* Aprovechar las capacidades de la nube para desarrollar aplicaciones en la nube más seguras.

Las siguientes son algunas de las recomendaciones que propone el dominio:



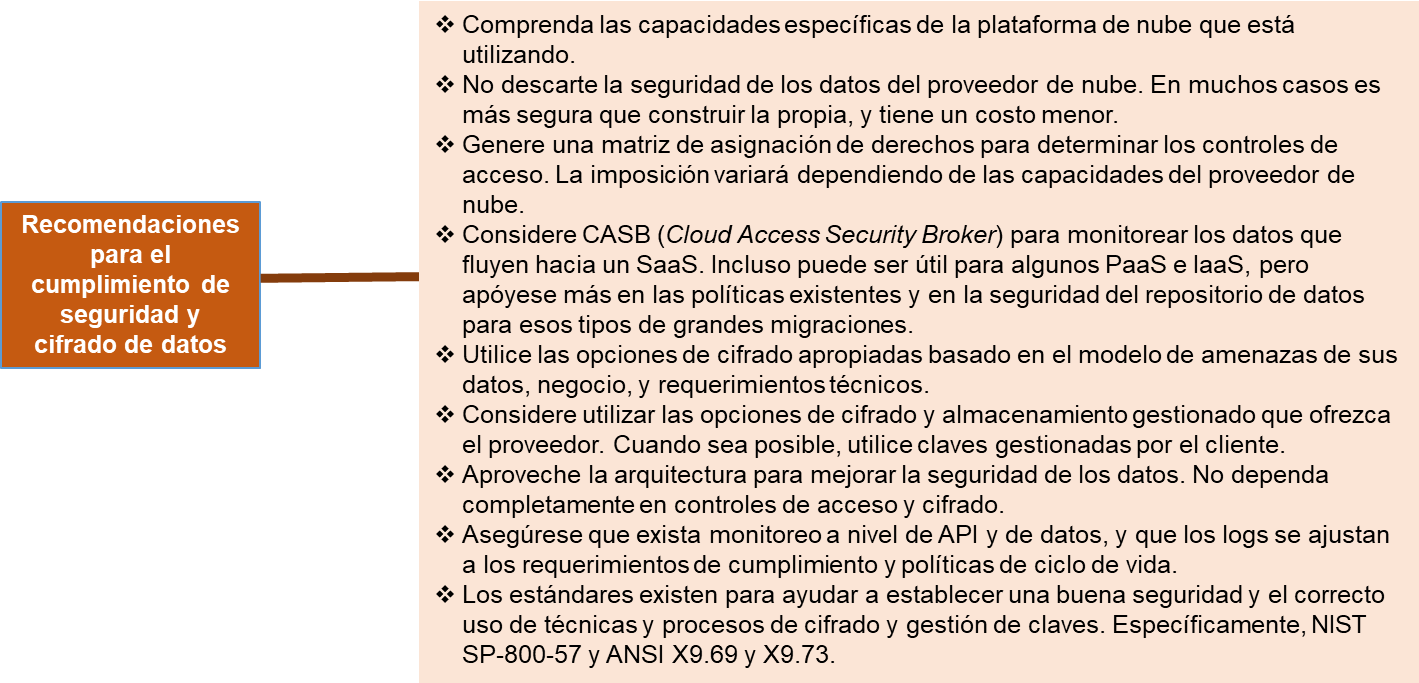
* **Dominio 11. Seguridad y cifrado de datos**

En relación al gobierno de la información, ya se ha visto que lo más importante es la seguridad de los datos, por esta razón, las organizaciones no confían gran volumen de datos y optan por el cifrado, con lo que la seguridad de la información se equipara a la seguridad de los datos; sin embargo, se debe focalizar en los controles relacionados con la protección de los propios datos, donde el cifrado es uno de los controles más importantes, entre otros.

Para garantizar el cumplimiento de este dominio, las siguientes son las recomendaciones:

**Figura 13**

*Recomendaciones para el cumplimiento de seguridad y cifrado de datos.*



Nota. Adaptada de la Guía de seguridad de áreas críticas para la computación en la nube V4.0

[*https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf*](https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf)

* **Dominio 12. Gestión de identidades, derechos y accesos.**

Este dominio se centra principalmente en la gestión de identidades y el control de acceso entre una organización y los proveedores de servicio, o bien entre los proveedores y los servicios ofrecidos.

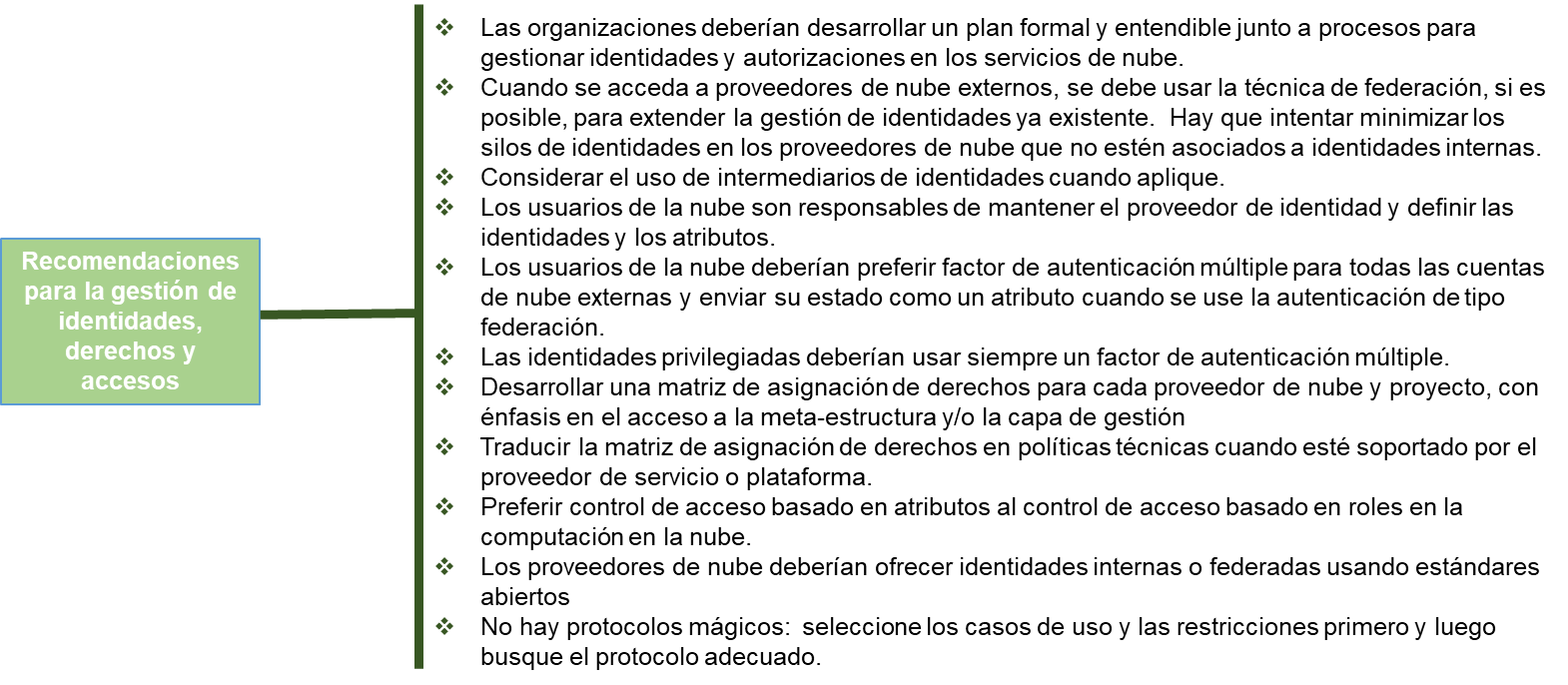
La diferencia principal es la relación entre el proveedor de servicio de nube y el usuario de la nube, incluso si se trata de nubes privadas. La gestión de identidades y el control de acceso no pueden ser gestionados por uno de los actores de manera individual, sino que se requieren relaciones de confianza y delegación de responsabilidades, que son implementadas por diferentes mecanismos técnicos. Normalmente, estos mecanismos técnicos se implementan como una federación de identidades. Esto se complica por el hecho de que muchas organizaciones tienen diferentes (a veces cientos) proveedores de nube, para los que es necesario extender dicha gestión.

Gartner define la Gestión de Identidades y Control de Accesos como “la disciplina en seguridad que habilita a las diferentes identidades para acceder a los recursos adecuados, en el momento oportuno y por la razón necesaria”.

Las siguientes son las recomendaciones para este dominio:

**Figura 14**

*Recomendaciones para la gestión de identidades, derechos y accesos*



Nota. Adaptada de la Guía de seguridad de áreas críticas para la computación en la nube V4.0

[*https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf*](https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf)

* **Dominio 13. Seguridad como servicio**

Si bien el guía de seguridad de áreas críticas para la computación en la nube v4.0 se centra en la protección de los servicios, plataformas y despliegues hechos en la nube, los proveedores de servicios *cloud* han desarrollado el servicio **SecaaS** (Seguridad como servicio), ofreciendo a través de este nuevo modelo capacidades de seguridad como servicio.

La seguridad como servicio se corresponde con un abanico amplio de tecnologías, que de forma general deben cumplir con los siguientes criterios:

* **SecaaS** incluye seguridad de productos o servicios que se entregan como un servicio en la nube.
* Para ser considerado **SecaaS**, los servicios deben cumplir con las características esenciales de **NIST** para la computación en la nube, tal como se definen en el Dominio 1.

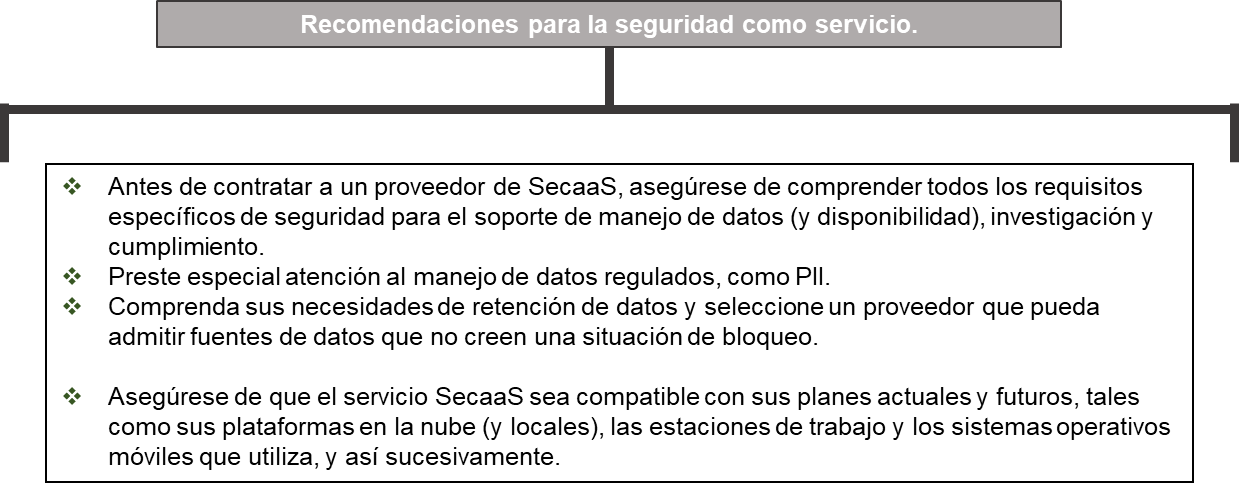
Entre otras, las siguientes son las categorías que incluyen este tipo de servicio:

* Gestión de identidades, derechos y accesos
* Agentes de acceso y seguridad a la nube – *Cloud Security Gateway*
* Seguridad de correo electrónico
* Evaluación de seguridad
* Cortafuegos de aplicaciones web
* Detección y prevención de intrusiones (IDS/IPS)
* Gestión de eventos y seguridad SIEM
* Cifrado y gestión de claves
* Planes de recuperación de desastres y continuidad del negocio
* Administración de la seguridad

Las siguientes son las recomendaciones a tener en cuenta para este dominio.

**Figura 15**

*Recomendaciones para la seguridad como servicio*



Nota. Adaptado de la Guía de seguridad de áreas críticas para la computación en la nube V4.0

[*https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf*](https://www.ismsforum.es/ficheros/descargas/csaguide-v4-es-20181525872082.pdf)

1. **Controles NIST Marco del Instituto Nacional de Estándares y Tecnología**

Si bien el marco **NIST** es un estándar que hace parte del Departamento de Comercio de los Estados Unidos y que, por supuesto, es ampliamente utilizado en este país, también es un buen referente a nivel internacional como un marco muy popular para la ciberseguridad.

**NIST** es exhaustivo y está basado en el riesgo, lo que lo hace conveniente para organizaciones en una amplia variedad de industrias; dispone de equivalencias con otros marcos internacionales, como la norma **ISO/IEC 27001**: **2013,** para orientarse en su aplicación.

El marco (*framework*) **NIST** está enfocado en la gestión de la ciberseguridad y está compuesto por tres partes: el núcleo del marco, los niveles de implementación del marco y los perfiles del mismo, donde cada componente está conectado e impulsa el desarrollo de actividades de ciberseguridad en cada uno de ellos.

A continuación, se hace una descripción general de cada uno de estos componentes:

**4.1 Núcleo**

Para el CTRL-IT (2015), grupo de expertos dedicados a las tecnologías de la información, el núcleo presenta estándares, directrices y prácticas de la industria de una manera que permite la comunicación de las actividades y los resultados de ciberseguridad a toda la organización, desde el nivel ejecutivo hasta el nivel de implementación/operaciones.

El núcleo consta de cinco funciones simultáneas y continuas:

**Figura 16**

*Funciones del CSF*



Nota. Tomada de Marco de Ciberseguridad NIST / Un abordaje integral de la Ciberseguridad

<https://usecim.net/2019/09/04/un-abordaje-integral-de-la-ciberseguridad-funciones-del-cybersecurity-framework-csf/>

A continuación, se presentan las funciones que tiene el núcleo en los controles **NIST**:





**4.2 Niveles de implementación ("*TIERs*")**

Para la revista UCESIM (2021), de México, los niveles detallan el grado en que las prácticas de gestión de riesgos de ciberseguridad de una organización exhiben las características definidas en el marco. Estos niveles se presentan desde el nivel 1, correspondiente a Parcial, hasta el nivel 4, que es el Adaptativo, describiendo de forma ascendente el grado de rigurosidad, qué tan bien integradas están las decisiones de riesgo de ciberseguridad en decisiones de riesgo más amplias, y el grado en que la organización comparte y recibe información de ciberseguridad de fuentes externas.

El nivel de implementación permite que las organizaciones determinen qué nivel de implementación o **TIER** desean lograr, el cual debe ser seleccionado a partir de la gestión de riesgos, amenazas, los requisitos legales y reglamentarios, los objetivos de negocio/misión y las limitaciones organizacionales, con el objetivo de mitigar o reducir el riesgo de ciberseguridad de los activos y recursos críticos a niveles aceptables para la organización.

En la Figura 17, podrá observar la distribución de los *Tiers*, de manera general:

**Figura 17**

*Niveles de implementación* ***NIST*** *(Tiers)*



Nota. Tomada de Un abordaje integral de la ciberseguridad OEA White Paper Series

[https://miro.medium.com/max/982/1\*hm-53j3FRWud2baCO9JeDg.png](https://miro.medium.com/max/982/1*hm-53j3FRWud2baCO9JeDg.png)

A continuación, se entrega una descripción un poco más detallada de los diferentes *Tiers*, los cuales se miden en tres aspectos fundamentales:

* Proceso de gestión de riesgos
* Programa integrado de gestión de riesgos
* Participación externa



* 1. **Perfil del marco**

Los perfiles son la única formación de una organización, a nivel de sus requisitos y objetivos organizacionales, la tolerancia al riesgo y los recursos, con respecto a los resultados deseados del *Framework* *Core*. Pueden utilizarse para identificar las oportunidades de mejora frente a la ciberseguridad, mediante una comparación entre el perfil “actual” y el perfil “objetivo”.

En relación con el perfil actual, este permite a las organizaciones hacer una revisión objetiva-real (sin que implique auditorías formales u otras evaluaciones técnicas) del programa de ciberseguridad que se sigue, en relación con el CFS, y de esta forma, enterarse de cuál es la situación que se vive. De acuerdo con el riesgo organizacional, los requisitos de cumplimiento y los objetivos organizacionales, se puede generar el perfil objetivo, que, al ser comparado con el perfil actual, ofrecerá la estrategia de liderazgo y las prioridades para: contratación, capacitación, cambio o actualización de políticas, cambios en los procedimientos y adquisición de tecnología.

**4.2 Cómo utilizar el *framework* CSF**

El *framework* está diseñado para complementar las operaciones *core* del negocio y de las actividades de ciberseguridad existentes; este permite ser utilizado en la creación de una nueva estrategia o plan de seguridad, o la mejora de uno ya existente.

A continuación, se ofrecen siete (7) pasos que ilustran la manera en que se puede utilizar el *framework*:



**Síntesis**

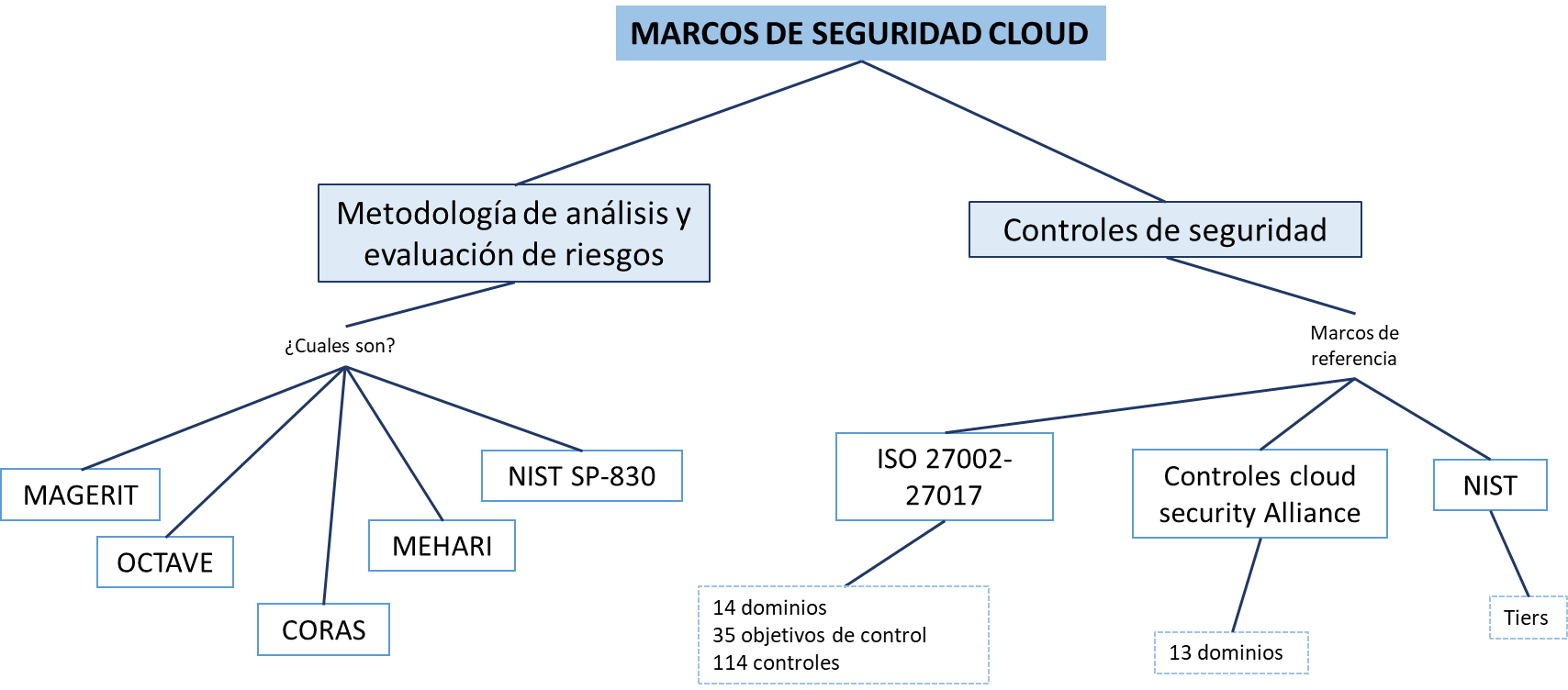
La seguridad en la nube y los datos de los clientes son una prioridad asumida en los contenidos de este componente, así como la orientación en la implementación de controles y procesos de administración diseñados para mitigar riesgos y mejorar los servicios de sus productos.

Estos controles y procesos se crean mediante algunos principios que generan reglas generales y directrices que se relacionan con las organizaciones, sus políticas y procedimientos internos, y que corresponden con:

* Riesgo: entendiendo que la administración de riesgos comprende las posibles amenazas y el cálculo del riesgo, teniendo en cuenta a todos los responsables de la toma de decisiones.
* Control: que establece un equilibrio entre eficacia y eficiencia, implementando los controles adecuados para el riesgo asociado.
* Seguridad: proporciona funciones preventivas y de protección, para garantizar un servicio seguro.

Esta responsabilidad compartida para la seguridad se logra cuando son asumidos los roles que desempeñan cada una de las personas o los procesos que hacen parte de la seguridad en la nube. Pues no basta con que el proveedor de servicios en la nube garantice seguridad en su infraestructura física, sino que también corresponde al cliente y al usuario seguir pautas y pasos para responder, de igual forma, a los desafíos generados en el avance que tiene la tecnología en la actualidad.

El siguiente mapa ofrece una vista rápida de los contenidos de este componente formativo:

****

**C. Actividades didácticas (opcionales si son sugeridas)**

| **DESCRIPCIÓN DE ACTIVIDAD DIDÁCTICA** | |
| --- | --- |
| Nombre de la Actividad | **Conceptos de marcos de seguridad en la auditoría técnica en *cloud*** |
| Objetivo de la actividad | Afianzar algunos de los conceptos más importantes de la ciberseguridad en *cloud* |
| Tipo de actividad sugerida | Selección múltiple. |
| **Archivo de la actividad**  **(Anexo donde se describe la actividad propuesta)** | Anexo Actividad didáctica 1 |

**D. Material complementario**

| **Tema** | **Referencia APA del Material** | **Tipo de material**  **(Video, capítulo de libro, artículo, otro)** | **Enlace del Recurso o**  **Archivo del documento o material** |
| --- | --- | --- | --- |

| **Controles cloud Security Alliance** | Superintendencia de Industria y Comercio. (s. f.). *Guía para la implementación del principio de responsabilidad demostrada (Accountability)*. <https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf> | Documento | <https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia-Accountability.pdf> |
| --- | --- | --- | --- |

| **Controles de seguridad y marcos de referencia para servicios cloud** | Normas ISO. (s. f.). *ISO 27001 Seguridad de la información*. <https://www.normas-iso.com/iso-27001/> | Página web | https://www.normas-iso.com/iso-27001/ |
| --- | --- | --- | --- |

**E. Glosario**

| **TÉRMINO** | **SIGNIFICADO** |
| --- | --- |
| Amenaza (*Threat*) | Son eventos o incidentes que pueden provocar daño o pérdidas en un recurso informático. |
| Ciberseguridad | Conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos. |
| Control | Directrices y buenas prácticas que deben ser validadas e implementadas en actividades y procesos de adopción de la ciberseguridad. |
| Dominio | Conjunto que incluye todos los activos de la información que deben proteger y cumplir en su totalidad. |
| ISO | Organización de Estándares Internacionales |
| ISO 27000 | Conjunto de normas de la Organización de Estándares Internacionales orientadas al uso y aplicación de buenas prácticas en relación con el diseño, la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI). |
| NIST | Instituto Nacional de Estándares y Tecnología americano |
| Riesgo | Es la probabilidad en la ocurrencia de una amenaza a la seguridad provocando un impacto determinado. |
| Salvaguarda | Estrategia o control implementado para la mitigación de los riesgos. |
| Vulnerabilidad (*Vulnerability*) | Es un punto débil o de fallo de un activo o control que puede ser explotado por una o más amenazas. |

**F. Referencias bibliográficas**

Federation of European Risk Management Associations [FERMA]. (2003). *Estándares de gerencia de riesgos*. <https://www.theirm.org/media/6836/rm_standard_spanish_15_11_04-1.pdf>

International Organization for Standardization [ISO]. (s. f.). *ISO 31000 — Risk management*. Popular Standards. <https://www.iso.org/iso-31000-risk-management.html>

International Organization for Standardization [ISO]. (2018). *ISO/IEC 27005:2018(en) Information technology — Security techniques — Information security risk management*. Online Browsing Platform. <https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-3:v1:en>

Jesaja, M. (2019). *Construcción de modelos de conocimiento de NIST SP 800-181*. Universidad Carlos III de Madrid. <https://e-archivo.uc3m.es/handle/10016/30383>

Mogull, R., Arlen, J., Gilbert, F., Lane, A., Mortman, D., Peterson, G. y Rothman, M. (2017). *Security guidance for critical areas of focus in cloud computing v4. 0*. Cloud Security Alliance. <https://downloads.cloudsecurityalliance.org/assets/research/security-guidance/security-guidance-v4-FINAL.pdf>

Mohanan, S., Sridhar, N., y Bhatia, S. (2021). Comparative Analysis of Cloud Computing Security Frameworks for the Financial Sector. En: X-S Yang, S. Sherratt, N. Dey, A. Joshi (eds) *Proceedings of Sixth International Congress on Information and Communication Technology*. <https://doi.org/10.1007/978-981-16-2380-6_90>

Rizzo, D. (2019). Ciberseguridad implementando el “Nist Cybersecurity Framework”. Universidad de Buenos Aires. <http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1460_RizzoD.pdf>

Ruben.Ramiro. (2018). *Cómo implantar el Framework NIST*. Ciberseguridad.BLOG. <https://ciberseguridad.blog/como-implantar-el-framework-nist>

**G. Control del documento**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** |
| --- | --- | --- | --- | --- |
| **Autor(es)** | Henry Eduardo Bastidas Paruma | Experto Temático | Regional Cauca, Centro de teleinformática y producción industrial | Diciembre 2021 |
| María Inés Machado López | Diseñadora Instruccional | Regional Distrito Capital, Centro de Diseño y Metrología | Diciembre 2021 |
| Silvia Milena Sequeda Cárdenas | Evaluadora Instruccional | Regional distrito capital - Centro de gestión industrial. | Diciembre 2021 |
| Darío González | Corrección de estilo | Regional Tolima – Centro Agropecuario La Granja | Diciembre 2021 |

**H. Control de cambios**

|  | **Nombre** | **Cargo** | **Dependencia** | **Fecha** | **Razón del cambio** |
| --- | --- | --- | --- | --- | --- |
| **Autor(es)** |  |  |  |  |  |