GUÍA MODELO DE ARQUITECTURA DE SEGURIDAD

DIRECCIÓN DE GESTIÓN DEL ORDENAMIENTO SOCIAL DE LA PROPIEDAD - DGOSP

SUBDIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE TIERRAS - SSIT

COLOMBIA POTENCIA DE LA VIDA

Agricultura

CONTENIDO

LISTA DE TABLAS

ILUSTRACIONES

INTRODUCCIÓN

La política de Gobierno Digital establece como habilitador transversal la seguridad y privacidad de la información, esta define de forma detallada la implementación de controles de seguridad de la información con el fin de asegurar de manera eficaz la información, los sistemas de información, la plataforma tecnológica, la infraestructura física, los servicios en el entorno de las entidades públicas. Además, ofrece los lineamientos necesarios que permite a las entidades proteger frente a posibles interrupciones en la prestación de los servicios de la Entidad, mediante la gestión eficaz, eficiente y efectiva de los activos de información.

Este documento desarrollado por la Subdirección de Sistemas de Información de Tierras - SSIT presenta el Modelo de la Arquitectura de Seguridad de la Agencia Nacional de Tierras – ANT, sirve de guía en la implementación de los componentes de seguridad digital puesto que este define los lineamientos para la implementación de la estrategia de seguridad digital, pretende apoyar la formalización al interior de la Agencia, del sistema de gestión de seguridad y privacidad de la información y seguridad digital. Cada una de las acciones indicadas en este documento se basan en el Marco de Referencia de Arquitectura Empresarial (MRAE)[1] del MinTIC y el Manual de Gobierno Digital[2].

El modelo de la Arquitectura de Seguridad descrito en este documento, establece seis lineamientos a tratar: la auditoria y trazabilidad de componentes de información, la protección y privacidad de componentes de información, la seguridad y privacidad de los sistemas de información, la auditoría y trazabilidad de los sistemas de información, el análisis de riesgos y, por último, la Ciberseguridad o Seguridad Informática.

[1] Marco de Referencia de Arquitectura Empresarial: https://www.mintic.gov.co/marcodereferencia/
[2] Manual de Gobierno Digital: http://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf

1. DEFINICIONES

Acceso no autorizado a la información, Modificación no autorizada de la información: El acceso no autorizado es una forma de ciberdelito en la que el atacante accede de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, cuya motivación para el atacante es variada, va desde la obtención de: una satisfacción de carácter intelectual, económica (robo de información), sabotaje, espionaje o terrorismo. La ingeniería social y el error humano de configuración software son las mayores causas.

Activo de información: es un objeto tangible o intangible, análogo o digital que le genera valor a la organización, por ejemplo, los colaboradores, los documentos físicos, las bases de datos, el hardware, el software, el cableado y las redes, y los dispositivos de almacenamiento.

Amenaza: Es la causa u origen potencial de un daño sobre un activo de información que puede llegar a impactar negativamente a la organización.

Análisis de riesgos: (Process Hazards Analysis) es la acción sistemática que estudia los probables eventos y amenazas identificando los posibles daños a los activos de información y sus consecuencias.

Anti Malware: Software de seguridad informática, que engloba la protección ante todo tipo de software malicioso.

Antispam: Antispam es una solución de software que permite a los usuarios prevenir o restringir la entrega de spam (correos no deseados).

Ataque 0day: es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para los usuarios y para el fabricante del producto. Se le llama ataque 0day porque aún no existe ninguna revisión para mitigar el aprovechamiento de la vulnerabilidad.

Ataque de denegación de servicio (DoS, DDoS): Con este tipo de ataque, un sistema es bombardeado con tantos paquetes que las operaciones se retrasan o el sistema colapsa. Algunos ejemplos DoS son ICMP e inundaciones SYN, ataques de teardrop[3] y bombardeos de mail's. DDoS a menudo se basa en ataques DoS que se originan en botnets, pero también existen otros escenarios como ataques de amplificación DNS. Sin embargo, la disponibilidad también puede verse afectada por acciones locales (destrucción, interrupción del suministro de energía, etc.), fallas espontáneas o error humano, sin mala intención o negligencia.

CIO (Chief Information Officer) Oficial de Seguridad: líderes de la gestión estratégica de Tecnologías de Información, encargados de planificar, organizar, coordinar, gestionar y controlar la estrategia de uso y apropiación de TI, y todo lo que conlleva esta tarea.

Cloud: Permite alquilar tecnologías de la información y capacidad de computo a través de Internet y pagar por lo que se consume.

COLCERT: Grupo Interno de Trabajo de Respuesta a Emergencias Cibernéticas de Colombia.

Catálogo de componentes de información: Es el listado detallado y documentado del conjunto de componentes de información que tiene una institución o sector.

Confidencialidad: es un principio del SGSI, consisten en disponer los mecanismos necesarios para controlar el acceso a la información privada, sensible o clasificada.

Componente de información: Es el término agrupador utilizado para referirse al conjunto de los datos, entidades de negocio, unidades de información, los servicios de información y los flujos de información bajo un único nombre.

Compromiso de cuenta privilegiada Compromiso de cuenta sin privilegios, Compromiso de Aplicación: Un compromiso exitoso de un sistema o aplicación (servicio). Esto puede haber sido causado de forma remota por una vulnerabilidad

[3] Teardrop: Un ataque de goteo es un tipo de ataque de denegación de servicio (DoS; ataque que intenta poner fuera de servicio un recurso informático inundando la red o el servidor con solicitudes y datos). Fuente: https://www.f5.com/es_es/glossary/teardrop-attack.

conocida o nueva, pero también por un acceso local no autorizado. También incluye ser parte de una botnet.[4]

Controles: Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

Control de Accesos: Hace referencia al mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos.

CSIRT gobierno: El CSIRT del sector Gobierno, surge como necesidad de realizar una adecuada gestión y reaccionar ante los incidentes cibernéticos de modo centralizado, para lo cual realiza seguimiento de manera unificada a las principales tipologías de ciberincidentes que atentan contra la defensa del Gobierno, para realizar de manera eficiente la gestión de sus riesgos.

Datos abiertos: Todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

Datos maestros: Son datos transversales a toda la organización que describen las entidades de negocio como ciudadano, institución, trámite, centros de costos, centros de atención, reportes, entre otros. Estos son compartidos por los diferentes sistemas de información de la institución. El formato y rango de valores de estos datos se establecen a partir de reglas de negocio y un único valor de la verdad.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

[4] Botnet: Es una red de equipos infectados que se pueden controlar a distancia y a los que se puede obligar a enviar spam, propagar malware o llevar a cabo un ataque DDoS, y todo sin la autorización del dueño del dispositivo. Fuente: https://www.avast.com/es-es/c-botnet

Defacement: Ataque cibernético consistente en el enmascaramiento de un sitio web para dar al visitante o usuario la apariencia de no estar en el sitio web corresto, la estrategia consiste en cambiar la apariencia de la página web (imágenes, colores, etc.).

Disponibilidad: es un principio del SGSI, es la capacidad para el acceso y utilización oportuno de la información que ofrecen las organizaciones a los usuarios a través de los medios de comunicación (portal web, formularios web, Apps, etc.).

DLP (Data Loss Prevention): Sistema para la prevención de la pérdida de datos.

DNS (Domain Name System): sistema de nombres de dominio es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada.

EDR (Endpoint Detection Response): es un sistema de protección de los equipos e infraestructuras de la empresa. Combina el antivirus tradicional junto con herramientas de monitorización e inteligencia artificial.

Ethical Hacking: es una práctica autorizada para eludir la seguridad del sistema e identificar posibles violaciones de datos y amenazas en una red.

Explotación de vulnerabilidades conocidas: Un intento de comprometer un sistema o interrumpir cualquier servicio explotando vulnerabilidades conocidas que ya cuentan con su clasificación estandarizada CVE (por ejemplo, el BufferOverFlow, Backdoor, CrossFrame Scripting,[5] etc.).

Filtrado de Contenido: Programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web.

Firewall (Cortafuegos): Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

[5] Cross-Frame Scripting (XFS) también conocido como iFrame Injections son un tipo de ataque de phishing dirigido contra navegadores.

Fuzzing: Técnica de testeo automatizado mediante la que se introducen datos inválidos, aleatorios o inesperados a un sistema informático. Estos datos de entrada podrían dar origen a algún error**.**

Habeas data: Es una acción jurisdiccional propia del derecho, normalmente constitucional, que confirma el derecho de cualquier persona física o jurídica para solicitar y obtener la información existente sobre su persona, y de solicitar su eliminación o corrección si fuera falsa o estuviera desactualizada.

Hardening: endurecimiento, es la acción de eliminar todas las configuraciones por defecto, con el fin de mitigar las vulnerabilidades de las aplicaciones y la infraestructura que las soportan.

ICMP (Internet Control Message Protocol): utilizado para enviar mensajes de error e información operativa indicando, por ejemplo, que un host no puede ser localizado o que un servicio que se ha solicitado no está disponible. Estos mensajes del protocolo ICMP se envían a la dirección IP de origen del paquete.

Información estructurada: Se refiere a aquella que está definida y sujeta a un formato concreto que facilita su procesamiento. Por ejemplo, la información organizada y estructurada en bases de datos relacionales u hojas de cálculo se considera estructurada.

Información no estructurada: Es aquella que no posee una estructura predefinida, no están organizada de acuerdo a algún patrón. Entre esta se encuentra la información de tipo multimedia (video, voz, imagen), información generados en las redes sociales, foros, e-mails, presentaciones Power Point o documentos Word.

Información Privada: es aquella que por versar sobre información personal y por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones.

Información Pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712/2014.

Información pública reservada: Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712/2014.

Información semiestructurada: Es aquella que contiene marcas (elementos de estructura) y no posee una estructura predefinida, sin esquema definido. Esta información no está orientada a tablas de bases de datos y por lo tanto su estructura puede ser variable, se representa mediante un conjunto de etiquetas-valor. Por ejemplo, documentos SGML (Por sus siglas en inglés Standard Generalized Markup Language) y XML.

Ingeniería Social: Recopilación de información de un ser humano de una manera no técnica (por ejemplo, mentiras, trucos, sobornos o amenazas).

ISO 27001: Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en las entidades.

Integridad: es un principio del SGSI, define mecanismos que aseguran la fidelidad, exactitud y completitud de la información en todo momento.

Malware, Virus, Gusanos, Troyanos, Spyware, RootKits: Software que se incluye o inserta intencionalmente en un sistema con propósito dañino. Normalmente, se necesita una interacción del usuario para activar el código.

MREA (Marco de Referencia de Arquitectura Empresarial): instrumento que facilita a las entidades la adopción de la práctica de Arquitectura Empresarial, definida como uno de los cuatro habilitadores de la Política de Gobierno Digital.

MITM (Ataque de intermediario): un ataque de intermediario es un ataque en el que se adquiere la capacidad de leer, insertar y modificar a voluntad. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas y procurar que ninguna de las víctimas conozca que el enlace entre ellos ha sido violado.

MSPI (Modelo de Seguridad y Privacidad de la Información): imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información.

NIST- CFS (Cybersecurity Framework - NIST): Ayuda a las entidades a comprender mejor sus riesgos de ciberseguridad, administrar y reducir sus riesgos, y proteger sus redes y datos. Este Marco es voluntario. Brinda una reseña de las mejores prácticas.

On premise (En las instalaciones propias): Capacidad de cómputo y entorno informático propios de la entidad, ubicados en sitio.

Phishing: Técnicas de suplantación de identidad.

Riesgo: es el grado de exposición de un activo de información que hace que las amenazas saquen provecho de una vulnerabilidad provocando daños que impactan a la organización.

Scanning: Ataques que envían solicitudes a un sistema para descubrir puntos débiles. Se incluye también algún tipo de proceso de prueba para reunir información sobre hosts, servicios y cuentas. Ejemplos: fingerd, consultas DNS, ICMP, SMTP (EXPN, RCPT, …), escaneo de puertos.

Seguridad de la información: Acciones encaminadas a asegurar la preservación de la confidencialidad, integridad y disponibilidad de la información, también involucra otros

atributos, como la autenticidad, la responsabilidad, el no repudio y la confiabilidad. Estos atributos aseguran que la información confidencial solo se divulgue a las partes autorizadas (confidencialidad), evite la modificación no autorizada de la información (integridad) y garantice que las partes autorizadas puedan acceder a los datos cuando lo solicite (disponibilidad).

SGSI (Sistema de Gestión de Seguridad de la información): consiste en el conjunto de políticas, procedimientos y directrices junto a los recursos y actividades asociados que son administrados colectivamente por una organización, en la búsqueda de proteger sus activos de información esenciales.

SIEM (Security Information Event Management): es la principal herramienta del SOC ya que permite gestionar los eventos de un SI.

Single Sing On (Inicio de Sesión Unificado): Es un procedimiento de autenticación que habilita a un usuario determinado para acceder a varios sistemas con una sola instancia de identificación.

SMTP (Simple Mail Transfer Protocol): protocolo de red utilizado para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA, teléfonos móviles, impresoras, etc.). Es, en otras palabras, un protocolo de conexión de Internet.

Sniffing: Observar y registrar el tráfico de la red (escuchas telefónicas o redes de datos).

SOC (Security Operation Center): equipo responsable de garantizar la seguridad de la información. El SOC es una plataforma que permite la supervisión y administración de la seguridad del sistema de información a través de herramientas de recogida, correlación de eventos e intervención remota.

Software o sistemas abiertos: Sistemas «Open Resolvers», impresoras abiertas a todo el mundo, vulnerabilidades aparentes detectadas con nessus u otros aplicativos, firmas de virus no actualizadas, etc.

Tratamiento de datos: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

WAF (Web Application Firewall): protege de múltiples ataques al servidor de aplicaciones web en el backend.

2. OBJETIVOS

Proveer un documento de consulta en la identificación de procesos y controles de seguridad digital que guíe al equipo de colaboradores encargado de la seguridad de la información y a los responsables de la información a su cargo. Este instrumento procedimental determina por medio de actividades, los pasos que se deben ejecutar para cumplir con uno o varios lineamientos indicados en el Marco de Referencia de Arquitectura Empresarial – MRAE bajo el dominio de la Arquitectura de seguridad.

3. ALCANCE

El Modelo de Arquitectura de Seguridad de la ANT cubre los componentes de laseguridad digital, en particular hace referencia a los componentes de información, de aplicaciones o sistemas de información, el análisis de riesgos de estos y la Ciberseguridad o Seguridad Informática.

Este documento sirve como hoja de ruta que apoya la identificación de procesos y controles de seguridad digital, útil para asegurar la protección de nuevos activos de información de TI generados durante la dinámica de los procesos de negocio de la ANT.

4. MARCO NORMATIVO

Ley 1341 de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.

Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2, del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015 los sujetos obligados deberán articular su

orientación estratégica, su modelo de gestión, su plan de transformación digital, y su estrategia de Tecnologías de información y las Comunicaciones, con el objetivo de dar cumplimiento de la nueva Política de Gobierno Digital, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 1078 2015.Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Decreto 2758 2012.Por el cual se modifica la estructura del Ministerio de Defensa Nacional y se dictan otras disposiciones (Artículos 2 y 5).

Resolución 500 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".

La Resolución 1519 de 2020-ANEXO 3.

Conpes 3995 2020. Política Nacional De Confianza Y Seguridad Digital.

Conpes 3854 2016. Política Nacional De Seguridad Digital.

Conpes 3701 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.

Directiva presidencial 03 de 15 de marzo de 2021. Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

Artículo 15 de la Constitución Política. "*Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución*."

Ley 1581 de 2012. Artículo 1°. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Ley 1266 de 2008. Se regula el manejo de la información contenida en bases de datos personales (hábeas data), en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1712 de 2014. Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

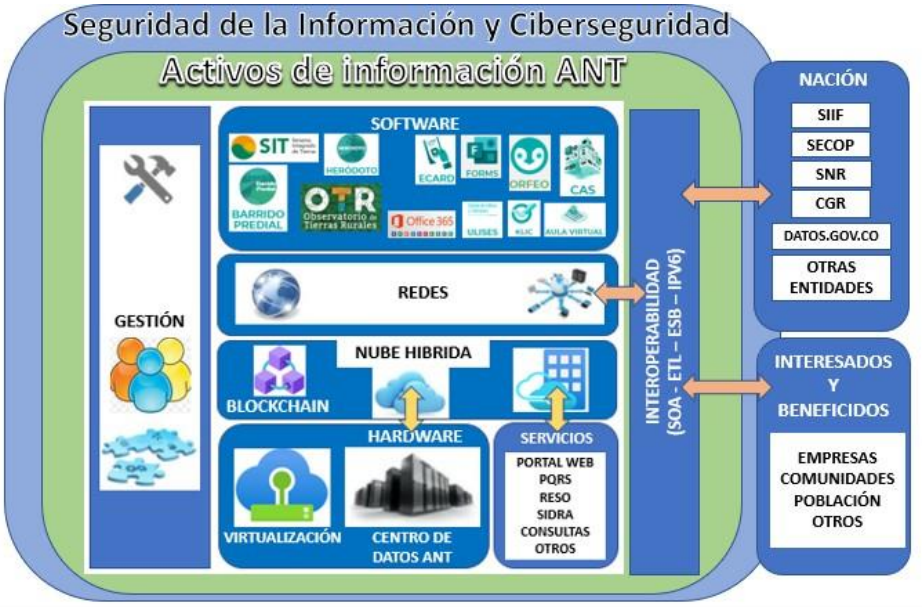
Ley 79 de 1993. Regula la realización de los Censos de Población y Vivienda en todo el territorio nacional.

5. DOMINIO DE ARQUITECTURA DE SEGURIDAD

El dominio de arquitectura de seguridad digital en la ANT permite identificar cada uno de los activos de información, sus relaciones y encaminar los esfuerzas para desarrollar procedimientos y controles de seguridad necesarios para garantizar la protección de estos activos de información con una visión arquitectural.

En la ilustración 1 se puede observar la Arquitectura de Seguridad de la ANT, en la que se puede observar que la Seguridad de la Información y la Ciberseguridad son actividades transversales y engloban la responsabilidad de seguridad sobre todos los activos de información en la Agencia (colaboradores y proveedores, los sistemas de información o software, la infraestructura tecnológica como el hardware, máquinas virtuales, redes, comunicaciones, etc., y los servicios tecnológicos). Esta Arquitectura de Seguridad representa una vista de alto nivel de cada uno de los componentes que conforman los activos de información, durante la gestión de estos activos y como parte de la administración es compromiso de la entidad identificar y definir los riesgos, las vulnerabilidades y los controles que ofrezcan capacidades para prevenir, detectar, responder y actuar oportunamente con el fin de proteger la operación en la ANT.

Ilustración 1. Vista de alto nivel de la Arquitectura de Seguridad ANT



Fuente: Elaboración propia ANT

5.1 Auditoria y trazabilidad de Componentes de Información

En este primer lineamiento, se establece en la Agencia los criterios o mecanismos necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los Componentes de Información durante el proceso de gestión de dichos componentes.

Lo anterior es posible, si la ANT cuenta con un catálogo de componentes de información o inventario detallado de los componentes de información, este representa el punto de partida para la construcción de la arquitectura de información y es la base para iniciar los procesos de calidad de la información, y puede ayudar a atender requerimientos de interoperabilidad entre entidades, este es un instrumento con un alto valor agregado para la Agencia. Surge la necesidad de conocer que componentes de información posee y sus características con el objetivo de proyectar nuevos servicios de información, identificar fuentes únicas de información, oportunidades de mejora en seguridad y calidad de los datos e información, identificar datos maestros, datos abiertos, definir controles y mejorar el nivel de acceso a la información y demás actividades propias de la gestión de información.

Ilustración 2. Actividades para construir el catálogo de componentes de información

Fuente: Guía Cómo construir el catálogo de Componentes de Información. MinTIC, 2016.

Con el fin de elaborar e implementar el Catálogo de Componentes de Información en la ANT, que nos permita asegurar la trazabilidad y auditoría sobre cada uno de los Componentes de la Información, se adopta la guía técnica de MinTIC “Instrumento de Guía Como construir el catálogo de componentes de Información”. El instrumento guía es una hoja de cálculo que dispone de cinco hojas, cada detalla los Atributos de Información, Atributos de Datos, Atributos de Flujo de Información, Atributos de Flujo de Información Sectorial, y Atributos de Servicios de Información.

Este catálogo de activos de información debe tener registrado datos como: Código, tipo de Información (Resolución, Autos, Oficios), Descripción, Área Responsable, Productor (fuente oficial), Clasificación (Pública, Pública Reservada, y Pública Clasificada), Tipo de Información (estructurada, no estructurada, semiestructurada), Frecuencia de Generación, Soporte (Físico, Digital), Formato, etc.

En la ilustración 3, se plantea desarrollar auditorías y trazabilidad en cada etapa del procesamiento sobre cada componente de información.

Haciendo uso y aprovechamiento del Catálogo de Componentes de Información diligenciado y actualizado periódicamente (se recomienda actualizar anualmente), se identifica y delega en cada responsable de la información el chequeo de los controles y su efectividad, así como el reporte de los incidentes de seguridad presentados durante la operación.

A su vez, el CEO de seguridad de la Agencia o quien haga sus veces, debe programar auditorías internas anuales en cada una de las áreas misionales para evaluar, mantener, suprimir y ajustar los controles de seguridad implementados, luego, generar el reporte de auditoría correspondiente con las sugerencias, observaciones y propuestas que haya lugar, en pro de mejorar la seguridad de la información; al finalizar estas actividades, debe elaborar y presentar el reporte a los líderes de los procesos y a la Subdirección de Sistemas de Información de Tierras – SSIT, con el fin tomar las medidas del caso.

Ilustración 3. Auditoría y trazabilidad de componentes de información

Fuente: Elaboración propia ANT

Para una adecuada gestión del ciclo de vida de los datos (ver la ilustración 4), se recomienda aplicar la guía de MinTIC “G.INF.003 Guía técnica de Información-Ciclo de vida del dato”, la cual facilita la implementación de los lineamientos del Marco de Referencia de AE para la Gestión de TI, relacionados con el ciclo de vida del dato y apoya la planeación del ciclo de vida para diferentes componentes de información de características específicas como, por ejemplo, el ciclo de vida de la información geográfica, multimedia, etc.
Con el objetivo de guiar el desarrollo del Modelo de Arquitectura de Seguridad de la ANT, se aplican seis (6) de los quince (15) factores de éxito del ciclo de vida del dato.

Definición procesos y servicios: establecer formalmente los procesos y servicios que generan y modifican datos, y que dan soporte a las diferentes áreas de la entidad, prestando especial atención a las relaciones entre dichas áreas, e incluyendo los procesos y servicios propios de la Subdirección de Sistemas de Información de Tierras - SSIT e incluir al Equipo de Infraestructura y Soporte Tecnológico dado que este equipo responde por el Sistema de Gestión Documental de la ANT, sistema que ofrece servicios transversales (misional y apoyo).

Recopilación de evidencias: contar con mecanismos que permitan registrar y recopilar evidencias del proceso de enmascaramiento de los datos, dichas evidencias serán objeto de análisis en las auditorías y el control interno de las instituciones.

Ilustración 4. Factores de éxito para una adecuada gestión del ciclo de vida del dato

Fuente: MinTIC, 2019.

Custodia de RAW DATA: establecer mecanismos para la protección de los datos primarios (RAW DATA), que aseguren su integridad, confidencialidad y disponibilidad, acorde a las políticas de seguridad y privacidad establecidas por la institución.

Coordinación en las ejecuciones: definir procedimientos que soporten la coordinación de las diferentes ejecuciones y pruebas con los responsables tanto de los datos, como de los sistemas de información que los generan, modifican o usan.

Procedimientos de marcha atrás: establecer procedimientos formales de marcha atrás (Tipo rollback), que como mínimo, sean tenidos en cuenta en las operaciones que manejan los datos, que la Agencia ha establecido como críticos y registrados en la matriz "Infraestructura Crítica Cibernética-ANT".

Identificación de campos no triviales: identificar los campos de datos que contienen información compleja, susceptible de ser tratada, como pueden ser imágenes, documentos, audio, entre otros.

Con el fin de tener controles de seguridad adicionales, los sistemas de información deben implementar los criterios de trazabilidad y auditoría definidos para los Componentes de información que maneja.

5.2 Protección y privacidad de Componentes de información

Tabla 1. Atributos de Información

Ítem	Atributo	Descripción
1	Código	Consecutivo o código interno asignado por la entidad al registro de información.
2	Información	Nombre de la información o activo de información.
3	Descripción	Es una breve descripción que hace referencia el activo de información o la información.
4	Área Responsable	Corresponde al área, dependencia o unidad de la entidad responsable de la custodia o control de la información, para efectos de permitir su acceso.
5	Productor (fuente oficial)	Nombre de la entidad externa o área interna que tiene como responsabilidad oficial, generar o producir dicha información.
6	Clasificación	Clasificación de acuerdo a la Ley 1712 de 2014. Esta puede ser pública, publica clasificada, pública reservada.
7	Tipo de Información	Se refiere a si la unidad de información está disponible en formato estructurado, semiestructurado y no estructurado
8	Frecuencia de Generación	Identifica la frecuencia con que se genera la información, de acuerdo a su naturaleza y a la normativa aplicable.
9	Soporte	Establece el mecanismo en el cual está soportado la información: documento físico, medio electrónico o por algún otro tipo de formato audio visual entre otros. (Físico- análogo o digital- electrónico).
10	Formato	Identifica la forma, tamaño o modo en la que se presenta la información o se permite su visualización o consulta, tales como: hoja de cálculo, imagen, audio, video, documento de texto, etc.
11	Datos Abiertos	Se coloca SI o No, según SI la fuente de información son datos abiertos.
12	Tipo de datos	Este atributo sólo es utilizado si la respuesta en el atributo de Datos Abiertos es SI. Corresponde al tipo de clasificación temática, tales como: Agrícola y pesquera, Ambiental, Científica, Cultural, Económica y

		Comercial, Geográfica, Política, Sistema Legal, Social, Transporte y Tráfico y demás que sean identificados.
13	URL de publicación.	Este atributo sólo es utilizado si la respuesta en el atributo de Datos Abiertos es SI. Dirección electrónica del lugar donde se encuentra disponibles los datos abiertos y dispuestos para su descarga.
14	Cobertura Geográfica	Este atributo sólo es utilizado si la respuesta en el atributo de Datos Abiertos es SI. Hace referencia a la zona o área geográfica a la que corresponden los datos. Por ejemplo, Cundinamarca, el municipio de Soacha, Bogotá, Región amazónica.

Fuente: elaboración propia basado en el "Instrumento de Guía Como construir el catálogo de componentes de Información", MinTIC.

Este lineamiento establece la incorporación, en los atributos de los Componentes de información, la información asociada con los responsables y políticas de la protección y privacidad de la información, conforme con la normativa de protección de datos de tipo personal y de acceso a la información pública.

Una de las actividades para la construcción del Catálogo de Componentes de Información es la identificación de la información que produce la Agencia, en la tabla 1 se listan los 14 atributos que requieren ser registrados.

En el Catálogo de Componentes de Información, en la hoja "1_Atributos_de_información", se debe identificar y diligenciar cada registro, la información asociada con los responsables y políticas de la protección y privacidad de la información, conforme a la normativa de protección de datos de tipo personal (Ley 1581 de 2012) y de acceso a la información pública (Ley 1712 de 2014). Este es un atributo muy importante, porque hace conocer con certeza qué información del carácter de "Pública clasificada" se tiene en la entidad y el área responsable de la información.

A continuación, se establecen las fases para la identificación de la información en el ANT:

a. Identificar y reunir las fuentes de información: entre las fuentes de información que la entidad debe identificar y revisar son el registro de activos de información que definió la entidad en virtud de la Ley de acceso y transparencia a la información pública (Ley 1712 de 2014), los datos abiertos que tiene publicados, el listado de datos maestros, y otras

fuentes de información que posea la Agencia y que sirvan de insumo para la consolidación de la información que produce.
b. Identificar a partir de las funciones y obligaciones legales de la entidad que información debe producir.
c. Realizar la validación de la información identificada con todas las áreas, con el fin de identificar información faltante.

No se debe confundir el concepto de Inventario de Activos de Información con el de Catálogo de Componentes de Información, para el primero un activo es mucho más amplio y en el contexto de la seguridad de la información hace referencia a todo lo que tiene valor para una entidad (información, aplicaciones infraestructura TI, edificios, personas, redes, etc.), en el segundo, hace referencia a la información que genera la institución.

El Registro de Activos de Información y el Índice de Información Clasificada y Reservada que deben tener todas las entidades conforme lo exige Ley de transparencia y del derecho de acceso a la información pública nacional (Ley 1712 de 2014), sirve como insumo del catálogo de componentes de información.

Debemos tener claro que, las entidades deben conocer en detalle la información que genera, procesa, custodia, archiva y entrega, esto es, que deben saber entre otros, qué información tiene atributo de “publica clasificada” dar tratamiento a la misma tal y como lo establece la Ley 1581 de 2012 sobre el tratamiento y protección de datos personales y si no se cumple puede acarrear sanciones a la Entidad.

5.3 Seguridad y privacidad de los sistemas de información

La ANT debe analizar e incorporar aquellos componentes de seguridad y privacidad de la información que sean necesarios durante todas las fases del ciclo de vida de los sistemas de información. La Resolución 1519 de 2020-ANEXO 3 “*Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos*”, indica lo anterior como una obligación de la Agencia.

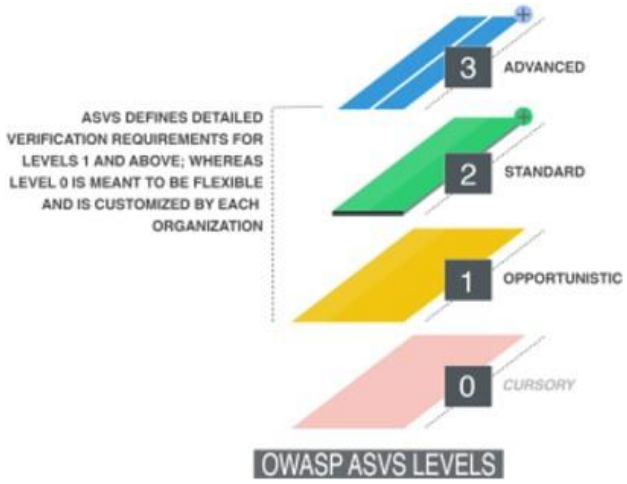
Actualmente la ANT cuenta con componentes de seguridad y privacidad de la información, así como los correspondientes al ciclo de vida de las aplicaciones, mantiene actualizado en el SIG las políticas, lineamientos, procedimientos, planes y gestión.

Dentro del plan de mejora de la seguridad de la información, este Modelo de Arquitectura de Seguridad propone la adopción e implementación formal del OWASP (Open Web Applicaction Security Project) Proyecto de Seguridad en la Aplicaciones Web, este es un Estándar de Verificación de Seguridad en Aplicaciones que establece una lista de requerimientos de seguridad o pruebas que permite definir el nivel de seguridad en las aplicaciones y ayuda a las organizaciones en el desarrollo y mantenimiento aplicaciones seguras.

El Estándar de Verificación de Seguridad en Aplicaciones define tres niveles de verificación de seguridad, incrementando la profundidad con cada nivel, para cada nivel se utiliza una lista de chequeo de seguridad:

- ASVS nivel 1 se encuentra dirigido a todo tipo de software.
- ASVS nivel 2 es para aplicaciones que contienen datos sensibles, que requieren protección.
- ASVS nivel 3 es para las aplicaciones más críticas - aplicaciones que realizan transacciones de alto valor, contienen datos médicos confidenciales, o cualquier aplicación que requiera el más alto nivel de confianza.

- **Ilustración 5**. Estándar de Verificación de Seguridad en Aplicaciones



Fuente: OWASP, 2017.

Nivel 1: Oportunista (es el mínimo requerido para todas las aplicaciones)
Una aplicación alcanza el nivel 1 si defiende adecuadamente controles contra vulnerabilidades de seguridad de aplicaciones que son fáciles de detectar.
El nivel 1 es recomendado para sistemas de información donde se requiere escasa confianza en el uso correcto de los controles de seguridad o para apoyar la elaboración de una lista de requerimientos de seguridad con prioridades como parte de un esfuerzo de múltiples fases. Este nivel puede ser aplicado automáticamente por herramientas o manualmente sin acceso al código fuente.
Las amenazas a la aplicación probablemente provendrán de atacantes que utilizan técnicas simples y de bajo esfuerzo para identificar vulnerabilidades fáciles de encontrar y de explotar.

Una amenaza común a todas las organizaciones son los ataques oportunistas, estos buscarán cualquier aplicación vulnerable fácilmente explotable. Se recomienda aplicar este nivel como punto de partida para manejar los riesgos más fáciles de encontrar, además, se debe observar detenidamente los riesgos específicos de la Agencia basados en la naturaleza de su negocio.

Nivel 2: Estándar
En este nivel una aplicación defiende controles adecuadamente contra la mayoría de los riesgos asociados con el software. Aquí se asegura que controles de seguridad se encuentran en el lugar adecuado, son efectivos y son utilizados dentro de la aplicación. Este nivel es generalmente apropiado para aplicaciones que manejan transacciones business-to-business, información de privada, implementan funciones sensibles o críticas para el negocio o incluyen el proceso de otros activos sensibles.
Las amenazas están motivadas por atacantes los cuales se centran en objetivos concretos, utilizando herramientas y técnicas efectivas en el descubrimiento y explotación de vulnerabilidades dentro de las aplicaciones.

Nivel 3: Avanzado
Este es el nivel recomendado a aplicar en la ANT, es el nivel más alto nivel de verificación, está reservado normalmente para aplicaciones que requieren niveles significativos de verificación de seguridad enfocado a aplicaciones que realizan funciones críticas, donde una falla de seguridad podría afectar significativamente sus operaciones.
Una aplicación alcanza el nivel avanzado si se defiende adecuadamente contra vulnerabilidades de seguridad avanzadas y también demuestra los principios de un buen diseño de seguridad. Una aplicación en el nivel 3 requiere un análisis de mayor profundidad, arquitectura, codificación y Testing en todo nivel.

Aplicaciones de este nivel son modularizadas para facilitar su resiliencia, escalabilidad, y sobre todo, capas de seguridad. Cada módulo está separado por conexiones de la red o instancias físicas, se encarga de sus responsabilidades de seguridad (defensa en profundidad) y debe ser debidamente documentada. Las responsabilidades incluyen controles para asegurar la confidencialidad (cifrado), integridad (transacciones, validación de la entrada), disponibilidad (manejo de carga), autenticación (incluyendo autenticación entre sistemas), no repudio, autorización y auditoría (bitácoras).

5.4 Auditoría y trazabilidad de los sistemas de información

La Agencia ha desarrollado mecanismos que aseguran el registro histórico de las acciones realizadas por los usuarios sobre los Sistemas de Información, manteniendo la trazabilidad y apoyando los procesos de auditoria.

La tabla 2, presenta las recomendaciones básicas sobre seguridad en las empresas de los sectores gobierno, manufactura, transporte, defensa, etc.

Tabla 2. Tabla de recomendaciones

Perfil de amenazas	L1 Recomendación	L2 Recomendación	L3 Recomendación
Los agentes de amenaza que suelen atacar a las entidades del gobierno son más propensos a realizar ataques enfocados con más tiempo, habilidad y recursos. A menudo la información sensible o los sistemas no son fáciles de localizar y requieren utilizar o manipular individuos que trabajen dentro de la organización, utilizando técnicas de ingeniería social. Los ataques pueden involucrar individuos que trabajan dentro de la organización, extraños a la organización, o una combinación de ambos. Sus objetivos pueden incluir acceso a la propiedad intelectual para obtener ventajas estratégicas o tecnológicas. Los atacantes que buscan abusar la funcionalidad de la aplicación para influenciar el comportamiento de la aplicación o alterar sistemas sensibles. La mayoría de los atacantes buscan información sensible que puede ser utilizada directa o indirectamente para beneficiarse al incluir datos personales a la información de pago. A menudo los datos pueden utilizarse para una variedad de esquemas de fraude, robo de identidad o pagos fraudulentos.	Todas las aplicaciones accesibles desde la red.	Aplicaciones que contienen información interna o información sobre empleados que pueden aprovecharse utilizando la ingeniería social. Aplicaciones que contiene información poco esencial, pero de importante propiedad intelectual o secretos comerciales.	Aplicaciones que contiene valiosa propiedad intelectual, secretos comerciales o secretos del gobierno que es fundamental para la supervivencia o el éxito de la organización. Aplicaciones que controlan funcionalidad sensible (p. ej. transporte, fabricación de equipos, sistemas de control) o que tienen la posibilidad de amenazar la seguridad

Fuente: Elaboración propia basado en OWASP, 2017.

El Estándar de Verificación de Seguridad en Aplicaciones en la ANT o lista de chequeo debe incluirse en la generación de casos de uso e historias para cuestiones de seguridad funcional, tales como la mejor manera de implementar la funcionalidad para iniciar la sesión en la aplicación. Una forma de incluir la lista de chequeo de seguridad es recogiendo los requisitos que se adhieren al sprint actual, y lo agregan directamente a la acumulación del sprint si es un requisito funcional, o como una limitación a casos de uso existentes si no son funcionales. Por ejemplo, la adición de la autenticación TOTP (Contraseña de un solo uso basada en tiempo), junto con las políticas de contraseñas y servicio web que de detección de ataques de fuerza bruta. En los sprints futuros, los requisitos adicionales se seleccionarán basados en el criterio "justo a tiempo", o que "no se va a necesitar".

Se debe implementar una lista de chequeo de revisión por pares, lo que ayuda a que un código inseguro no sea ingresado en el repositorio. La lista de verificación se puede utilizar como parte de la unidad de seguridad de verificación automatizada y conjuntos de pruebas de integración, casos de abuso y casos de prueba a través de "fuzzing". El objetivo es reducir el riesgo de la "metodología de catarata" el cual pone el "test de penetración al final" causando costosos esfuerzos de re-factorización de código cuando se deben entregar ciertas metas dentro del sistema. Como podrían promoverse nuevas características del software después de cada sprint, no es suficiente confiar en una actividad única de aseguramiento. Así, mediante la automatización de las pruebas, no debería haber cuestiones de suma importancia que puedan ser encontradas por un pentester calificado con tan solo semanas para probar la aplicación.

5.5 Análisis de riesgos

La ANT debe realizar mínimo una vez al año el análisis y gestión de los riegos asociados a su infraestructura tecnológica, aplicaciones y componentes de información, haciendo énfasis en aquellos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de los servicios de la entidad durante la ejecución de los ejercicios de arquitectura empresarial.

Para el análisis de riesgos de seguridad de la ANT, se recomienda tomar como guía o referencia, el documento de la ANT “Plan de Tratamiento de Riesgos de la ANT” aplicando los capítulos:

5.6 Ciberseguridad o Seguridad informática

La Entidad tiene diseñado controles de seguridad informática para gestionar los riesgos que atentan contra la disponibilidad, integridad y confidencialidad de la información identificados durante la ejecución de los ejercicios de arquitectura empresarial.

El Modelo de Seguridad y Privacidad de la Información en la fase de Planificación se realiza la selección de controles, y durante la fase Implementación se ejecuta la implementación de controles de seguridad de la información, por lo cual se cuenta con el anexo de controles del estándar ISO 27002.

En la tabla de requisitos de verificación detallada, se establece la lista de chequeo del cumplimiento de los elementos de seguridad más importantes sobre el código en las aplicaciones o sistemas de información.

Tabla 3. Requisitos de verificación detallada

Verifica	Descripción
V1.	Arquitectura, diseño y modelado de amenazas
V2.	Autenticación
V3.	Gestión de sesiones
V4.	Control de acceso
V5.	Manejo de entrada de datos maliciosos
V7.	Criptografía en el almacenamiento
V8.	Gestión y registro de errores
V9.	Protección de datos
V10.	Comunicaciones

V11.	Configuración de seguridad HTTP
V13.	Controles Maliciosos
V15.	Lógica de negocio
V16.	Archivos y recursos
V17.	Móvil
V18.	Servicios Web
V19.	Configuración (nuevo en 3.0)

Fuente: Elaboración propia ANT, basado en OWASP, 2017.

V1: Arquitectura, diseño y modelado de amenazas

Objetivo de control
Asegurar que una aplicación verificada satisfaga los siguientes requisitos de alto nivel (ver tabla 4):
• Nivel 1, los componentes de la aplicación son identificados y tienen una razón de ser.
• Nivel 2, se ha definido la arquitectura y el código se adecúa a ésta.
• Nivel 3, la arquitectura y el diseño son los indicados, se utilizan y resultan eficaces.

V2: Requisitos de verificación de autenticación

Objetivo de control
Autenticación es el acto de establecer o confirmar, algo (o alguien) como auténtico, esto es, que lo que reclama sobre aquello es verdadero. Se debe asegurar que la aplicación satisface los siguientes requisitos de alto nivel, ver la tabla de requisitos en el documento de referencia OWASP:

• Verifica la identidad digital del remitente de una comunicación.
• Asegura que sólo los usuarios autorizados son capaces de autenticarse y que las credenciales sean transportadas de forma segura.

Tabla 4. Requisitos de alto nivel de Arquitectura, diseño y modelado de amenazas

#	Descripción	1	2	3	Desde
1.1	Verificar que todos los componentes de la aplicación se encuentran identificados y asegurar que son necesarios.	X	X	X	1.0
1.2	Verificar todos los componentes, tales como bibliotecas, módulos y sistemas externos, que no son parte de la aplicación pero que la misma los necesita para funcionar se han identificado.		X	X	1.0
1.3	Verificar que se ha definido una arquitectura de alto nivel para la aplicación.		X	X	1.0
1.4	Verificar que todos los componentes de la aplicación se definen de acuerdo a las funciones de negocio o de seguridad que proporcionan.			X	1.0
1.5	Verificar que todos los componentes que no son parte de la aplicación pero que son necesarios para su funcionamiento, sean definidos de acuerdo a las funciones de negocio o de seguridad que proporcionan.			X	
1.6	Verificar que se ha realizado un modelo de amenazas para la aplicación en cuestión y que éste cubre riesgos asociados con la suplantación de identidad, manipulación, repudio, revelación de información y elevación de privilegios (STRIDE).			X	
1.7	Verificar que todos los controles de seguridad (incluyendo las bibliotecas que llaman a servicios de seguridad externos) tienen una implementación centralizada.		X	X	
1.8	Verificar que los componentes están separados unos de otros mediante controles de seguridad, tales como segmentación de la red, reglas de firewall, o grupos de seguridad basados en la nube.		X	X	
1.9	Verificar que la aplicación tiene una clara separación entre la capa de datos, la capa de control y la capa de presentación, tal que las decisiones de seguridad pueden aplicarse en sistemas confiables.		X	X	
1.10	Verificar que no hay ninguna lógica de negocio sensible, claves secretas u otra información propietaria en el código del lado del cliente.		X	X	
1.11	Verificar que todos los componentes de la aplicación, bibliotecas, módulos, frameworks, plataformas y sistemas operativos se encuentran libres de vulnerabilidades conocidas		X	X	3.0.1

Fuente: Elaboración propia ANT, basado en OWASP, 2017.

V3: Requisitos de verificación de gestión de sesiones

Objetivo de control

Uno de los componentes básicos de cualquier aplicación web es el mecanismo por el cual controla y mantiene el estado de un usuario al interactuar con ésta. Esto se refiere a manejo de sesiones y se define como el conjunto de todos los controles que rigen el estado completo de interacción entre un usuario y la aplicación basada en la web.

Se debe asegurar que la aplicación verificada satisface los siguientes requerimientos de manejo de sesiones de alto nivel, ver la tabla de requisitos en el documento de referencia OWASP:

• Las sesiones son únicas para cada individuo y no conjeturadas o compartidas

• Las sesiones son invalidadas cuando ya no son necesarias y el tiempo es limitado durante los períodos de inactividad.

V4: Requisitos de verificación del Control de acceso

Objetivo de control

Autorización es el concepto de permitir acceso a los recursos únicamente a aquellos que les ha sido permitido utilizarlos. Se debe asegurar que la aplicación verificada satisface los siguientes requisitos de alto nivel, ver la tabla de requisitos en el documento de referencia OWASP:

• Personas que acceden a recursos poseen credenciales válidas para hacerlo.

• Los usuarios se encuentran asociados con un conjunto bien definido de roles y privilegios.

• Los metadatos de Roles y permisos se encuentran protegidos de ataques de reutilización o manipulación.

V5: Requisitos de verificación para Manejo de entrada de datos maliciosos y
V6: Codificación / escape de salidas de datos

Objetivo de control

La debilidad más común de seguridad de las aplicaciones web es la falla en validar apropiadamente el ingreso de datos que provienen del cliente o del ambiente antes de ser utilizada. Esta debilidad conduce a casi todas las vulnerabilidades encontradas en aplicaciones web, tales como cross site scripting (XSS), inyecciones SQL, inyección de

intérprete, ataques locale/Unicode, ataques a sistemas de archivos y desbordamientos de búfers.

Se debe asegurar que la aplicación verificada satisface los siguientes requisitos de alto nivel, ver la tabla de requisitos en el documento de referencia OWASP:

• Todas las entradas son correctamente validadas y adecuadas para el propósito previsto.

• No debe confiarse en datos de una entidad externa o del cliente y deben ser tratados como tales.

V7: Requisitos de verificación para la criptografía en el almacenamiento

Objetivo de control

Asegure que una aplicación verificada satisfaga los siguientes requisitos de alto nivel, ver la tabla de requisitos en el documento de referencia OWASP:

• Que todos los módulos criptográficos fallen de forma segura y que los errores sean gestionados correctamente.

• Que se utilice un generador de números aleatorios adecuado cuando se requiere la aleatoriedad.

• Que el acceso a claves se gestiona de forma segura.

V8: Requisitos de verificación de gestión y registro de errores

Objetivo de control

El objetivo principal de la gestión y registro de errores es proporcionar una reacción útil para los usuarios, administradores y equipos de respuesta a incidentes. El objetivo no es crear cantidades masivas de registros, sino crear registros de alta calidad, con información útil y desechando ruido.

Los registros de bitácora de alta calidad a menudo contienen datos confidenciales y también deben ser protegidos según las leyes de privacidad de datos o directivas. Esto debe incluir, ver la tabla de requisitos en el documento de referencia OWASP:

• No recoger o registrar información confidencial si no es necesaria.

• Garantizar que toda la información registrada se gestiona de forma segura y es protegida según su clasificación de datos.

• Asegurar que los registros de bitácora no sean almacenados indeterminadamente, sino que posean un ciclo de vida útil lo más corta posible.

Si los registros contienen datos privados o confidenciales, cuya definición varía de país a país, éstos se convierten en parte de la información sensible y por lo tanto resulta muy atractiva para los atacantes.

V9: Requisitos de Verificación de Protección de Datos

Objetivo de control

Hay tres elementos clave para la protección de datos: Confidencialidad, Integridad y Disponibilidad (CIA por sus siglas en inglés). Este estándar asume que la protección de datos se aplica en un sistema de confianza, como un servidor, que ha sido protegido debidamente y dispone de protecciones suficientes.

Las aplicaciones web deben asumir que todos los dispositivos de un usuario puedan ser comprometidos de alguna manera. Cuando una aplicación transmite o almacena información sensible dentro de dispositivos inseguros, como equipos compartidos, teléfonos y tabletas, la aplicación es responsable de que los datos almacenados en estos dispositivos sean cifrados y no pueden ser fácilmente o ilícitamente obtenidos, alterados o divulgados.

Se debe asegurar que la aplicación verificada satisface los siguientes requisitos de protección de datos de alto nivel, ver la tabla de requisitos en el documento de referencia OWASP:

• Confidencialidad: los datos deben ser protegidos de observación no autorizada o la divulgación tanto en tránsito como cuando están almacenados.

• Integridad: los datos deben protegerse siendo creados maliciosamente, alterados o eliminados por los intrusos no autorizados.

• Disponibilidad: los datos deben estar disponibles para usuarios autorizados cuando sea necesario

V10: Requisitos de Verificación de Seguridad de las Comunicaciones

Objetivo de control

Se debe asegurar que la aplicación verificada satisfaga los siguientes requisitos de alto nivel, ver la tabla de requisitos en el documento de referencia OWASP:

• Que se utilice TLS donde se transmite información sensible

• Que se utilicen algoritmos y cifradores fuertes en todo momento.

V11: Requisitos de verificación de configuración de seguridad HTTP y
V12: Requisitos de verificación de configuración de seguridad

Objetivo de control
Asegure que la aplicación verificada satisfaga los siguientes requisitos de alto nivel, ver la tabla de requisitos en el documento de referencia OWASP:
• El servidor de aplicaciones está convenientemente endurecido de una configuración preestablecida
• Toda respuesta HTTP contiene su tipo de contenido establecido utilizando un conjunto de caracteres seguro.

V13: Requisitos de verificación para Controles Malicioso y
V14: Requisitos de verificación de seguridad interna
Objetivo de control
Asegure que la aplicación verificada satisfaga los siguientes requisitos de alto nivel, ver la tabla de requisitos en el documento de referencia OWASP:
• La actividad maliciosa se debe manejar con seguridad y adecuadamente para no afectar el resto de la aplicación.
• No posee bombas de tiempo ni otros ataques basados en tiempo
• No realiza "phone home" a destinos malintencionados o no autorizados
• La aplicación no posee puertas traseras, huevos de Pascua, ataques salami o fallos de lógica que pueden ser controlados por un atacante
El código malicioso es extremadamente raro difícil de detectar. La revisión manual línea por línea del código puede ayudar a encontrar bombas lógicas, pero incluso el más experimentado revisor de código tendrá que esforzarse para encontrar código malicioso, aunque sepa que existe.

V15: Requisitos de verificación para lógica de negocios
Objetivo de control
Asegure que la aplicación verificada satisfaga los siguientes requisitos de alto nivel, ver la tabla de requisitos en el documento de referencia OWASP:
• El flujo de la lógica de negocio es secuencial y en orden
• La Lógica de negocios incluye límites para detectar y evitar ataques automatizados, como las continuas transferencias de fondos pequeños, agregando 1 millón amigos uno a uno y así sucesivamente.

• Flujos de lógica de negocios de alto valor han considerado casos de abuso y agentes maliciosos y poseen protecciones contra la falsificación, alteración, repudio, revelación de información y ataques a la elevación de privilegios.
V16: Requisitos de verificación de archivos y recursos
Objetivo de control
Asegure que la aplicación verificada satisfaga los siguientes requisitos de alto nivel:
• Datos no confiables deben ser gestionados como tales y de forma segura
• Datos Obtenidos de fuentes no confiables sean almacenan fuera del webroot y posean permisos limitados.

6. SIGLAS

COLCERT: Grupo de Respuesta a Emergencias Cibernéticas del Ministerio de Defensa Nacional.
CSIRT: Grupo de Respuestas a Incidentes de Seguridad Informática del Gobierno Nacional.
Token de CSRF: Código único de seguridad que es utilizado para validar la identidad de un usuario.

7. REFERENCIA BIBLIOGRÁFICA

- MAE.G.GEN.01 – Documento Maestro del Modelo de Arquitectura Empresarial – Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. Noviembre, 2022.
- G.INF.07 Guía Cómo construir el catálogo de Componentes de Información. MinTIC, 2016.
- Estándar de Verificación de Seguridad en Aplicaciones. OWASP. Abril, 2017.
- G.INF.03 Guía técnica de Información-Ciclo de vida del dato. MinTIC. Octubre, 2019.
- Lineamientos Modelo de Arquitectura Empresarial. MinTIC. Noviembre, 2022.

  - MAE.LI.AS.01 – AUDITORIA Y TRAZABILIDAD DE COMPONENTES DE INFORMACIÓN.
  - MAE.LI.AS.02 - PROTECCIÓN Y PRIVACIDAD DE COMPONENTES DE INFORMACIÓN.

- MAE.LI.AS.03 - SEGURIDAD Y PRIVACIDAD DE LOS SISTEMAS DE INFORMACIÓN.
- MAE.LI.AS.04 - AUDITORÍA Y TRAZABILIDAD DE LOS SISTEMAS DE INFORMACIÓN.
- MAE.LI.AS.05 - ANÁLISIS DE RIESGOS.
- MAE.LI.AS.06 - SEGURIDAD INFORMÁTICA.

HISTORIAL DE CAMBIOS		
Fecha	**Versión**	**Descripción**
	1	Creación del documento. Documento en primera versión. Disponer a la ANT de un documento de consulta en la identificación de procesos y controles de seguridad digital que guíe al equipo de colaboradores encargado de la seguridad de la información y a los responsables de la información a su cargo. Este instrumento procedimental determina por medio de actividades, los pasos que se deben ejecutar para cumplir con uno o varios lineamientos indicados en el Marco de Referencia de Arquitectura Empresarial versión 3 bajo el dominio de la Arquitectura de seguridad.

Elaboró:	**Revisó:**	**Aprobó:**
Carlos Eduardo Alfonso Pinilla	Diana Lucia Herrera Riaño	Tony Luís Lozano Berrocal
Cargo: Contratista - Subdirección de Sistemas de Información de Tierras	**Cargo:** Subdirectora de Sistemas de Información de Tierras.	**Cargo:** Director de Gestión de Ordenamiento Social de la Propiedad
Firma: **ORIGINAL FIRMADO**	**Firma:** **ORIGINAL FIRMADO**	**Firma:** **ORIGINAL FIRMADO**