DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI EN LA AEROCIVIL PARA EL PROCESO DE GESTION DE TECNOLOGIAS DE INFORMACIÓN (GINF 6.0).

SIXTA ALEXANDRA QUIROGA CASTILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, CUNDINAMARCA
2020

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI EN LA AEROCIVIL PARA EL PROCESO DE GESTION DE TECNOLOGIAS DE INFORMACIÓN (GINF 6.0).

SIXTA ALEXANDRA QUIROGA CASTILLO

Proyecto de Grado – Aplicado presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

JOEL CARROLL
Tutor de Curso
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ, CUNDINAMARCA
2020

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., 04 de junio de 2021

DEDICATORIA

Este logro primeramente lo dedico a Dios que, pese a las dificultades siempre escuchó mis plegarias y me dio la salud y la fortaleza para seguir adelante, a mi hija por que ha sido el motor de mi vida y por animarme cada vez que quería renunciar, a mi madre de quien he aprendido que pese a las dolencias siempre ha sido mi ejemplo de tenacidad y fortaleza y a mi padre (QEPD) quien con su nobleza me enseñó a ser humilde y paciente, a todos y cada uno de mis familiares y amigos por su apoyo incondicional.

AGRADECIMIENTOS

Agradezco a Dios por darme paciencia, tranquilidad, fortaleza y sabiduría para alcanzar esta meta propuesta, sin sus bendiciones no podría haberlo logrado.

A la empresa Aeronáutica Civil que la quiero mucho porque gracias a mi estabilidad laboral, he podido superarme a nivel profesional y me ha brindado todo el apoyo en lo requerido para la recolectar la información y documentación de apoyo para desarrollar el proyecto.

A mi director de proyecto, el Ingeniero Joel Carroll, por ser un guía incondicional y brindarme sus conocimientos cada vez que lo requería y así poder culminar este proyecto de la mejor manera.

A la universidad Nacional Abierta y A Distancia – UNAD por recibirme después de mucho tiempo y homologarme algunos créditos, lo que permitía continuar con mis estudios y por su metodología a distancia que permite un aprendizaje de autoestudio y permitirme programar mi tiempo para dedicar a la familia, al trabajo y al estudio.

CONTENIDO

pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

GLOSARIO

Amenaza: Es la acción que aprovechando una vulnerabilidad puede desencadenar un incidente de seguridad, lo cual conlleva a producir daños a un sistema o a una entidad.

Confidencialidad: "La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización"[1].

Contraseñas: "Una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se les permite el acceso. A aquellos que desean acceder a la información se les solicita una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso"[2].

Datos: "El dato es una representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o variable cuantitativa. Los datos describen hechos empíricos, sucesos y entidades. Es un valor o referente que recibe el computador por diferentes medios, los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo"[3].

Debilidad: "Las debilidades se refieren a todos aquellos elementos, recursos, habilidades y actitudes que la empresa ya tiene y que constituyen barreras para lograr la buena marcha de la organización. (en este caso un sistema)"[4].

Disponibilidad: "La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean

---

[1]EVALUANDOSOFTWARE.COM. Seguridad de la Información. [www.evaluandosoftware.com]. [Consulta realizada el 14 de abril de 2020]. Disponible en: https://www.evaluandosoftware.com/seguridad-la-informacion-empresarial/.

[2] WIKIPEDIA. Contraseña. [es.wikipedia.org]. [Consulta realizada el 14 de abril de 2020]. Disponible en: https://es.wikipedia.org/wiki/Contrase%C3%B1a.

[3] WIKIPEDIA. Dato. [es.wikipedia.org]. [Consulta realizada el 14 de abril de 2020]. Disponible en: https://es.wikipedia.org/wiki/Dato.

[4] WIKIPEDIA. Análisis FODA. [es.wikipedia.org]. [Consulta realizada el 14 de abril de 2020]. Disponible en: https://es.wikipedia.org/wiki/An%C3%A1lisis_FODA.

personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la
información y a los sistemas por personas autorizadas en el momento que así lo requieran"[5].

"En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración"[6].

Fallos: "Es un estado o situación en la que se encuentra un sistema formado por dispositivos, equipos, aparatos y/o personas en el momento que deja de cumplir la función para el cual había sido diseñado.". Si se desea diseñar un sistema robusto, confiable, es necesario tener siempre presente las situaciones de fallas y avanzar a esta situación mediante métodos matemáticos y científicos"[7].

Integridad: Es la "propiedad que busca mantener los datos libres de modificaciones no autorizadas. (No es igual a integridad referencial en bases de datos.) Grosso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados"[8].

Publicación: "Son todas aquellas definiciones de la serie de normas ISO/IEC 27000 las cuales aportan recomendaciones para implementar un SGSI, describen los pasos para establecer, monitorear, mantener y mejorar de un SGSI, La última

[5]SITES. Seguridad en la red. Disponible en: https://sites.google.com/site/seguridadenlaared/concepcion-de-la-seguridad-de-la-informacion/disponibilidad.

[6] MORÁN DELGADO, Pedro Enrique. [en línea]. Tesis de grado previa a la obtención del título de ingeniero en sistemas e informática. Universidad Regional Autónoma de los Andes Uniandes, 2016. [Consulta realizada en mayo del 2020]. Disponible en: http://dspace.uniandes.edu.ec/bitstream/123456789/4222/1/TUSDSIS030-2016.pdf.

[7] INFORMATICAEET12016. [Anónimo]. La seguridad informática. [informaticaeet12016.blogspot.com]. 16 de mayo de 2016. [Consulta realizada el 14 de abril de 2020]. Disponible en: http://informaticaeet12016.blogspot.com/2016/05/1-hacker-es-alguien-que-descubre-las.html.

[8] SEGURIDAD INFORMATICA. [seguridad-informatica5.webnode.es]. (20, mayo, 2013). [Consulta realizada el 14 de abril de 2020]. Disponible en: https://seguridad-informatica5.webnode.es/news/confidencialidad-integridad-y-disponibilidad-de-la-informacion/.

edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua."[9].

ISO/IEC 27001: "Publicada el 15 de octubre de 2005, revisada el 25 de septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones"[10].

Política de seguridad: Las Políticas de seguridad de la Información son definidas para establecer el comportamiento que debe tener cada uno de los funcionarios responsables de la información y usuarios de Activos de Información (contratistas, terceros, estudiantes en pasantía, funcionarios de entidades de control, delegados de convenios nacionales e internacionales y asociados), sin excepción, en el manejo de la información y de los componentes tecnológicos de una organización, a través de las directrices expresadas por la Alta Gerencia.

Procedimientos: "Es un conjunto de acciones u operaciones que tienen que realizarse de la misma forma, para obtener siempre el mismo resultado bajo las mismas circunstancias (por ejemplo, procedimiento de emergencia)"[11].

Recursos: Son todas aquellas provisiones utilizadas para producir un beneficio.

Riesgo. Es la combinación de la probabilidad de un evento y sus consecuencias

SGSI: "Es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de Información Security Management System"[12].

---

[9] UNIVERSIDAD AUTONOMA DEL ESTADO DE MEXICO; Gestión de la Seguridad de la Información ISO / IEC 27000; [Blog]; [Consulta realizada en mayo del 2020]. Disponible en: https://www.academia.edu/19056080/GESTION_DE_LA_SEGURIDAD_DE_LA_INFORMACIO.

[10] ISO27000.ES. Serie "27000". [www.iso27000.es]. [Consulta realizada el 14 de abril de 2020]. Disponible en: http://www.iso27000.es/iso27000.html.

[11] WIKIPEDIA. Procedimiento. [es.wikipedia.org]. [Consulta realizada el 14 de abril de 2020]. Disponible en: https://es.wikipedia.org/wiki/Procedimiento.

[12] SGSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información. [Consulta realizada el 15 de abril de 2020]. Disponible en: https://www.pmg-ssi.com/2015/07/que-es-sgsi/.

Sistema de detección de intrusos: "(o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos crackers o Hackers que utilizan programas escritos de otros para penetrar algún sistema, red de computadora o página web, también conocidos como Script Kiddies"[13].

Vulnerabilidad. "Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas"[14].

[13] SGSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información. [Consulta realizada el 15 de abril de 2020]. Disponible en: https://www.pmg-ssi.com/2015/07/que-es-sgsi/.

[14] MAGAZCITUM.COM.MX. Vulnerabilidades, amenazas y riesgo en "texto claro". [Consulta realizada el 15 de abril de 2020]. Disponible en:https://www.magazcitum.com.mx/?p=2193#.XrSrfWhKiUl.

RESUMEN

Actualmente las organizaciones y entidades gubernamentales están expuestas a diferentes riesgos o amenazas de tipo informático y ataques cibernéticos, por lo que la mayor preocupación se centra en la seguridad de la información en sus tres componentes (confidencialidad, integridad y la disponibilidad) y en la no afectación de sus servicios, teniendo en cuenta lo anterior, en la Aeronáutica Civil como entidad gubernamental y como infraestructura crítica expuesta a diferentes tipos de ataques, es necesario diseñar un Sistema de Gestión de Seguridad de la Información, basándose en un diagnóstico del estado actual de la entidad que permita realizar un comparativo de los procesos actuales con que cuenta la Aerocivil con los lineamientos y en cumplimiento de la ISO/IEC 27001 y poder establecer prioridades y enfocar los esfuerzos para poder incrementar la seguridad de la información, diseñando la política general y las específicas del SGSI, de igual manera es necesario diseñar una metodología para levantamiento de Activos de Información y gestión de riesgos de seguridad para el proceso de Gestión de Tecnologías de Información, con el fin de contribuir al incremento de la seguridad de la información que permita mitigar estos riesgos y amenazas las cuales aprovechan cualquier vulnerabilidad existente inherente a su infraestructura.

PALABRAS CLAVE: Sistema de Gestión de Seguridad de la Información - SGSI, Vulnerabilidad, Riesgo, Amenaza, Seguridad, Activo de Información, PHVA, Norma ISO, Políticas de seguridad, Controles de seguridad.

ABSTRACT

Currently, organizations and government entities are exposed to different risks or threats of the computer type and cyber attacks, so the main concern is focused on information security in its three components (confidentiality, integrity and availability) and on the non-affecting its services, taking into account the above, in Civil Aeronautics as a governmental entity and as a critical infrastructure exposed to different types of attacks, it is necessary to design an Information Security Management System, based on a diagnosis of the current state of the entity that allows a comparison of the current processes that the Aerocivil has with the guidelines and in compliance with ISO / IEC 27001 and to establish priorities and focus efforts to increase information security, designing the general policy and the specific ones of the ISMS, likewise it is necessary to design ar a methodology for raising Information Assets and security risk management for the Information Technology Management process, in order to contribute to the increase in information security that mitigates these risks and threats which exploit any vulnerability existing inherent in its infrastructure.

Keywords: Information Security Management System - ISMS, Vulnerability, Risk, Threat, Security, Information Asset, PHVA, ISO Standard, Security Policies, Security controls.

INTRODUCCIÓN

La información es el activo más valioso para toda organización, desde el momento en que se genera, hasta que deja de ser útil, las tecnologías de información han venido evolucionando cada vez más rápido, hasta el punto de que se han vuelto críticas en la operación de toda empresa.

Continuamente las organizaciones sufren cambios, como cambios en su entorno, nuevos requisitos, en su regulación, en adquisiciones etc., "mientras más grande sea una empresa, más grande es el número de cambios por sufrir, cada uno de esos cambios producidos trae asociados una serie de riesgos los cuales nacen resultados desde lo más inofensivo hasta lo más desastroso, esto hace que las empresas traten de conseguir un mayor grado de resiliencia posible y poder ser capaces de absorber las perturbaciones sin alterar elocuentemente sus características de organización y funcionalidad y así poder regresar a su estado original una vez que la perturbación haya terminado"[15].

La seguridad informática está enfocada principalmente en la protección de la infraestructura computacional y es por tanto la habilidad de identificar y eliminar vulnerabilidades respecto a temas informáticos. Además de esto puede ser definida como la "preservación de la confidencialidad, la integridad y la disponibilidad de los sistemas de información. Dependiendo de las diferentes organizaciones pueden existir tipos de amenazas ya sean de agentes externos e internos, es decir de eventos accidentales o intencionales que puedan ocasionar daños en el sistema informático provocando pérdidas financieras, materiales, entre otras. Para disminuir el riesgo son utilizados los controles de seguridad informática que pueden ser controles físicos, controles lógicos o técnicos y controles administrativos"[16].

"Las metodologías de análisis de riesgo difieren esencialmente en la manera de estimar la probabilidad de ocurrencia de una amenaza y en la forma de determinar el impacto en la organización, es usado el estándar internacional ISO/IEC 27001 el cual adopta una metodología de análisis de riesgos cualitativa para los sistemas de gestión de la seguridad informática"[17].

---

[15] VARGAS, Elmer Charles. RISK IT. Tópicos II. [Consultado el 12 de abril de 2020]. Dispobible en: http://cuevabardalesriskti.weebly.com/iquestqueacute-es-el-riesgo-de-ti.html.

[16] TIPTON. Information Security Management Handbook, 5th Ed., CRC Press. 2006. Disponible en: https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/.

[17] GARCIA, Juan Manuel y MARTINEZ, Carol. Análisis y control de riesgos de seguridad informática: control adaptativo. [Consultado el 12 de abril de 2020]. Disponible en: http://acistente.acis.org.co/typo43/fileadmin/Revista_105/JMGarcia.pdf.

La información es un activo que como otros es esencial para la operación y negocio de una organización, por tanto, debe ser protegido adecuadamente. El riesgo es la medida de la probabilidad de que una amenazada aproveche una vulnerabilidad y consiga afectar a un activo de información.

El enfoque de la seguridad informática se basa en la protección de la infraestructura de las TIC (Tecnologías de Información y Comunicación) como: redes, impresoras, computadores, servidores, estaciones de trabajo; mientras que la seguridad de la información se enfoca en la protección de los Activos de Información críticos y que son indispensables para el normal funcionamiento de la organización como: bases de datos, correos electrónicos, contratos, páginas web, documentos, entre otros. Se ostenta que la información está asegurada cuando posee las siguientes propiedades: Confidencialidad (la información no será conocida por personas, entidades o procesos no autorizados), Integridad (la información será confiable, completa, exacta y no alterada), Disponibilidad (la información estará al alcance en el momento en que es requerida por una entidad autorizada), no repudiación (garantiza que quien genere un evento de forma válida no pueda retractarse, pues se puede probar la ocurrencia de un evento y quien lo origina).

El manejo de la seguridad de la información requiere una gestión integral por procesos, de los recursos humanos, recursos tecnológicos, leyes y reglamentos, en concordancia con las metas organizacionales, un sistema que realiza esta función es denominado Sistema de Gestión de Seguridad de la Información, más conocido por sus siglas como SGSI.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

El uso de los medios digitales en el sector transporte en Colombia para el desarrollo de sus actividades económicas y sociales, en los últimos años ha venido creciendo a pasos agigantados, esto acarrea incertidumbres y riesgos inherentes de seguridad digital que deben ser gestionados permanentemente, el no hacerlo, podría resultar en la materialización de amenazas o ataques cibernéticos, generando efectos no deseados de tipo económico o social para el país, y afectando la integridad de los ciudadanos en estos contextos.

"Los ciberataques son las amenazas de más rápido crecimiento, y quizás los más peligrosos, que enfrentan las organizaciones actualmente, está relacionado con el crecimiento progresivo de la ciberdelincuencia, ya que, con esto, los piratas informáticos aprovechan las malas prácticas, las limitadas capacidades de aplicación de la ley y la mala gobernanza de la ciberseguridad"[18]. Por tal motivo, "las juntas directivas de grandes organizaciones deben asumir un papel de liderazgo en la supervisión y en la mejora de la seguridad de los sistemas cibernéticos"[19], sin embargo, "una investigación reciente de la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo encontró que en general las juntas corporativas en América Latina poseen niveles de madurez bajos o medios relacionados con la ciberseguridad, por tanto es posible que no sean conscientes de cómo esas amenazas cibernéticas puedan afectar específicamente y de manera directa a sus organizaciones"[20]. "Una de las posibles amenazas que se pueden presentar son las amenazas persistentes avanzadas, que implementan malware dirigidos contra sistemas y personas, insertándose en un sistema generalmente de

[18] CARTER, William. Forces shaping the cyber threat landscape for financial institutions. Swift institute working paper no. 2016-004. 2017. [Consultado el 12 de abril de 2020]. Disponible en: https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf

[19] INTER AMERICAN DEVELOPMENT BANK. Cybersecurity: Are We Ready in Latin America and the Caribbean?. Organization of American States. 2016. [Consultado el 12 de abril de 2020]. Disponible en: https://digital-iadb.leadpages.co/publicacion-cibersecurity/

[20] ORGANIZACIÓN DE LOS ESTADOS AMERICANOS, INTERNET SECURITY ALLIANCE BOARD OF DIRECTORS. Manual de supervisión de riesgos cibernéticos para juntas corporativas. 2017. [Consultado el 12 de abril de 2020]. Disponible en: https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf.

forma encubierta, con la intención de comprometer la confidencialidad, integridad o disponibilidad de los datos, aplicaciones o sistema operativo de las víctimas"[21].
"Las empresas aeronáuticas son el principal objetivo de acciones de diferentes agentes maliciosos como por ejemplo de piratas informáticos, es necesario evitar que estas empresas sufran ataques ya que las consecuencias pueden ser mayores como por ejemplo la investigación realizada por la compañía especializada Oliver Wyman, los cuales afirman que se encuentran preparados para un posible ataque cibernético"[22].

La Aeronáutica Civil como infraestructura crítica cibernética, está expuesta a un sin número de amenazas las cuales aprovechan cualquier vulnerabilidad existente inherente a su infraestructura crítica, "pueden someter a los mismos a diversas formas de espionaje, fraude, sabotaje o vandalismo, estas técnicas de ataques dirigidos contra usuarios finales, la adopción de malware móvil y los ataques de denegación de servicio son algunos de los ejemplos más comunes y conocidos, además de estos, es preciso considerar los riesgos causados voluntaria o involuntariamente desde el interior de la organización o aquellos provocados accidentalmente por catástrofes naturales o fallas técnicas"[23].

1.2 FORMULACIÓN DEL PROBLEMA

¿De qué manera el diseño del SGSI en la Unidad Administrativa Especial de Aeronáutica Civil – AEROCIVIL contribuirá al incremento de la seguridad de la información para el proceso de Gestión de Tecnologías de Información (GINF 6.0)?

[21] SCARFONE, Karen., MELL, Peter. Guide to Intrusion Detection and Prevention Systems (IDPS) National Institute of Standards and Technology. [Consultado el 15 de abril de 2020]. Disponible en: https://csrc.nist.gov/publications/detail/sp/800-94/rev-1/draft
[22] MICÓ, Joseph. Los hackers se fijan ahora en las aerolíneas. La Vanguardia. 2018. Disponible en: https://www.lavanguardia.com/tecnologia/20180504/443211359106/aerolineas-hackers-ataques-seguridad.html.
[23] GALLEGO YUSTE, Alberto. [en línea]. Proyecto fin de carrera. delitos informáticos: malware, fraudes y estafas a través de la red y cómo prevenirlos. Universidad Carlos III de Madrid, Leganés, octubre de 2012. [Consulta realizada en mayo del 2020]. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/16868/pfc_alberto_gallego_yuste.pdf?sequence=1.

2 JUSTIFICACIÓN

La UNIDAD ADMINISTRATIVA ESPECIAL DE AERONAUTICA CIVIL es una Entidad de carácter técnico adscrita al Ministerio de Transporte, con personería jurídica, autónoma administrativa y patrimonio independiente, con sede principal en la ciudad de Bogotá D.C.

El Artículo 2° del Decreto 260 del 28 de enero de 2004 (Por el cual se modifica la estructura de la Unidad Administrativa Especial de Aeronáutica Civil — AEROCIVIL) señala que la AEROCIVIL, es la autoridad en materia aeronáutica en todo el territorio nacional y le compete regular, administrar, vigilar y controlar el uso del espacio aéreo colombiano por parte de la aviación civil, y coordinar las relaciones de esta con la aviación de Estado; desarrollando las políticas, estrategias, planes, programas y proyectos sobre la materia, contribuyendo de esta manera al mantenimiento de la seguridad y soberanía nacional.

Por lo anterior la AERONAUTICA CIVIL, tiene como objeto “Garantizar el desarrollo ordenado de la aviación civil, de la industria aérea y la utilización segura del espacio aéreo colombiano, facilitando el transporte intermodal y contribuyendo al mejoramiento de la competitividad del país”.

La Dirección de Informática perteneciente a la Secretaría General de la Aeronáutica Civil presta sus servicios brindando apoyo tecnológico a las diferentes áreas y dependencias a nivel nacional, mediante el suministro de tecnologías de la información: sistemas de información, aplicaciones, soluciones y servicios de información y tecnológicos, todo lo anterior soportada bajo la infraestructura de hardware, software, red de datos y comunicaciones, indispensables para el acceso y la ejecución adecuada a los diferentes usuarios de la Entidad a nivel nacional, para aumentar la eficiencia y efectividad de la ejecución de los procesos misionales, administrativos, estratégicos y de control de la Entidad en cumplimiento de sus funciones, fortaleciendo así la capacidad de la AERONAUTICA CIVIL para soportar y cubrir las necesidades que se demandan en materia de Tecnologías de la Información.

Para la UAEAC es de vital importancia implementar los mejores esquemas para protección de la información, acordes con la normatividad establecida, como son el Sistema de Gestión de Seguridad de la Información SGSI a la luz de las Normas

ISO27001, ISO27002 e ISO27005 y los últimos estándares internacionales; ya que en el mundo digital el intercambio de información juega un papel fundamental en un ambiente cada vez más globalizado y competitivo y la información es considerada uno de los activos más valiosos. Para lograr este objetivo, se requiere evaluar periódicamente los riesgos que constantemente amenazan los activos de información y que por ende afectan la continuidad en la prestación de los servicios tecnológicos informáticos que apoyan su normal funcionamiento e implementar los controles de seguridad necesarios para mitigar el riesgo tecnológico.

Teniendo en cuenta que la Aerocivil no cuenta con un Sistema de Gestión de Seguridad de la Información - SGSI, se hace necesario el diseño del mismo, que esté orientado a asegurar la Disponibilidad, Integridad y Confidencialidad de la información y de los componentes tecnológicos buscando hacer el mejor uso de los Recursos Informáticos que provee la Entidad y establecer los lineamientos para el comportamiento que debe tener cada uno de los funcionarios, responsables de la información y usuarios de activos de información, así como los contratistas, terceros, estudiantes en pasantías, funcionarios de entidades de control, delegados de convenios nacionales e internacionales y asociados de la UAEAC, sin excepción, en el manejo de la información y de los componentes tecnológicos informáticos de la Entidad, a través de las directrices expresadas por la Dirección General.

El Sistema de Gestión de Seguridad de la Información, permite aumentar la confianza en la Entidad, ya que es una garantía de su compromiso con la protección de sus datos y la de sus clientes, usuarios y proveedores; adicionalmente, contribuye a evitar sanciones relacionadas con los riesgos económicos, legales, estratégicos, operativos, de imagen y de privacidad y protección de datos sensibles, mediante la integración de políticas de seguridad a las normativas y requisitos legales tanto nacionales como internacionales.

Por otro lado, el Decreto 1078 del 2015, “por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, establece los principios para desarrollar la Política de Gobierno Digital, encontrándose entre ellos el de la “Seguridad de la Información”, el cual busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la Confidencialidad, Integridad y Disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano”[24].

[24]COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACION Y LAS

Que el Ministerio de Tecnologías de la Información y las Comunicaciones “creó el componente de Seguridad y Privacidad de la Información con el objetivo de garantizar que las entidades aseguren la información y la privacidad de los datos de ciudadanos y funcionarios, de acuerdo con lo establecido en la legislación colombiana”[25].

Que la implementación del Sistema de Gestión de Seguridad de la Información - SGSI “busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la Confidencialidad, Integridad, Disponibilidad y Privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado.”

COMUNICACIONES. Decreto 1078 de 2015. (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. En: Diario Oficial. Diciembre, 2015. No. 49.523. Bogotá: [Consultado el 15 de abril de 2020]. Disponible en: https://www.redjurista.com/Documents/decreto_1078_de_2015_presidencia_de_la_republica.aspx#/.

[25] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. Fortalecimiento de la Gestion TI en el estado. [Consultado el 15 de abril de 2020]. Disponible en: https://mintic.gov.co/portal/inicio/Iniciativas/Servicios/Fortalecimiento-de-las-TI-de-la-informacion-en-la-gestion-del-Estado-y-la-informacion-publica/.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Diseñar el SGSI en la Unidad Administrativa Especial de Aeronáutica Civil - AEROCIVIL, con el fin de realizar un comparativo de los procesos actuales que tiene la Entidad con los lineamientos de cumplimiento de la norma ISO/IEC 27001 y establecer en qué áreas o procesos se debería priorizar y enfocar los esfuerzos y así incrementar la seguridad de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Diagnosticar el estado actual de la Entidad frente al SGSI y diseñar un Modelo de Gestión de Seguridad de la Información para el proceso de Gestión de Tecnologías de Información (GINF. 6.0).

- Diseñar la Política General y las específicas del SGSI

- Diseñar la metodología de Activos de Información y Riesgos para el proceso GINF. 6.0 Gestión de Tecnologías de Información, bajo los lineamientos de MinTic.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO Y MARCO CONCEPTUAL

La seguridad informática se enfoca principalmente en la protección de la infraestructura computacional y es por tanto la habilidad de identificar y eliminar vulnerabilidades respecto a temas informáticos. Además de esto puede ser definida como la preservación de la confidencialidad, la integridad y la disponibilidad de los sistemas de información. “Dependiendo de las diferentes organizaciones pueden existir tipos de amenazas ya sean de agentes externos e internos, es decir de eventos accidentales o intencionales que puedan ocasionar daños en el sistema informático provocando pérdidas financieras, materiales, entre otras. Para disminuir el riesgo son utilizados los controles de seguridad informática que pueden ser controles físicos, controles lógicos o técnicos y controles administrativos”[26].

La Gestión de Riesgos de Seguridad de la Información permite a una organización evaluar el nivel de riesgo de los Activos de Información y provee información para determinar las necesidades o requerimientos adicionales de control para prevenir la materialización de los riesgos de Seguridad de la Información o para mitigar los posibles impactos. Según la guía 7 para la Administración del Riesgo emitida por el Departamento Administrativo de la Función Pública - DAFP, la administración del riesgo ayuda al conocimiento y mejoramiento de la entidad, contribuyendo a elevar la productividad y a garantizar la eficiencia y la eficacia en los procesos organizacionales, permitiendo definir estrategias de mejoramiento continuo, brindándole un manejo sistémico a la entidad.

“El Sistema de Gestión de Seguridad de la Información, es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, roles, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua, bajo el ciclo PHVA (Planear, Hacer, Verificar y Actuar), con el fin de preservar la seguridad de la información en sus tres

[26] CUBILLOS, Myrian. et al. Guía para la Administración del Riesgo. Departamento Administrativo de la Función Pública. Dirección de control interno y racionalización de trámites. Colombia. Cuarta edición. 2011. [Consultado el 15 de abril de 2020]. Disponible en: https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba.

pilares; los cuales son confidencialidad, el cual indica que los Activos de Información sólo sean accedidos por los usuarios, procesos o terceros autorizados y con las condiciones de seguridad adecuadas, el segundo; la Integridad la cual es la propiedad de los Activos de Información que se refiere a la exactitud y completitud de estos y tercero la Disponibilidad, la cual indica que deben estar accesibles para los usuarios autorizados, cuando se requiera (ahora y en el futuro) y en los medios necesarios para su uso".

4.2 ANTECEDENTES O ESTADO ACTUAL

El SGSI propone un enfoque sistemático buscando "garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados, es por ello que se debe tener un plan de gestión de seguridad que contemple la identificación de los Activos de Información y sus propietarios, identificación de las amenazas para cada uno de los activos, identificación de las vulnerabilidades del sistema e identificación de los posibles impactos de las vulnerabilidades encontradas y así poder gestionarlos, ya sea evitándolos, lo que quiere decir que se deben suprimir las causas del riesgos o transferirlos ya sea a un seguro o un Outsourcing o poder reducirlo o aceptarlo"[27].

Las organizaciones que pretenden implementar un sistema integrado basado en la seguridad de la información y que sea certificado internacionalmente, deberían desarrollar e implementar un Sistema de Gestión de Seguridad de la Información – SGSI basado en las normas ISO/IEC 27001:2013, estándar certificable y actualmente aprobado en Colombia por ICONTEC, ésta es la principal norma de la familia ISO 27000 y contiene los requisitos básicos, describe los objetivos y controles recomendados para la seguridad de la información y guía de las mejores prácticas para la seguridad.

El objetivo de implementar un sistema el SGSI en una organización, es que brinda seguridad a todos los Activos de Información más relevantes a través de los resultados del análisis de riesgo y otorgando que la confiablidad de la seguridad, lo anterior, "basado en lineamientos primordiales que deben ser utilizados por los responsables de la seguridad de la información y poder gestionar la clasificación de sus activos de información, con el fin de levantar un inventario y determinar que

[27]COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [www.mintic.gov.co]. Bogotá: MINTIC, Guía para la Gestión y Clasificación de Activos de Información. [Consulta realizada en mayo del 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-482_G5_Gestion_Clasificacion.pdf.

activos posee la entidad, de cómo deben ser utilizados, cuáles son los roles y responsabilidades que tienen los funcionarios sobre estos y, reconocer el nivel de clasificación de la información que a cada activo debe dársele", por otra parte, lo que persigue un SGSI es proteger la información como recurso valioso, para lo cual debe proteger de igual forma los diferentes medios a través de los cuales se genera, almacena, procesa, transmite, circula y transforma en un recurso útil para los negocios. Estos medios son las TIC en su conjunto.

4.3 PRESENTACIÓN DE LA EMPRESA UNIDAD ADMINISTRATIVA ESPECIAL DE AERONÁUTICA CIVIL – AEROCIVIL.

"La Aeronáutica Civil de Colombia es una empresa del estado, con la Ley 105 del 30 de diciembre de 1993, por la cual se organiza el sector y el Sistema Nacional de Transporte adscribiendo nuestra institución al Ministerio de Transporte, como órgano rector de la política y ejecución de las funciones relativas al transporte aéreo; se diseñó un organigrama institucional que atiende a la naturaleza de las dos grandes tareas a la entidad: la aeronavegación y el servicio aeroportuario; en consecuencia se crean la Secretaria Técnica y la Secretaria Aeroportuaria.

La Aeronáutica Civil es el resultado de la fusión del Departamento Administrativo de Aeronáutica Civil y el Fondo Aeronáutico Nacional, ordenado par el Art. 67 del Decreto 2171 de 1992.

En la actualidad la entidad se rige por el Decreto 260 del 28 de enero de 2004 con un nuevo ordenamiento administrativo y con nuevas dependencias.

Figura 1. Edificio Aerocivil

Fuente: http://intranet.aerocivil.gov.co/

Misión

Trabajamos por el crecimiento ordenado de la aviación civil, la utilización segura del espacio aéreo colombiano, la infraestructura ambientalmente sostenible, la conexión de las regiones entre sí y con el mundo, impulsando la competitividad y la industria aérea y la formación de un talento humano de excelencia para el sector.

Visión

Al 2030, movilizar 100 millones de pasajeros y duplicar el transporte de carga partiendo del 2018, en un entorno institucional claro, competitivo, conectado, seguro y sostenible, soportado en una infraestructura renovada, una industria robustecida y un talento humano de excelencia.

Objetivos Institucionales

Institucionalidad

Consolidar los roles de autoridad, de prestación del servicio y de investigación de accidentes para dinamizar el crecimiento del transporte aéreo, contribuyendo a la aviación civil colombiana.

Conectividad

Construir una red de servicios de transporte aéreo eficiente que una las regiones del país con los principales centros de producción y de consumo nacionales y del mundo, aprovechando su capacidad integradora.

Competitividad

Desarrollar políticas, públicas y estrategias que fortalezcan el factor de productividad del transporte aéreo y estimulen los servicios para el crecimiento de la aviación civil en Colombia.

Infraestructura y sostenibilidad ambiental

Lograr que la infraestructura, los servicios aeroportuarios, de navegación aérea y la intermodalidad, cuenten con capacidad y eficiencia para atender el crecimiento de la demanda del sector en un contexto ambientalmente sostenible.

Industria aeronáutica y cadena de suministro

Potenciar la industria aeronáutica como un importante proveedor de piezas, partes y componentes aeronáuticos certificados para la región y como punto focal en la producción de aeronaves livianas (ALS) y no tripuladas (UAS – RPAS), impulsando a su vez servicios de mantenimiento y reparación de aeronaves

Desarrollo del Talento Humano en el sector

Fortalecer la gestión del conocimiento para lograr el desarrollo integral y sostenible del talento humano, en línea con el crecimiento de la aviación civil en Colombia.

Seguridad Operacional y de la Aviación Civil

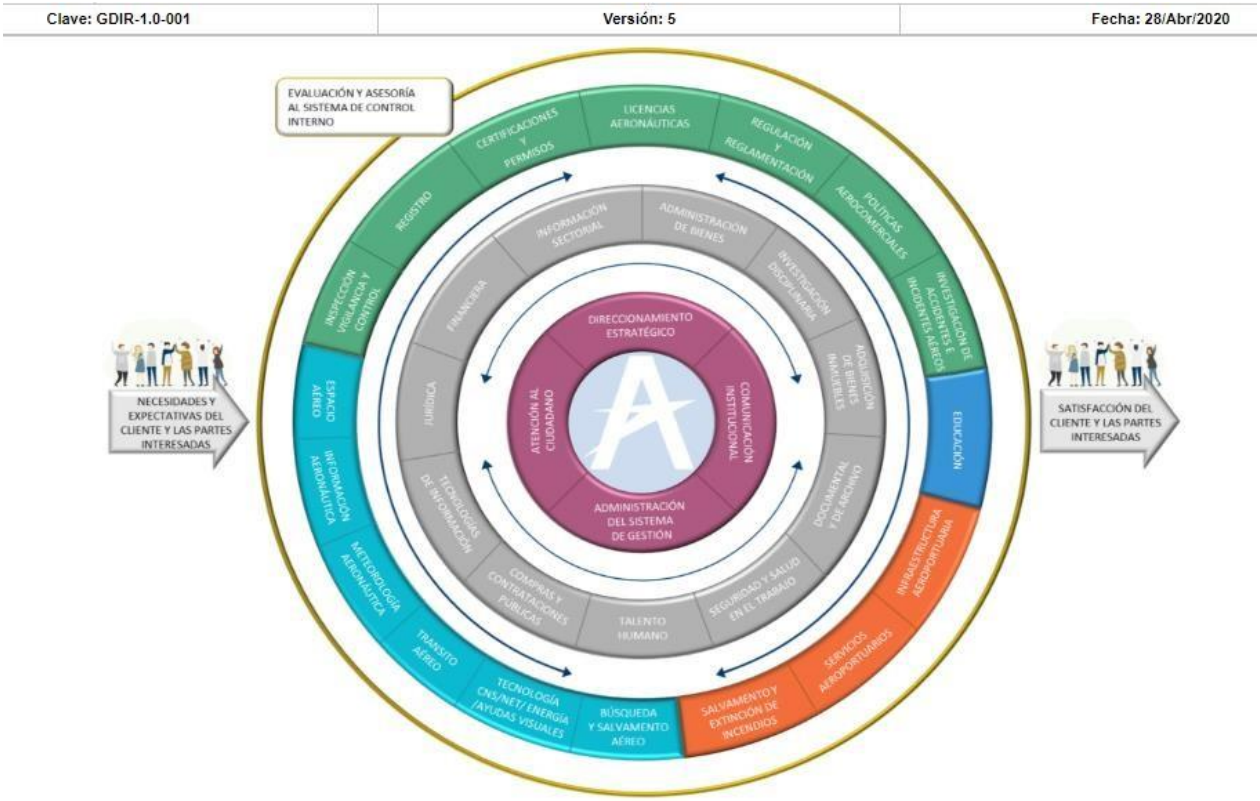
Posicionar al país con el mayor nivel de implementación efectiva de estándares y mejores prácticas en seguridad operacional (safety), seguridad de la aviación civil (security) y facilitación, en un entorno de confianza y de cultura justa en compañía del sector.

La transformación institucional a la modernidad

Fortalecer la gestión institucional de la Entidad a través del desarrollo del talento humano, fortalecimiento de la estructura organizacional, implementando un sistema de gestión del conocimiento especializado en la Entidad, afianzando el Sistema Integrado de Gestión, apalancando la transformación institucional a través del PETI, fortaleciendo la política anticorrupción y la gestión jurídica"[28].

Mapa de procesos

Figura 2. Mapa de Procesos



Fuente: http://www.aerocivil.gov.co/aerocivil/procesos

[28] UNIDAD ADMINISTRATIVA ESPECIAL DE AERONAUTICA CIVIL DE COLOMBIA. [www.aerocivil.gov.co]. Bogotá: AEROCIVIL, [Consulta realizada en mayo de 2020]. Disponible en: http://www.aerocivil.gov.co/.

4.4 MARCO CIENTÍFICO O TECNOLÓGICO

El Ministerio de Tecnologías de la Información y las Comunicaciones creó el componente de Seguridad y Privacidad de la Información con el objetivo de garantizar que las entidades aseguren la información y la privacidad de los datos de ciudadanos y funcionarios, de acuerdo con lo establecido en la legislación colombiana, la implementación del Sistema de Gestión de Seguridad de la Información - SGSI "busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos, este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado.[29]".

4.5 MARCO LEGAL

"Para una adecuada implementación de un SGSI, es necesario conocer los estándares, su estructura y la relación existente entre cada uno de ellos, el más conocido y aplicado a nivel internacional es el estándar basado en la serie de la ISO/IEC 27000 publicadas por la ISO y la Comisión Electrotécnica Internacional (IEC), la cual está compuesta aproximadamente por 17 normas, que se clasifican en cuatro categorías: La ISO/IEC 27000 que contiene el vocabulario, la ISO/IEC 27001 y la norma ISO/IEC 27006 que contiene los requerimientos, las guías ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27004, ISO/IEC 27005, ISO/IEC 27007, TR 27008, ISO/IEC 27013, ISO/IEC 27014, TR 27016, ISO/IEC 27032 y ISO/IEC 27010, ISO/IEC 27011, TR 27015 y TS 27017 que son las normas para sectores específicos, pero a pesar de la cantidad de normas de la serie ISO/IEC 27000, las que se aplican y sirven como referente para la implementación de un SGSI son: la ISO27001:2013 que indica las Técnicas de seguridad y requerimientos necesarios, la ISO27005: 2008 refiere las líneas base de gestión del riesgo de un SGSI, la ISO27003:2010 presenta la guía de práctica para la implementación de un SGSI y

[29] COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [www.mintic.gov.co]. Bogotá: MINTIC, Guía para la Implementación de Seguridad de la Información en una MIPYME. [Consulta realizada en mayo del 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf.

la ISO/IEC 27002: 2013 la cual indica las prácticas para controles de seguridad de la información [30]".

"Enfatizando en el nivel estatutario en Colombia, regido por la Constitución Política y por una serie de Leyes y decretos como son la Ley 1581 de 2012 de Protección de datos personales, cuyo objeto es desarrollar el derecho constitucional que tiene las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ella en bases de datos o archivos; así como el derecho a la información consagrado la art. 20 de la Constitución Política; Decreto 1377 de 2013 del Ministerio de Comercio, Industria y Turismo en el que reglamenta parcialmente la ley 1581/12"[31], la "Ley 1266 del 31 de diciembre del 2008: Habeas Data, 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. Esta ley desarrolla una regulación integral del derecho fundamental de las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en banco de datos y en archivos de entidades públicas y privadas"[32] , "Ley 1341 del 30 de julio de 2009 determina el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información[33]", la Ley 1273 de 2009. "Por medio de la cual se

[30] DÍAZ, Andrés. et al. Implementación de un sistema de gestión de seguridad de la información (SGSI) en la comunidad nuestra señora de gracia, alineado tecnológicamente con la norma ISO 27001. [Consulta realizada en mayo del 2020]. Disponible en: http://www.konradlorenz.edu.co/images/stories/articulos/SGSI.pdf[30]

[31] COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Ley estatutaria 1581 de 2012. (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. Bogotá: La Presidencia. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf.

[32] SECRETARÍA DEL SENADO. Ley estatutaria 1266 de 2008. Diario Oficial No. 47.219. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html.

[33] ALCALDIA DE BOGOTÁ. [www.alcaldiabogota.gov.co]. Bogotá: ALCALDIA DE BOGOTÁ, documentos para TELECOMUNICACIONES. Tecnologías de la Información y las Comunicaciones-TIC. [Consulta realizada en mayo del 2020]. Disponible en:

modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones[34]", la Constitución Política de Colombia en su "artículo 15 establece que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, siendo obligación del Estado respetarlos y hacerlos respetar, igualmente tienen derecho a conocer, actualizar y rectificar la información que se haya recogido de las diferentes fuentes de información[35]", la Ley 1712 del 6 de marzo de 2014, se crea la "Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y a través de esta se regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información. Así mismo, mediante el Decreto 1494 del 13 de julio de 2015, se corrigen algunos yerros de la citada Ley conforme lo ordenado por la Corte Constitucional en Sentencia C-653/15[36]", el Decreto 1078 del 2015, por medio del cual "se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, establece los principios para desarrollar la Política de Gobierno Digital, encontrándose entre ellos el de la "Seguridad de la Información", el cual busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la Confidencialidad, Integridad y Disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano[37]", "el Decreto 1008, el determina los elementos de la Política de Gobierno Digital, en la Sección 2 y en su artículo 2.2.9.1.2.1. Estructura, establece que la Política de Gobierno Digital será definida por el Ministerio de Tecnologías de Información y las Comunicaciones y se desarrollará a través de componentes y habilitadores transversales allí descritos que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC, conforme se describe en el citado artículo, así mismo el citado Decreto 1008 en su Sección 3 artículo 2.2.9.1.3.2 y siguientes, define como responsable institucional de la Política de Gobierno Digital al representante legal de la Entidad, así como también establece que el Comité

https://www.alcaldiabogota.gov.co/sisjur/listados/tematica2.jsp?subtema=28474&cadena=t

[34] SECRETARÍA DEL SENADO. Ley estatutaria 1273 de 2009. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

[35] CONSTITUCION POLITICA DE COLOMBIA. Artículo 15.2003.

[36] SECRETARÍA DISTRITAL DE HACIENDA. Transparencia y acceso a información pública - Ley 1712 de 2014. 2020.

[37] PRESIDENCIA DE LA REPÚBLICA. Decreto 1078 de 2015. Disponible en: http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201078%20DEL%2026%20DE%20MAYO%20DE%202015.pdf.

Directivo es el responsable de orientar la implementación de la Política y el Director de Informática es el responsable de liderar la implementación de la Política de Gobierno Digital [38]“, por otro lado el Ministro de Transporte encargado, en comunicación de 12 de junio de 2019 dirigida a las entidades del Sector Transporte, dentro del marco del “CONPES 3854 de 2016 (Política Nacional de Seguridad Digital) y el Decreto 1008 de 2018 (Política de Gobierno Digital) ha establecido unos lineamientos para la “Implementación de Seguridad de la Información y Protección de Infraestructuras Críticas Cibernéticas” a través de la generación del “Plan de Protección de Infraestructuras Críticas – Sector Transporte v1.0”, solicitando a las entidades del Sector la toma de acciones urgentes y la obligación de ejecutar las actividades que se enlistan en la mencionada comunicación, sobre las cuales dicho Ministerio realizará los seguimientos necesarios para velar por su cumplimiento. El Decreto 1499 del 11 de septiembre de 2017, adoptó el Modelo Integrado de Planeación y Gestión – MIPG, como un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio, regulando así mismo las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de Gobierno Digital y Seguridad Digital [39]“.

[38] COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [estrategia.gobiernoenlinea.gov.co]. Bogotá: MINTIC, Manual de Gobierno Digital. Implementación de la Política de Gobierno Digital. [Consulta realizada en mayo del 2020]. Disponible en: https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf.

[39] COLOMBIA. FUNCIÓN PÚBLICA. Decreto 1499 de 2017. (11, septiembre, 2017). Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. Bogotá: La Función Pública. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83433.

5 DISEÑO METODOLÓGICO

Este proyecto se desarrolló bajo la técnica y los parámetros de tipo de Investigación, basado en las mejores prácticas internacionales y referenciado en las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013, Modelo de Seguridad y Privacidad de la Información – MSPI de MinTic.

Teniendo en cuenta las características del proyecto, se llevó a cabo una investigación de tipo aplicada, en la que se realizó un análisis inicial de la situación actual de la seguridad de los Activos de Información del proceso Gestión de Tecnologías de Información (GINF. 6.0), y poder aplicar los conocimientos adquiridos, analizando y clasificando cada activo de información, detectando las posibles amenazas para finalmente diseñar controles que ayuden a mitigar los riesgos a los que están expuestos los Activos de Información del proceso en mención.

Tomando como referencia la norma ISO/IEC 27001:2013, se puede determinar que la línea de investigación de este proyecto se relaciona con los siguientes temas: Seguridad de la Información, Tecnología de la información, Gestión de Sistemas, Gestión de la Seguridad, Gestión de Riesgos y Sistema de Gestión de Seguridad de la Información.

Se realizaron las siguientes fases:

Fase I. Diagnosticar el estado actual de la Entidad frente al SGSI.

Aprovechando que la estudiante trabaja en la Aerocivil en la Dirección de Informática y del conocimiento que tiene de la misma, se realizó un diagnóstico el cual permitió hacer un comparativo de los procesos actuales de acuerdo con los lineamientos de MinTic, específicamente en: Guía 2 Política General MSPI, Guía 5 Gestión de Activos, Guía 7 Gestión de Riesgos y en el cumplimiento de la ISO/IEC 27001:2013 en los numerales: 5.2 Política (Anexo A.5), A.6 Responsabilidades y organización de seguridad de la información, A:8 Gestión de Activos: A.8.1 Responsabilidad por los activos, A.8.2 Clasificación de la información y A.9 Control de accesos, con el fin de establecer la prioridad y dónde enfocar los esfuerzos para incrementar la seguridad de la información en el proceso GINF-6.0 Gestión de Tecnologías de Información.

Para la recolección de la información, en esta fase se utilizaron algunos mecanismos como:

- Diligenciamiento de un cuestionario con el objetivo de determinar el nivel de cumplimiento de la entidad con relación a los dominios de la norma ISO/IEC 27001:2013, se realizaron entrevistas al encargado de la Seguridad de la información, administradores de componentes tecnológicos, administradores de seguridad de la información conocedores del proceso Gestión de Tecnologías de Información GINF-6.0.
- Se revisa la documentación existente en el Sistema de Gestión Calidad de la entidad, relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.
- Fuentes externas, como guías de autoevaluación como lo es el instrumento de identificación de la línea base de seguridad, lineamientos y la estrategia de gobierno Digital y las guías de implementación del Modelo de Seguridad y Privacidad de la Información de Ministerio de Tecnologías de la Información y las Comunicaciones – MinTic.

Fase II. Diseñar un Modelo de Gestión de Seguridad de la Información

A nivel metodológico es importante tener presente que el diseño del Modelo de Gestión de Seguridad de la Información se realizó para el proceso de Gestión de Tecnologías de Información (GINF. 6.0), de acuerdo con lo establecido en el Modelo de Seguridad y Privacidad de la Información – MSPI de MinTic, para ello se definió un conjunto de documentos, como: Principios, Políticas, Normas, Estándares y Roles los cuales tendrán como objetivo mejorar la Seguridad de la Información, buscando con ello, hacer el mejor uso de los recursos informáticos de la Entidad.

Fase III. Diseño de la Política general y las específicas del SGSI.

La Política general de seguridad y privacidad de la información y las políticas específicas, se diseñaron de acuerdo con lo establecido en la Guía 2 – Política General MSPI V1, del Modelo de Seguridad y Privacidad de la Información de MinTic., los principios, políticas, normas, estándares y roles están contenidas en un documento con el nombre “Modelo de Gestión de Seguridad de la Información-Proceso GINF-6.0”, en el contenido de estos documentos se describe el objetivo, alcance y el nivel de cumplimiento, que garanticen el adecuado uso de los Activos de información al interior de la Entidad; definiendo las responsabilidades generales y específicas para la gestión de la seguridad de la información.

Fase IV. Diseño de la metodología de Activos de Información para el proceso GESTIÓN DE TECNOLOGIAS DE INFORMACIÓN (GINF. 6.0).

Se diseñó una metodología de Gestión de Activos de Información de acuerdo con la Guía No 5 - Gestión de Activos del Modelo de Seguridad y Privacidad de la Información de MinTic., lo cual permitirá generar un inventario de Activos de Información exacto, actualizado y consistente, que a su vez permita definir la criticidad de los activos de información, sus propietarios, custodios y usuarios.

Se diseñó un instrumento en formato (.doc) para el diligenciamiento de la matriz donde se relaciona el Inventario de Activos de Información específico, en el que se relacionará el objetivo del instructivo, los responsables del desarrollo de las actividades del instructivo, frecuencia de actualización, fuente de información y contenido.

Se diseñó un formato (.xls) Matriz para la gestión y clasificación de activos de información para la gestión de Activos de Información en el que se relacionará el objetivo del procedimiento donde se establecen las actividades para la identificación, valoración y clasificación de Activos de Información en el marco del Sistema de Gestión de Seguridad de la Información – SGSI y los lineamientos impartidos por MinTic en Guía 5 - Gestión Clasificación de Activos.

Para el levantamiento del inventario de Activos de Información del proceso Gestión de Tecnologías de Información (GINF - 6.0), la información de interés será recolectada de forma directa de la fuente, mediante entrevistas estructuradas y reuniones al Líder del Proceso o responsable del Activo de Información, quien debe tener un conocimiento amplio de la operación del proceso, estas entrevistas constituyen un interrogatorio, a través de la preparación previa de un conjunto de preguntas, formuladas siempre en el mismo orden y en los mismos términos; donde el interrogador anotará las respuestas en forma textual o atendiendo a un código.

Fase V. Diseño de la metodología de riesgos para el proceso GESTIÓN DE TECNOLOGIAS DE INFORMACIÓN (GINF. 6.0).

Se diseñó una metodología de Gestión del Riesgo enfocada al Proceso Gestión de Tecnologías de Información (GINF. 6.0), la cual permitirá identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información a los que estén expuestos estos activos. Para conseguir una integración adecuada entre el MSPI y

la guía de gestión del riesgo emitida por el DAFP respecto a este procedimiento, es conveniente emplear los criterios de evaluación (impacto y probabilidad) y niveles de riesgo emitidos por esta entidad. Se realizó bajo la Guía No 7 - Gestión de Riesgos emitida por el MinTic.

Se diseñó un instructivo formato (.doc) para el diligenciamiento del Formato de Riesgo de Activos de Información, en el que se relacionará el objetivo del instructivo, los responsables del desarrollo de las actividades del instructivo, frecuencia de actualización, fuente de información y contenido.

Se diseñó un procedimiento formato (.doc) para la gestión de Riesgos de Activos de Información en el que se relacionará el objetivo del procedimiento donde se establecen las actividades para la identificación y valoración de los riesgos de seguridad de la información asociados a los Activos de Información en el marco del Sistema de Gestión de Seguridad de la Información - SGSI.

Por otro lado, se diseñó un formato (.xls) para gestionar los riesgos de los Activos de Información del proceso Gestión de Tecnologías de Información (GINF - 6.0), de acuerdo con los lineamientos impartidos por MinTic, levantamiento de esta información, se realizará mediante entrevistas estructuradas al Líder del Proceso o responsable del Activo de Información, quien debe tener un conocimiento amplio de la operación del proceso.

6 DESARROLLO DE LOS OBJETIVOS

6.1 **DESARROLLO DE OBJETIVO 1:** DIAGNOSTICAR EL ESTADO ACTUAL DE LA ENTIDAD FRENTE AL SGSI Y DISEÑAR UN MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL PROCESO DE GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN (GINF. 6.0).

6.1.1 DIAGNOSTICO DEL ESTADO ACTUAL DE LA ENTIDAD FRENTE AL SGSI

Para el cumplimiento del objetivo número 1, se desarrolló un instrumento en formato Excel con el fin de identificar la línea base de seguridad y verificar de acuerdo con el Anexo A de la ISO 27001, si la Entidad cuenta con una Política de Seguridad de la Información, verificar a cargo de quien se encuentra las responsabilidades y organización de seguridad de la información en la Entidad, validar si la Entidad cuenta con una metodología para levantamiento de activos de información y con un inventario de Activos de Información y si existe una política de control de acceso a la información.

Para la recolección de la información, se solicita al Coordinador de Grupo de Seguridad de la Información de la Entidad, pruebas y evidencias para analizar los ítems tanto de las pruebas administrativas como de las pruebas técnicas a validar de acuerdo con los objetivos del presente proyecto.

De acuerdo con el resultado del diagnóstico de los ítems validados, se puede evidenciar que la Entidad se encuentra en un 20% de madurez frente al cumplimiento con lo establecido en cuanto al MSPI.

Se identificaron algunas brechas de acuerdo con los ítems evaluados:

PRUEBAS ADMINISTRATIVAS

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Evaluación:
Se cuenta con una política general y unas específicas, pero no están alineadas con los objetivos institucionales de la Entidad.

Revisión:
a) La política no define que es Seguridad de la Información.
b) hay algunos roles, pero no se definen específicamente con el compromiso de la Entidad

c) Los procesos para manejar las desviaciones y las excepciones.
Hay un responsable por Seguridad de la Información, quien se encarga de establecer los lineamientos de seguridad
Las políticas existentes no se revisan y actualizan

RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN

Existen algunos roles con las responsabilidades del Coordinador de Grupo Seguridad de la Información, responsabilidades funcionales y operativas y algunas normas de seguridad de la información y de propiedad Información.

Revisión de la estructura del SGSI:
1. No se ve el apoyo de la dirección a través de la ejecución de comités de seguridad.
2. Hay un documento con el rol del jefe de grupo de seguridad y sus miembros, sin embargo, sus funciones están limitadas a TI.
3. La propiedad de la información y Activos asociados con los servicios de procesamiento de información está establecida. El control está reglamentado a través de algunos documentos de Propiedad de la Información y Seguridad Física
4. No hay definidos roles para la Gestión de Riesgos de Seguridad de la Información.
5. Hay una matriz de roles y perfiles, dentro de la cual se definen privilegios de acceso a la plataforma tecnológica de TI.
6. Se asignó presupuesto para contratar una consultoría para diseñar el SGSI - MSPI de la Entidad.

Existe un rol para administrar la seguridad, que se encarga de gestionar los accesos y temas de seguridad para este ítem.
Existe una regla (norma) para administración, a través del cual se definen las directrices para el control de acceso de los funcionarios y contratistas a los sistemas de información y a los componentes tecnológicos, pero no están alineadas con los objetivos instituciones de la Entidad.

No hay una matriz de contacto con autoridades formalizada y documentada por parte del Grupo de Seguridad de la Información.

El responsable de Seguridad de la Información participa en:
- Comité de líderes de infraestructuras críticas de Colombia.
Así mismo, también se promueve la asistencia a eventos y foros especializados en Seguridad de la Información.

a) Para proyectos tecnológicos, en los pliegos de condiciones incluyen compromisos y requisitos de Seguridad de la Información.

Para otros proyectos que no involucran componentes tecnológicos, no se tienen en cuenta requerimientos de Seguridad de la Información, sin embargo, con el nuevo Manual de contratación, se busca alinear el proceso de contratación con la herramienta del estado SECOP II.
b) Hay una matriz de riesgos estándar para los proyectos, la cual incluye Seguridad de la Información. Sin embargo, estos riegos son incluidos de acuerdo con el criterio del responsable del proyecto.
c) No hay un lineamiento que indique que Seguridad de la Información sea parte de todas las fases del proyecto.

GESTIÓN DE ACTIVOS:

Inventario de Activos

Se cuenta con un inventario de Activos de infraestructura tecnológica informática no aprobado por la alta dirección administrado por el Coordinador de Mesa de Servicios.

No hay un inventario de Activos de Información dentro de la Entidad.
Actualmente está en proceso de construcción.

Propiedad de los Activos:

Se cuenta con un inventario de Activos de infraestructura tecnológica informática no aprobado por la alta dirección administrado por la Coordinación de Mesa de Servicios.

Dentro del Grupo Seguridad de la Información hay lineamientos donde se define la propiedad de los Activos de Información; sin embargo, no hay un procedimiento de gestión de Activos de Información y riesgos de seguridad.

Dentro de las directrices de Seguridad de la Información de responsabilidad de los usuarios se menciona que es responsabilidad de los usuarios de componentes tecnológicos de la UAEAC: Garantizar la integridad, disponibilidad y confidencialidad de la información asignada para el cumplimiento de sus funciones, hacer uso adecuado de la información de propiedad de la UAEAC, administrar la información a su cargo, utilizar correctamente las contraseñas, mantener la confidencialidad de las contraseñas y velar por el adecuado almacenamiento de la información.

El proceso de desvinculación incluye diligenciar el formato de VISADO INVENTARIAL que incluye el visto bueno del jefe inmediato, Talento Humano, Carnetización, Almacén y Archivo.

Para el caso de retiro de accesos se solicita a través de un oficio al funcionario o contratistas solicitar al Grupo de Seguridad de la Información el retiro de sus permisos de acceso.

No hay un procedimiento que permita definir cómo clasificar la información de acuerdo con su nivel de sensibilidad.

No hay un procedimiento que indique como etiquetar y tratar la información de acuerdo con su nivel de sensibilidad.

Recomendaciones:

- Documentar e implementar un procedimiento de etiquetado y tratamiento de la información.
- Documentar e implementar un procedimiento de clasificación de la información.

PRUEBAS TECNICAS

REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO

CONTROL DE ACCESO

Se cuenta con unas políticas específicas y algunas reglas o normas, pero no están alineadas con los objetivos institucionales de la Entidad, algunas de estas son:

- Política de Acceso a la Información.
- Norma de responsabilidad de los usuarios
- Norma de administración de cuentas de usuario
- Norma para la administración de accesos a componentes tecnológicos.

Documentos de TI:
Existe un formato "GINF-6.0-06-017 Formato de solicitud de acceso a componentes tecnológicos.

Política de control de acceso
Revisar:
a) En la política de Acceso a la información define que: Todos los funcionarios que laboran para la UAEAC deben tener acceso únicamente a la información necesaria para el desempeño de sus funciones.
b) En la Norma de responsabilidad de usuarios define que: Todos los usuarios de la UAEAC son responsables del manejo adecuado de la

información y se comprometen a respetar su carácter de confidencialidad, integridad y disponibilidad.
c) En la Norma administración de cuentas de usuario se define que: El acceso a la información debe ser autorizado por el área responsable de la información de acuerdo con las funciones a desempeñar, previo análisis de la justificación y manteniendo una adecuada segregación de funciones.
d) No se identifica.
e) En la norma acceso a internet, se definen los perfiles de acceso a internet.
f) En la norma de administración de accesos a componentes tecnológicos, se define que la autorización es para la creación, eliminación, modificación o inactivación de perfiles de acceso es responsabilidad directa del área responsable de la información y será aprobada por el Grupo Seguridad Informática.
g) En el formato GINF-6.0-12-001 SOLICITUD DE ACCESO A COMPONENTES TECNOLOGICOS, se relacionan los requisitos para la solicitud de acceso a componentes tecnológicos.
h) El Grupo Seguridad Informática, los Administradores de Seguridad de los Sistemas de Información y Aplicativos, los Administradores del Componente Tecnológico, la Oficina de Control Interno y los responsables de la Información serán responsables de velar por que los perfiles de acceso existentes se encuentren acordes con las funciones realizadas por cada uno de los usuarios.
i) Norma de autorización para la creación, bloqueo, eliminación, modificación o inactivación de perfiles de acceso es responsabilidad directa del área responsable de la información y será aprobada por el Grupo Seguridad Informática.
j) Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios con el objeto de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información.
k) Las personas que por sus funciones requieran un perfil de usuario privilegiado deben solicitarlo siguiendo el procedimiento establecido para administración de usuarios privilegiados de los componentes tecnológicos: GINF-6.0-06-022 Control de Acceso a Usuarios Privilegiados y GINF 4.0-12-09 SOLICITUD DE ACCESO A USUARIOS PRIVILEGIADOS.

Acceso a redes y a servicios en red
a) Existe una regla de Acceso Internet.
b) El responsable del proceso, solicita al Grupo de Seguridad de la Información los accesos a través del formato GINF-6.0-12-001 Solicitud de acceso a componentes tecnológicos.
c) Existe una regla de Acceso Internet
d) Existe el estándar de configuración seguridad de red inalámbrica y acceso remoto vía VPN.

Recomendación: Diseñar una metodología de Gestión de Activos y elaborar el inventario de Activos de Información de los procesos definidos dentro del alcance del Sistema de Gestión de Seguridad de la Información.

Este instrumento permite a la entidad generar un plan de seguridad de la información poder desarrollarlo en su interior y poder dar cumplimiento a lo establecido por MinTic.

ENTIDAD EVALUADA	**Unidad Administrativa Especial de Aeronáutica Civil de Colombia**									
FECHAS DE EVALUACIÓN	15 de abril de 2020									
CONTACTO	Nicolás Ortiz Espitia									
ELABORADO POR	Sixta Alexandra Quiroga Castillo									
ADMINISTRATIVAS										
ID. ITEM	CARGO	ITEM	DESCRIPCION	ISO	MSPI	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001 N/A 20 40 60 80 100	RECOMENDACIÓN
POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN										
AD.1	**Responsable de SI**	**POLITICAS DE SEGURIDAD DE LA INFORMACIÓN**	**Orientación de la dirección para gestión de la seguridad de la información**	**A.5**	**Componente planificación y modelo de madurez nivel gestionado**					

AD.1.1	Responsable del SI	Documento de la política de seguridad y privacidad de la Información	Se debe definir un conjunto de políticas para la seguridad de la información aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes	A.5.1.1	Componente planificación y modelo de madurez inicial	Solicite la política de seguridad de la información de la entidad y evalúe: a) Si se definen los objetivos, alcance de la política b) Si esta se encuentra alineada con la estrategia y objetivos de la entidad c) Si fue	Políticas del SGSI - "Política General de Seguridad de la Información".	Evaluación: Se cuenta con una política general y unas específicas, pero no están alineadas con los objetivos institucionales de la Entidad Revisió	20	

AD.1.2	Responsable de SI	Revisión y evaluación	Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.	A.5.1.2	componente planificación	debidamente aprobada y socializada al interior de la entidad por la alta dirección Revise si la política: a)Define que es seguridad de la información b) La asignación de las responsabilidades generales y específicas para la gestión de la seguridad de la información, a roles definidos; c) Los procesos para manejar		n: a) La política no define que es Seguridad de la Información. b) hay algunos roles pero no se definen específicamente con el compromiso de la Entidad c) Los procesos para manejar las desviaciones y las excepciones. Hay un responsable por Seguridad de la		

						las desviaciones y las excepciones. Indague sobre los responsables designados formalmente por la dirección para desarrollar, actualizar y revisar las políticas. Verifique cada cuanto o bajo qué circunstancias se revisan y actualizan, verifique la última fecha de emisión de la política frente a la fecha actual y que cambios a		Información, quien se encarga de establecer los lineamientos de seguridad Las políticas existentes no se revisan y actualizan		

						sufrido, por lo menos debe haber una revisión anual. **Para la calificación tenga en cuenta que:** 1) Si se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información, están en 20. 2) Si se revisan y se aprueban las				

						políticas de seguridad y privacidad de la información, están en 40. 3) Si se divulgan las políticas de seguridad y privacidad de la información, están en 60.				
RESPONSABILIDADES Y ORGANIZACIÓN SEGURIDAD INFORMACIÓN										

A2	**Responsable de SI**	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**	**Marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización Garantizar la seguridad del teletrabajo y el uso de los dispositivos móviles**	**A.6**						
AD.2.1	**Responsable de SI**	**Organización Interna**	**Marco de referencia de gestión para iniciar y controlar la**	**A.6.1**	**Componente planificación y modelo de madur**					

			implementación y la operación de la seguridad de la información dentro de la organización		**ez gestionado**					
AD.2.1.1	Responsable de SI	Roles y responsabilidades para la seguridad de la información	Se deben definir y asignar todas las responsabilidades de la seguridad de la información	A.6.1.1	Componente planificación	Revise la estructura del SGSI: 1) Tiene el SGSI suficiente apoyo de la alta dirección?, esto se ve reflejado en comités donde se discutan temas como la política de SI, los riesgos o incidentes. 2) Están claramente definidos los roles y responsabilidades y	Existen algunos roles con las responsabilidades del Coordinador de Grupo Seguridad de la Información, responsabilidades funcionales y operativas y algunas normas de Seguridad de la informaci	Revisión de la estructura del SGSI: 1. No se ve el apoyo de la dirección a través de la ejecución de comités de seguridad. 2. Hay un documento con el rol del jefe de	20	

						asignados a personal con las competencias requeridas?, 3) Están identificadas los responsables y responsabilidades para la protección de los activos? (Una práctica común es nombrar un propietario para cada activo, quien entonces se convierte en el responsable de su protección) 4) Están definidas las	ón y de propiedad Información.	grupo de seguridad y sus miembros, sin embargo sus funciones están limitadas a TI. 3. La propiedad de la información y Activos asociados con los servicios de procesamiento de información está establecida. El control está reglamentado a través de		

						responsabilidades para la gestión del riesgo de SI y la aceptación de los riesgos residuales? 5) Están definidos y documentados los niveles de autorización? 6) Se cuenta con un presupuesto formalmente asignado a las actividades del SGSI (por ejemplo, campañas de sensibilización en seguridad de la		algunos documentos de Propiedad de la Información y Seguridad Física 4. No hay definidos roles para la Gestión de Riesgos de Seguridad de la Información. 5. Hay una matriz de roles y perfiles, dentro de la cual se definen privilegios de acceso a la platafor		

						información)		ma tecnológica de TI. 6. Se asignó presupuesto para contratar una consultoría para diseñar el SGS - MSPI de la Entidad.		
AD.2.1.2	Responsable de SI	Separación de deberes / tareas		A.6.1.2		Indague como evitan que una persona pueda acceder, modificar o usar activos sin autorización ni detección. La mejor práctica dicta que el inicio de un evento	Norma: Administración accesos a componentes Tecnológicos Rol: Administrador de seguridad	Existe un rol para administrar la seguridad, que se encarga de gestionar los accesos y temas de seguridad para	20	

						deber estar separado de su autorización. Al diseñar los controles se debería considerar la posibilidad de confabulación. Tenga en cuenta que para las organizaciones pequeñas la separación de deberes puede ser difícil de lograr, en estos casos se deben considerar controles compensatorios como revisión periódica de, los		este ítem. Existe una regla (norma) para administración, a través del cual se definen las directrices para el control de acceso de los funcionarios y contratistas a los sistemas de información y a los componentes tecnológicos. pero no están alinead		

						rastros de auditoría y la supervisión de cargos superiores.		as con los objetivos institucionales de la Entidad.		
AD.2.1.3	Responsable de SI	Contacto con las autoridades.	Las organizaciones deben tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debe contactar a las autoridades (por ejemplo, las encargadas de hacer cumplir la ley, los organismos de reglamentación y las	A.6.1.3		Solicite los procedimientos establecidos que especifiquen cuándo y a través de que autoridades se debería contactar a las autoridades, verifique si de acuerdo a estos procedimientos se han reportado eventos o incidentes de SI de forma consistente.	No se encontró evidencia.	No hay una matriz de contacto con autoridades formalizada y documentada por parte del Grupo de Seguridad de la Información.	20	

			autoridades de supervisión), y cómo se debe reportar de una manera oportuna los incidentes de seguridad de la información identificados (por ejemplo, si se sospecha una violación de la ley).							
AD.2.1.4	Responsable de SI	Contacto con grupos de interés especiales	Se deben mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales	A.6.1.4		Pregunte sobre las membrecías en grupos o foros de interés especial en seguridad de la información en los que se	Correos de invitación al coordinador de seguridad de la información a eventos de seguridad.	El responsable de Seguridad de la Información participa en:- Comité de líderes de infraest	20	

			especializadas en seguridad. Por ejemplo, a través de una membresía			encuentran inscritos las personas responsables de la SI.		ructuras críticas de Colombia.Así mismo, también se promueve la asistencia a eventos y foros especializados en Seguridad de la Información.		
AD.2.1.5	Responsable de SI	Seguridad de la información en la gestión de proyectos	La seguridad de la información se debe integrar al(los) método(s) de gestión de proyectos de la organización, para asegurar que los	A.6.1.5		Pregunte como la Entidad integra la seguridad de la información en el ciclo de vida de los proyectos para asegurar que para asegurar	Existen un Acuerdo de Confidencialidad para contratos alianzas o convenios con terceros. Documentos de	a) Para proyectos tecnológicos, en los pliegos de condiciones incluyen compromisos y requisitos de	20	

			riesgos de seguridad de la información se identifiquen y traten como parte de un proyecto. Esto se aplica generalmente a cualquier proyecto, independientemente de su naturaleza, por ejemplo, un proyecto para un proceso del negocio principal, TI, gestión de instalaciones y otros procesos de soporte.			que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto. Tenga en cuenta que esto no solamente aplica para proyectos de TI, por ejemplo, puede aplicar en proyectos de traslado de activos de información, gestión de instalaciones, personal en outsourcing que soporta procesos de la organizaci	otros procesos: - Manual de contratación.	Seguridad de la Información. Para otros proyectos que no involucran componentes tecnológicos, no se tienen en cuenta requerimientos de Seguridad de la Información, sin embargo, con el nuevo Manual de contratación, se busca alinear		

						ón. Las mejores prácticas sugieren: a) Que los objetivos de la seguridad de la información se incluyan en los objetivos del proyecto; b) Que la valoración de los riesgos de seguridad de la información se lleve a cabo en una etapa temprana del proyecto, para identificar los controles necesarios; c) Que la seguridad		el proceso de contratación con la herramienta del estado SECOP II. b) Hay una matriz de riesgos estándar para los proyectos, la cual incluye Seguridad de la Información. Sin embargo, estos riegos son incluidos de acuerdo con el criterio del		

						de la información sea parte de todas las fases de la metodología del proyecto aplicada.		responsable del proyecto. c) No hay un lineamiento que indique que Seguridad de la Información sea parte de todas las fases del proyecto.		
GESTIÓN DE ACTIVOS										
AD.4	**Responsable de SI**	**GESTIÓN DE Activos**		**A.8**						
AD.4.1	**Responsable de SI**	**Responsabilidad de los Activos**	**Identificar los Activos organizacionales y definir las responsabilidades de protecció**	**A.8.1**	**Modelo de Madurez Gestionado**					

			n apropiadas.							
AD.4.1.1	Responsable de SI	Inventario de Activos	Se deben identificar los Activos asociados con la información y las instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos Activos.	A.8.1.1	Componente Planificación Modelo de madurez inicial	Solicite el inventario de Activos de Información, revisado y aprobado por la alta Dirección y revise: 1) Ultima vez que se actualizó 2) Que señale bajo algún criterio la importancia del activo 3) Que señale el propietario del activo Indague quien(es) el(los) encargado(s) de actualizar y revisar el inventario de Activos y cada cuanto se	Se cuenta con un inventario de Activos de infraestructura tecnológica informática no aprobado por la alta dirección administrado por el Coordinador de Mesa de Servicios.	No hay un inventario de Activos de Información dentro de la Entidad. Actualmente está en proceso de construcción. Se cuenta con un inventario de Activos de infraestructura tecnológica informática no aprobado por	20	Diseñar una metodología de Gestión de Activos y elaborar el inventario de Activos de Información de los procesos definidos dentro del alcance del Sistema de Gestión de Seguridad de la Información.

						realiza esta revisión. Tenga en cuenta para la calificación: 1) Si Se identifican en forma general los Activos de Información de la Entidad, están en 40. 2) Si se cuenta con un inventario de Activos de Información física y lógica de toda la Entidad, documentado y firmado por la alta dirección, están en 60. 3) Si se revisa y		la alta dirección administrado por la Coordinación de Mesa de Servicios.		

						monitorean periódicamente los Activos de Información de la Entidad, están en 80.				
AD.4.1.2	Responsable de SI	Propiedad de los Activos	Los Activos mantenidos en el inventario deben tener un propietario.	A.8.1.2		Solicite el procedimiento para asegurar la asignación oportuna de la propiedad de los Activos. Tenga en cuenta que la propiedad se debería asignar cuando los Activos se crean o cuando son entregados a la Entidad.De acuerdo		Dentro del Grupo Seguridad de la Información hay lineamientos donde se define la propiedad de los Activos de Información; sin embargo, no hay un procedi	20	

						a las mejores prácticas el propietario de los Activos (individuo o Entidad, que es responsable por el activo) tiene las siguientes responsabilidades:a) asegurarse de que los Activos están inventariados; b) asegurarse de que los Activos están clasificados y protegidos apropiadamente; c) definir y revisar periódicamente las restricciones y		miento de gestión de Activos de Información y riesgos de seguridad.		

						clasificaciones de acceso a Activos importantes, teniendo en cuenta las políticas de control de acceso aplicables; d) asegurarse del manejo apropiado del activo cuando es eliminado o destruido.				
AD.4.1.3	Responsable de SI	Uso aceptable de los Activos	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de Activos asociados con información e	A.8.1.3		Pregunte por la política, procedimiento, directriz o lineamiento que defina el uso aceptable de los Activos, verifique que es conocida		Dentro de las directrices de Seguridad de la Información de responsabilidad de los usuarios se menciona que es	20	

			instalaciones de procesamiento de información.			por los empleados y usuarios de partes externas que usan Activos de la Entidad o tienen acceso a ellos.		responsabilidad de los usuarios de componentes tecnológicos de la UAEAC: Garantizar la integridad, disponibilidad y confidencialidad de la información asignada para el cumplimiento de sus funciones, Hacer uso adecuado de la información de		

								propiedad de la UAEAC, administrar la información a su cargo, utilizar correctamente las contraseñas, mantener la confidencialidad de las contraseñas y velar por el adecuado almacenamiento de la información.		

AD.4.1.4	Responsable de SI	Devolución de Activos	Todos los empleados y usuarios de partes externas deben devolver todos los Activos de la Entidad que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	A.8.1.4		Revisar las políticas, normas, procedimientos y directrices relativas a los controles de Seguridad de la Información durante la terminación de la relación laboral, por ejemplo, la devolución de los Activos de Información (equipos, llaves, documentos, datos, sistemas), las llaves físicas y de cifrado, la eliminación de los derechos de acceso, etc. En		El proceso de desvinculación incluye diligenciar el formato de VISADO INVENTARIAL que incluye el visto bueno del jefe inmediato, Talento Humano, Carnetización, Almacén y Archivo. Para el caso de retiro de accesos se solicita	20	Realizar actividades de monitoreo del cumplimiento del reporte oportuno de retiros por parte de funcionarios.

						caso de que un funcionario o tercero sea el dueño del activo indague como se asegura la transferencia de la información a la Entidad y el borrado seguro de la información de la Entidad. En caso en que un empleado o usuario de una parte externa posea conocimientos que son importantes para las operaciones regulares, esa		a través de un oficio al funcionario o contratistas solicitar al Grupo de Seguridad de la Información el retiro de sus permisos de acceso		

						información se debería documentar y transferir a la Entidad. Durante el período de notificación de la terminación, la Entidad debería controlar el copiado no autorizado de la información pertinente (por ejemplo, la propiedad intelectual) por parte de los empleados o contratistas que han finalizado el empleo.				

AD.4.2	**Responsable de SI**	**Clasificación de información**	**Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la Entidad.**	**A.8.2**						
AD.4.2.1	Responsable de SI	Clasificación de la información	La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	A.8.2.1	Modelo de Madurez Inicial	Solicite el procedimiento mediante el cual se clasifican los Activos de Información y evalué: 1) Que las convenciones y criterios de clasificación sean claros y estén documentados 2) Que se defina cada cuanto	No se encontró evidencia.	No hay un procedimiento que permita definir cómo clasificar la información de acuerdo con su nivel de sensibilidad.	20	Documentar e implementar un procedimiento de clasificación de la información.

						debe revisarse la clasificación de un activo 3) La clasificación debería valorarse analizando la confidencialidad, integridad y disponibilidad. Solicite muestras de inventarios de Activos de Información clasificados y evalué que se aplican las políticas y procedimientos de clasificación definidos. Evalué si				

						los procesos seleccionados aplican de manera consistente estas políticas y procedimientos.				
AD.4.2.2	Responsable de SI	Etiquetado de la información		A.8.2.2		Solicite el procedimiento para el etiquetado de la información y evalúe: 1) Aplica a Activos en formatos físicos y electrónicos (etiquetas físicas, metadatos) 2) Que refleje el esquema de clasificación establecido 3) Que las etiquetas	No se encontró evidencia.	No hay un procedimiento que indique como etiquetar y tratar la información de acuerdo con su nivel de sensibilidad.	20	Documentar e implementar un procedimiento de etiquetado y tratamiento de la información.

						se puedan reconocer fácilmente 4) Que los empleados y contratistas conocen el procedimiento de etiquetado Revise en una muestra de Activos el correcto etiquetado				
AD.4.2.3	Responsable de SI	Manejo de Activos		A.8.2.3		Solicite los procedimientos para el manejo, procesamiento, almacenamiento y comunicación de información de conformidad con su clasificación. De acuerdo a las mejores	No se encontró evidencia.	No hay un procedimiento que indique como etiquetar y tratar la información de acuerdo con su nivel de sensibilidad.	20	Documentar e implementar un procedimiento de etiquetado y tratamiento de la información.

						prácticas evidencie si se han considerado los siguientes asuntos: a) Restricciones de acceso que soportan los requisitos de protección para cada nivel de clasificación; b) Registro formal de los receptores autorizados de los Activos; c) Protección de copias de información temporal o permanente a un nivel coherente				

						con la protección de la información original; d) Almacenamiento de los Activos de TI de acuerdo con las especificaciones de los fabricantes; e) Marcado claro de todas las copias de medios para la atención del receptor autorizado.				
TECNICAS										
ID. ITEM	CARGO	ITEM	DESCRIPCION	ISO	MSPI	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	
CONTROL DE ACCESO										

T.1.1	Responsable de SI	REQUISITOS DEL NEGOCIO PARA CONTROL DE ACCESO	Se debe limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1	Modelo de madurez definido					
T.1.1.1	Responsable de SI	Política de control de acceso	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de Seguridad de la Información.	A.9.1.1		Revisar que la política contenga lo siguiente: a) los requisitos de seguridad para las aplicaciones del negocio; b) las políticas para la divulgación y autorización de la información, y los niveles de Seguridad de la Informació	Se cuenta con unas políticas específicas y algunas reglas o normas, pero no están alineadas con los objetivos institucionales de la Entidad Política de Acceso a la Informaci ón. Norma de responsa	Revisar: a) En la política de Acceso a la información define que: Todos los funcionarios que laboran para la UAEAC deben tener acceso únicamente a la información	40	

						n y de clasificación de la información; c) la coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes; d) la legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios; e) la gestión de los derechos de acceso en un entorno	bilidad de los usuarios Norma de administración de cuentas de usuario Norma para la administración de accesos a componentes tecnológicos. Documentos de TI: -"GINF-6.0-06-017 Formato de solicitud de acceso a componentes tecnológicos.	necesaria para el desempeño de sus funciones. b) En la Norma de responsabilidad de usuarios define que: Todos los usuarios de la UAEAC son responsables del manejo adecuado de la información y se comprometen a respetar su carácte		

						distribuido y en red, que reconoce todos los tipos de conexiones disponibles; f) la separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso); g) los requisitos para la autorización formal de las solicitudes de acceso; h) los requisitos para la revisión periódica de los		r de confidencialidad, integridad y disponibilidad. c) En la Norma administración de cuentas de usuario se define que: El acceso a la información debe ser autorizado por el área responsable de la información de acuerdo con las funciones a		

						derechos de acceso; i) el retiro de los derechos de acceso; j) el ingreso de los registros de todos los eventos significativos concernientes al uso y gestión de identificación de los usuarios, e información de autenticación secreta, en el archivo permanente; k) los roles de acceso privilegiado;		desempeñar, previo análisis de la justificación y manteniendo una adecuada segregación de funciones. d) No se identifica. e) En la norma acceso a internet, se definen los perfiles de acceso a internet. f) En la norma de		

								administración de accesos a componentes tecnológicos, se define que la autorización es para la creación, eliminación, modificación o inactivación de perfiles de accesoes responsabilidad directa del área responsable de la información y será aproba		

								da por el Grupo Seguridad Informática. g) En el formato GINF-6.0-12-001 SOLICITUD DE ACCESO A COMPONENTES TECNOLOGICOS, se relacionan los requisitos para la solicitud de acceso a componentes tecnológicos. h) El Grupo		

								Seguridad Informática, los Administradores de Seguridad de los Sistemas de Información y Aplicativos, los Administradores del Componente Tecnológico, la Oficina de Control Interno y los responsables de la Información serán responsables de velar por que		

								los perfiles de acceso existentes se encuentren acordes con las funciones realizadas por cada uno de los usuarios. i) Norma de autorización para la creación, bloqueo, eliminación, modificación o inactivación de perfiles de acceso		

								es responsabilidad directa del área responsable de la información y será aprobada por el Grupo Seguridad Informática. j) Mediante el registro de eventos en los diversos componentes de la plataforma tecnológica se efectuará un seguimi		

								ento a los accesos realizados por los usuarios con el objeto de minimizar los riesgos de pérdida de integridad, disponibilidad y confidencialidad de la información. k) Las personas que por sus funciones requieran un perfil de usuario privilegi		

								ado deben solicitarlo siguiendo el procedimiento establecido para administración de usuarios privilegiados de los componentes tecnológicos: GINF-6.0-06-022 Control de Acceso a Usuarios Privilegiados y GINF 4.0-12-09 SOLICI		

								TUD DE ACCESO A USUARIOS PRIVILEGIADOS.		
T.1.1.2	Responsable de TICs/ Responsable por SI	Acceso a redes y a servicios en red	Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	A.9.1.2		Revisar la política relacionada con el uso de redes y de servicios de red y verificar que incluya: a) las redes y servicios de red a los que se permite el acceso; b) los procedimie	Se cuenta con unas reglas o normas, pero no están alineadas con los objetivos institucionales de la Entidad. Administración de Cuentas Administración Accesos	a) Existe una regla de Acceso Internet. b) El responsable del proceso, solicita al Grupo de Seguridad de la Información los acceso	20	

						ntos de autorización para determinar a quién se permite el acceso a qué redes y servicios de red; c) los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y a los servicios de red; d) los medios usados para acceder a las redes y servicios de red (uso de VPN o redes inalámbricas); e) los	a Componentes Tecnológicos Acceso Internet". Conexiones Remotas Algunos estándares para contraseñas y parámetros de acceso, acceso remoto Vía VPN y configuración de seguridad de red inalámbrica. Documentos de TI: - "GINF-6.0-06-003 Administración de Red de	s a través del formato GINF-6.0-12-001 Solicitud de acceso a componentes tecnológicos. c) Existe una regla de Acceso Internet d) Existe el estándar de configuración seguridad de red inalámbrica y acceso remoto vía VPN.		

						requisitos de autenticación de usuarios para acceder a diversos servicios de red; f) el seguimiento del uso de servicios de red.	Datos". - "GINF-6.0-06-017 Solicitud de acceso a componentes tecnológicos".			

6.1.2 DISEÑO DEL MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - PROCESO GINF-6.0.

AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL	**MODELO**		
	Título: Seguridad de la Información de la Unidad Administrativa Especial de la Aeronáutica Civil.		
	PRINCIPIOS		
Clave: GINF-6.0-XX-XX	**Versión: XX**	**Fecha: XX/XX/XXXX**	**Pág.: de**

MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – MSPI

Es un conjunto de Principios, Políticas, Normas, Estándares y Roles definidos por la Dirección de Informática y que tiene como objetivo mejorar la Seguridad de la Información y de los Componentes Tecnológicos, buscando hacer el mejor uso de los Recursos Informáticos que nos provee la Entidad.

TABLA DE CONTENIDO

- ✓ **Estándares de Seguridad de la Información**
- ✓ ES-01 Software y Hardware Base en Computadores
- ✓ ES-02 Parámetros de Acceso
- ✓ ES-03 Software Base Servidores
- ✓ ES-04 Configuración de Seguridad Office
- ✓ ES-05 Seguridad Física

- ✓ **Roles y Responsabilidades de Seguridad de la Información**
- ✓ RL-01 Administrador de Seguridad de Usuarios
- ✓ RL-02 Administrador de Componente Tecnológico

6.2 **DESARROLLO DE OBJETIVO 2:** DISEÑAR LA POLÍTICA GENERAL Y LAS ESPECÍFICAS DEL SGSI.

Para el cumplimiento del objetivo número 2 y de acuerdo con los lineamientos de MinTic en la Guía 2 – Política General MSPI v1 y en conjunto con los funcionarios del Grupo de Seguridad de la Información y los Administradores de Componentes Tecnológicos, se revisa la documentación existente y se diseñaron los siguientes documentos en Word:

6.2.1 Diseño de los principios de seguridad de la información.

PRINCIPIOS DE SEGURIDAD DE LA INFORMACIÓN.

La Unidad Administrativa Especial de la Aeronáutica Civil, se encuentra alineada con el Gobierno Nacional en la protección de la Información, basándose en la gestión de riesgos sobre los Activos de Información, para garantizar su Integridad, Disponibilidad, Confidencialidad y Exactitud. La Información es un activo muy importante para la UAEAC y por lo tanto requiere una protección adecuada de acuerdo con los objetivos estratégicos; para ello encamina su esfuerzo con base en

los Principios de Seguridad de la Información, garantizando la continuidad de las actividades y minimizando los riesgos.

6.2.2 Diseño de la Política General del SGSI.

Las Políticas del Modelo de Seguridad y Privacidad de la Información han sido definidas para establecer el comportamiento que debe tener cada uno de los Servidores Públicos, Responsables de la información y Usuarios de Activos de Información, así como los Contratistas, Terceros, Estudiantes en Pasantía, Funcionarios de entidades de control, Delegados de convenios nacionales e internacionales y asociados de la UAEAC, sin excepción, en el manejo de la información y de los componentes tecnológicos de la Entidad, a través de las directrices expresadas por la Dirección General.

PO-00 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

La Unidad Administrativa Especial de Aeronáutica Civil se compromete a: Gestionar eficazmente la seguridad de la información, orientando sus esfuerzos en pro de garantizar su Integridad, Confidencialidad y Disponibilidad, contribuyendo al cumplimiento de los objetivos institucionales, en un entorno de mejora continua.

Asegurar que la información sea accesible a las personas debidamente autorizadas, que se conserve salvaguardando su precisión e integridad y esté disponible en el momento y en el formato que se requiera.

Cumplir con los requerimientos legales, reglamentarios y contractuales establecidos con respecto a la seguridad y privacidad de la información, orientados a gestionar y reducir los riesgos a un nivel aceptable, con una operación transparente que proteja los intereses del país.

Establecer los requisitos de seguridad de la información, mediante un conjunto de principios y reglas que indiquen como se gestionará la protección de los activos de información de manera consistente y efectiva, así como los mecanismos necesarios para evaluar y tratar los riesgos de acuerdo con la metodología de gestión de riesgos establecida.

6.2.3 Diseño de cinco políticas específicas.

PO-01 ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

La función de administración de la seguridad de la información es definir, establecer, divulgar, monitorear y verificar la aplicación de los lineamientos necesarios para garantizar la Integridad, Disponibilidad, Confidencialidad y Exactitud de la Información en la UAEAC.
La Alta Dirección debe apoyar activamente cada una de las actividades relacionadas con la seguridad de la información definiendo directrices, asignando responsabilidades y estableciendo compromisos para su implementación dentro de la UAEAC.

La Dirección General debe revisar y aprobar periódicamente la Política de Seguridad y Privacidad de la Información. El Grupo Seguridad de la Información se encargará de la revisión y actualización del Modelo de Gestión de Seguridad de la Información - MSPI de la UAEAC. El Grupo Seguridad de la Información debe participar en la definición de los controles requeridos en los componentes tecnológicos de la UAEAC con base en los riesgos identificados. Los jefes de Oficina, Secretarios, Directores de Área y Coordinadores de Grupo deben asegurar que la normatividad establecida en el Modelo de Gestión de Seguridad de la Información – MSPI se aplica correctamente dentro del área de su responsabilidad.

PO-02 ACCESO A LA INFORMACIÓN.

Los servidores públicos que laboran para la UAEAC deben tener acceso únicamente a la información necesaria para el desempeño de sus funciones. El acceso a la información debe ser autorizado por el área responsable de la información de acuerdo con las funciones a desempeñar, previo análisis de la justificación y manteniendo una adecuada segregación de funciones. En el caso de personal ajeno a la UAEAC el área responsable de la información debe autorizar el acceso a la misma atendiendo la clasificación de la información y las normas y procedimientos definidos para tal fin. Mediante el registro de eventos en los diversos componentes tecnológicos se efectuará un seguimiento a los accesos realizados por los usuarios, con el objeto de minimizar los riesgos de pérdida de Integridad, Disponibilidad, Confidencialidad y Exactitud de la información. Cuando se presenten eventos que pongan en riesgo la Integridad, Disponibilidad, Confidencialidad y Exactitud de la información se deberán documentar y realizar las acciones tendientes a mitigar el riesgo.

La UAEAC proporciona a sus servidores públicos los componentes tecnológicos necesarios para facilitar el desempeño de sus funciones, por tal motivo se permite

el acceso a la red de datos solo a los dispositivos autorizados formalmente por el Grupo Seguridad de la Información.

PO-3 PROPIEDAD DE LA INFORMACIÓN.

La información procesada y almacenada en los componentes tecnológicos de la UAEAC, pertenece a la Entidad a menos que en una ley o relación contractual se establezca lo contrario, sin embargo, la facultad de otorgar el acceso a la información es del responsable del área que la genera, a nivel de Coordinador de Oficina, Secretario o Director. La propiedad de la información no va en contra del carácter público de la misma, esto significa, que la información generada por la UAEAC debe estar disponible en el evento que sea requerida por personal interno o externo a la Entidad cuya solicitud atienda al proceso formal de solicitud de la información.

Para efectos de control del flujo de la información de los procesos de la Entidad, se deben asignar responsables, quienes deben asegurar y otorgar acceso a la información que genere su área, con el fin de lograr un adecuado ambiente de control y un buen nivel de segregación de funciones. En caso de uso indebido o divulgación no autorizada de la información en la UAEAC se deben aplicar los procedimientos establecidos por la Ley a través de los entes de control correspondientes.

PO-04 PROCESAMIENTO DE LA INFORMACIÓN.

El procesamiento de la información que se realice en los componentes tecnológicos de la UAEAC debe cumplir con lo establecido en materia de seguridad de la información de la UAEAC, con el fin de garantizar la Integridad, Disponibilidad, Confidencialidad y Exactitud de esta. En caso de ocurrencia de eventos que pongan en riesgo la disponibilidad de la información y con el fin de garantizar la continuidad de los servicios informáticos de la UAEAC, deben existir Planes de Contingencia que permitan recuperar el procesamiento de la información en los tiempos establecidos por la UAEAC, garantizando el menor impacto para la Entidad. En el Plan de Contingencia se deben considerar aspectos técnicos y administrativos, así como vínculos con instituciones externas.

Los Planes de Contingencia se deben revisar, probar y actualizar periódicamente y estar articulados en toda la Entidad. En el procesamiento de la información debe tenerse en cuenta la transmisión de esta de manera segura, sin interrupciones y libre de interceptaciones, garantizando su integridad y confidencialidad.

La información procesada en los componentes tecnológicos de la UAEAC debe estar debidamente almacenada, organizada y contar con políticas apropiadas de respaldo y recuperación. En las áreas donde se realice procesamiento de información debe contar con las condiciones de seguridad física y ambiental

apropiadas, disponer de sistemas de control y extinción de incendios, mecanismos de respaldo de energía eléctrica y aire acondicionado, y deben realizarse pruebas periódicas para certificar su funcionalidad y disponibilidad. Se deben establecer controles y mecanismos para asegurar que únicamente personal autorizado ingrese a las áreas donde se realiza el procesamiento de información.

PO-05 ALMACENAMIENTO Y RESPALDO DE LA INFORMACIÓN.

La información soportada en los componentes tecnológicos de la UAEAC debe ser almacenada y respaldada de acuerdo con la normatividad emitida por la Dirección de Informática, de tal forma que se garantice su Integridad, Disponibilidad y Confidencialidad.

La Dirección de Informática debe garantizar la existencia de una estrategia formal para la generación, retención y rotación de copias de respaldo de la información soportada en los componentes tecnológicos de la UAEAC. El almacenamiento de los medios magnéticos de respaldo deber realizarse dentro y fuera de las instalaciones de la Entidad, en condiciones ambientales que garanticen su preservación y de acuerdo con el grado de criticidad de la información y su importancia para la operación de la UAEAC, con el fin de garantizar su disponibilidad en caso de pérdida, alteración, daño o desastre. El área responsable de la información debe definir juntamente con el Grupo Seguridad de la Información y la Dirección de Informática, la estrategia a seguir para el respaldo y recuperación de la misma.

6.2.4 Diseño de cinco normas de seguridad de la información.

Las Normas del Modelo de Seguridad y Privacidad de la Información, han sido definidas con el propósito de orientar a cada uno de los Servidores Públicos, Responsables de la Información y Usuarios de Activos de Información, así como Contratistas, Terceros, Estudiantes en pasantía, funcionarios de Entidades de Control, delegados de convenios nacionales e internacionales y asociados de la UAEAC, sin excepción; en los lineamientos que debe cumplir para mantener un ambiente tecnológico seguro.

NO-01 FUNCIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

Normatividad Relacionada.

PO-01 Administración de la Seguridad de la Información

Objetivo

Establecer la función de administración de la Seguridad de la Información de la UAEAC.

Alcance

Esta norma aplica a la Dirección General de la UAEAC.

Descripción

- Debe existir un área responsable de la administración de la seguridad de la información la cual debe asegurar la integridad, disponibilidad, confidencialidad y exactitud de la información de la UAEAC y velar por el cumplimiento de las Políticas, Normas, Estándares y Roles del Modelo de Seguridad de la Información.
- El área responsable de Seguridad de la Información debe controlar el uso de los recursos informáticos asignados a los usuarios para el cumplimiento de las funciones.
- El área responsable de Seguridad de la Información debe participar en los procesos de evaluación de soluciones tecnológicas de hardware, software, Sistemas de Información y recomendar acciones para mejorar los niveles de Seguridad de la Información.
- Las funciones de administración de la Seguridad de la Información deben comprender como mínimo:
  - ✓ Gestionar las solicitudes de acceso a Componentes Tecnológicos.
  - ✓ Revisar, actualizar y divulgar las Políticas, Normas, Estándares y Roles del Modelo de Seguridad y Privacidad de la Información.
  - ✓ Realizar campañas de concientización en Seguridad de la información.
  - ✓ Monitorear la aplicación y cumplimiento de la normatividad establecida en el Modelo de Seguridad de la Información.
  - ✓ Aplicar acciones preventivas y correctivas para controlar el uso no autorizado de los recursos informáticos asignados a los usuarios, incluyendo la suspensión temporal del servicio cuyo uso no se ajuste a las funciones asignadas.
  - ✓ Definir los privilegios de los usuarios que realicen labores de administración y operación sobre los diferentes componentes tecnológicos de acuerdo con los roles establecidos.
  - ✓ Atender los incidentes de Seguridad de la Información.

- ✓ Generar recomendaciones para incrementar los niveles de seguridad de la información en los diferentes procesos.
- ✓ Verificar que la información que contiene Datos Personales es identificada, inventariada y tratada acorde a la política de protección de datos personales.

- La UAEAC definirá las directrices necesarias para las actividades de teletrabajo de acuerdo con las necesidades de la Entidad sin vulnerar los niveles de Seguridad de la Información.

NO-02 ADMINISTRACIÓN DE ACCESOS A COMPONENTES TECONOLÓGICOS.

Normatividad Relacionada.

PO-02 Administración de Acceso a la Información

Objetivo

Garantizar un adecuado control en la definición y mantenimiento de perfiles y roles de acceso de usuarios a los componentes tecnológicos de la UAEAC.

Alcance

Esta norma aplica a los usuarios de componentes tecnológicos de la UAEAC.

Descripción

- Debe existir un procedimiento formal para la creación, modificación, inactivación y eliminación de accesos a los diferentes componentes tecnológicos existentes en la UAEAC.

- La autorización para la creación, modificación, inactivación o eliminación de perfiles y roles de acceso es responsabilidad del área responsable de la información y será aprobada por el Grupo Seguridad de la Información.

- Toda novedad presentada (ingresos, traslados, vacaciones, licencias, sanciones, suspensiones, ascensos o retiros) con los servidores públicos, contratistas, estudiantes en práctica o terceros de la UAEAC debe ser reportada oportunamente por el jefe Inmediato, Supervisor de Contrato o Asesor de Pasantía al Grupo Seguridad de la Información de los diferentes Componentes Tecnológicos donde tenga accesos con el fin de realizar la respectiva modificación, inactivación o eliminación.

- El Grupo Seguridad de la Información, los Administradores de seguridad de los Sistemas de Información, los Administradores de los Componentes Tecnológicos, la Oficina de Control Interno y los Garantes de la Información

serán responsables de velar por que los perfiles de acceso existentes se encuentren acordes con las funciones realizadas por cada uno de los usuarios.

- El Grupo Seguridad de la Información deberá llevar el registro y control de las solicitudes de accesos de creación, modificación, inactivación, bloqueo y eliminación de accesos de los usuarios a los diferentes componentes tecnológicos.

NO-03 PROPIEDAD DE LA INFORMACIÓN.

Normatividad Relacionada.

PO-03 Propiedad de la Información

Objetivo

Establecer cual información almacenada en los componentes tecnológicos de la UAEAC es propiedad de la Entidad.

Alcance

Esta norma aplica a todos los usuarios de componentes tecnológicos de la UAEAC.

Descripción

- La información generada por y para la UAEAC es propiedad de la UAEAC a menos que una relación contractual aprobada por la Dirección General especifique lo contrario.

- La información existente en los componentes tecnológicos de la UAEAC se considera propiedad de la UAEAC, con excepción de aquella que contenga Datos Personales, que se considera propiedad de su titular.

- Todos los componentes tecnológicos de la UAEAC están sujetos a revisiones periódicas por parte de Auditoría Informática o por los servidores públicos que la UAEAC delegue para dicho fin.

- Es responsabilidad de cada usuario garantizar los derechos de propiedad de la información de la UAEAC.

- Se prohíbe el uso de la información de la UAEAC con propósitos comerciales o personales.

- Ningún tipo de información acerca de la misión de la UAEAC debe ser compartida con externos; solamente se hará cuando las características de la relación con externos lo requieran.

- Los servidores públicos, contratistas o estudiantes en pasantía que desarrollen o creen software o hardware durante su vinculación laboral con la UAEAC deberán ceder a ésta los derechos patrimoniales.

NO-04 ACCESO A ÁREAS DE PROCESAMIENTO Y ALMACENAMIENTO DE INFORMACIÓN.

Normatividad Relacionada.

PO-04 Procesamiento de la Información

Objetivo

Garantizar un adecuado control de acceso a las áreas de procesamiento y almacenamiento de la información de la UAEAC.

Alcance

Esta norma aplica a todos los servidores públicos, contratistas, estudiantes en práctica y visitantes a las instalaciones de procesamiento y almacenamiento de la información de la UAEAC.

Descripción

- Se consideran áreas de procesamiento el centro de cómputo y los lugares donde se encuentren alojados los siguientes elementos:

    - ✓ Servidores
    - ✓ Centros de cableado
    - ✓ UPS
    - ✓ Componentes de red
    - ✓ Equipos de comunicaciones
    - ✓ Equipos de almacenamiento de información

- Se consideran áreas de almacenamiento de información las cintotecas y las instalaciones donde se encuentren alojados:

    - ✓ Medios magnéticos
    - ✓ Copias de respaldo
    - ✓ Información histórica

- El acceso físico a las áreas de almacenamiento o procesamiento debe ser controlado mediante dispositivos electrónicos o en su defecto por procedimientos manuales.
- El acceso permanente a las áreas de procesamiento y almacenamiento de la información estará restringido a los servidores públicos autorizados por el responsable del área de procesamiento o almacenamiento de la información.

- El responsable de las áreas de procesamiento y almacenamiento de información debe llevar un formato de control donde se registre la información de las personas autorizadas para ingresar a las áreas de procesamiento y almacenamiento de información. El formato debe contener por lo menos la siguiente información: Nombre de la persona, dependencia, fecha y hora de ingreso y de salida, actividad a realizar, área a la cual tiene acceso autorizado y servidor público quien autoriza.

- El ingreso y salida de personas a las áreas de procesamiento y almacenamiento de información debe ser registrado en el formato establecido para dicho fin.

- Con el fin de garantizar la confidencialidad de la información, los visitantes, contratistas y terceros a la UAEAC no tendrán acceso a los centros de procesamiento y almacenamiento de la información, a menos que sea estrictamente necesario para el cumplimiento de sus funciones.

- Toda persona que no tenga autorización de acceso permanente a las áreas de almacenamiento y procesamiento de información deberá permanecer en compañía de un servidor público autorizado durante su permanencia en las áreas de procesamiento y almacenamiento de información.

- Deben existir mecanismos de monitoreo de las actividades realizadas en las áreas de procesamiento y almacenamiento de información.

- Se deben reportar y documentar los incidentes ocurridos durante la ejecución de labores dentro del centro de cómputo.

- En las áreas de almacenamiento y procesamiento de información debe estar indicado mediante avisos la prohibición de las siguientes acciones:

    - ✓ Fumar
    - ✓ Consumir bebidas o alimentos
    - ✓ Ingresar o almacenar material inflamable o no autorizado.

NO-05 RESPALDO DE LA INFORMACIÓN.

Normatividad Relacionada.

PO-05 Almacenamiento y respaldo de la Información

Objetivo

Garantizar que toda la información almacenada en los componentes tecnológicos de la UAEAC se encuentre debidamente respaldada con el fin de asegurar su disponibilidad, la capacidad de recuperación en caso de desastre y el cumplimiento de los objetivos de la Entidad.

Alcance

Esta norma aplica a los servidores públicos de la UAEAC y específicamente a los responsables de los componentes tecnológicos.

Descripción

- Debe existir una estrategia formal que incluya los procedimientos de generación, retención y rotación de copias de respaldo, así como un esquema de rotulación y vida útil de los medios y de las copias de respaldo.

- Con el objetivo de garantizar la continuidad del negocio, se determina de carácter obligatorio, la ejecución de la estrategia y de los procedimientos relacionados con copias de respaldo para la información almacenada en Componentes Tecnológicos de la UAEAC.

- Debe existir un procedimiento que determine qué información se debe respaldar, las actividades, la periodicidad, el responsable y los mecanismos de almacenamiento de las copias de respaldo de la información almacenada en Componentes Tecnológicos de la UAEAC.

- La realización de las copias de respaldo y su almacenamiento es responsabilidad del Grupo Soporte Informático.

- La responsabilidad de verificar la correcta realización de las copias de respaldo y las pruebas de recuperación y la restauración de la información es del Grupo Soporte Informático.

6.2.5 Diseño de cinco estándares de seguridad de la información.

Los Estándares del Modelo de Seguridad y Privacidad de la Información, han sido definidas por la Dirección de Informática de la UAEAC con el propósito de establecer la configuración que deben tener los Componentes Tecnológicos y Sistemas de Información de la Entidad, la cual debe ser conocida y aplicada por cada uno de los Administradores, Responsables, Líderes Técnicos y Líderes Funcionales para mantener un ambiente tecnológico seguro.

ES-01 SOFTWARE Y HARDWARE BASE EN COMPUTADORES.

Normatividad Relacionada

NO-05 Respaldo de la Información

Objetivos

Establecer el hardware y software básico que deben tener instalados todos los computadores de escritorio y portátiles de propiedad de la UAEAC para garantizar su correcto funcionamiento y configuración.

Componentes Tecnológicos Afectados

Todos los computadores de escritorio y portátiles de la UAEAC.

Descripción

Este estándar establece el hardware y software base que deberán tener instalados todos los computadores de escritorio y portátiles de propiedad de la UAEAC.

Software

Todos los computadores de escritorio y portátiles de propiedad de la UAEAC deben tener instalados los siguientes productos de software:

- Sistema Operativo Windows 7 o superior con soporte para red administrada, dominios e impresión.
- Microsoft Office 365 o Superior.
- Antimalware corporativo con las últimas actualizaciones.
- Agente de Control Remoto corporativo.
- Internet Explorer 10 o versión superior compatible con los Sistemas de Información de la UAEAC.
- Visio Viewer
- Acrobat Reader & Adobe Digital Edition
- Última versión de Java
- Plugins de Macromedia
- Plugins Audio y Video

Cualquier software adicional deberá ser previamente definido y aprobado por la Dirección de Informática.

Hardware

Los componentes de hardware que deben tener instalados todos los computadores de escritorio y portátiles de propiedad de la UAEAC para su correcto funcionamiento y operación son: CPU, monitor, teclado y mouse.

La instalación de hardware adicional debe ser solicitada a la Dirección de Informática y será autorizada siguiendo los procedimientos establecidos para dicho fin.

La configuración del hardware base es definida y administrada por la Dirección de Informática; cualquier modificación debe ser solicitada y previamente autorizada.

ES-02 PARÁMETROS DE ACCESO.

Normatividad Relacionada

NO-02 Administración de accesos a Componentes Tecnológicos

Objetivos

Establecer los patrones básicos de administración de parámetros de acceso de los componentes tecnológicos.

Componentes Tecnológicos Afectados

Todos los componentes tecnológicos de la UAEAC que utilicen parámetros de acceso.

Descripción

Patrones básicos de administración de parámetros de acceso:

- Tiempo de expiración de usuarios sin actividad: 90 días
- Intentos fallidos de conexión: 3 veces
- Eliminación de cuentas inactivas: Si una cuenta de acceso a Red ó VPN no ha sido utilizada por el usuario por más de noventa (90) días, debe eliminarse previa confirmación del Director de Informática y el Coordinador del Grupo Seguridad de la Información.
- Bloqueo de cuentas inactivas: La cuenta de usuario de acceso a los Sistemas de Información que permanezca inactiva por más de noventa (90) días, es decir, no ha sido utilizada por el usuario, debe inactivarse o bloquearse.
- Todas las cuentas de usuario deben pertenecer a un grupo o tener asignado mínimo un (1) rol.
- Las cuentas de usuario, los grupos o los roles innecesarios o que se encuentren en desuso, se eliminaran o inactivaran previa aprobación de la Dirección de Informática y el Coordinador del Grupo Seguridad de la Información.
- Cualquier parámetro requerido e implementado en los Sistemas de Información que permita el acceso a consultar y/o actualizar información del Sistema, debe ser solicitado o reportado aplicando el procedimiento de solicitudes de acceso a componentes tecnológicos y debe ser autorizado por el Coordinador del Grupo de Seguridad de la Información.

ES-03 SOFTWARE BASE SERVIDORES.

Normatividad Relacionada

NO-02 Administración de Accesos a Componentes Tecnológicos.

Objetivos

Establecer los parámetros mínimos de seguridad en la instalación de software que deben cumplir todos los servidores de la UAEAC.

Componentes Tecnológicos Afectados

Todos los servidores de la UAEAC.

Descripción

- Los servidores de la UAEAC deben tener instalados los siguientes productos de software:
  - ✓ Sistema Operativo Windows 2012 Server R2 o Superior (Según la funcionalidad del servidor)
  - ✓ Sistema Operativo Unix - Linux Server (Según la funcionalidad del servidor).
  - ✓ Software de administración y monitoreo propio de cada Sistema Operativo.
- Agente Antimalware corporativo con las últimas Actualizaciones.
- Debe ejecutarse un procedimiento de aseguramiento (hardening) de servidores en el momento de su instalación y cada vez que se realice una actualización de software.
- Los servicios, usuarios, puertos y permisos configurados en el servidor deben estar documentados.

ES-04 CONFIGURACIÓN DE SEGURIDAD OFFICE.

Normatividad Relacionada

NO-02 Administración de accesos a Componentes Tecnológicos

Objetivos

Establecer los patrones básicos de configuración de seguridad para las herramientas de Office 365 en los computadores de escritorio y portátiles de propiedad de la UAEAC, para asegurar que los usuarios hagan uso adecuado, minimizando la pérdida de información.

Componentes Tecnológicos Afectados

Todos los computadores de escritorio y portátiles de propiedad de la UAEAC.

Descripción

- Los componentes de Office 365 que deben tener instalados los equipos cliente, son:
    - ✓ Microsoft Office 365 ProPlus – es-es
    - ✓ Visio Viewer.
- Para cada uno de estos componentes, se deben configurar los siguientes parámetros:
    - ✓ Guardar archivos en segundo plano
    - ✓ Auto-guardar archivos cada 10 minutos
    - ✓ Deshabilitar la ejecución de macros
- Configurar para cada usuario del computador una ruta de almacenamiento por defecto para archivos Office 365, en una partición diferente a la que reside el Sistema Operativo. Ej.:
    - ✓ D:\$[Nombre.Apellido] = D:\$Pedro.Perez
    - ✓ Aplicar permisos de control total para el Usuario y el Administrador, únicamente en la carpeta creada para el usuario.
    - ✓ Direccionar la carpeta Documentos a la Carpeta creada en D:\\, para el usuario.
    - ✓ Verificar que al guardar un documento quede almacenado en la ruta establecida.
    - ✓ Explicar al usuario donde serán almacenados sus documentos.

ES-05 SEGURIDAD FISICA.

Normatividad Relacionada

NO-04 Acceso a áreas de procesamiento y almacenamiento de Información

Objetivos

Establecer los patrones básicos para garantizar la seguridad física de los Componentes Tecnológicos de la UAEAC.

Componentes Tecnológicos Afectados

Todos los componentes tecnológicos de la UAEAC.

Descripción

- Todos los componentes tecnológicos de la UAEAC deben tener asignado un responsable.

- Se debe restringir el acceso físico al servidor y a los elementos que lo componen, utilizando racks con puertas de acceso y cerraduras.

- En las áreas de procesamiento o almacenamiento de información, deben existir sistemas de detección de intrusión física como: sensores de movimiento, cámaras, alarmas, controles de acceso biométrico o con tarjeta inteligente.

- Las áreas de procesamiento o almacenamiento de información deben contar con fuentes de energía redundantes como; UPS y plantas eléctricas.

- El ingreso de contratistas o proveedores a las áreas de procesamiento o almacenamiento de información debe estar autorizado y monitoreado durante la actividad por el responsable del área.

- El ingreso a las áreas de procesamiento o almacenamiento de información debe quedar registrado en una bitácora o planilla de control de ingreso con la fecha, hora, nombre de la persona que ingresa, actividad a realizar, nombre de la persona que lo autoriza y hora de salida.

- Todos los componentes tecnológicos de la UAEAC deben estar protegidos de posibles variaciones de voltaje.

  - Está prohibido: fumar, consumir alimentos o bebidas en las áreas de procesamiento o almacenamiento de la información.

- En las áreas de procesamiento o almacenamiento de información, deben existir: detectores de humo, alarmas de calor, controles de humedad y aire acondicionado. Todos estos dispositivos deben ser monitoreados permanentemente.

- En las áreas de procesamiento o almacenamiento de información, deben existir sistemas de detección, control y extinción de incendios o extintores adecuados para combatir conflagraciones en este tipo de ambientes, deben estar vigentes y contener el agente correspondiente.

- Los sistemas de detección, control y extinción de incendios o extintores deben ser monitoreados y probados periódicamente para garantizar su

efectividad y se debe capacitar en su uso al personal responsable de las áreas de procesamiento o almacenamiento de información y al personal de vigilancia y seguridad física.

- Todos los sistemas de comunicaciones, incluido el cableado estructurado, deben estar debidamente identificados y organizados para una adecuada administración y su documentación debe estar actualizada.

6.2.6 Diseño de dos roles.

Los Roles y Responsabilidades del Modelo de Seguridad y Privacidad de la Información han sido definidos con el propósito de establecer las funciones relacionadas con la Seguridad de la Información para los Administradores y Responsables de los componentes tecnológicos de la Entidad, con el fin de garantizar la Confidencialidad, Integridad y Disponibilidad de la información de propiedad de la UAEAC.

RL-01 ADMINISTRADOR DE SEGURIDAD DE USUARIOS.

Normatividad Relacionada

NO-01 Función de la Seguridad de la Información

Descripción

Es el responsable de crear, bloquear, inactivar o modificar los usuarios y mantener actualizados los grupos, perfiles de usuarios y roles para cada uno de los módulos que conforman el Sistema de Información o Componente Tecnológico, atendiendo las Solicitudes de Acceso a Componentes Tecnológicos, las novedades administrativas que se presenten y los requerimientos de los responsables de la información; con el fin de garantizar protección a la información y aplicando los lineamientos establecidos por Seguridad de la Información de la UAEAC.

Responsabilidades

- Garantizar un adecuado uso y administración de las cuentas de Usuarios Privilegiados y Superusuarios, creadas en los Componentes Tecnológicos de la UAEAC.

- Utilizar las contraseñas de Usuarios Privilegiados y de Superusuarios de Sistemas de Información, creadas a nivel de Base de Datos, exclusivamente para el cumplimiento de las funciones asignadas.

- Coordinar, definir e implementar con los responsables de la información y el Coordinador del Grupo Seguridad de la Información, los esquemas de seguridad de acceso al Sistema de Información o Componente Tecnológico.

- Garantizar un adecuado control en la definición y mantenimiento de perfiles y roles de usuarios a los componentes tecnológicos de la UAEAC.

- Diseñar, documentar y mantener actualizadas las definiciones de grupos, roles, perfiles de usuario y seguridades en conjunto con los responsables de la información.

- Definir, configurar y administrar los Usuarios, Grupos, Roles y Perfiles de usuarios del Sistema de Información aplicando los lineamientos de Seguridad de la Información.

- Crear, modificar, inactivar, bloquear o eliminar los usuarios del Sistema de Información atendiendo las Solicitudes de Acceso a Componentes Tecnológicos, las novedades administrativas que se presenten y los requerimientos de los responsables de la información.

- Inactivar o bloquear indefinidamente las cuentas de usuario en los diferentes componentes tecnológicos, si así lo establece el Jefe Inmediato, el Líder responsable de la información, el Grupo Seguridad de la Información o la Oficina de Control Interno, como resultado de alguna de sus revisiones periódicas.

- Planear y ejecutar revisiones periódicas de los usuarios y los permisos asignados a cada uno en los Sistemas de Información, verificando que el acceso corresponde a la necesidad de información para el cumplimiento de sus funciones y aplicar los correctivos necesarios.

- Establecer mecanismos que permitan que las actividades de administración y monitoreo ejecutadas sobre los Componentes Tecnológicos queden almacenadas en los registros de auditoría de cada componente.
- Revisar frecuentemente los registros de auditoría y las actividades de acceso a información sensible o critica, con el fin de detectar posibles irregularidades

que atenten contra la Disponibilidad, Integridad, Confidencialidad y Exactitud de la Información.

- Reportar al responsable del Componente Tecnológico, los problemas relacionados con los perfiles de usuario, grupos y roles del módulo de Administración de Seguridad de Usuarios y verificar su solución.

- Investigar continuamente y generar recomendaciones sobre nuevas y mejores formas de asignar seguridad a la Gestión de Usuarios del Sistema de Información o del Componente Tecnológico de acuerdo con la evolución tecnológica.

- Implementar las recomendaciones generadas por el Grupo Seguridad de la Información para mejorar los niveles de seguridad de la información.

- Actualizar los protocolos de Administración de Seguridad de Usuarios a su cargo.

- Atender la Auditoria de Sistemas cuando sea requerido.

Documentación

- Manuales de Administración de Usuarios del Sistema de Información.
- Protocolos de Administración de Seguridad de Usuarios.

Herramientas

Módulo de Administración de Usuarios del Sistema de Información.

RL-02 ADMINISTRADOR DE COMPONENTE TECNOLÓGICO.

Normatividad Relacionada

NO-01 Función de la Seguridad de la Información
NO-02 Administración de Accesos a Componentes Tecnológicos

Descripción

Es el responsable de mantener y administrar los niveles de seguridad de los Componentes Tecnológicos como: Red, Correo Electrónico, Internet, Intranet, Sistemas de Información, Servidor de Archivos, Plataforma de Respaldo y Restauración de Información, equipos activos de red LAN/WAN, Access Point, Firewall, entre otros; con el fin de garantizar el adecuado acceso y protección a la información, aplicando los lineamientos y buenas prácticas establecidas por el Grupo Seguridad de la Información de la UAEAC.

Responsabilidades

- Definir y establecer los procedimientos necesarios para asegurar el debido respaldo y restauración de la información y del Componente Tecnológico a cargo.

- Coordinar, definir e implementar con el responsable de la información y el Coordinador del Grupo Seguridad de la Información; los esquemas de seguridad para el acceso al Componente Tecnológico a cargo.

- Participar en la evaluación y aprobación de los cambios que afecten el Componente Tecnológico a cargo, cuidando que no disminuyan los niveles de seguridad existentes.

- Documentar y mantener actualizados los procedimientos de administración y monitoreo, del Componente Tecnológico a cargo.

- Documentar y entregar para custodia la información de los usuarios privilegiados del Componente Tecnológico a cargo.

- Crear, modificar, inactivar, bloquear o eliminar los usuarios locales del Componente Tecnológico, atendiendo las Solicitudes de Acceso a Usuarios Privilegiados.

- Definir, configurar y administrar los usuarios y roles locales del Componente Tecnológico, aplicando los lineamientos definidos por Seguridad de la Información.

- Planear y ejecutar revisiones periódicas de la seguridad del Componente Tecnológico e implementar las acciones necesarias, para mejorar los niveles de seguridad y protección, aplicando las mejores prácticas.

- Investigar continuamente y generar recomendaciones sobre nuevas y mejores formas de asignar seguridad al Componente Tecnológico administrado, de acuerdo con la evolución de la tecnología.

- Implementar las recomendaciones generadas por el Grupo Seguridad de la Información, para mejorar los niveles de seguridad del Componente Tecnológico.

- Atender la Auditoria de Seguridad de la Información cuando sea requerido.

Documentación

- Manuales Técnicos del Componente Tecnológico, provistos por el fabricante.

- Procedimientos de Administración y Monitoreo del Componente Tecnológico.

Herramientas

- Módulo de Administración de Usuarios del Componente Tecnológico.
- Herramientas centralizadas de monitoreo del Componente Tecnológico.
- Software de Administración y Monitoreo del Componente Tecnológico, suministrado por el fabricante.

6.3 **DESARROLLO DE OBJETIVO 3:** DISEÑAR LA METODOLOGÍA DE ACTIVOS DE INFORMACIÓN Y RIESGOS PARA EL PROCESO GINF. 6.0 GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN, BAJO LOS LINEAMIENTOS DE MINTIC.

6.3.1 Diseño de la metodología de Activos de Información para el proceso GESTIÓN DE TECNOLOGIAS DE INFORMACIÓN (GINF. 6.0).

A continuación, se describen los documentos que hacen parte de la fase IV.

- **Metodología de gestión y clasificación de Activos de Información:** Este es un procedimiento para la gestión y clasificación de los activos de información, cuyo objetivo es, establecer las actividades para la identificación, actualización, clasificación y valoración del inventario de Activos de Información de la UAEAC, a fin de salvaguardar su confidencialidad, integridad y disponibilidad.

AERONÁUTICA CIVIL UNIDAD ADMINISTRATIVA ESPECIAL	**PROCEDIMIENTO**			
	GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN			
	Clave: GINF-6.0-06-XX	**Versión: 1.0**	**Fecha: 04/08/2020**	**Página:** de

OBJETIVO

Establecer las actividades para la identificación, actualización, clasificación y valoración del inventario de Activos de Información pertenecientes a la UAEAC, a fin de salvaguardar su confidencialidad, integridad y disponibilidad.

ALCANCE

La gestión y clasificación de activos de información es aplicable a todos los procesos, programas, planes y proyectos definidos en el Sistema de Gestión de la UAEAC y a todas las acciones ejecutadas por los servidores públicos durante el ejercicio de sus funciones a nivel nacional.

RESPONSABLES

Los usuarios responsables de las actividades del procedimiento son:

Proceso	Responsable

DIRECCIONAMIENTO ESTRATÉGICO	Comité Institucional de Gestión y Desempeño.
TODOS LOS PROCESOS	Líderes de Proceso. Responsables de la Información.
ADMINISTRACIÓN DEL SISTEMA DE GESTIÓN	Jefe Oficina Asesora de Planeación. Coordinador Grupo Organización y Calidad Aeronáutica.
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Director de Informática. Coordinador Grupo Seguridad de la Información.
GESTIÓN JURÍDICA	Jefe Oficina Asesora Jurídica.

Tabla 1. Responsables
Fuente: Elaboración propia.

La identificación, revisión, aprobación, modificación, anulación, control de cambios y divulgación de este procedimiento, será responsabilidad del Equipo de Gerencia del respectivo proceso en coordinación con el jefe del Grupo de Organización y Calidad Aeronáutica.

DEFINICIONES

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, entre otros) que tenga valor para la organización. (Modelo de Seguridad y Privacidad de la Información 3.0.2 - MINTIC).

- **Activo de información:** Un activo de información es, cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización y debe protegerse. (ISO/IEC 27001:2013).

- **Información:** Conjunto organizado de datos contenidos en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen y por su caracterización o atributos, son elementales para las actividades de la Entidad. (Ley 1712 de 2014).

- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (MINTIC, 2016).

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera, (MINTIC, 2016).

- **Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. (MINTIC, 2016).

- **Infraestructura crítica cibernética:** Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. (Ministerio de Defensa de Colombia).

PUNTOS IMPORTANTES

- La ejecución del procedimiento Gestión y Clasificación de Activos de Información es responsabilidad del Líder del proceso con el apoyo del Coordinador Grupo Organización y Calidad Aeronáutica y cuando sea requerido se solicitará apoyo al responsable de Seguridad de la Información.

- El Coordinador Grupo Seguridad de la Información es responsable de la actualización del procedimiento cuando se considere necesario.

- El procedimiento de Gestión y Clasificación de Activos de Información se enfoca en las siguientes actividades alineadas con la Guía No. 5 para la Gestión y Clasificación de Activos de Información del MSPI, MINTIC.

Ilustración 1. Gestión y Clasificación de Activos de Información.
Fuente: Elaboración propia.

Para la ejecución del Procedimiento de Gestión y Clasificación de Activos de Información, es indispensable la participación del Líder del proceso correspondiente o quien él designe.

Los inventarios de Activos de Información deben ser revisados y actualizados al menos una vez al año, sin embargo, se pueden requerir actualizaciones debido a:

- Inclusión de un nuevo activo de información en el proceso.
- Reorganización de procesos o dependencias.
- Cambios en las características de los Activos de Información.
- Solicitudes de los organismos de control de la Entidad (Normograma, Normatividad vigente, otros).
- Hallazgos de auditorías o revisiones.
- Cuando se identifique, que los Activos de Información dejan de pertenecer al proceso y/o se encuentran identificados en la Matriz para la gestión y clasificación de activos de información, con una fecha de retiro del Activo.
- Cuando se identifiquen cambios en las Tablas de Retención Documental.

EXPLICACIÓN

DESCRIPCIÓN DEL PROCESO DE LA GESTIÓN Y CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

CONTEXTO DEL PROCESO

El primer paso para la identificación de Activos de Información consiste en el entendimiento del contexto del proceso y por ello se debe:

- Conocer la caracterización del proceso, disponible en la herramienta del Sistema de Gestión.
- Revisar la Tabla de Retención Documental.
- Revisar el Listado Maestro de Documentos existente en la herramienta del Sistema de Gestión, para el proceso objeto del levantamiento de información.
- Revisar el Normograma asociado al proceso.
- Cuando sea una actualización, se debe revisar el inventario de Activos de Información existente.
- Identificar si existen otros Activos de Información, que tienen un valor agregado para el proceso.

VERIFICAR EL INVENTARIO DE ACTIVOS DE INFORMACIÓN

El Líder del proceso o quien éste delegue, en conjunto con el Grupo Organización y Calidad Aeronáutica, debe verificar si existe un Inventario de Activos de Información del proceso y en caso de que exista, este será tomado como insumo para la actualización de los Activos de Información.

IDENTIFICAR LOS ACTIVOS DE INFORMACIÓN

El Líder del proceso, Gestor de Calidad o a quien estos deleguen en conjunto con el Grupo Organización y Calidad Aeronáutica, deben realizar la identificación de los Activos de Información que tienen valor para la UAEAC, registrándolos en el formato “Matriz para la gestión y clasificación de activos de información”, según las siguientes características:

INFORMACIÓN BÁSICA

- **Identificador del Activo de Información:** Número consecutivo único que identifica el Activo de Información, este identificador es la unión de código del Macroproceso, el código del proceso y el número consecutivo del Activo.

- **Proceso que identifica el activo:** Nombre del proceso según el mapa de procesos de la UAEAC.

- **Nombre del Activo de Información:** Nombre del archivo, documento, registro, otros, que identifica el Activo de Información.

- **Descripción / Observaciones del Activo:** Se refiere a la descripción del Activo de Información, en cuanto a su contenido y/o detalle, que permite identificar el nivel de importancia de este activo dentro de las actividades del proceso**.**

TIPO DE ACTIVO

- **Información:** Son DATOS, que se alojan en diferentes tipos de documentos y/o registros utilizados en el proceso y que son almacenados física o electrónicamente, por ejemplo: Documentos (papel, carpetas, folios, actas, informes, etc.), datos de configuración, datos de gestión interna, logs, código fuente, datos de prueba, Bases de Datos, entre otros).

- **Hardware**: Son aquellos dispositivos físicos, donde se alojan o reposan los DATOS o la Información, y que por su contenido son considerados críticos o importantes, por ejemplo: servidores, portátiles, equipos de mesa, celulares, agendas electrónicas, switch, router, firewall, discos duros, discos virtuales, CD-ROM, DVD, memorias USB, cintas magnéticas, entre otros.

- **Software**: Son programas computacionales que son responsabilidad de la UAEAC y que cumplen con diversas funcionalidades de procesamiento de información como son: sistemas operativos, procesadores de texto, hojas de cálculo electrónico, sistemas de gestión de base de datos, servicios web y gestión documental, entre otros. El software puede ser comercial o desarrollado localmente.

- **Servicios**: Son aquellos servicios de computación o comunicaciones que por su criticidad son insumo para activos de información de uno o más procesos de la entidad. Dentro de este tipo de activo se encuentran los servicios provistos por entidades externas y que están por fuera del alcance de la gestión de la entidad y cuyos requerimientos de seguridad deben verse reflejados en un contrato, acuerdo o regulación que los garantice, por ejemplo: correo electrónico, Teams, Intranet, SECOP, SIIF Nación, SNIES, SACES, SPADIES, NASA, IDEAM, entre otros.

- **Recurso humano:** Son aquellas personas que, por su experiencia y criticidad para el proceso, conocen información importante, que no reposa en ningún otro medio para su uso o consulta y por ello son considerados un activo de información crítico para el proceso y para la Entidad.

- **Bases de datos personales:** Conjunto organizado de datos personales en medio físico (papel impreso o manuscrito) o electrónico (texto, hoja de cálculo electrónico, sistemas de bases de datos, pdf, entre otros) la clasificación de estas bases de datos según la SIC es de tres tipos, empleados, clientes y proveedores.

- **Datos abiertos:** Son 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. (MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información).

- **Infraestructura crítica cibernética**: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (Documento Conpes 3854, Política Nacional de Seguridad Digital, 2016).

PROPIEDAD

- **Propietario de la información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso. (MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información).

- **Custodio:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. (MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información).

  SERIES, SUBSERIES Y TIPOS DOCUMENTALES

  Es la identificación utilizada en las Tablas de Retención Documental TRD y en este campo se debe señalar la serie, subserie y tipo documental correspondiente al activo de información en la TRD. (Adaptado MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información).

- **Frecuencia de generación y/o actualización:** Identifica la periodicidad con la que se actualiza la información de acuerdo con su naturaleza y la normatividad aplicable, por ejemplo: anual, semestral, trimestral, bimensual, mensual, semanal, diario, permanente, por demanda. (Adaptado MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información).

- **Formato de conservación:** Estándar en el cual la información ha sido generada; ejemplo: (.xlsx, .docx, .pdf, .jpg, .avi, papel, etc.). (Elaboración propia Grupo Seguridad de la Información).

- **Idioma**: español, inglés, otros.

- **Medio de conservación:** Establece el soporte en el que se encuentra la información, esto quiere decir si el activo reposa sobre un elemento físico y/o digital según corresponda. (Elaboración propia Grupo Seguridad de la Información).

- **Información** publicada: Indica que el Activo de Información es de libre acceso, ya sea por medios virtuales o físicos y no requiere de ninguna solicitud. (Elaboración propia Grupo Seguridad de la Información).

- **Ubicación del activo de información**

  - **Física**: (Regional / Nombre del edificio / piso / área o nombre de Dependencia / Archivo de Gestión, otros).

  - **Digital**: (Ruta de almacenamiento o sistema de información según sea el caso, otros).

  CALIFICACIÓN DE DATOS PERSONALES

- **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. Este NO puede ser objeto de tratamiento a menos que sea requerido para salvaguardar un interés vital del titular o este se encuentre incapacitado y su obtención haya sido autorizada expresamente. (Ley 1581 de 2012).

- **Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular" esto significa que un dato privado es cualquier información que se refiere a la vida privada de una persona como lo son sus datos personales, tales como, correo electrónico personal, teléfono, dirección de vivienda, datos laborales, nivel de escolaridad, sobre infracciones administrativas o penales, los datos administrados por algunas entidades como tributarias, financieras o de la seguridad social, fotografías, videos, y cualquier otro dato que referencien el estilo de vida de la persona. Dicha información no debe ser observada o tener acceso indebido por ningún órgano público o privado, ya que el titular tiene derecho a controlar cuando y quien puede acceder a esa información que hace parte de su vida privada. (Ley 1266 de 2008).

- **Dato semiprivado:** El dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, Historias crediticias, datos financieros, reporte en las centrales de riesgo, precisando que este tipo de datos requieren de autorización previa del titular para ser reportados a las bases de datos, o centrales de riesgos. Para su tratamiento se requiere la autorización expresa del titular de la información, (Ley 1266 de 2008).

- **Dato público:** Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva, para este no es necesaria la autorización del titular de la información. (Ley 1581 de 2012).

- **Dato de niños, niñas y adolescentes:** Los datos personales de los menores de edad tienen una especial protección y por lo tanto su tratamiento está prohibido, excepto cuando se trate de datos de naturaleza pública, de

conformidad con lo establecido en el artículo 7° de la Ley 1581 de 2012 y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.
- Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos. Para este fin deberán aplicarse los principios y obligaciones establecidas en la Ley 1581 de 2012 y su decreto reglamentario. (SIC, Superintendencia de Industria y Comercio – Respuesta: Protección de datos personales).

- **Usuarios**: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información. (Adaptado MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información).
- **Fecha de identificación o actualización:** Corresponde a la fecha en que el activo de información se identificó o actualizó dentro de la Matriz para la gestión y clasificación de activos de información. (Elaboración propia Grupo Seguridad de la Información).
- **Fecha de retiro:** Corresponde a la fecha en la cual el activo deja de ser parte del Inventario de Activos de Información. (Elaboración propia Grupo Seguridad de la Información).

CLASIFICACIÓN DEL ACTIVO SEGÚN SU CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

La clasificación de los Activos de Información tiene como objeto identificar la Confidencialidad, Integridad y la Disponibilidad de los mismos, con el fin de identificar su nivel de importancia o criticidad para los procesos de la Entidad. A continuación, se describen estas propiedades:

- **Clasificación de acuerdo con la confidencialidad**

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, esta se debe definir de acuerdo con las características de los activos que se manejan en la Entidad. Para esta clasificación se definieron tres (3) niveles alineados con los tipos de información definidos en la Ley 1712 del 2014.

En la siguiente tabla muestra los niveles de confidencialidad:

Clasificación	Descripción
ALTA	Información que, al ser divulgada o conocida a terceros, sin previa autorización puede generar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica. Información clasificada bajo la Ley 1712 del 2014 como pública reservada. Información clasificada bajo la Ley 1581 del 2012 como sensible o privada y/o información de niños y niñas adolescentes.
MEDIA	Información que por su contenido y a quienes va dirigido, su divulgación no autorizada puede generar impactos negativos a más de una Dependencia o Proceso. Esta información no puede ser conocida por terceros sin que sea autorizada por el propietario. Información clasificada bajo la Ley 1712 del 2014 como pública clasificada. Información clasificada bajo la Ley 1581 del 2012 como semiprivada.
BAJA	Información que puede ser entregada o publicada, sin restricciones a cualquier persona dentro y fuera de la Entidad, sin que implique daños a terceros ni a las actividades o procesos de la Entidad. Información clasificada bajo la Ley 1712 del 2014 como pública. Información clasificada bajo la Ley 1581 del 2012 como pública.

Tabla 2. Clasificación de acuerdo con la confidencialidad
Fuente: Tomado de MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información.

- **Clasificación de acuerdo con la integridad**

  La integridad se refiere a la exactitud y completitud de la información, esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción. (NTC: ISO/IEC ISO 27001:2013).

  En la siguiente tabla se muestra la clasificación de acuerdo con la integridad:

Tabla 3. Clasificación de acuerdo con la integridad.
Fuente: Tomado de MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información.

- **Clasificación de acuerdo con la disponibilidad**

  La disponibilidad es la propiedad de la información, que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona, entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso. (MINTIC, Guía 5 – Guía para la Gestión y Clasificación de Activos de Información).

  En la siguiente tabla se muestra la clasificación de acuerdo con la disponibilidad:

Clasificación	Descripción
ALTA	La no disponibilidad de la información o de los Activos de Información, puede generar un impacto negativo **severo o alto**, ya sea de tipo legal, económico, de imagen, o de afectación en los tiempos de ejecución de los procesos.
MEDIA	La no disponibilidad de la información o de los Activos de Información, puede generar un impacto negativo **moderado o medio**, ya sea de tipo legal, económico, de imagen, o de afectación en los tiempos de ejecución de los procesos.
BAJA	La no disponibilidad de la información o de los Activos de Información, NO conlleva a un impacto significativo para la Entidad.

Tabla 4. Clasificación de acuerdo con la disponibilidad.
Fuente: Tomado de MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información.

- **Criticidad del activo de información**

  La criticidad del Activo de Información permite identificar aquellos Activos que son importantes o elementales para los procesos y para la Entidad en general, y que a su vez deben ser evaluados mediante un Análisis de Riesgos con el fin de minimizar posibles afectaciones de tipo legal, económico, de imagen, o tiempos de ejecución de los procesos.

  Para poder determinar cuáles son aquellos Activos de Información críticos, se evalúan los niveles de Confidencialidad, Integridad y Disponibilidad, de cada activo y según la clasificación (Alta, Media, Baja), debe arrojar como resultado (ALTA o MEDIA), para que se considere como un activo crítico.

  En la siguiente tabla se muestra como está estructurada la fórmula para identificar cuáles son los activos críticos:

Clasificación	Descripción
ALTA	Cuando el activo en (2) o en las (3) propiedades de su Confidencialidad, Integridad y Disponibilidad, estén catalogadas o seleccionadas como “Alta”, se considera que es un activo de información crítico para la Entidad.
MEDIA	Cuando el activo de información en (1) de sus propiedades de Confidencialidad, Integridad y Disponibilidad, este catalogada o seleccionada como Alta o si en alguna de ellas está catalogada como “Media”, se considera que es un activo de información crítico para la Entidad.
BAJO	Cuando el activo de información puede afectar una tarea aislada de la operación o del proceso. Las pérdidas o afectación serían menores y no incurrirían en sanciones.

Tabla 5. Criticidad del activo de información.
Fuente: Tomado de MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información.

CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN, CONFORME A LA LEY 1712 DE 2014

Si el Activo es de “**Tipo**”, “**Información**”, se debe clasificar conforme a la Ley 1712 de 2014, como:

- **Información pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal. (Ley 1712 de 2014).

- **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 de 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 de 2014.

- **Información no clasificada:** Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como Activos de Información PUBLICA RESERVADA. (MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información).

- **Objetivo legítimo de la excepción:** Identificación de la excepción que, dentro de las previstas en los artículos 18 y 19 de la Ley 1712 de 2014, cobija la calificación de información pública reservada o pública clasificada. (Ley 1712 de 2014).

- **Fundamento constitucional o legal:** Fundamento, que justifica la clasificación o la reserva, señalando expresamente la norma, artículo, inciso o párrafo que la ampara. (Ley 1712 de 2014).

- **Fundamento jurídico de la excepción:** Se menciona la norma jurídica que sirve como fundamento para la clasificación de la Información pública clasificada o pública reservada.

- **Excepción total o parcial:** Este campo solo debe ser diligenciado si la información se clasificó como: Información pública clasificada o Información pública reservada; el fundamento constitucional, legal o jurídico que justifica la clasificación o la reserva, señalando expresamente la norma, artículo, inciso, o párrafo que la ampara.

- **Fecha de la calificación:** Fecha de la calificación de la información como reservada o clasificada.

- **Plazo de la clasificación o reserva:** Tiempo que cobija la clasificación o reserva; de acuerdo con la Ley 1712 de 2014 la reserva de la información puede durar como máximo quince (15) años desde la generación del documento.

- **Información disponible:** Indica que el Activo de información está a disposición inmediata para ser consultada o solicitada, pero esta información no está publicada.

FORMALIZAR EL INVENTARIO DE ACTIVOS DE INFORMACIÓN

Finalizadas las actividades mencionadas anteriormente, el Grupo Organización y Calidad Aeronáutica, debe formalizar la aprobación del inventario de Activos de Información con el Líder del Proceso o con quien éste delegue. La formalización se hará mediante un Acta en la cual el Líder del proceso acepta sus Activos de Información. Por otra parte, el Comité Institucional de Gestión y Desempeño, se encarga de la aprobación de los Activos de Información, y posterior a ello se publica el Inventario de Activos de Información por proceso, en la herramienta del Sistema de Gestión y se publicará en la página web institucional, por parte del Web Máster del Grupo Comunicación y Prensa.

ACTUALIZAR EL INVENTARIO DE ACTIVOS DE INFORMACIÓN

El Líder del proceso, Gestor de Calidad o quien éste delegue en conjunto con el Grupo Organización y Calidad Aeronáutica verifican el inventario de Activos de Información con el propósito de establecer si en cualquiera de los campos establecidos, se han presentado cambios con el fin que el inventario permanezca siempre actualizado, teniendo en cuenta la importancia de cada uno de los Activos de Información, para los objetivos estratégicos de la Entidad.

PUNTOS DE CONTROL

Actividad	¿Qué se controla?	¿Con qué frecuencia?	¿Quién lo controla?	Riesgos asociados
Actualizar el inventario de Activos de Información	Que el inventario de Activos de Información se encuentre siempre actualizado.	Cuando se hayan presentado cambios en los campos o características de los Activos y/o mínimo una (1) vez al año.	Líder del proceso, Gestor de Calidad o quien éste delegue.	Afectación en los procesos, en el momento que se materialice un riesgo y no se identifique los niveles de criticidad de los Activos de Información.

Tabla 6. PUNTOS DE CONTROL.
Fuente: Elaboración propia.

NORMATIVIDAD APLICABLE

- **Ley 1712 de 2014**: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Ley 1581 de 2012**: Por la cual se dictan disposiciones generales para la protección de datos personales.

- **Capítulo 26 del Decreto Único 1074 de 2015**: Por medio del cual, se reglamenta la información mínima que debe contener el RNBD y los términos y condiciones bajo los cuales se deben inscribir en éste las bases de datos sujetas a la aplicación de la Ley 1581 de 2012.

- **Decreto 1008 de 2018**: Por medio del cual se expide el Decreto Único Reglamentario del Sector Cultura.

- **Decreto 106 de 2015 de la 1712**: Por el cual se reglamenta el Título VIII de la Ley 594 de 2000 en materia de inspección, vigilancia y control a los archivos de las entidades del Estado y a los documentos de carácter privado declarados de interés cultural; y se dictan otras disposiciones.

- **Guías de MSPI**: Por el cual, se establece el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia de Gobierno Digital.

ANEXOS

- Instrumento para el diligenciamiento de la matriz de activos de la información
- Matriz para la gestión y clasificación de activos de información

  - **Instrumento para el diligenciamiento de la matriz de AI:** Instructivo para el diligenciamiento de la matriz de inventario de activos de información, cuyo objetivo es describir las instrucciones para el diligenciamiento de la matriz de inventario de activos de información.

OBJETIVO

Describir las instrucciones para el diligenciamiento de la matriz de inventario de activos de información.

RESPONSABLES

Los usuarios responsables del desarrollo de las actividades del instructivo son:

Proceso	Responsable
DIRECCIONAMIENTO ESTRATÉGICO	Comité Institucional de Gestión y Desempeño.
TODOS LOS PROCESOS	Líderes de Proceso. Responsables de la Información.
ADMINISTRACIÓN DEL SISTEMA DE GESTIÓN	Jefe Oficina Asesora de Planeación. Coordinador Grupo Organización y Calidad Aeronáutica.
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Director de Informática. Coordinador Grupo Seguridad de la Información.
GESTIÓN JURÍDICA	Jefe Oficina Asesora Jurídica.

Tabla 1. Responsables
Fuente: Elaboración propia.

FRECUENCIA

Cada vez que surjan cambios significativos en alguno de los campos o características del activo de información se debe actualizar la matriz de inventario de activos de información y como mínimo se debe actualizar una vez al año.

FUENTE DE INFORMACIÓN

Entrevistas con los Líderes de Proceso o con sus respectivos delegados.

PUNTOS IMPORTANTES

- La ejecución del procedimiento Gestión y Clasificación de Activos de Información es responsabilidad del Líder del proceso con el apoyo del Gestor del Grupo Organización y Calidad Aeronáutica y cuando sea requerido se solicitará apoyo al responsable de Seguridad de la Información.
- El Coordinador Grupo Seguridad de la Información es responsable de la actualización del instructivo cuando se considere necesario.
- El procedimiento de Gestión y Clasificación de Activos de Información se enfoca en las siguientes actividades alineadas con la Guía No. 5 para la Gestión y Clasificación de Activos de Información del MSPI, MINTIC.
- El Inventario de Activos de Información debe ser actualizado al menos una (1) vez al año.

CONTENIDO

A continuación, se describe el instructivo para el diligenciamiento de la matriz de inventario de activos de información.

<table>
<tr><th>ITEM</th><th>NOMBRE</th><th>DESCRIPCIÓN</th></tr>
<tr><td colspan="3">Información básica</td></tr>
<tr><td>1</td><td>ID Numérico</td><td>Indicar el número consecutivo del activo de información en la matriz.</td></tr>
<tr><td>2</td><td>Identificador del activo</td><td>Indicar cuál es el código del macroproceso, el código del proceso y el número consecutivo del activo de información.

<table>
<tr><th>Código del Macroproceso</th><th>Código del Proceso</th><th>Número Consecutivo</th></tr>
<tr><td>GINF</td><td>6.0</td><td>001</td></tr>
<tr><td>Gestión de Tecnologías de Información</td><td>Gestión de Tecnologías de Información</td><td>001, 002, 003, 004…</td></tr>
<tr><td colspan="3">Ejemplo: GINF-6.0/001</td></tr>
</table>
</td></tr>
<tr><td>3</td><td>Proceso que identifica el activo</td><td>Indicar el nombre del proceso, según el mapa de procesos de la UAEAC.</td></tr>
<tr><td>4</td><td>Nombre del activo</td><td>Indicar el nombre del archivo, documento, registro, otros, que identifica el Activo de Información.

Es importante tener en cuenta que el nombre debe ser lo suficientemente claro para que pueda ser entendido por todas las partes interesadas.
Ejemplo:
Actas de levantamiento de…
Formulario de diligenciamiento de…
Pruebas críticas de…
Resultados importantes de…
Informe crítico de…
Comunicaciones privadas de…
Actas de entrega o de eliminación de…
Certificados médicos de…
Análisis de laboratorio de…</td></tr>
</table>

ITEM	NOMBRE	DESCRIPCIÓN
5	**Descripción / Observaciones del Activo**	En este campo se describen las características en cuanto a su contenido y/o detalle, que permite identificar el nivel de importancia de este activo dentro de las actividades del proceso.
6	**Tipo**	Seleccionar de la lista desplegable el tipo de activo de información, según corresponda: **Información:** Son DATOS, que se alojan en diferentes tipos de documentos y/o registros utilizados en el proceso y que son almacenados física o electrónicamente, por ejemplo: Documentos (papel, carpetas, folios, actas, informes, etc.), datos de configuración, datos de gestión interna, logs, código fuente, datos de prueba, Bases de Datos, entre otros). **Hardware:** Son aquellos dispositivos físicos, donde se alojan o reposan los DATOS o la Información, y que por su contenido son considerados críticos o importantes, por ejemplo: servidores, portátiles, equipos de mesa, celulares, agendas electrónicas, switch, router, firewall, discos duros, discos virtuales, CD-ROM, DVD, memorias USB, cintas magnéticas, entre otros. **Software**: Son programas computacionales que son responsabilidad de la UAEAC y que cumplen con diversas funcionalidades de procesamiento de información como son: sistemas operativos, procesadores de texto, hojas de cálculo electrónico, sistemas de gestión de base de datos, servicios web y gestión documental, entre otros. El software puede ser comercial o desarrollado localmente. **Servicios:** Son aquellos servicios de computación o comunicaciones que por su criticidad son insumo para activos de información de uno o más procesos de la entidad. Dentro de este tipo de activo se encuentran los servicios provistos por entidades externas y que están por fuera del alcance de la gestión de la entidad y cuyos requerimientos de seguridad deben verse reflejados en un contrato, acuerdo o regulación que los garantice, por ejemplo: correo electrónico, Teams, intranet, SECOP, SIIF Nación, SNIES, SACES, SPADIES, NASA, IDEAM, entre otros. **Recurso humano:** Son aquellas personas que, por su experiencia y criticidad para el proceso, conocen información importante, que no reposa en ningún otro medio para su uso o consulta y por ello son considerados un activo de información crítico para el proceso y para la Entidad.

ITEM	NOMBRE	DESCRIPCIÓN
		Bases de datos personales: Conjunto organizado de datos personales en medio físico (papel impreso o manuscrito) o electrónico (texto, hoja de cálculo electrónico, sistemas de bases de datos, pdf, entre otros) la clasificación de estas bases de datos según la SIC es de tres tipos, empleados, clientes y proveedores. **Datos abiertos:** Son 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. **Infraestructura crítica cibernética**: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.
Propiedad		
7	**Propietario de la información**	Mencionar el propietario, una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.
8	**Custodio**	Mencionar él o los custodios, quienes son parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.
Series y/o tipos documentales		

ITEM	NOMBRE	DESCRIPCIÓN
9	**Series, subseries y/o tipos documentales (TRD)**	En este campo se debe indicar la serie, subserie y tipo documental correspondiente al activo de información en las Tablas de Retención Documental (TRD).
Frecuencia de generación de la información		
10	**Frecuencia de generación y/o actualización**	Seleccionar de la lista desplegable la periodicidad con la que se actualiza la información de acuerdo con su naturaleza y la normatividad aplicable: anual, semestral, trimestral, bimensual, mensual, semanal, diario, permanente, por demanda.
Formato de conservación		
11	**Formato**	Indicar el tipo de formato en el cual la información ha sido generada; ejemplo: (.xlsx, .docx, .pdf, .jpg, .avi, papel, etc.).
Idioma del activo		
12	**Idioma**	Indicar el idioma en el que se encuentra el activo de información (español, inglés, otros).
Medio de conservación del activo		
13	**Medio de conservación**	Seleccionar de la lista desplegable el medio en el que se encuentra la información, esto quiere decir si el activo reposa sobre un elemento físico y/o digital según corresponda.
Información publicada		
14	**Información publicada**	Seleccionar de la lista desplegable si la Información está (publicada o no publicada) esto quiere decir si es de libre acceso, ya sea por medios virtuales o físicos y no requiere de ninguna solicitud. Ejemplo: Los resultados de las elecciones, contrataciones públicas, pruebas saber del SENA, códigos únicos de medicamentos, otros.
Ubicación del activo de información		

ITEM	NOMBRE	DESCRIPCIÓN
15	**Ubicación física**	Indicar donde se encuentra ubicada la información o el Activo de Información. Ejemplo: Regional / Nombre del edificio / piso / área o nombre de Dependencia / Archivo de Gestión, otros según corresponda.
16	**Ubicación digital**	Indicar donde se encuentra ubicada la información o el Activo de Información. Ejemplo: Nombre del servidor - (nombre de la carpeta) URL: OneDrive de la Entidad / Office 365
Clasificación de Datos Personales		
17	**Sensible**	Si el activo de información contiene datos personales de este tipo se debe marcar con una X: Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. Este NO puede ser objeto de tratamiento a menos que sea requerido para salvaguardar un interés vital del titular o éste se encuentre incapacitado y su obtención haya sido autorizada expresamente.
	Privado	Si el activo de información contiene datos personales de este tipo se debe marcar con una X: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular" esto significa que un dato privado es cualquier información que se refiere a la vida privada de una persona como lo son sus datos personales, tales como, correo electrónico personal, teléfono, dirección de vivienda, datos laborales, nivel de escolaridad, sobre infracciones administrativas o penales, los datos administrados por algunas entidades como tributarias, financieras o de la seguridad social, fotografías, videos, y cualquier otro dato que referencien el estilo de vida de la persona. Dicha información no debe ser

ITEM	NOMBRE	DESCRIPCIÓN
		observada o tener acceso indebido por ningún órgano público o privado, ya que el titular tiene derecho a controlar cuando y quien puede acceder a esa información que hace parte de su vida privada.
	Semiprivado	Si el activo de información contiene datos personales de este tipo se debe marcar con una X: El dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, Historias crediticias, datos financieros, reporte en las centrales de riesgo, precisando que este tipo de datos requieren de autorización previa del titular para ser reportados a las bases de datos, o centrales de riesgos. Para su tratamiento se requiere la autorización expresa del titular de la información.
	Público	Si el activo de información contiene datos personales de este tipo se debe marcar con una X: Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva, para este no es necesaria la autorización del titular de la información.
	Niños, niñas y adolescentes	Si el activo de información contiene datos personales de este tipo se debe marcar con una X: Los datos personales de los menores de edad tienen una especial protección y por lo tanto su tratamiento está prohibido, excepto cuando se trate de datos de naturaleza pública, de conformidad con lo establecido en el artículo 7° de la Ley 1581 de 2012 y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos: a) Que responda y respete el interés superior de los niños, niñas y adolescentes.

ITEM	NOMBRE	DESCRIPCIÓN
		b) Que se asegure el respeto de sus derechos fundamentales. c) Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto. Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos.
Usuarios		
18	**Usuarios**	Mencionar en este campo, los usuarios (cargos, procesos, otros) quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.
Fecha de identificación o actualización y de retiro		
19	**Fecha de identificación o actualización**	Colocar la fecha en que el activo de información se identificó o actualizó dentro de la matriz de inventario de activos de información. (DD/MM/AAAA)
20	**Fecha de retiro**	Colocar la fecha en la cual el activo deja de ser parte del Inventario de activos de información. (DD/MM/AAAA)
Clasificación (confidencialidad, integridad, disponibilidad)		
Seleccionar de la lista desplegable el nivel de valoración (alto, medio o bajo), de acuerdo los a criterios definidos a continuación:		
21	**Valoración de Confidencialidad**	La Confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, esta se debe definir de acuerdo con las características de los activos que se manejan en la Entidad.

<table>
<tr><th>ITEM</th><th>NOMBRE</th><th>DESCRIPCIÓN</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><th>Clasificación</th><th>Descripción</th></tr>
<tr><td>ALTA</td><td>Información que, al ser divulgada o conocida a terceros, sin previa autorización puede generar un impacto negativo de índole legal, operativa, de pérdida de imagen o económica.

Información clasificada bajo la Ley 1712 del 2014 como pública reservada.

Información clasificada bajo la Ley 1581 del 2012 como sensible o privada y/o información de niños y niñas adolescentes.</td></tr>
<tr><td>MEDIA</td><td>Información que por su contenido y a quienes va dirigido, su divulgación no autorizada puede generar impactos negativos a más de una Dependencia o Proceso. Esta información no puede ser conocida por terceros sin que sea autorizada por el propietario.

Información clasificada bajo la Ley 1712 del 2014 como pública clasificada.

Información clasificada bajo la Ley 1581 del 2012 como semiprivada.</td></tr>
<tr><td>BAJA</td><td>Información que puede ser entregada o publicada, sin restricciones a cualquier persona dentro y fuera de la Entidad, sin que implique daños a terceros ni a las actividades o procesos de la Entidad.

Información clasificada bajo la Ley 1712 del 2014 como pública.

Información clasificada bajo la Ley 1581 del 2012 como pública.</td></tr>
</table>
Tabla 2. Confidencialidad
Fuente: Tomado de MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información.
</td></tr>
<tr><td>22</td><td>Valoración de Integridad</td><td>La integridad se refiere a la exactitud y completitud de la información, esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción.
<table>
<tr><th>Clasificación</th><th>Descripción</th></tr>
<tr><td>ALTA</td><td>Información que, de ser alterada o manipulada, cuya pérdida de exactitud y/o completitud, puede generar un impacto negativo <u>severo o alto</u>, ya sea de tipo legal, económico, de imagen, o de afectación en los tiempos de ejecución de los procesos.</td></tr>
<tr><td>MEDIA</td><td>Información que, de ser alterada o manipulada, cuya pérdida de exactitud y/o completitud, puede generar un impacto negativo <u>moderado o medio</u>, ya sea de tipo legal, económico, de imagen, o de afectación en los tiempos de ejecución de los procesos.</td></tr>
<tr><td>BAJA</td><td>Información que, de ser alterada o manipulada, cuya pérdida de exactitud y/o completitud, <u>NO</u> conlleva a un impacto significativo para la Entidad.</td></tr>
</table>
Tabla 3. Integridad
Fuente: Tomado de MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información.
</td></tr>
</table>

<table>
<tr><th>ITEM</th><th>NOMBRE</th><th>DESCRIPCIÓN</th></tr>
<tr><td>23</td><td>Valoración de disponibilidad</td><td>La disponibilidad es la propiedad de la información, que se refiere a que ésta debe ser accesible y utilizable por solicitud de una persona, Entidad o proceso autorizada cuando así lo requiera esta, en el momento y en la forma que se requiere ahora y en el futuro, al igual que los recursos necesarios para su uso.
<table>
<tr><th>Clasificación</th><th>Descripción</th></tr>
<tr><td>ALTA</td><td>La no disponibilidad de la información o de los Activos de Información, puede generar un impacto negativo <u>severo o alto</u>, ya sea de tipo legal, económico, de imagen, o de afectación en los tiempos de ejecución de los procesos.</td></tr>
<tr><td>MEDIA</td><td>La no disponibilidad de la información o de los Activos de Información, puede generar un impacto negativo <u>moderado o medio</u>, ya sea de tipo legal, económico, de imagen, o de afectación en los tiempos de ejecución de los procesos.</td></tr>
<tr><td>BAJA</td><td>La no disponibilidad de la información o de los Activos de Información, <u>NO</u> conlleva a un impacto significativo para la Entidad.</td></tr>
</table>
Tabla 4. Disponibilidad
Fuente: Tomado de MINTIC, Guía 5 - Guía para la Gestión y Clasificación de Activos de Información.</td></tr>
<tr><td colspan="3">Clasificación de los activos de información, conforme a la Ley 1712 de 2014</td></tr>
<tr><td>24</td><td>Información pública</td><td>Seleccionar de la lista desplegable si el activo de información de acuerdo con la Ley 1712 de 2014, denominada Ley de Transparencia y del derecho de acceso a la información pública nacional, es información (pública).
Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.</td></tr>
<tr><td>25</td><td>Información pública clasificada</td><td>Seleccionar de la lista desplegable si el activo de información de acuerdo con la Ley 1712 de 2014, denominada Ley de Transparencia y del derecho de acceso a la información pública nacional, es 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 esta Ley.</td></tr>
<tr><td>26</td><td>Información pública reservada</td><td>Seleccionar de la lista desplegable si el activo de información de acuerdo con la Ley 1712 de 2014, denominada Ley de Transparencia y del derecho de acceso a la información pública nacional, es 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</td></tr>
</table>

ITEM	NOMBRE	DESCRIPCIÓN
		cumplimiento de la totalidad de los requisitos consagrados en el **Artículo 19** de esta Ley.
27	**Información no clasificada**	Seleccionar de la lista desplegable si el activo de información de acuerdo con la Ley 1712 de 2014, denominada Ley de Transparencia y del derecho de acceso a la información pública nacional, es información (no clasificada). Activos de Información que deben ser incluidos en el inventario y que aún no han sido clasificados, deben ser tratados como Activos de Información PUBLICA RESERVADA.
28	**Información disponible**	Seleccionar de la lista desplegable, si el activo de información está (disponible) a disposición inmediata para ser consultada o solicitada, pero esta información no está publicada, o por el contrario está (no disponible).
29	**Objetivo legítimo de la excepción**	Identificar la excepción, que dentro de las previstas en los artículos 18 y 19 de la Ley 1712 de 2014, cobija la calificación de información pública reservada o pública clasificada. (Ley 1712 de 2014).
30	**Fundamento constitucional o legal**	Indicar el fundamento que justifica la clasificación o la reserva, señalando expresamente la norma, artículo, inciso o párrafo que la ampara. (Ley 1712 de 2014).
31	**Fundamento jurídico de la excepción**	Mencionar la norma jurídica que sirve como fundamento para la clasificación de la Información pública clasificada o pública reservada.
32	**Excepción total o parcial**	Seleccionar de la lista desplegable, (parcial o total) dado el caso y solo si la información se clasificó como: pública clasificada o pública reservada; el fundamento constitucional, legal o jurídico que justifica la clasificación o la reserva, señalando expresamente la norma, artículo inciso o párrafo que la ampara.
33	**Fecha de la calificación**	Fecha de la calificación de la información como reservada o clasificada.
34	**Plazo de la clasificación o reserva**	Indicar cuál es tiempo que cobija la clasificación o reserva; de acuerdo con la Ley 1712 de 2014, la reserva de la información puede durar como máximo quince (15) años desde la generación del documento.

Tabla 2. Campos de la Matriz de inventario de activos de información
Elaboración propia.

ANEXOS

- Matriz para la gestión y clasificación de activos de información

- **Matriz para la gestión y clasificación de AI:** Es un formato en Excel para la gestión y clasificación de activos de información.

AERONÁUTICA CIVIL
UNIDAD ADMINISTRATIVA ESPECIAL

FORMATO

MATRIZ PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

Principio de Procedencia: 3403.20	Clave: GINF-6.0-06-XX	Versión: 1.0	Fecha: 04/08/2020	Página: 1 de 1											
INFORMACIÓN BÁSICA					**Tipo**	**PROPIEDAD**		**Series, Subseries y/o Tipos Documentales (TRD)**	**Frecuencia de Generación y/o Actualización**	**Formato de conservación**	**Idioma**	**Medio de Conservación**	**Información Publicada**	**UBICACIÓN DEL ACTIVO DE INFORMACIÓN**	
ID Numérico	**Identificador del Activo de Información**	**Proceso que Identifica el Activo**	**Nombre del Activo de Información**	**Descripción / Observaciones del Activo**		**Propietario de la Información**	**Custodio**							**Ubicación Física**	**Ubicación Digital**

FORMATO

MATRIZ PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

CLASIFICACIÓN DE DATOS PERSONALES					Usuarios	Fecha de Identificación o actualización (DD / MM / AAAA)	Fecha de Retiro (DD / MM / AAAA)	CLASIFICACIÓN							Criticidad
Sensible	Privado	Semiprivado	Público	Niños, niñas y Adolescentes				Valoración Confidencialidad	No Eliminar - Formulación	Valoración Integridad	No Eliminar - Formulación	Valoración Disponibilidad	No Eliminar - Formulación	Justificación Valoración Disponibilidad	
									0		0		0		

FORMATO
MATRIZ PARA LA GESTIÓN Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

LEY DE TRANSPARENCIA (LEY 1712 DE 2014) - JURÍDICA							
Acceso a la Información de acuerdo con la LEY 1712 DE 2014	Información Disponible	Objetivo Legítimo de la Excepción (Artículo 18 y 19)	Fundamento Constitucional o Legal	Fundamento Jurídico de la Excepción	Excepción (Total, Parcial)	Fecha de la Calificación (DD / MM / AAAA)	Plazo de la Clasificación

- **Inventario AI Gestion de Tecnologías de la Información - GINF 6.0:** En este instrumento se relaciona el inventario de Activos de Información del proceso Gestion de Tecnologías de la Información - GINF 6.0.

Principio de Procedencia: 3403.250	Clave: GINF-6.0-06-XX	Versión: 1.0	Fecha: 24/07/2020	Página: 1 de 1												
INFORMACIÓN BÁSICA					**Tipo**	**PROPIEDAD**		**Series y/o Tipos Documentales (TRD)**	**Frecuencia de Generación de la Información**	**Formato**	**Idioma**	**Medio de conservación**	**Información publicada**	**UBICACIÓN**	
ID Numérico	**Identificador del Activo**	**Proceso que Identifica el Activo**	**Nombre del Activo**	**Descripción / Observaciones del Activo**		**Propietario de la Información**	**Custodio**							**Ubicación Física**	**Ubicación Digital**

1	GINF-6.0/001	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Proyectos de tecnologías de la información	Gestión de los proyectos de tecnologías de la información con el fin de proveer e implementar nuevas soluciones de infraestructura de tecnologías de la información (TI), servicios informáticos, sistemas de inform	Información	Grupo proyectos de tecnología de información	Funcionario encargado del archivo Grupo de Soporte Informático	340145011	Por demanda	EXCEL/PAPEL/Doc	Español	Ambos	No Publicada	Archivo del grupo de trabajo	Bog 7

				ación, seguridad informática y de la información. Contiene: • Estudio de viabilidad • Especificaciones técnicas • Requerimiento funcional • Manual del administrador • Manual de operación												

				• Manual del usuario • Solicitud de inscripción de soporte lógico - software • Registro de derechos de autor											
2	GINF-6.0/002	GESTIÓN DE TECNOLOGÍAS DE INFORMA	Documentos de Isolucion para la gestión del proceso de Gestió	Documentos en Isolucion que se encuentra dentro del Siste	Información	Grupo proyectos de tecnología de información	Grupo de Soporte Informático Planeación	N/A	Por demanda	Word, Excel, PDF	Español	Ambos	Publicada	Archivo del grupo de trabajo	Servidor ISOLUCION

		CIÓN	n de la educación.	ma de Gestión SG de la entidad.											
3	GINF-6.0/003	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Instrumentos de control de acceso a componentes tecnológicos	Contiene documentos informativos de las actividades para controlar la creación, modificación, inactivación, eliminación y/o bloqueo de accesos de los usuarios a los diferentes	Información	Grupo seguridad de la información	Funcionario encargado del archivo Grupo de Soporte Informático	340329002	Por demanda	EXCEL/PAPEL/Doc.	Español	Ambos	No Publicada	Archivo del grupo de trabajo	Bog 7

				Componentes Tecnológicos de la UAEAC. Está compuesto por: • Solicitud de acceso a componentes tecnológicos • Solicitud de acceso a sistemas de información y aplicativos usuarios externos •											

				Registro y control de solicitudes de acceso a CT											
4	GINF-6.0/004	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Instrumentos de control de acceso a usuarios privilegiados	Contenido informativo: Actividades para controlar la creación, modificación, bloqueo, inactivación	Información	Grupo seguridad de la información	Funcionario encargado del archivo Grupo de Soporte Informático	340329003	Por demanda	EXCEL/PAPEL/Doc	Español	Ambos	No Publicada	Archivo del grupo de trabajo	Bog 7

				y/o eliminación de accesos de los usuarios privilegiados a los sistemas operativos, bases de datos, elementos activos de red (switches, enrutadores) o cualquier otro Componente Tecnológico de la											

				UAEAC. Compuesto por: • Solicitud de acceso a Usuarios Privilegiados • Informe de creación del acceso solicitado • Informe de negación del acceso solicitado											

5	GINF-6.0/005	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Instrumentos de control para el acceso, autorización de software y aplicaciones	Contenido informativo: controles para la entrada y salida de equipos de las instalaciones de la Aerocivil, así como las autorizaciones para el acceso a páginas web y la instalación de software requerido	Información	Grupo seguridad de la información	Funcionario encargado del archivo Grupo de Soporte Informático	340329021	Por demanda	EXCEL/PAPEL/Doc	Español	Ambos	No Publicada	Archivo del grupo de trabajo	Bog 7

				por los funcionarios de la entidad. Conformado por: • Autorización de acceso a páginas Web • Autorización para el acceso a puertos											
6	GINF-6.0/006	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Instrumentos de control para la administración de cupos certificados de	Contenido informativo: Administrar los cupos para la U.A.E.A.C.	Información	Grupo seguridad de la información	Funcionario encargado del archivo Grupo de Soporte	340329036	Por demanda	EXCEL/Doc.	Español	Digital	No Publicada	N/A	Bog 7

			firma digital	debido a que se manej a un mayor volum en de Certifi cados Digital es. Renov ar los Certifi cados Digital es (Toke n) de los usuari os de la U.A.E. A.C. debido a que tienen vigenc ia de (2) años y poster iorme nte pierde n su			Infor mátic o							

				vida útil. Conformado por: • Cuadro control de usuarios • Cédula de ciudadanía • Certificación laboral • Mensaje de preaprobación • Notificación de renovación y aprobación											

7	GINF-6.0/007	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Registros, modificación y eliminación de usuarios y perfiles SIIF Sistema Integrado de Información Financiera.	Contenido informativo: actividades necesarias para la creación, modificación y eliminación de usuarios y asignación de perfiles y ámbitos de acceso que se requieran en el Sistema de Información SIIF	Información	Grupo seguridad de la información	Funcionario encargado del archivo Grupo de Soporte Informático	340348029	Por demanda	EXCEL/Doc.	Español	Ambos	Publicada	Archivo del grupo de trabajo	Bog 7

				NACIÓN. Conformado por: • Solicitud Asignación Certificado de Firma Digital Usuario SIIF Nación • Solicitud de creación cuenta de usuario • Solicitud de modificación cuenta de usuario •												

				Notificación del registro de la solicitud - correo electrónico											
8	GINF-6.0/008	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Instrumentos de control de copias de seguridad - Backus	Contenido informativo: copias de seguridad del sistema operativo, de actualizaciones de aplicaciones, de datos, de archivos de configuración, de softwa	Información	Grupo de soporte informático	Funcionario encargado del archivo Grupo de Soporte Informático	340229007	Por demanda	EXCEL/Doc/PDF	Español	Digital	No Publicada	N/A	Bog 7

				re de red, compiladores, códigos de fuente desarrollado, software de aplicación, archivos de seguridad, librerías de programas. Compuesto por Licencia de software.												

9	GINF-6.0/009	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Instrumentos de control para la administración de licencias de software	Contenido informativo: administración del software licenciado de la Aeronáutica Civil, así como de aquel que se encuentra obsoleto o que ya cumplió su vida útil, definiendo las actividades y los diferentes cuenta	Información	Grupo de soporte informático	Funcionario encargado del archivo Grupo de Soporte Informático	340229038	Por demanda	EXCEL/Doc/PDF	Español	Digital	No Publicada	N/A	Bog 7

				dantes o respo nsable s que intervi enen en el proces o La elimin ación de los docum entos se efectú a en la vigenc ia siguie nte a la termin ación de los period os de retenci ón. Los docum entos en soport e papel											

				se eliminan mediante la técnica de triturado bajo la supervisión y control del Coordinador del Grupo de Archivo General. Los documentos electrónicos se eliminan mediante técnicas de borrado seguro bajo												

				la coordinación del Coordinador del Grupo de Seguridad de la Información. La eliminación de documentos debe ser autorizada por el Comité Institucional de Gestión y Desempeño previa la public											

				ación durante sesenta (60) días de los inventarios documentales en la página Web dejando evidencia del proceso en la respectiva Acta de Eliminación de Documentos Compuesto por: • Licencia de softwa re											

				• Solicitud de baja de la licencia de software • Concepto técnico de baja de licencia de software • Requerimiento de software											
10	GINF-6.0/010	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Instrumentos de control para la gestión de cambios	Contenido informativo: atención de requerimientos para el desarr	Información	Grupo de soporte informático	Funcionario encargado del archivo Grupo de Soporte	340229059	Por demanda	EXCEL/Doc/PDF	Español	Digital	No Publicada	N/A	Bog 7

				ollo y mejoramiento de funcionalidades de los sistemas de información de la Aerocivil. Compuesto por: • Control de cambios • Listado de asistencia al comité de cambios			Informático							

11	GINF-6.0/011	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Políticas de impresión	Contiene los lineamientos sobre la utilización del servicio de impresión a nivel nacional con el propósito de buscar concienciа a la construcción de buenas prácticas de la racionalización de los recursos natura	Información	Grupo de soporte informático	Funcionario encargado del archivo Grupo de Soporte Informático	340242004	Por demanda	EXCEL/Doc	Español	Digital	No Publicada	N/A	Bog 7

				les, colaborando en la eficiencia y eficacia en la reducción del uso del papel en los diferentes trámites y procedimientos de la entidad.											
12	GINF-6.0/012	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Registros de entrega de información o componente tecnológico	Contiene el acta de entrega de las funciones, tareas y actividades de un	Información	Grupo de soporte informático	Funcionario encargado del archivo Grupo de Soporte Infor	3402948012	Por demanda	EXCEL/Doc	Español	Digital	No Publicada	N/A	Bog 7

				componente de TI. o sistema de información que haga parte del inventario de la Dirección de Informática, bajo la responsabilidad del servidor público dependiente de la Dirección, ya sea por retiro, traslado, o			mático								

				asignación de nueva administración o liderazgo técnico. Compuesto por: • Ficha técnica del componente de TI. o sistema de información • Lista de Chequeo - Revisión de documentación • Acta de entreg												

				a y recibo a satisfacción de sistema de información o componente tecnológico											
13	GINF-6.0/013	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Equipos de cómputo de Gestión de tecnología de información	Portátiles o pc´s de usuario con información del proceso Gestión de tecnologías de información en los discos.	Hardware	Gestión de tecnología de información	Usuarios del área	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

14	GINF-6.0/014	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo proyectos de tecnología de información	Lidera la gestión el proceso. Diseña estrategia del área.	Recurso Humano	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
15	GINF-6.0/015	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo seguridad de la información	Lidera la gestión el proceso. Diseña estrategia del área.	Recurso Humano	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
16	GINF-6.0/016	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo de soporte informático	Lidera la gestión el proceso. Diseña estrategia del área.	Recurso Humano	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

17	GINF-6.0/017	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Administradores de Infraestructura y Sistemas de Información del Grupo de soporte informático	Gestionar la administración de la Infraestructura y Sistemas de Información de la entidad.	Recurso Humano	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
18	GINF-6.0/018	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Director de Dirección Informática	Lidera la gestión el proceso. Diseña estrategia del área.	Recurso Humano	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
19	GINF-6.0/019	GESTIÓN DE TECNOLOGÍAS DE INFO	Secop II	Herramienta que permite el manejo de contratación	Servicio	Gestión de tecnología de información	Colombia Compra Eficiente.	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

		RMACIÓN		pública. Colombia Compra Eficiente.											
20	GINF-6.0/020	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	SIIF Nación	Herramienta que pertenece al Ministerio de Hacienda.	Servicio	Gestión de tecnología de información	Ministerio de Hacienda (BD SIIF)	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
21	GINF-6.0/021	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de Controlador de Dominio	Servicio configurado dentro de la UAEAC para DHCP, DNS, SMTP, Impresión tercerizada, DIRECTOR	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo Aeropuertos: BAQ,	No Aplica

				IO ACTIVO (LDAP), repositorio de antivirus, repositorio de actualizaciones de Windows, de almacenamiento de forma centralizada de todas las contraseñas de usuarios de red. Este compuesto por:									RNG, AXM, AUC, BGA, VUP, CTG, SMR, PSO, PPN, CLO, MED, ADZ, MTR, NVA, PEI, AXM, VVC, YOP, EJA, GY	

				- Servidor controlador de dominio principal y Servidores controladores de dominio readonly en Aeropuertos.										M, LET, CUC.	
22	GINF-6.0/022	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio SMTP	Protocolo para él envió de correos desde los Sistemas de Información.	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				- Servidor donde está configurado el protocolo. - Office 365											
23	GINF-6.0/023	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio DNS Externo	Sistema de nombres de dominio, base de datos que sirve para resolver nombres fuera del dominio. Este compuesto por:	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				- Servidores DNS externos											
24	GINF-6.0/024	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de WSUS	Servicio centralizado de actualizaciones de Windows. Este compuesto por: Ambiente de producción: - Servidor de Repositorio principal - Servidores de	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo Aeropuertos: BAQ, RNG, AXM, AUC, BGA, VUP, CTG,	No Aplica

				Repositorios en aeropuertos.										SMR, PSO, PPN, CLO, MED, ADZ, MTR, NVA, PEI, AXM, VVC, YOP, EJA, GYM, LET, CUC.	
25	GINF-6.0/025	GESTIÓN DE TECNOLOGÍAS	Servicio NTP	Protocolo de internet para sincronizar	Servicio	Gestión Tecnologías de Informaci	Gestión Tecnologías de Informaci	N/A	N/A	N/A	N/A	Físico	Publicada	Bogotá - CNA Piso 1 - Cen	No Aplica

		DE INFORMACIÓN		los relojes de los sistemas informáticos. Está compuesto por: Ambiente de producción: - Servidores		ón - Dirección de Informática	ón - Dirección de Informática							tro de Computo	
26	GINF-6.0/026	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Sistema de Control de Acceso a Oficinas de Informática y Centro de Computo	Sistema de control de acceso de las Oficinas de la Dirección de Informática y al Centro de Computo.	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				Este compuesto por: Ambiente de producción: - Servidor de aplicación - Cuatro dispositivos biométricos											
27	GINF-6.0/027	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de Backups y Restauración	Servicio para respaldar la información contenida en los servidores de la Entidad, mediante un sistema de	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				Backup con el Software Data protector. Está compuesto por: Ambiente de producción: - Servidor de aplicación - Librerías: MSL_LINUX, MSL_Windows, MSL_LINUX, MSL_Windows - BD												

				en Postgres - Catalogo de BD Oracle: Servidor Físico											
28	GINF-6.0/028	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de Monitoreo	Servicio para la gestión y monitoreo de la infraestructura tecnológica del Centro de Computo Principal y los Sistemas de Información	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Ambos	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	http://sitescope.aerocivil.gov.co:8080/SiteScope/ https://obm.aerocivil.gov.co/topaz/TopazSiteServlet https://ucmdb.aerocivil.gov.co:8443/ucmdb-ui/login_page.jsp

				de la Aeronáutica. Está compuesto por: Ambiente de producción: - Servidores - BD: Servidor físico											
29	GINF-6.0/029	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de Virtualización	Plataforma utilizada para la Virtualización. Está compuesto por: Ambiente de producción: -	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	Permanente	N/A	N/A	Ambos	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	https://vmware.aerocivil.gov.co:9443/vsphere-client/?csp

				Servidores de virtualización											
30	GINF-6.0/030	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de Intelegencia de Negocios Power BI Online	Conjunto de herramientas para el análisis empresarial, con conexión de datos de los sitios de Project online. Hace parte de la Suite de Office 365 y está en la nube.	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	Permanente	N/A	N/A	N/A	Publicada	No Aplica	No Aplica

31	GINF-6.0/031	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Project Online	Consola de administración de proyectos de infraestructura de la Aeronáutica Civil. Este compuesto por: - Sitio de estructuración de proyectos de infraestructura- Ministerio de Transporte. - Sitio de ejecución de proyectos de	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	Project	N/A	Digital	Publicada	No Aplica	https://aerocivil.sharepoint.com/sites/estructuracion/default.aspx https://aerocivil.sharepoint.com/sites/pwaerocivil/default.aspx https://aerocivil.sharepoint.com/sites/Plan_De_Accion/default.aspx

				infraestructura. - Sitio de plan de acción de la Aeronáutica Civil.											
32	GINF-6.0/032	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio Entidad Certificadora	Gestión de certificados digitales de seguridad internos. Este compuesto por un Servidor	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	Publicada	Bogotá - CNA Piso 1 - Centro de cómputo	No Aplica
33	GINF-6.0/033	GESTIÓN DE TECNOLOGÍAS DE INFORMA	Administración de usuarios de ATS	Modulo que sirve para administrar y parametrizar los usuari	Servicio	Gestión Tecnologías de Información - Dirección	Gestión Tecnologías de Información - Dirección	N/A	N/A	Base de datos	Español	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Co	No Aplica

		CIÓN		os y aplicativos desarrollados en la base de datos de ATS. La administración del módulo es compartida con los líderes funcionales (parametrización), seguridad de la información (gestión de usuarios) y Línea 3000		de Informática	de Informática							mputo	

				(Desbloqueo de cuentas por cambio de contraseña). Administra usuarios y parámetros de las siguientes aplicaciones: ALDIA, Permisos especiales, Plan de Vuelo, RVE, AIS, ELITE. Está compuesto por:											

				Ambiente de producción: - Servidores con los ejecutables de los aplicativos - BD: Servidor físico: AERO 01 Servidor físico: AERO 01 - Software Cognos (reportes) Ambiente de												

				desarrollo y pruebas: - Servidor de aplicaciones - BD: Servidor físico: DSIAC											
34	GINF-6.0/034	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Fajas de progreso	Ingreso de fajas de progreso (información generada en las torres de control de los diferentes aeropuertos) a nivel	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	Base de datos	Español	Ambos	Publicada	Bogotá - CNA Piso 1 - Centro de Computo	Ambiente Cliente/Servidor accedido desde los equipos de los usuarios.

				nacional. Actualmente es de solo CONSULTA. Está compuesta por: Ambiente de producción: - Servidores con los ejecutables de los aplicativos - BD: Servidor físico Servidor físico - Softw												

				are Cognos (reportes) Ambiente de desarrollo y pruebas: - Servidor de aplicaciones - BD: Servidor físico											
35	GINF-6.0/035	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Sistema de Información SCORE	Sistema de Coordinación de Slots, sirve para asignar franjas horarias a las aeronaves. Está	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	Permanente	Base de datos	Español e Ingles	Ambos	Publicada	Bogotá - CNA Piso 1 - Centro de Computo Hosting Ubicació	http://aerocivil.pdc.com

				compuesto por: Ambiente de producción: - Servidor de aplicación (replica de la información que está en hosting) - Hosting con PDC Aviación										n: Dinamarca	

36	GINF-6.0/036	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de Impresión (Interno)	Servicio de las impresoras propias de la Entidad, el cual se encuentra en proceso de baja. Actualmente hay 100 impresoras en red para aeropuertos. El servicio centralizado interno de impresión está	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				compuesto por: - Servidores											
37	GINF-6.0/037	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Project On Premise	Herramienta de ofimática, Project 2013 que corresponde a 50 licencias propias de la entidad.	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	N/A	Publicada	No Aplica	No Aplica

38	GINF-6.0/038	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Sistema de Información Aranda - Modulo Assent Management	Sistema de información utilizado para inventario de computadores de escritorio, portátiles y licencias. Adicionalmente permite gestionar los requerimientos e incidentes del servicio de línea 3000. Está	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	Base de datos	Español	N/A	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				compuesto por: Ambiente de producción: Servidor de aplicaciones: BD: Servidor físico											
39	GINF-6.0/039	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Software Solar Winds (Monitoreo de Red)	Servicio para la gestión y monitoreo de la infraestructura de red de la Aeronáutica. Está compuesto por: Ambie	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	N/A	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				nte de producción: - BD - Servidor de monitoreo de rendimiento de red - Servidor de análisis de tráfico Próximamente BSM											
40	GINF-6.0/040	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de WIFI	Servicio inalámbrico brindado para facilitar las comunicaciones institucionales	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				móviles entre los funcionarios desde cualquier punto de las instalaciones de la UEAC. Está compuesto por: - Controladora WIFI - Acces point - Servidor virtual (centro de cómputo)											

41	GINF-6.0/041	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de balanceador de carga para aplicativos	Servicio que permite distribuir y balancear carga de las aplicaciones configuradas en estos dispositivos. Son dos y están configurados en modo activo - pasivo.	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	N/A	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica
42	GINF-6.0/042	GESTIÓN DE TECNOLOGÍAS DE INFO	Exchange Online (Correo electrónico)	Servicio informático para el envío y recepc	Servicio	Gestión Tecnologías de Información - Direc	Gestión Tecnologías de Información - Direc	N/A	N/A	N/A	N/A	N/A	No Publicada	No Aplica	No Aplica

		RMACIÓN		ión de mensajes electrónicos a nivel externo e interno de la Entidad. Está compuesto por: Ambiente de producción: Servidor de aplicación: BOG169 Ambiente de desarrollo y pruebas: Servidor de aplicación:		ción de Información	ción de Información								

				BOG109 Sistemas de Información que los utilizan: - ADI. - AIS. - ELITE. - ISOLUCION. - Plan de Vuelo. - Permisos Especiales DSNA. - Quejas Vuelos. - RVE. - Softw												

				are HOPEX (Fabricante MEGA). - SIGA - SITAH. Servicios que lo utilizan: - Herramienta de Monitoreo. - Herramienta de back up y restauración. - Servicio de almacenamiento -											

				Sistema de Información Aranda - Modulo Assets Manager											
43	GINF-6.0/043	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Skype for Bussines (Cloud)	Servicio de mensajería instantánea utilizado para videoconferencia.	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	N/A	No Publicada	No Aplica	No Aplica
44	GINF-6.0/044	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Yammer	Servicio en la nube adquirido con Microsoft	Servicio	Gestión Tecnologías de Información - Dirección de Infor	Gestión Tecnologías de Infor	N/A	N/A	N/A	N/A	N/A	Publicada	No Aplica	No Aplica

						mática	mática								
45	GINF-6.0/045	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Office 365 (Word, Excel, power point)	Servicio en la nube adquirido con Microsoft	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Digital	No Publicada	No Aplica	http://portal.office365.com/
46	GINF-6.0/046	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Share Point Online	Es una plataforma de servicios basados en la nube que hace parte del Plan Office 365 que actualmente	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Digital	No Publicada	No Aplica	http://portal.office365.com/

				tienen los usuarios de la Entidad, el cual permite compartir, colaborar y tener acceso a sitios internos, documentos y otra información desde cualquier lugar: en la oficina, en casa, o desde un dispositivo												

				móvil mediante acceso web.											
47	GINF-6.0/047	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	OneDrive	Servicio de almacenamiento en la nube ofrecido por Office 365	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Digital	No Publicada	No Aplica	http://portal.office365.com/
48	GINF-6.0/048	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Dirsync Office 365	Servicio de sincronización entre Aerocivil y Cloud de Microsoft. Está compuesto por: -	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				Servidor de aplicación											
49	GINF-6.0/049	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de Impresión (Tercerizado)	Servidores desde donde se gestiona el control y la operación del servicio de impresoras que están contratadas en la UAEAC. Está compuesto por: - Servidor de impresión -	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				Servidor de impresión edificio NEA											

50	GINF-6.0/050	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Sistema de Información SIGMA	Sistema de Información de apoyo que permite registrar las labores de mantenimiento de equipos con el fin de tener la supervisión y control de estaciones aeronáuticas, herramientas y/o repuestos para sistem	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	Permanente	Base de datos	Español	Ambos	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	Acceso desde la Intranet

				as y equipos aeronáuticos y aeroportuarios; así como del factor humano del sector de soporte técnico aeronáutico para lograr una adecuada planeación y programación de los mantenimientos correctivos,											

				preventivos, predictivos y así establecer indicadores y estadísticas de gestión. Está compuesto por: Ambiente de Producción: - Servidor de aplicaciones - BD: Servidor físico Servidor Virtual Ambie											

				nte de Desarrollo: - Servidor de desarrollo - BD: Servidor físico											

51	GINF-6.0/051	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	IPS	Previene intrusión o ataques a la red, basándose en vulnerabilidades. Está compuesto por: - Appliance McAfee - Servidor	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica
52	GINF-6.0/052	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Web Gateway	Proxy, es el canal único de salida de la red LAN a internet y hace filtro	Servicio	Gestión Tecnologías de Información - Dirección de Infor	Gestión Tecnologías de Información - Dirección de Infor	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				de control de acceso a sitios web. Está compuesto por: - Infraestructura: Appliance de McAfee. - Máquina virtual		mática	mática								
53	GINF-6.0/053	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Firewall perimetral	Equipo que permite monitorear y controlar el tráfico de la red LAN al exterior y viceve	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Físico	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				rsa. Está compuesto por: - 2 Appliance Firewall - Servidor de administración											
54	GINF-6.0/054	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Digitur no	Herramienta utilizada para generar los turnos en la oficina de atención al ciudadano. Está compuesta por: Ambiente de	Softwar e	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	Base de datos	Español	Físico	Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				producción: - Servidor de aplicaciones - BD: Servidor virtual											
55	GINF-6.0/055	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Sistema Integrado de Gestión MECI y Calidad (ISOLUCION)	Herramienta que apoya el Sistema Integrado de Gestión y permite realizar la gestión de auditorías, hallazgos, no conformidades tanto	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	PDF WORD PPT EXCEL MP4	Español	Ambos	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	Acceso desde la Intranet e Internet

				de la Oficina Asesora Planeación como de la Oficina de Control Interno; así mismo mantener actualizado y centralizado el mapa de procesos, el mapa MECI y la documentación oficial que genera el sistem												

				a de información. Está compuesto por: Ambiente de producción: - Servidor de aplicaciones - BD: Servidor físico Ambiente de desarrollo y pruebas: - BD: Servidor físico											

56	GINF-6.0/056	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de almacenamiento	Servicio de almacenamiento de información. Está compuesto por: - Servidor de administración	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	Ambos	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	En los componentes descritos en el activo
57	GINF-6.0/057	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Plataforma de capacitaciones MOODLE	Herramienta de gestión de aprendizaje utilizada para realizar cursos virtuales al interior de la UAEAC y al	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Programas Académicos	Diario	Base de datos	Español	Ambos	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	http://CEAVIRTUAL.AEROCIVIL.GOV.CO

				público en general. Está compuesta por: - Servidores de aplicaciones - Base de datos: MySQL											
58	GINF-6.0/058	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de Certihuella	Sistema de información biométrica en línea ofrecido por la Registraduría Nacional, a través del cual se	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	Español	Digital	No Publicada	N/A	Equipos de usuario (cliente servidor)

				realiza la validación de la identidad de las persona que presentan el plan de vuelo personalmente y tramite de licencias de personal aeronáutico.											
59	GINF-6.0/059	GESTIÓN DE TECNOLOGÍAS DE INFORMA	Sistema de Información Aeronáutica de la Gestión de Información	Herramienta que apoya los procesos misionales para la	Software	Gestión Tecnologías de Información - Dirección de	Gestión Tecnologías de Información - Dirección de	N/A	N/A	Base de datos	Español e Ingles	Ambos	Publicada	Bogotá - CNA Piso 1 - Centro de Co	Equipos de usuarios.

		CIÓN	Aeronáutica (SIA-AIM)	generación de procedimientos de tránsito aéreo, manual AIP, cartas aeronáuticas y análisis de cobertura para radio ayudas. Esta compuesta por: - Equipos de clientes: Dirección de Servicios a la Naveg		Informática	Informática							mputo	

				ación Aérea (10 equipos), Dirección de Telecomunicaciones y Ayudas a la Navegación Aérea (2 equipos). - BD: Servidor físico AERO 01, Servidor virtual: ADI-VIRTUAL.											
60	GINF-6.0/060	GESTIÓN DE TECNOLOGÍAS	Software de Antivirus	Herramienta que permite detectar,	Servicio	Gestión Tecnologías de Informaci	Gestión Tecnologías de Informaci	N/A	N/A	N/A	N/A	Físico	Publicada	Bogotá - CNA Piso 1 - Cen	No Aplica

		DE INFORMACIÓN		limpiar y eliminar malware en los dispositivos informáticos, computadores de escritorio, computadores portátiles y servidores. Está compuesto por: - Servidor de aplicación: Consola EPO MCAFEE		ón - Dirección de Informática	ón - Dirección de Informática							tro de Computo	

				- BD - Repositorios en 23 aeropuertos: Controladores de dominio read only en aeropuertos.											
61	GINF-6.0/061	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servidor de Archivos	Servicio de almacenamiento de información oficial de la UAEAC. Está compuesto por: - Servidores:	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	PDF WORD PPT EXCEL MP4	Español	Ambos	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	Equipos de usuarios.

				(Configurados en Clúster activo - pasivo). - Discos presentados desde la SAN (Servicio de almacenamiento).											
62	GINF-6.0/062	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Procesos Judiciales Software Orión	Sistema de Información de apoyo, que permite el registro, consulta y seguimiento de las etapas	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Procesos Judiciales y Cobros Coactivos	Diario	Base de datos	Español	Digital	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	Acceso desde la Intranet

				de los procesos judiciales a cargo de los abogados en la UAEAC. Ambiente de producción: - Servidor de aplicaciones - BD: Servidor físico - Partición Virtual Ambiente de pruebas: - Servidor de aplica											

				ciones - BD: Servidor físico											
63	GINF-6.0/063	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Compendios Jurídicos	Software para consulta de la legislación vigente, que esta publicado en el diario oficial. Está compuesto por: Servidor de aplicación	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	Mensual	Repositorio de documentos	Español	Digital	Publicada	Bogotá - CNA Piso 1 - Centro de Computo	Acceso desde la Intranet
64	GINF-6.0/064	GESTIÓN DE TECNOLOGÍAS	WINISIS	Software de apoyo para Bibliot	Software	Gestión Tecnologías de Informaci	Gestión Tecnologías de Informaci	N/A	N/A	N/A	Español	N/A	Publicada	Bogotá - CNA Piso 1 - Cen	No Aplica

		DE INFORMACIÓN		eca, que permite construir y administrar bases de datos estructuradas no numéricas, es decir, base de datos constituida principalmente por textos Servidor de aplicación		ón - Dirección de Informática	ón - Dirección de Informática							tro de Computo	

65	GINF-6.0/065	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Portal Web de la Entidad (www.aerocivil.gov.co)	Servicio utilizado para divulgar información de la UAEAC al público en general. Está compuesto por: - Servidores Front End - Servidores Back End - Servidores OWA - DB Primario	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	Permanente	PDF WORD PPT EXCEL MP4	Español e Ingles	Digital	Publicada	Bogotá - CNA Piso 1 - Centro de Computo	Acceso desde Internet

				- DB Secundario - Balanceador F5: Servidores virtuales											
66	GINF-6.0/066	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de canal de Internet	Proveedor del canal para acceso a internet. Compuesto de: - Fibra óptica - Enrutador - Switch Core	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	N/A	Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica
67	GINF-6.0/067	GESTIÓN DE TECNOL	Intranet	Servicio utilizado para	Servicio	Gestión Tecnologías de	Gestión Tecnologías de	N/A	Permanente	PDF WORD PPT EXCE	Espa	Digital	No Publicada	Bogotá - CNA Piso	http://intranet

		OGÍAS DE INFORMACIÓN		divulgar información al interior de la UAEAC. Está compuesto por: - Servidores Front End. - Servidores Back End - Servidores OWA - DB Primario - DB Secundario - Balanceador F5		Información - Dirección de Informática	Información - Dirección de Informática			L MP4	ñol			1 - Centro de Computo	

68	GINF-6.0/068	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Sistema de Información AIS	Sistema de información para el manejo documental de la información publicada por la Oficina AIS, componente Client e-Servidor. Ambiente de producción: - Servidor de aplicaciones - BD: Servid	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	Base de datos	Español	Ambos	Publicada	Bogotá - CNA Piso 1 - Centro de Computo	Ambiente Cliente/Servidor accedido desde los equipos de los usuarios.

				or físico: AERO 01, Servidor virtual Servidor físico: AERO 02, Servidor virtual - Servicio SMTP Ambiente de desarrollo y pruebas - Servidor de aplicaciones - BD: Servidor físico												

69	GINF-6.0/069	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Sistema de Información de Automatización en Línea De Información Aeronáutica (ALDIA)	Sistema que permite el registro, actualización y consulta en línea de la información relacionada con pistas y permisos de operación y funcionamiento de empresas del sector aéreo. Está compuesto por:	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	Base de datos	Español	Físico	Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				Ambiente de producción: Servidor de aplicación - BD: Servidor físico Ambiente de desarrollo y pruebas: - Servidor de aplicaciones - BD: Servidor físico											
70	GINF-6.0/070	GESTIÓN DE TECNOLOGÍAS DE INFO	Sistema de Información de Administración Docum	Sistema de información que apoya la gestión	Software	Gestión Tecnologías de Información - Direc	Gestión Tecnologías de Información - Direc	Aplica la serie de Todas las Dependencias	Permanente	Base de datos Oracle	Español	Digital	Publicada	Bogotá - CNA Piso 1 - Centro de	Acceso desde la Intranet

		RMACIÓN	ental Inteligente (ADI)	documental de la entidad siguiendo la normatividad vigente con el fin de ofrecer un servicio ágil a los usuarios internos y externos. Está basado en el software mercurio versión 6.5 Ambiente de producción:		ción de Informática	ción de Informática							Computo	

				Servidor de aplicaciones BD: Servidor físico Servidor de Archivos Ambiente de desarrollo y pruebas: Servidor de aplicaciones BD: Servidor físico Servidor de Archivos											

71	GINF-6.0/071	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Sistema de Información SITAH	Sistema de Información que apoya los procesos de la Dirección de Talento Humano de tal forma que atiendan y den cumplimiento a las normas y decretos que le rigen; está basado en el software Kactus	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	3100,3101, 3102,3103, 3104,3105.	Permanente	Base de datos Oracle	Español	Digital	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	Acceso desde la Intranet

				HCM de nómina y gestión humana. Ambiente de producción Servidor de aplicaciones BD en clúster (RAC): - Servidor físico: AERO 01 - Servidor físico: AERO 02 - Servidor de Archivos												

				Ambiente de desarrollo y pruebas: Servidor de aplicaciones BD: Servidor físico: DSIAC - Servidor de Archivos											
72	GINF-6.0/072	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Software de Inteligencia de Negocios Power BI On Premise	Herramienta de Inteligencia de Negocios, que permite generar y publicar reportes	Software	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	Español	N/A	No Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				para consulta y toma de decisiones para la entidad. Servidor de aplicación											
73	GINF-6.0/073	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicio de canal de Internet para wifi	Proveedor del canal para acceso a internet para el servicio de wifi. Compuesto de: - Fibra óptica - Enruta	Servicio	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	N/A	N/A	N/A	N/A	N/A	Publicada	Bogotá - CNA Piso 1 - Centro de Computo	No Aplica

				dor - Switch core											
74	GINF-6.0/074	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Actas	Documento en el que se redacta lo sucedido, tratado, acordado y compromisos o plan de acción a seguir en una reunión, de igual manera permite realizar	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Actas	Permanente	PDF WORD	Español	Ambos	Publicada	Archivo del área	Servidor de almacenamiento BOG7

				seguimiento en la siguiente reunión y sirve como evidencia en los procesos de auditoria. Registro para realizar seguimiento y controla los compromisos establecidos en las reuniones de Equipo de Gerencia de											

				acuerdo a resolución 5466 de 2008											
75	GINF-6.0/075	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Circulares	Comunicación escrita de carácter informativa o normativa, que emite instrucciones sobre un tema en particular.	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Circulares	Por demanda	PDF WORD	Español	Ambos	Publicada	Archivo del área	Servidor de almacenamiento BOG7
76	GINF-6.0/076	GESTIÓN DE TECNOLOGÍAS DE INFO	Informes de Gestión	Documento que es una síntesis de las actividades	Información	Gestión Tecnologías de Información - Direc	Gestión Tecnologías de Información - Direc	Informes de Gestión	Permanente	PDF WORD	Español	Ambos	Publicada	Archivo del área	Servidor de almacenamiento BOG7

		RMACIÓN		desarrolladas en el marco del plan de acción que consolida la información sobre los avances en cada uno de los proyectos.		ción de Informática	ción de Informática								
77	GINF-6.0/077	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Acuerdo de Gestión	Establecimiento de una relación escrita y firmada entre el superior jerárquico y	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Acuerdo de Gestión	Permanente	PDF WORD	Español	Ambos	Publicada	Archivo del área	Servidor de almacenamiento BOG7

				el respectivo Directivo, con el fin de establecer los compromisos y resultados frente a la visión, misión y objetivos de la Entidad y los de su área; se pacta por un periodo determinado e incluye la definic											

				ión de indicadores a través de los cuales se evalúa el mismo.											
78	GINF-6.0/078	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Plan de Acción (Plan de gestión administrativo anual, plan de acción anual de inversión, ejecución presupuestal, informes)	Es un conjunto de programas, subprogramas y proyectos que debe ejecutar el área en el contexto del Plan Estratégico Institucional, definido a lograr	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Plan de Acción (Plan de gestión administrativo anual, plan de acción anual de inversión, ejecución presupuestal, informes)	Permanente	PDF WORD EXCEL	Español	Ambos	Publicada	Archivo del área	Servidor de almacenamiento BOG7

				sus objetivos a corto, mediano y largo plazo, de manera eficiente y eficaz. Los Planes de Acción son instrumentos gerenciales de programación y control que relacionan todos los proyectos de la											

				Entidad.											
79	GINF-6.0/079	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Encuestas (satisfacción de prestación de soporte a través de la Mesa de Servicios y Sistemas de Información).	Conjunto de preguntas especialmente diseñadas y pensadas para ser dirigidas a una muestra de Servidores Públicos con el objeto de conocer su opinión sobre temas específicos y nivel de	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Encuestas (satisfacción de prestación de soporte a través de la Mesa de Servicios y Sistemas de Información).	Permanente	PDF WORD	Español	Digital	Publicada	No Aplica	Servidor de almacenamiento BOG7

				satisfacción frente a servicios prestados.											
80	GINF-6.0/080	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Planes y Diseños de la Infraestructura Tecnológica	Estudios de viabilidad técnica y financiera.	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Planes y Diseños de la Infraestructura Tecnológica	Permanente	PDF WORD EXCEL	Español	Ambos	Publicada	Archivo del área	Servidor de almacenamiento BOG7
81	GINF-6.0/081	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Requerimientos de Tecnologías de la Información	Conjunto de necesidades identificadas con usuarios, para proveer soluciones tecnol	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Requerimientos de Tecnologías de la Información	Permanente	PDF WORD	Español	Ambos	Publicada	Archivo del área	Servidor de almacenamiento BOG7

				ógicas que apoyen los procesos de la Entidad.											
82	GINF-6.0/082	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Protocolos de operación	Conjunto de actividades previamente establecidas para llevar a cabo determinada función o servicio.	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Protocolos de operación	Permanente	PDF WORD	Español	Ambos	Publicada	Archivo del área	Servidor de almacenamiento BOG7 ISOLUCION
83	GINF-6.0/083	GESTIÓN DE TECNOLOGÍAS DE INFORMA	Registro y Gestión de Solicitudes	Procedimiento a través del cual se da respuesta a Ordenes de	Información	Gestión Tecnologías de Información - Dirección de	Gestión Tecnologías de Información - Dirección de	Registro y Gestión de Solicitudes	Permanente	PDF WORD	Español	Ambos	No Publicada	Archivo del área	Servidor de almacenamiento BOG7

		CIÓN		trabajo, bitácora de incidentes, control de cambios a componentes tecnológicos en producción, control de cambios a sistemas de información y aplicativos.		Informática	Informática								

84	GINF-6.0/084	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Sistemas de Información	Conjunto de documentos que describen la operación y gestión de cada uno de los Sistemas de Información de la Entidad (Manual técnico, manual de usuario, manual de administración de seguridad, protoc	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Sistemas de Información	Permanente	PDF WORD	Español	Ambos	No Publicada	Archivo del área	Servidor de almacenamiento BOG7

				olos de administración, bitácora de incidentes y documentación de errores).											
85	GINF-6.0/085	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Servicios de TI	Conjunto de documentos que describen la operación de los servicios de TI (Correo, Project, red, wifi, almacenamiento, virtualización,	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Servicios de TI	Permanente	PDF WORD	Español	Ambos	No Publicada	Archivo del área	Servidor de almacenamiento BOG7

				copias de respaldo, antivirus, impresión, etc.).											
86	GINF-6.0/086	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Atención de Incidentes de Seguridad de la Información (Informes, evidencias, cadena de custodia).	Documentación generada durante el proceso de atención de incidentes de Seguridad de la Información.	Información	Gestión Tecnologías de Información - Dirección de Informática	Gestión Tecnologías de Información - Dirección de Informática	Atención de Incidentes de Seguridad de la Información (Informes, evidencias, cadena de custodia).	Permanente	PDF WORD PPT EXCEL MP20	Español	Ambos	No Publicada	Archivo del área	Servidor de almacenamiento BOG7
87	GINF-6.0/087	GESTIÓN DE TECNOLOGÍAS DE INFORMA	Sensibilización en Seguridad de la Información (Estrategia	Documentos donde se relaciona la planificación,	Información	Gestión Tecnologías de Información - Dirección	Gestión Tecnologías de Información - Dirección	Sensibilización en Seguridad de la Información (Estrategia de sensibilización, campañas,	Permanente	PDF WORD PPT EXCEL MP23	Español	Ambos	Publicada	Archivo del área	Servidor de almacenamiento BOG7

		CIÓN	de sensibilización, campañas, presentaciones, comunicaciones).	desarrollo, informes y evidencias del Plan de Sensibilización en Seguridad de la Información de la Entidad.		de Informática	de Informática	presentaciones, comunicaciones).							
88	GINF-6.0/088	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Rack con equipos de comunicaciones de red	Rack con equipos de comunicaciones de red	Hardware	Líder Gestión de tecnología de información Coordinador Grupo soporte infor	Grupo soporte informático, administradores de componentes tecnológicos y líder	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

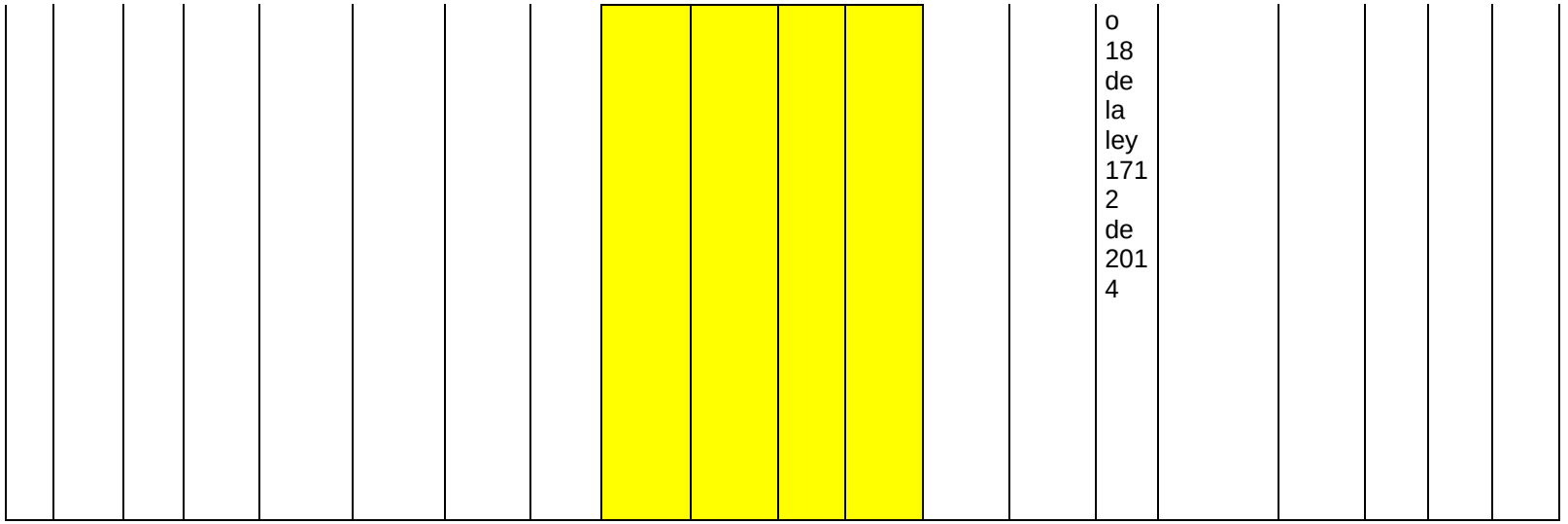
						mático, administradores de componentes tecnológicos y líderes técnicos	es técnicos								
89	GINF-6.0/089	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Rack con equipos servidores de red	Rack con equipos servidores de red	Hardware	Líder Gestión de tecnología de información Coordinador Grupo soporte informático, administra	Grupo soporte informático, administradores de componentes tecnológicos y líderes técnicos	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

						dores de componentes tecnológicos y líderes técnicos									
90	GINF-6.0/090	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Rack con equipos de Backup y respaldo	Rack con equipos de Backup y respaldo	Hardware	Líder Gestión de tecnología de información Coordinador Grupo soporte informático, administradores de componentes tecnológicos y líderes técnicos	Grupo soporte informático, administradores de componentes tecnológicos y líderes técnicos	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

						tes tecnológicos y líderes técnicos									
91	GINF-6.0/091	GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Impresoras de la entidad	Rack con equipos de Backup y respaldo	Hardware	Coordinador Grupo soporte informático, administradores de componentes tecnológicos y líderes técnicos	Grupo soporte informático, administradores de componentes tecnológicos y líderes técnicos	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

CLASIFICACIÓN DE DATOS PERSONALES					Usuarios	Fecha de Identificación o actualización (DD / MM / AAAA)	Fecha de Retiro (DD / MM / AAAA)	CLASIFICACIÓN			Criticidad	LEY DE TRANSPARENCIA (LEY 1712 DE 2014) - JURÍDICA							
Sensible	Privado	Semiprivado	Público	Niños, niñas y Adolescentes				Valoración Confidencialidad	Valoración Integridad	Valoración Disponibilidad		Acceso a la Información de acuerdo con la LEY 1712 DE 2014	Información Disponible	Objetivo Legítimo de la Excepción (Articulo 18 y 19)	Fundamento Constitucional o Legal	Fundamento Jurídico de la Excepción	Excepción (Total, Parcial)	Fecha de la Calificación (DD / MM / AAAA)	Plazo de la Clasificación
N/A	N/A	N/A	X	N/A	Proceso Gestión de Tecnologías de la Información	14/08/2020	N/A	Medio	Bajo	Bajo	MEDIA	Información Pública Clasificada	No Disponible	c) Los secretos comerciales, industriales y profesionales. Del	LEY 1712 DE 2014	articulo 18	Parcial	14/08/2020	N/A

														Articulo 18 de la ley 1712 de 2014					
N/A	**N/A**	**N/A**	**X**	**N/A**	Usuarios Internos / Ciudadano	13/08/2020	N/A	Bajo	Medio	Medio	MEDIA	Información Pública	Disponible	N/A	N/A	N/A	N/A	06/08/2020	N/A
N/A	**N/A**	**N/A**	**X**	**N/A**	Proceso Gestión de Tecnologías de la Información	19/08/2020	N/A	Medio	Medio	Medio	MEDIA	Información Pública Clasificada	No Disponible	c) Los secretos comerciales, industriales y profesionales. Del Articul	LEY 1712 DE 2014	articulo 18	Parcial	14/08/2020	N/A


o
18
de
la
ley
171
2
de
201
4

N/A	**N/A**	**N/A**	**X**	**N/A**	Proceso Gestión de Tecnologías de la Información	19/08/2020	N/A	Medio	Alto	Medio	MEDIA	Información Pública Clasificada	No Disponible	c) Los secretos comerciales, industriales y profesionales. Del Articulo 18 de la ley 1712 de 2014	LEY 1712 DE 2014	articulo 18	Parcial	14/08/2020	N/A

N/A	**N/A**	**N/A**	**X**	**N/A**	Proceso Gestión de Tecnologías de la Información	19/08/2020	N/A	Medio	Medio	Medio	MEDIA	Información Pública Clasificada	No Disponible	c) Los secretos comerciales, industriales y profesionales. Del Articulo 18 de la ley 1712 de 2014	LEY 1712 DE 2014	articulo 18	Parcial	14/08/2020	N/A

N/A	**N/A**	**N/A**	**X**	**N/A**	Proceso Gestión de Tecnologías de la Información	19/08/2020	N/A	Medio	Alto	Alto	ALTA	Información Pública Clasificada	No Disponible	c) Los secretos comerciales, industriales y profesionales. Del Articulo 18 de la ley 1712 de 2014	LEY 1712 DE 2014	articulo 18	Parcial	14/08/2020	N/A

N/A	**N/A**	**N/A**	**X**	**N/A**	Proceso Gestión de Tecnologías de la Información /Ciudadano	19/08/2020	N/A	Bajo	Medio	Alto	MEDIA	Información Pública	Disponible	N/A	N/A	N/A	N/A	06/08/2020	N/A
N/A	**N/A**	**N/A**	**X**	**N/A**	Proceso Gestión de Tecnologías de la Información	19/08/2020	N/A	Medio	Medio	Medio	MEDIA	Información Pública Clasificada	No Disponible	c) Los secretos comerciales, industriales y profesionales. Del Articulo 18 de la ley 1712	LEY 1712 DE 2014	articulo 18	Parcial	14/08/2020	N/A

														de 2014					
N/A	**N/A**	**N/A**	**X**	**N/A**	Proceso Gestión de Tecnologías de la Información	19/08/2020	N/A	Medio	Alto	Alto	ALTA	Información Pública Clasificada	No Disponible	c) Los secretos comerciales, industriales y profesionales. Del Articulo 18 de la ley 1712 de 2014	LEY 1712 DE 2014	articulo 18	Parcial	14/08/2020	N/A

N/A	**N/A**	**N/A**	**X**	**N/A**	Proceso Gestión de Tecnologías de la Información	19/08/2020	N/A	Medio	Medio	Medio	MEDIA	Información Pública Clasificada	No Disponible	c) Los secretos comerciales, industriales y profesionales. Del Articulo 18 de la ley 1712 de 2014	LEY 1712 DE 2014	articulo 18	Parcial	14/08/2020	N/A

N/A	**N/A**	**N/A**	**X**	**N/A**	Proceso Gestión de Tecnologías de la Información	19/08/2020	N/A	Medio	Medio	Medio	MEDIA	Información Pública Clasificada	No Disponible	c) Los secretos comerciales, industriales y profesionales. Del Articulo 18 de la ley 1712 de 2014	LEY 1712 DE 2014	articulo 18	Parcial	14/08/2020	N/A

N/A	**N/A**	**N/A**	**X**	**N/A**	Proceso Gestión de Tecnologías de la Información	19/08/2020	N/A	Medio	Alto	Medio	MEDIA	Información Pública Clasificada	No Disponible	c) Los secretos comerciales, industriales y profesionales. Del Articulo 18 de la ley 1712 de 2014	LEY 1712 DE 2014	articulo 18	Parcial	14/08/2020	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	13/08/2020	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	13/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	19/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	19/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	19/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	13/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	13/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**X**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Bajo	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Alto	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
X	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
X	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Medio	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**X**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Alto	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**X**	**N/A**	N/A	20/08/2020	N/A	Bajo	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Medio	Bajo	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**X**	**N/A**	N/A	20/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Medio	Alto	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Medio	Medio	Alto	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Medio	Medio	Alto	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	X	N/A	N/A	N/A	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**X**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Bajo	Bajo	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**X**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Medio	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**X**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Medio	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**X**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Medio	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**X**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Medio	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Medio	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

N/A	**X**	**N/A**	**N/A**	**N/A**	Secretaría de sistemas operacionales	20/08/2020	N/A	Medio	Medio	Bajo	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Medio	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
X	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
X	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**X**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
X	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Medio	Alto	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Alto	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**X**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Medio	Medio	Alto	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Alto	Alto	ALTA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Alto	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Medio	Alto	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Medio	Alto	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**X**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**X**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**X**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Medio	Bajo	Bajo	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	20/08/2020	N/A	Bajo	Bajo	Alto	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**X**	**N/A**	Dirección de Informática	20/08/2020	N/A	Bajo	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Bajo	Medio	Bajo	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Bajo	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Bajo	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Bajo	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Bajo	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Medio	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Alto	Medio	Medio	MEDIA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	Dirección de Informática	20/08/2020	N/A	Bajo	Bajo	Bajo	BAJA	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	13/08/2020	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	13/08/2020	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	13/08/2020	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
N/A	**N/A**	**N/A**	**N/A**	**N/A**	N/A	13/08/2020	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

6.3.2 Diseño de la metodología de riesgos para el proceso GESTIÓN DE TECNOLOGIAS DE INFORMACIÓN (GINF. 6.0).

A continuación, se describen los documentos que hacen parte de la fase V.

- **Metodología de Gestión de Riesgos:** Este documento establece los lineamientos que permitan la identificación, análisis, valoración, evaluación y tratamiento de los riesgos que pudieran afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos, y planes institucionales, estos lineamientos, deben ser acatados por todos los servidores públicos, contratistas y terceros de la entidad en el desarrollo de sus funciones y compromisos.

INTRODUCCIÓN

La UAEAC define la política de operación del riesgo tomando como referente los parámetros del Modelo Integrado de Planeación y Gestión - MIPG, la responsabilidad de las líneas de defensa definidas en el Modelo Estándar de Control Interno – MECI y los requerimientos de la Guía para la Administración del riesgo y el diseño de controles en entidades públicas - riesgos de gestión, corrupción y seguridad digital establecida por el Departamento Administrativo de la Función Pública y el Modelo de Seguridad y Privacidad de la Información del MINTIC.

El presente documento establece los lineamientos que permitan la identificación, análisis, valoración, evaluación y tratamiento de los riesgos que pudieran afectar la misión, el cumplimiento de los objetivos estratégicos y la gestión de los procesos, proyectos, y planes institucionales, estos lineamientos, deben ser acatados por todos los servidores públicos, contratistas y terceros de la entidad en el desarrollo de sus funciones y compromisos.

OBJETIVOS

Se presentan a continuación el objetivo general, y los objetivos específicos:

Objetivo general

Establecer los principios básicos y el marco general de actuación para la definición, control y la gestión de los riesgos, con el fin de fortalecer la toma de decisiones oportunas y minimizar los efectos adversos de la gestión del riesgo a los que se enfrenta la UAEAC.

Objetivos específicos

- Aumentar la probabilidad de alcanzar los objetivos estratégicos institucionales y proporcionar un aseguramiento razonable con respecto al logro de los mismos.
- Involucrar y comprometer a todos los servidores públicos de la Entidad, en la búsqueda de acciones encaminadas a prevenir los riesgos.
- Permitir el cumplimiento de los requisitos legales y reglamentarios pertinentes.
- Mejorar la gobernanza.
- Proteger los recursos bienes del Estado.
- Establecer una base confiable para la planeación y toma de decisiones.
- Asignar y utilizar eficientemente los recursos para el tratamiento de los riesgos.
- Mejorar la eficacia y eficiencia operativa.
- Identificar las situaciones que, por sus características, pueden originar prácticas corruptas.
- Ser consciente de la necesidad de identificar y tratar los riesgos en todos los niveles de la Entidad.

ALCANCE DE LA POLÍTICA

La política de operación de riesgos de gestión, corrupción y seguridad digital es aplicable a todos los procesos, programas, planes y proyectos definidos en el Sistema de Gestión de la UAEAC y a todas las acciones ejecutadas por los servidores públicos durante el ejercicio de sus funciones a nivel nacional.

MARCO NORMATIVO

- **Ley 87 de 1993** establece normas para el ejercicio del Control Interno en las entidades y organismos del Estado y dicta otras disposiciones.

- **Decreto 1537 de 2001** el Gobierno Nacional reglamentó parcialmente la Ley 87 de 1993 en cuanto a elementos técnicos y administrativos que fortalezcan el sistema de control interno de las entidades y organismos del Estado y en su artículo 4 dispuso sobre la administración de riesgos que, como parte integral del fortalecimiento de los sistemas de control interno en las entidades públicas, las autoridades correspondientes establecerán y aplicarán políticas de administración del riesgo. Para tal efecto, la identificación y análisis del riesgo debe ser un proceso permanente e interactivo entre la administración y las oficinas de control interno o quien haga sus veces, evaluando los aspectos tanto internos como externos que pueden llegar a representar amenaza para la consecución de los objetivos organizacionales, con miras a establecer acciones efectivas, representadas en actividades de control, acordadas entre los responsables de las áreas o procesos y las oficinas de control interno e integradas de manera inherente a los procedimientos.

- **Decreto 260 de 2004** artículo 9 numeral 3 facultó al Director General para “Planear, dirigir, administrar y aplicar las políticas particulares de la UAEAC y del modo de transporte aéreo y promover su desarrollo sectorial”.

- **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 del Espectro y se dictan otras disposiciones.

- **Ley 1474 de 2011** en su artículo 73° establece que cada entidad del orden nacional, departamental y municipal deberá elaborar anualmente una estrategia de lucha contra la corrupción y de atención al ciudadano que contemplará, entre otras cosas, el mapa de riesgos de corrupción en la respectiva entidad, las medidas concretas para mitigar esos riesgos, las estrategias anti-trámites y los mecanismos para mejorar la atención al ciudadano.

- **Ley 1581 de 2012** establece disposiciones generales para la protección de datos personales.

- **Decreto 1377 de 2013** por el cual se reglamenta parcialmente la Ley 1581 de 2012.

- **Ley 1712 de 2014** por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

- **Decreto 2573 de 2014** por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

- **Decreto 1081 de 2015** Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República, compiló el decreto 2641 de 2012, reglamentario de los artículos 73 y 76 de la ley 1474 de 2011, mediante el cual se estableció como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano, la establecida en el Plan Anticorrupción y de Atención al Ciudadano contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano”.

- **Decreto 1083 de 2015** por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública, entre otros aspectos establece que, se deben tomar medidas para administrar los riesgos en la entidad pública (Artículo 2.2.21.5.4).

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

- **Decreto 648 de 2017** por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública, y en su Artículo 2.2.21.1.6 literal g., establece dentro de las funciones del Comité Institucional de Coordinación de Control

Interno que se debe someter a aprobación del representante legal la política de administración del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.

- **Decreto 1499 de 2017** en su Artículo 2.2.22.3.2 definió el Modelo Integrado de Planeación y Gestión MIPG como marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.

- **Resolución 03738 de 2017** por la cual se establece el Comité Institucional de Coordinación de Control Interno en la UAEAC.

- **Decreto No. 1008 de 2018** por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del tirulo 9 de la parte 2 del libro del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de tecnologías de la Información y las Comunicaciones.

- **Guía DAFP versión octubre 2018** Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento de Administración de la Función Pública.

- **Resolución 02405 de 2018** por la cual se adopta el Modelo Integrado de Planeación y Gestión – MIPG y se integra el Comité Institucional de Gestión y Desempeño encargado de orientar su implementación y operación en la UAEAC.

- **Resolución 04076 de 2019** por la cual se adopta la política de operación de administración de riesgos, en la UAEAC.

- **Resolución 04215 de 2019** por la cual se adopta el Modelo de Seguridad y Privacidad de la Información (MSPI), en la UAEAC.

- **GINF-6.0-21-01 de 2018** por la cual se adoptan las Políticas de Seguridad de la Información.

NORMAS TÉCNICAS APLICABLES

- **Norma Técnica Colombiana NTC-ISO/IEC 27000:2012:** Glosario de seguridad de la información.
- **Norma Técnica Colombiana NTC-ISO 31001:2018:** Gestión del Riesgo. Principios y Directrices.

ADMINISTRACIÓN DE RIESGOS

Política de operación de administración de riesgos

La UAEAC se compromete a administrar los riesgos, definidos en el mapa de riesgos institucional, de acuerdo con las directrices establecidas en la política de operación de administración de riesgos para su tratamiento, manejo y seguimiento, dando cumplimiento a la misión, visión y objetivos institucionales.

NIVELES DE ACEPTACIÓN AL RIESGO

- **Riesgos de gestión:**
  Los riesgos de gestión valorados como bajos (Riesgo residual) pueden ser aceptables.
- **Riesgos de corrupción:**
  No hay tolerancia o niveles de aceptación para riesgos de corrupción.

- **Riesgos de seguridad digital:**
  Los riesgos de seguridad digital valorados como moderados (Riesgo residual) pueden ser aceptables.

RESPONSABILIDAD

A continuación, se describen las responsabilidades frente a los riesgos desde el rol de las líneas de defensa existentes para los diferentes niveles de la Entidad.

Líneas de defensa	Responsable	Responsabilidad frente al riesgo
Estratégica	Alta Dirección	Aprobar la Política de operación del riesgo la cual incluye los niveles de responsabilidad y compromisos frente al riesgo.
		Establecer objetivos institucionales alineados con el propósito fundamental, metas y estrategias de la Entidad.
		Analizar los cambios en el entorno (contexto interno y externo) que puedan tener un impacto significativo en la operación de la entidad y que puedan generar cambios en la estructura de riesgos y controles.
		Revisar los cambios en el “Direccionamiento estratégico” y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados.
		Hacer seguimiento en el Comité Institucional de Gestión y Desempeño - CIGD y en el Comité Institucional de Coordinación de Control Interno – CICCI, a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna.
	Comité Institucional de Gestión y	Definir la Política de operación del riesgo la cual incluye los niveles de responsabilidad y compromisos frente al riesgo.

Líneas de defensa	Responsable	Responsabilidad frente al riesgo
	Desempeño – CIGD	Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar el tratamiento de los riesgos.
		Revisar el cumplimiento de los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
		Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.
	Comité Institucional de Coordinación de Control Interno - CICCI	Someter a aprobación del representante legal la política de operación del riesgo y hacer seguimiento, en especial a la prevención y detección de fraude y mala conducta.
		Hacer seguimiento y pronunciarse sobre el perfil de riesgo inherente y residual de la entidad, de acuerdo con las políticas de tolerancia establecidas y aprobadas.
		De los riesgos que se han materializado en la entidad, detectar las causas que dieron origen a esos eventos.
		Retroalimentar al Comité Institucional de Gestión y Desempeño sobre los ajustes que se deban hacer frente a la gestión del riesgo.
Primera Línea de defensa	Equipos de Gerencia	Seguimiento trimestral a los controles definidos para verificar que cumplen con el tratamiento de riesgos para los cuales fueron implementados; cuando sea necesario proponer mejoras a la gestión del riesgo en su proceso.
		Revisar y reportar a la segunda y tercera línea de defensa, los riesgos que se han materializado. Analizando la información de todos los elementos involucrados que permitan ajustar los controles para no afectar el cumplimiento de los objetivos afectados por estos riesgos; se recomienda el uso de indicadores de estos objetivos para la correspondiente validación.
		Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.
	Líderes y gestores de procesos	Identificar, valorar y evaluar los riesgos que pueden afectar los programas, proyectos, planes y procesos a su cargo y actualizarlo cuando se requiera.

Líneas de defensa	Responsable	Responsabilidad frente al riesgo
		Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos.
		Desarrollar ejercicios de autoevaluación para establecer la eficiencia, eficacia y efectividad de los controles.
		Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos.
		Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos.
		Reportar en el Sistema de Gestión los avances y evidencias de la gestión de los riesgos a cargo del proceso asociado.
Segunda Línea de defensa	Oficina Asesora de Planeación	Apoyar a la línea estratégica en el análisis del contexto interno y externo, para la definición de la política de riesgo, el establecimiento de los niveles de impacto y el nivel de aceptación del riesgo.
		Revisar los cambios en el direccionamiento estratégico o en el entorno y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar en la actualización de las matrices de riesgos.
		Revisión de la adecuada definición y alineación de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
		Consolidar el Mapa de riesgos institucional y presentarlo al Comité Institucional de Gestión y Desempeño para análisis y seguimiento.
		Presentar al Comité Institucional de Gestión y Desempeño el seguimiento a la eficacia de los controles en las áreas identificadas en los diferentes niveles de operación de la entidad.
		Acompañar y orientar a los líderes de procesos en la identificación, análisis y valoración del riesgo.

Líneas de defensa	Responsable	Responsabilidad frente al riesgo
		Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
		Promover ejercicios de autoevaluación en la primera línea de defensa para establecer la eficiencia, eficacia y efectividad de los controles.
		Revisar el adecuado diseño de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y determinar las recomendaciones y seguimiento para el fortalecimiento de estos.
	Grupo Seguridad de la Información. (Para los riesgos de seguridad digital).	Liderar la gestión de riesgos de Seguridad Digital.
		Asesorar a los líderes y gestores de procesos en la identificación de riesgos relacionados con Seguridad Digital.
		Comunicar los riesgos de Seguridad Digital a los Líderes y gestores de procesos.
Tercera línea de defensa	Oficina de Control interno	Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y cómo estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
		Revisión de la adecuada definición y alineación de los objetivos institucionales a los objetivos de los procesos que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
		Revisar que se hayan identificado los riesgos significativos que afectan en el cumplimiento de los objetivos de los procesos.
		Identificar y evaluar cambios que podrían tener un impacto significativo en el Sistema de Control Interno durante las evaluaciones periódicas de riesgos y en el curso del trabajo de auditoría interna.
		Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de estos.

Líneas de defensa	Responsable	Responsabilidad frente al riesgo
		Revisar el perfil de riesgo inherente y residual por cada proceso consolidado y pronunciarse sobre cualquier riesgo que se encuentre por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
		Llevar a cabo el seguimiento a los riesgos consolidados en los mapas de riesgos de conformidad con el Plan Anual de Auditoria y reportar los resultados a través de las reuniones del CICCI.
		Revisar que los riesgos de los procesos se encuentren documentados y actualizados en los procedimientos y los planes de mejora como resultado de las auditorías efectuadas, además, que se lleven a cabo de manera oportuna, se establezcan las causas raíz del problema y se evite, en lo posible, la repetición de hallazgos y la materialización de los riesgos.
		Recomendar mejoras a la política de operación de riesgos.

Tabla 5. Líneas de defensa.
Fuente: Adaptado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018

Para seguridad digital: Las inquietudes en la aplicación de la Metodología serán resueltas por el Grupo de Seguridad de la información, bajo el liderazgo de su coordinador.

METODOLOGÍA PARA LA ADMINISTRACIÓN DE RIESGOS

La metodología para la administración del riesgo requiere de un análisis inicial, relacionado con el estado actual de la estructura de riesgos y su gestión en la entidad. Aplica los tres (3) pasos básicos para su desarrollo:

- Política de administración de riesgos
- Identificación de riesgos
- Valoración de riesgos

A continuación, se puede observar la estructura completa con sus desarrollos básicos:

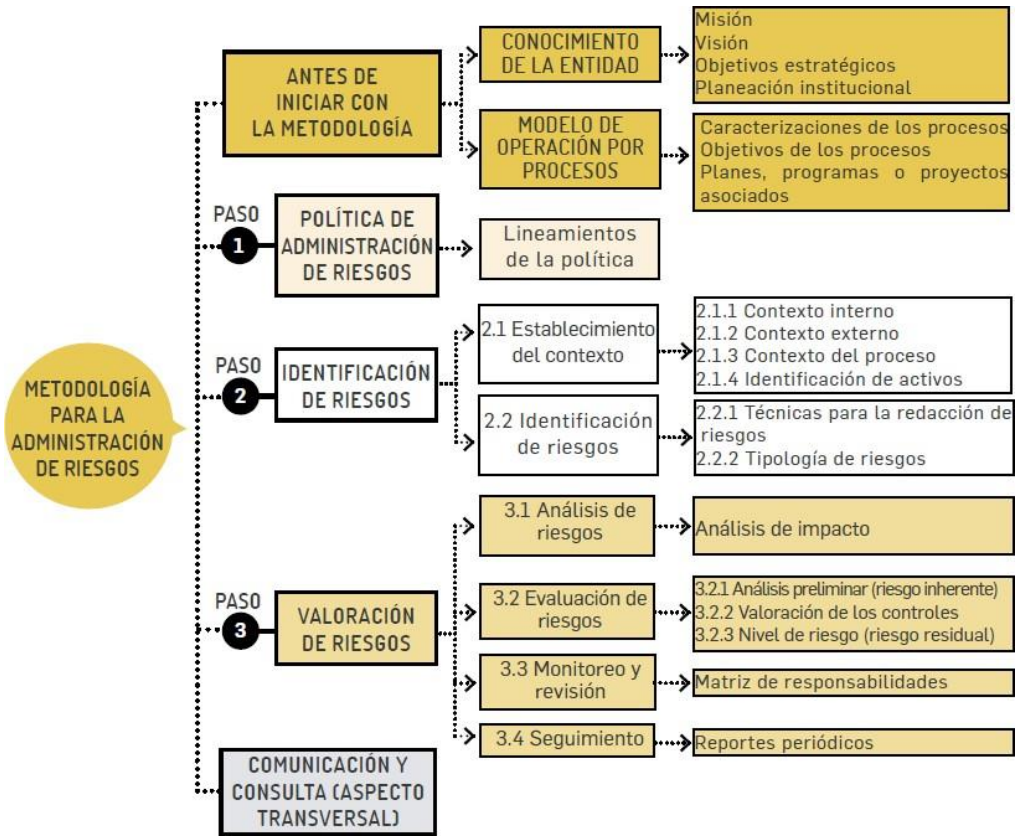


Ilustración 2. Metodología para la administración del riesgo.
Fuente: Tomado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

La UAEAC establece que el comportamiento de los riesgos de la entidad (mapa de riesgos) deben ser revisados mínimo cada trimestre de la vigencia, de acuerdo con los criterios establecidos por los equipos de gerencia (Líderes de proceso y la dirección de la entidad), que busca fortalecer los mecanismos de seguimiento y control a la gestión existente en los procesos, promoviendo la mejora continua, la integridad y la legalidad, en el marco del desarrollo del MIPG- Modelo Integrado de Planeación y Gestión.

IDENTIFICACIÓN DEL RIESGO

Establecimiento del contexto

Para seguridad digital:

Para la identificación de los riesgos de seguridad de la información de la UAEAC, se debe conocer el proceso objeto del levantamiento de información, con el propósito de ejecutar una asesoría oportuna, para la identificación de los riesgos, El Líder del proceso o quien éste delegue, debe ejecutar los siguientes pasos:

- Conocer la caracterización del proceso, disponible en la herramienta del Sistema de Gestión.

- En caso de una actualización, se debe revisar la Matriz de Riesgos de Seguridad Digital (Matriz GINF-6.0-12-XX) del proceso, disponible en la herramienta del Sistema de Gestión.
- Conocer los factores internos y externos que influyen en la probabilidad de ocurrencia del riesgo o el impacto del mismo.

Factores internos y externos

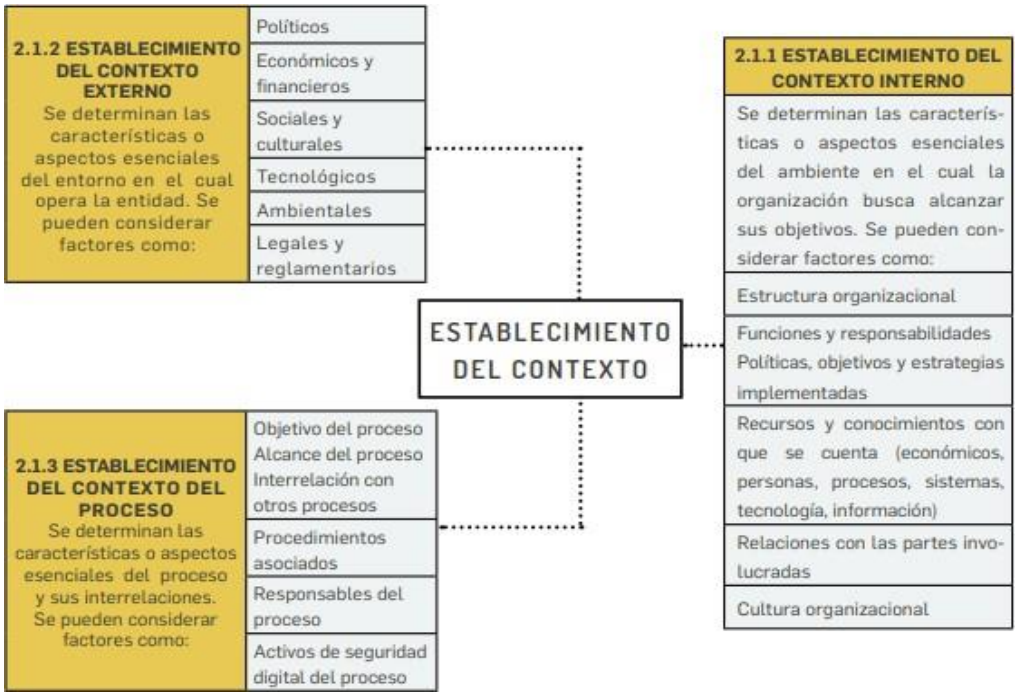


Ilustración 3. Factores internos y externos.
Fuente: Tomado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

Contexto externo	Contexto interno	Contexto del Proceso
•**POLÍTICOS:** Cambios de gobierno, legislación, políticas públicas, regulación. •**ECONÓMICOS Y FINANCIEROS: D**isponibilidad de capital, liquidez, mercados financieros, desempleo, competencia. •**SOCIALES Y CULTURALES: D**emografía, responsabilidad social, orden público. •**TECNOLÓGICOS:** Avances en tecnología, acceso a sistemas de información externos, gobierno en línea. •**AMBIENTALES: E**misiones y residuos, energía, catástrofes naturales, desarrollo sostenible. •**LEGALES Y REGLAMENTARIOS:** Normatividad externa (leyes, decretos, ordenanzas y acuerdos).	•**FINANCIEROS**: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada. •**PERSONAL: C**ompetencia del personal, disponibilidad del personal, seguridad y salud ocupacional. •**PROCESOS: C**apacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento. •**TECNOLOGÍA:** Integridad, confidencialidad y disponibilidad de datos y sistemas, desarrollo, producción o mantenimiento de sistemas de información. •**ESTRATÉGICOS:** Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo. •**COMUNICACIÓN INTERNA: C**anales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones.	•**DISEÑO DEL PROCESO: C**laridad en la descripción del alcance y objetivo del proceso. •**INTERACCIONES CON OTROS PROCESOS: Re**lación precisa con otros procesos en cuanto a insumos, proveedores, productos, usuarios o clientes. •**TRANSVERSALIDAD:** Procesos que determinan lineamientos necesarios para el desarrollo de todos los procesos de la entidad. •**PROCEDIMIENTOS ASOCIADOS:** Pertinencia en los procedimientos que desarrollan los procesos. •**RESPONSABLES DEL PROCESO:** Grado de autoridad y responsabilidad de los funcionarios frente al proceso. •**COMUNICACIÓN ENTRE LOS PROCESOS:** Efectividad en los flujos de información determinados en la interacción de los procesos. •**ACTIVOS DE INFORMACIÓN DEL PROCESO: I**nformación, aplicaciones, hardware, software, bases de datos personales, entre otros, que se deben proteger para garantizar el funcionamiento interno de cada proceso, como de cara al ciudadano.

Ilustración 4. Factores para cada categoría del contexto.
Fuente: Adaptado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

Matriz de Inventario de Activos de Información

Para seguridad digital:

El Líder del proceso o quien éste delegue, debe validar la existencia del Inventario de activos del proceso como insumo para el análisis de riesgos.

Los activos de Información que tengan un nivel de criticidad ***ALTO y MEDIO***, serán a los cuales se les realizará la gestión y tratamiento de riesgos, dejando el registro en la Matriz de Riesgos de Seguridad Digital (Matriz GINF-6.0-12-XX) del proceso objeto de tratamiento.

Identificar el riesgo

La Guía DAFP 2018, emplea las siguientes preguntas claves como parte de la identificación del riesgo:

- **¿QUÉ PUEDE SUCEDER?** Identificar la afectación del cumplimiento del objetivo estratégico o del proceso según sea el caso.
- **¿CÓMO PUEDE SUCEDER?** Establecer las causas a partir de los factores determinados en el contexto.
- **¿CUÁNDO PUEDE SUCEDER?** Determinar de acuerdo con el desarrollo del proceso.
- **¿QUÉ CONSECUENCIAS TENDRÍA SU MATERIALIZACIÓN?** Determinar los posibles efectos por la materialización del riesgo.

Técnicas para la redacción de los Riesgos

Para la redacción del riesgo se deben tener en cuenta los siguientes parámetros:

- Evitar iniciar con palabras negativas como: “No…”, “Que no…”, o con palabras que denoten un factor de riesgo (causa) tales como: “ausencia de”, “falta de”, “poco(a)”, “escaso(a)”, “insuficiente”, “deficiente”, “debilidades en… (tomado de Guía DAFP 2018)”.
- Generar en el lector o escucha la imagen del evento como si ya estuviera sucediendo. (tomado de Guía DAFP 2018).

Tipología de riesgo

Para seguridad digital:

Los riesgos de seguridad digital se basan en la afectación de la Integridad, Confidencialidad o Disponibilidad de los activos de información identificados y valorados en cada proceso de la entidad. Los riesgos de seguridad digital (propiedad afectada) son:

- Pérdida de confidencialidad de los activos de información.
- Pérdida de la integridad de los activos de información.
- Pérdida de la disponibilidad de los activos de información.

Nota: La descripción del riesgo facilita su análisis, relacionando el riesgo(s) de seguridad digital con las causas y las consecuencias que puedan causar su materialización.

La tipología de riesgos depende de la misión de la UAEAC, las normas que regulan su operación, entre otros factores, en la Tabla 2 (Tipología de Riesgos) se describe la clasificación de la Tipología de Riesgos:

TIPOLOGÍA DE RIESGOS	DESCRIPCIÓN
Riesgos estratégicos	Posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
Riesgos gerenciales	Posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
Riesgos operativos	Posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad.
Riesgos financieros	Posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
Riesgos tecnológicos	Posibilidad de ocurrencia de eventos que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
Riesgos de cumplimiento	Posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales.
Riesgo de imagen o reputacional	Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.
Riesgos de corrupción	Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
Riesgos de seguridad digital	Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
Otras tipologías de riesgos	Ambiental, Riesgo seguridad física, Riesgos informáticos, entre otros.

Tabla 6. Tipología de Riesgos.
Fuente: Tomado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018

Para cada riesgo, se debe asociar el grupo de activos específicos del proceso, y conjuntamente analizar las posibles amenazas y causas que podrían producir su materialización. A continuación, se menciona un listado de las causas y amenazas comunes para riesgos de seguridad digital.

Causas

	ID	CAUSAS
1. Recurso Humano	**1.1**	No se hace gestión de vulnerabilidades de la plataforma tecnológica.
	1.2	Ausencia de personal idóneo.
	1.3	Debilidades en las políticas de retiro de personal.
	1.4	Ausencia de capacitaciones periódicas en el uso de los Sistemas de Información.
	1.5	Ausencia de Políticas, Normas, Roles o Procedimientos de Seguridad de la Información.
	1.6	Falta de conciencia en el reporte de incidentes de Seguridad de la Información.
	1.7	Incumplimiento o Desconocimiento de Políticas, Normas, Estándares o Procedimientos de Seguridad de la Información.
	1.8	Falta de conciencia en Seguridad de la Información.
	1.9	Ausencia o incumplimiento de políticas para el buen uso de los servicios informáticos (Red, Correo, Internet, Sistemas de Información, Chat, Skype, Redes Sociales, etc.).
	1.10	Incumplimiento de Procedimientos y Protocolos operativos.
	1.11	Uso inadecuado de software y hardware.
	1.12	Personal inconforme.
	1.13	Ausencia de capacitación o entrenamiento a los Servidores Públicos.
	1.14	Incorrecta asignación de funciones.
	1.15	Ausencia del personal en las capacitaciones o entrenamientos.
	1.16	Falta de capacitación al personal de la UAEAC sobre la operación o funcionamiento de los Sistemas de Información.
	1.17	Falta de documentación técnica sobre los componentes tecnológicos.
	1.18	Enfermedades pandémicas.
2. Procesos	**2.1**	Almacenamiento de información, medios o documentos sin adecuadas medidas de protección.
	2.2	Ausencia de procedimiento formal para la divulgación de información al público.

	ID	CAUSAS
	2.3	Ausencia de procedimientos para clasificar y/o gestionar información.
	2.4	Ausencia de lineamientos de seguridad de la información durante todo el ciclo de vida de la relación contractual entre la Entidad y sus Servidores Públicos sean directos, contratistas, estudiantes en pasantía, terceros o proveedores.
	2.5	Ausencia de pruebas de vulnerabilidad regulares.
	2.6	Ausencia de procedimientos de gestión de parches.
	2.7	Ausencia de rastros de auditoría.
	2.8	Falta de revisión de rastros de auditoría.
	2.9	Inexistencia de la validación de los planes de vuelo registrados en el Sistema de Información.
3. Infraestructura Física	**3.1**	Insuficiencia o mal funcionamiento de controles de acceso físico.
	3.2	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y recintos.
	3.3	Falta de mantenimiento a la infraestructura física.
	3.4	Ubicación en un área susceptible de inundación.
	3.5	Susceptibilidad a la humedad, polvo y suciedad.
	3.6	Susceptibilidad a caída de avión.
	3.7	Susceptibilidad a terremoto o ventisca.
	3.8	Ausencia o deficiencia en los controles para prevención de incendios.
	3.9	Falta de mantenimiento de la planta eléctrica, de las UPS o del aire acondicionado.
4. Sistemas de Información / Servicios informáticos / Información	**4.1**	Gestión deficiente de contraseñas.
	4.2	Asignación errada de privilegios de acceso.
	4.3	Ausencia de mecanismos de identificación y autenticación de usuario.
	4.4	Inadecuada segregación de funciones, roles y perfiles de usuario.
	4.5	Ausencia de un proceso formal para la revisión periódica de los permisos de acceso de los usuarios.
	4.6	Notificación inoportuna de novedades de usuario a Seguridad de la Información.
	4.7	Ausencia de documentación actualizada de los Sistemas de Información.
	4.8	Imposibilidad de actualización de los Sistemas de Información por integración con otros.
	4.9	Ausencia de protección a los datos de producción en los ambientes de prueba.
	4.10	Uso de software desactualizado o que no cumple con los requerimientos de los usuarios.
	4.11	Falta de control en el cumplimiento de estándares de actualización de software.

	ID	CAUSAS
	4.12	Ausencia o insuficiencia de pruebas de software.
	4.13	Conexiones a redes públicas sin mecanismos de protección.
	4.14	Configuraciones por defecto.
	4.15	Los ambientes de pruebas, desarrollo y producción no se encuentran separados.
	4.16	Incapacidad del sistema para atender un alto volumen de conexiones.
	4.17	Ejecución de sesiones simultáneas del mismo usuario en el sistema de información o servicio.
5. Tecnología	**5.1**	Mantenimiento inadecuado o inoportuno de los componentes tecnológicos.
	5.2	Ausencia de mantenimientos preventivos programados.
	5.3	Ausencia o deficiencia en los procedimientos de control de cambios.
	5.4	Ausencia o deficiencia en los procedimientos de notificación de cambios técnicos y operativos al personal y grupos de trabajo.
	5.5	Falta de antivirus y/o antivirus desactualizado.
	5.6	Falta o fallas de sincronización de reloj del servidor.
	5.7	Debilidades en la seguridad perimetral de la red de datos.
	5.8	Arquitectura de red de datos interna insegura.
	5.9	Falta de separación de capas de red (presentación, aplicación, datos).
	5.10	Ausencia de documentación de los puertos que utilizan los Sistemas de Información o Servicios Informáticos.
	5.11	Acceso directo a las Bases de datos de producción.
	5.12	Difusión SSID.
	5.13	Tráfico sensible sin protección o sin cifrado.
	5.14	Ausencia de líneas base para la instalación de los Componentes Tecnológicos.
	5.15	Puertos abiertos a internet con servicios innecesarios.
	5.16	Habilitación de Servicios innecesarios.
	5.17	Ausencia de control para "terminar sesión" luego de un tiempo determinado de inactividad.
	5.18	Ausencia de control sobre dispositivos móviles.
	5.19	Ausencia o deficiencia en los procedimientos de monitoreo a los recursos de procesamiento de información.

	ID	CAUSAS
	5.20	Ausencia de auditorías regulares.
	5.21	Ausencia de Planes de Continuidad o Planes de Recuperación de Desastres (DRP).
	5.22	Ausencia de sistemas redundantes (Alta Disponibilidad).
	5.23	Tener un solo proveedor de Internet.
	5.24	Ausencia de Pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP).
	5.25	Ausencia o insuficiencia de ANS (Acuerdos de Niveles de Servicio).
	5.26	Susceptibilidad a las variaciones de temperatura.
	5.27	Susceptibilidad a las variaciones de voltaje.
	5.28	Versión desactualizada de software y medios de almacenamiento para las Copias de Respaldo.
	5.29	Falta de pruebas de verificación de las copias de respaldo.
	5.30	Ausencia de almacenamiento externo de los medios de almacenamiento para las Copias de Respaldo.
	5.31	Obsolescencia de medios de respaldo y recuperación de información.
	5.32	Obsolescencia Tecnológica.
	5.33	Ausencia de alertas de seguridad en los componentes tecnológicos.
	5.34	Uso de protocolos inseguros.
	5.35	Deficiencia en la capacidad de almacenamiento del correo electrónico.

Tabla 7. Causas comunes.
Fuente: Elaboración propia UAEAC.

Amenazas

En la *Tabla* 4 (Listado de Amenazas), se presenta el listado de amenazas comunes identificadas por la UAEAC:

	ID	Amenazas
1. Recurso Humano	1.1	Empleados inconformes.
	1.2	Sobrecarga laboral.
	1.3	Ingeniería social.
	1.4	Hurto información o medios de soporte.
	1.5	Alta rotación de personal.

	ID	Amenazas
	1.6	Errores Humanos en la operación.
2. Infraestructura Física	2.1	Contaminación, Polvo, Corrosión.
	2.2	Temperatura o humedad extremas.
	2.3	Fallas de electricidad.
	2.4	Señales de interferencia.
	2.5	Daño en instalaciones físicas.
	2.6	Fallas en el aire acondicionado.
	2.7	Fallas en las UPS.
	2.8	Fallas en la planta eléctrica.
	2.9	Desastres naturales.
	2.10	Fuego / Incendio.
	2.11	Agua / Inundación.
	2.12	Asonada/Conmoción civil / Terrorismo.
	2.13	Desastre accidental.
3. Sistemas de Información / Servicios informáticos / Información	3.1	Divulgación no autorizada o robo de Información.
	3.2	Errores Humanos en la operación.
	3.3	Ingeniería social.
	3.4	Interceptación de información o Espionaje Remoto.
	3.5	Recuperación de información de componentes tecnológicos reciclados o desechados.
	3.6	Acceso físico no autorizado.
	3.7	Acceso no autorizado a la información o a componentes tecnológicos.
	3.8	Alteración de la información.
	3.9	Corrupción de los datos.
	3.10	Suplantación de usuarios o Falsificación de derechos de acceso.
	3.11	Uso indebido de la información o los componentes tecnológicos.
	3.12	Abuso de privilegios.
	3.13	Dependencia de servidores públicos críticos.
	3.14	Dependencia de terceras partes.
	3.15	Ausencia de Información.
	3.16	Errores Humanos en el soporte de los Sistemas de Información.
4. Tecnología	4.1	Código malicioso o virus.
	4.2	Denegación de servicios.
	4.3	Fallas en los componentes tecnológicos.
	4.4	Software defectuoso.

	ID	Amenazas
	4.5	Plataforma computacional con múltiples vulnerabilidades.
	4.6	Datos incorrectos.
	4.7	Falla de medios de respaldo y recuperación.
	4.8	Fallas en el aire acondicionado.
	4.9	Actos malintencionados.
	4.10	Ataques o Intrusiones a los componentes tecnológicos.
	4.11	Ejecución de código remoto.
	4.12	Hurto de equipos, medios magnéticos o documentos.
	4.13	Ciberdelincuencia en conexiones de Teletrabajo.

Tabla 8. Listado de Amenazas.
Fuente: Elaboración propia UAEAC.

Consecuencias

Son los efectos ocasionados por la materialización de un riesgo que afecta los objetivos o procesos de la Entidad, pueden ser una pérdida, un daño, un perjuicio o un detrimento.

Para seguridad digital:

En la fase de identificación de riesgos en la Matriz de Riesgos de Seguridad Digital (Matriz GINF-6.0-12-XX), se registra la siguiente información:

- Identificador del activo
- Nombre del activo
- Proceso
- Propietario del riesgo
- Propiedad afectada
- Amenazas
- Causas
- Consecuencias
- Descripción del riesgo

VALORACIÓN DEL RIESGO

Análisis de Riesgos

Para seguridad digital:

El Líder del proceso y el Gestor de Calidad o quien éste delegue, realizan el análisis con base en la información obtenida durante la etapa de identificación del riesgo, se establece la probabilidad de ocurrencia del riesgo y el nivel de impacto, con el fin de valorar la zona de riesgo inicial (riesgo inherente).

Análisis de la probabilidad:

Es la posibilidad de ocurrencia del riesgo durante un cierto período de tiempo o de factibilidad de ocurrencia, teniendo en cuenta la presencia de factores de riesgo, aunque éste no se haya materializado.

Bajo el criterio de FRECUENCIA se analizan el número de eventos en un periodo determinado, se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo.

Bajo el criterio de FACTIBILIDAD se analiza la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que se dé.

Bajo el criterio de PROBABILIDAD, el riesgo se debe medir a partir de las especificaciones según la Tabla 5 (Análisis por probabilidad), a continuación:

ANÁLISIS POR PROBABILIDAD		
Descripción	**Nivel**	**Frecuencia**
Rara vez	1	No se ha presentado en los últimos cinco años.
Improbable	2	Al menos una vez en los últimos cinco años.
Posible	3	Al menos una vez en los últimos dos años.
Probable	4	Al menos una vez en el último año.
Casi seguro	5	Más de una vez al año.

Tabla 9. Análisis por probabilidad.
Fuente: Adaptado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

Nota: Si no se cuenta con datos históricos sobre el número de eventos que se hayan materializado en un periodo de tiempo, se podrá calificar el nivel de probabilidad en términos de factibilidad (factores internos y externos que pueden propiciar el riesgo) y esto se realizará de acuerdo con la experiencia de los responsables que desarrollan el proceso objeto del tratamiento, utilizando la siguiente matriz de priorización de probabilidad (Ver Tabla 6. Matriz de priorización de probabilidad) y teniendo en cuenta los niveles para calificar la probabilidad (ver Tabla 5. Análisis por probabilidad):

N.°	RIESGO	P1	P2	P3	P4	P5	P6	TOTAL	PROMEDIO	RESULTADO
1	Inoportunidad en la adquisición de los bienes y servicios requeridos por la entidad	5	4	3	5	3	4	24	4	PROBABLE
2	Otros riesgos identificados									
3	Otros riesgos									
Convenciones: N.°: Número consecutivo del riesgo - P1: participante 1.										

Tabla 6. Matriz de priorización de probabilidad.
Fuente: Adaptado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018

Análisis por impacto:

Por impacto se entienden las consecuencias que puede ocasionar a la UAEAC la materialización del riesgo para las siguientes variables:

- **Población:** Se define teniendo en cuenta el establecimiento del contexto externo de la entidad, es decir, que la consideración de población va a estar asociada a las personas a las cuales se les prestan servicios o trámites en el entorno digital y que de una u otra forma pueden verse afectadas por la materialización de algún riesgo en los activos identificados (DAFP, 2018).
- **Presupuesto:** Es la consideración de presupuesto afectado por la entidad debido a la materialización del riesgo, contempla sanciones económicas o impactos directos en la ejecución presupuestal (DAFP, 2018).
- **Ambiental:** Estará también alineada con la afectación del medio ambiente por la materialización de un riesgo de seguridad digital. Esta variable puede no ser utilizada en la mayoría de los casos, pero debe tenerse en cuenta, ya que en alguna eventualidad puede existir afectación ambiental (DAFP, 2018).

Niveles para calificar el impacto

De acuerdo con lo establecido en la guía para la administración del riesgo y diseño de controles en entidades públicas (DAFP, 2018); los criterios para calificar el impacto de los riesgos son:

Nivel	Riesgo	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
CATASTRÓFICO		- Impacto que afecte la ejecución presupuestal en un valor ≥50%.	- Interrupción de las operaciones de la Entidad por más de cinco (5) días.

Nivel	Riesgo	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
	- **Seguridad digital** (Genera afectación muy grave de la confidencialidad, integridad y disponibilidad de la información debido al interés particular de funcionarios, contratistas y terceros).	- Pérdida de cobertura en la prestación de los servicios de la entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la entidad.	- Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR	- **Seguridad digital** (Genera afectación grave de la confidencialidad, integridad y disponibilidad de la información debido al interés particular	- Impacto que afecte la ejecución presupuestal en un valor ≥20% - Pérdida de cobertura en la prestación de los servicios de la entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la	- Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno.

Nivel	Riesgo	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
	de funcionarios, contratistas y terceros).	normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la entidad.	- Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
MODERADO	- **Seguridad digital** (Genera afectación leve de la confidencialidad, integridad y disponibilidad de la información debido al interés particular de funcionarios, contratistas y terceros).	- Impacto que afecte la ejecución presupuestal en un valor ≥5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la entidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias
MENOR	- **Seguridad digital** (Genera	- Impacto que afecte la ejecución presupuestal en un valor ≥1%. - Pérdida de cobertura en	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que

Nivel	Riesgo	Impacto (consecuencias) Cuantitativo	Impacto (consecuencias) Cualitativo
	afectación leve de la confidencialidad, integridad o disponibilidad del activo de información analizado).	la prestación de los servicios de la entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥1%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la entidad.	implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE	- **Seguridad digital** (No genera afectación de la confidencialidad, integridad o disponibilidad del activo de información analizado).	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5%. - Pérdida de cobertura en la prestación de los servicios de la entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5% del presupuesto general de la entidad.	- No hay interrupción de las operaciones de la entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Tabla 10. Calificación del impacto.
Fuente: Adaptado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018

Mapa de Calor

En la **¡Error! No se encuentra el origen de la referencia.**), se muestra La calificación dada p ara la probabilidad y el impacto. Para esto, se tiene definido el mapa de calor del riesgo, tal como se muestra a continuación:

MAPA DE CALOR DEL RIESGO						
PROBABILIDAD DE OCURRENCIA	**5 Casi seguro**	Alto (5)	Alto (10)	Extremo (15)	Extremo (20)	Extremo (25)
	4 Probable	Moderado (4)	Alto (8)	Alto (12)	Extremo (16)	Extremo (20)
	3 Posible	Bajo (3)	Moderado (6)	Alto (9)	Extremo (12)	Extremo (15)
	2 Improbable	Bajo (2)	Bajo (4)	Moderado (6)	Alto (8)	Extremo (10)
	1 Rara vez	Bajo (1)	Bajo (2)	Moderado (3)	Alto (4)	Alto (5)
IMPACTO		**1 Insignificante**	**2 Menor**	**3 Moderado**	**4 Mayor**	**5 Catastrófico**

Ilustración 5. Mapa de calor del riesgo.
Fuente: Adaptado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

Para seguridad digital:

El Líder del proceso o quien éste delegue, deben revisar el análisis de riesgos de seguridad digital, reflejado en la Matriz de riesgos. Y de esta forma cumplir con las siguientes actividades:

- Definir la opción de tratamiento de riesgos (Aceptar, Reducir, Transferir, Evitar) más adecuada para la reducción o eliminación del riesgo, teniendo en cuenta la Tabla 8 (Tratamiento a seguir según la zona de riesgo).
- Establecer las acciones concretas a desarrollar conforme a la opción de tratamiento seleccionada para cada riesgo.

ZONA DE RIESGO	NRA	TRATAMIENTO A SEGUIR
Bajo	Aceptable	Asumir
Moderado	Aceptable	Asumir
Alto	No Aceptable	Reducir-Evitar-Compartir
Extremo	No Aceptable	Reducir-Evitar-Compartir

Tabla 11. Tratamiento a seguir según la zona de riesgo.
Fuente: Elaboración propia UAEAC.

En la fase de valoración del riesgo, se registra automáticamente la siguiente información en la Matriz de riesgos de seguridad digital (Matriz GINF-6.0-12-XX):

- Probabilidad (Tabla 5. Análisis por probabilidad).
- Impacto (Tabla 7. Calificación del impacto).
- Zona de riesgo (Generado automáticamente, como resultado de la multiplicación entre la Probabilidad y el Impacto).
- Tratamiento del riesgo.

Evaluación de Riesgos

En esta fase se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (riesgo residual) y evaluar si estos controles se ejecutan como fueron diseñados.

Valoración de Controles

Los controles deben ser definidos, para que den un tratamiento costo efectivo a los riesgos identificados. A continuación, en la Ilustración 5 (Pasos para diseñar un control), se establecen los pasos para diseñar un control:

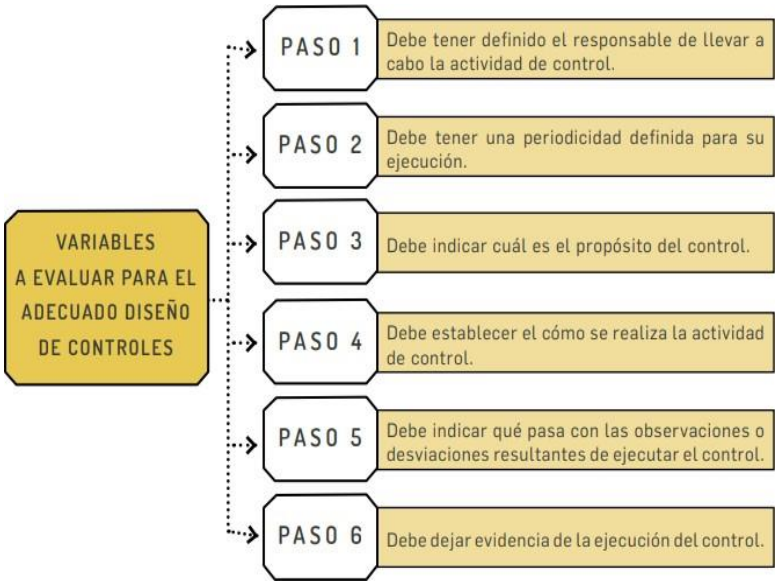


Ilustración 6. Pasos para diseñar un control.
Fuente: Tomado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

Control ISO 27001:2013

Se toma como base las recomendaciones de la norma ISO 27001:2013, en el Anexo A, el cual contiene los controles de seguridad de la información. El control que no esté asociado a los controles contenidos en el Anexo A, se adiciona en el campo otros controles.

Análisis y evaluación del diseño del control

Por cada riesgo inherente, se deben identificar los controles existentes, asimismo, se deben determinar las cualidades y características de cada control, que tienen la posibilidad de disminuir el nivel de riesgo, desplazándolas en el mapa de calor a una zona de riesgo menor a la del riesgo inherente, para determinar si es aceptable su nivel de riesgo residual.

Lo anterior significa que, dependiendo de la efectividad de los controles existentes asociados a la gestión de cada riesgo, se obtiene un nuevo valor de probabilidad y un nuevo valor de impacto.

Criterios para la evaluación del Control, se determinarán por medio de los siguientes parámetros, como se puede observar a continuación, en la *Tabla* 9 (Parámetros de evaluación de efectividad del control existente):

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
1.1 Asignación del responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No Asignado	0
1.2 Segregación y autoridad del responsable	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
		Inadecuado	0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo?, Ej.: verificar, validar, cotejar, comparar, revisar, etc.	Prevenir	15
		Detectar	10
		No es un control	0
4. Cómo se realizó la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15
		No confiable	0

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN	PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	10
		Incompleta	5
		No existe	0

Tabla 12. Parámetros de evaluación de efectividad del control existente.
Fuente: Tomado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

Evaluación del diseño del control

Una vez que el Líder del proceso y el Gestor de Calidad o quien éste delegue, en conjunto con el Coordinador Grupo Organización y Calidad Aeronáutica identifiquen los controles, se debe analizar cada uno de ellos, teniendo en cuenta la Tabla 9. (Parámetros de evaluación de efectividad del control existente), esto con el fin de determinar las calificaciones del control, que se ve reflejado con el desplazamiento del riesgo dentro del mapa de calor. En el caso que el riesgo tenga implementado más de un control, los valores que aportan el grado de efectividad serán promediados.

Cada criterio seleccionado aporta un peso en la evaluación del diseño del control, donde la sumatoria máxima arrojada por los parámetros de es de 100 y la sumatoria mínima es de 0.

Este cálculo debe ser realizado utilizando la Matriz de Riesgos de Seguridad Digital (Matriz GINF-6.0-12-XX).

Rango de calificación del diseño	Resultado – Peso en la evaluación del diseño del control	Resultado- Peso de la ejecución del control
Fuerte	Calificación entre 96 y 100	El control se ejecuta de manera consistente por parte del responsable.
Moderado	Calificación entre 86 y 95	El control se ejecuta algunas veces por parte del responsable.

Rango de calificación del diseño	Resultado – Peso en la evaluación del diseño del control	Resultado- Peso de la ejecución del control
Débil	Calificación entre 0 y 85	El control no se ejecuta por parte del responsable.

Tabla 13. Criterios de evaluación del diseño del control.
Fuente: Tomado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

Tratamiento de riesgos

Para modificar los riesgos de cada proceso, es necesario que los líderes y gestores realicen reuniones en forma trimestral con el objeto de:

- Definir si los riesgos identificados afectan el cumplimiento del objetivo del proceso y de las funciones del área.
- Revisar si los controles definidos son relevantes para eliminar la causa de los riesgos identificados y se encuentran alineados con la metodología adoptada.
- Definir si los controles implementados ayudan a prevenir o detectar la materialización de los riesgos identificados de manera eficaz.
- Identificar la posible materialización del riesgo.

Si en el equipo de gerencia se detectó la desviación de alguno de los puntos mencionados, se debe proceder con la revisión y actualización del mapa de riesgos del proceso a cargo y reportarlo a la segunda y tercera línea de defensa.

Solidez del conjunto de controles para la mitigación del riesgo

Teniendo en cuenta que un riesgo puede tener varias causas al mismo tiempo que varios controles, en este sentido la calificación del riesgo se realiza evaluando el conjunto de controles asociados al riesgo, (Ver Ilustración 6. Solidez del conjunto de controles).

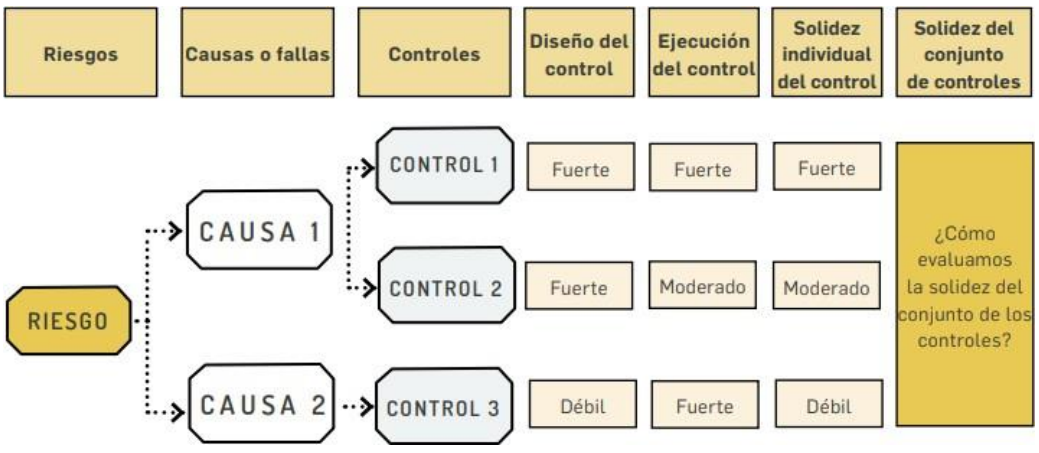


Ilustración 7. Solidez del conjunto de controles.

Fuente: Tomado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

La solidez del conjunto de controles se obtiene calculando el promedio aritmético simple de los controles por cada riesgo, en la Tabla 11 (Calificación de la solidez del conjunto de controles), se clasifica la solidez:

Calificación de la solidez del conjunto de controles	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Tabla 14. Calificación de la solidez del conjunto de controles.
Fuente: Tomado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

Para seguridad digital:

En esta fase se realiza la valoración de controles y se registra la siguiente información en el formato Matriz de Riesgos de Seguridad Digital (Matriz GINF-6.0-12-XX):

- Identificador del control.
- Descripción del control.
- Control del Anexo A de la ISO 27001 (Seguridad digital, ver Anexo A).
- Control independiente del Anexo A de la ISO 27001.
- Cargo Responsable del Control.
- Periodicidad del Control.
- Evidencia.
- Observaciones o desviaciones resultantes de ejecutar el control.
- Naturaleza del control.

En los criterios para la evaluación del Control se registra la siguiente información en la Matriz de Riesgos de Seguridad Digital (Matriz GINF-6.0-12-XX):

- Asignación del responsable.
- Segregación y autoridad del responsable.
- Periodicidad.
- Propósito.
- Cómo se realiza la actividad de control.
- Qué pasa con las observaciones o desviaciones.
- Evidencia de la ejecución del control.

Después de asignar los puntajes en la evaluación del control se genera automáticamente el puntaje final y la valoración del control.

El control es ejecutado por los responsables del riesgo, y para la solidez individual se registra la siguiente información en los campos del formato de la Matriz de Riesgos de Seguridad Digital (Matriz GINF-6.0-12-XX):

- Solidez individual (de cada control).
- Aplica plan de acción para fortalecer el control.
- Solidez del conjunto de los controles.
- Controles que ayudan a disminuir la probabilidad.
- Controles que ayudan a disminuir impacto.

Valoración del riesgo residual

Dependiendo de la efectividad de los controles existentes a la gestión de cada riesgo, se obtiene un nuevo valor de probabilidad y un nuevo valor de impacto, que permitirán determinar el riesgo residual, así como el tipo de tratamiento que se le dará a cada uno de los riesgos de seguridad digital inaceptables. La ilustración No. 7 y la tabla No. 12, presenta los desplazamientos en el mapa de calor según el riesgo residual:

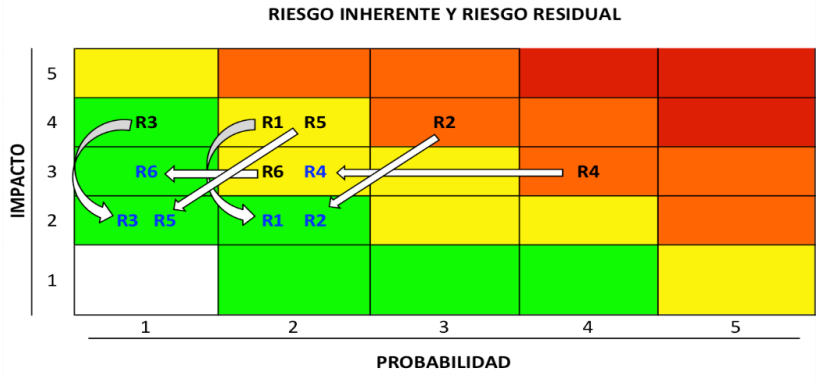


Ilustración 8. Riesgo Residual.
Fuente: Tomado de Blog de Nahun Frett, enlace: http://nahunfrett.blogspot.com/2013/09/riesgo-inherente-versus-riesgo-residual.html

SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	CONTROLES AYUDAN A DISMINUIR LA PROBABILIDAD	CONTROLES AYUDAN A DISMINUIR IMPACTO	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPEJA EN EL EJE DE LA PROBABILIDAD	# COLUMNAS EN LA MATRIZ DE RIESGO QUE SE DESPLAZA EN EL EJE DE IMPACTO
fuerte	directamente	directamente	2	2
fuerte	directamente	indirectamente	2	1
fuerte	directamente	no disminuye	2	0
fuerte	no disminuye	directamente	0	2
moderado	directamente	directamente	1	1
moderado	directamente	Indirectamente	1	0
moderado	directamente	no disminuye	1	0
moderado	no disminuye	directamente	0	1

Tabla 15. Desplazamientos según el riesgo residual.

Fuente: Tomado de la guía para la administración del riesgo y diseño de controles en entidades públicas DAFP versión 2018.

Para seguridad digital:

En esta fase se realiza la valoración del riesgo residual y se registra la siguiente información en la Matriz (Matriz GINF-6.0-12-XX):

- Probabilidad.
- Impacto.
- Nivel del riesgo.

Acciones asociadas al control:

- Acciones.
- Responsable.
- Indicador.

Monitorear y realizar seguimiento

Para seguridad digital:

En esta fase se deben tener en cuenta las siguientes situaciones:

- Modificaciones a los valores de criticidad de los activos de información.
- Nuevas causantes de riesgos (amenazas y vulnerabilidades).
- Incidentes de seguridad digital relacionados con los activos con un nivel de criticidad ***ALTO o MEDIO***.
- Cambios en los factores de riesgo.
- Inclusión de nuevos Activos en la Matriz de Inventario de Activos de Información.
- Cambios en la ubicación de los Activos de Información.
- Cambios en los componentes tecnológicos que soportan el proceso.
- Solicitudes de organismos de control internos o externos.

Comunicación Del Riesgo

Para seguridad digital:

La comunicación del riesgo se genera en las siguientes instancias:

- Al realizar el proceso de gestión de riesgos de seguridad digital, la comunicación es generada por parte del Líder del proceso y el Gestor de Calidad, quedando la comunicación en el repositorio definido para la recolección de evidencias.
- Al materializarse un riesgo de nivel “Alto” o “Extremo” se realiza una reunión con el Líder del proceso, el Gestor de Calidad y los funcionarios que estimen pertinente incluir.
- Anualmente en reunión de revisión por la Alta Dirección.
- En sesiones de capacitación a las partes interesadas.

Formalizar la Matriz de riesgos de seguridad digital

Se debe formalizar la Matriz de riesgos de seguridad digital (Matriz GINF-6.0-12-XX), mediante el levantamiento de un acta, la cual incluye la aprobación del plan de tratamiento de riesgos de seguridad digital y la aceptación del riesgo residual por parte del dueño del riesgo. El acta formalizada queda disponible en la herramienta del Sistema de Gestión de la Entidad en la siguiente documentación:

- Matriz de Riesgos de Seguridad Digital (Matriz GINF-6.0-12-XX).
- Plan de Tratamiento de Riesgos de Seguridad Digital.

CONCLUSIONES

La gestión de seguridad de la información logra sus objetivos si se basa en una aplicación exitosa de la metodología de gestión de riesgos en todos los procesos, de esta forma es fundamental que todos los colaboradores de la UAEAC entiendan y apliquen este documento para una identificación, clasificación, valoración, evaluación y tratamiento efectivo de los riesgos que pueden causar incertidumbre en el cumplimiento de los objetivos de la organización.

GLOSARIO

- **Mapa de Riesgos:** Documento que resume los resultados de las actividades de gestión de riesgos, incluye una representación gráfica en modo de mapa de calor de los resultados de la evaluación de riesgos.
- **Riesgos de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.
- **Riesgos de Gestión:** Posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.
- **Riesgos de Seguridad digital:** Combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.
- **Tolerancia del Riesgo**: Magnitud y tipo de riesgo que una organización está dispuesta a buscar, retener o aceptar**.**

Glosario seguridad digital:

- **Activo:** En el contexto de seguridad digital, son elementos tales como aplicaciones de la organización, servicios web, redes, hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital. (Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018).
- **Aceptación del riesgo:** Decisión informada de tomar un riesgo particular. (ISO/IEC 27001:2013).

- **Administración de Riesgos:** Conjunto de Elementos de Control que, al interrelacionarse, permiten a la Entidad evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos, que permitan identificar oportunidades para un mejor cumplimiento de su función.
- **Alta dirección:** Persona o grupo de personas que dirige y controla una organización, al nivel más alto. **(**ISO/IEC 27001:2013).
- **Amenaza:** Todo elemento o acción capaz de atentar contra la seguridad digital, ejemplo: errores humanos en la operación, divulgación no autorizada o robo de Información, acceso no autorizado a la información o a componentes tecnológicos. Las amenazas en un contexto de seguridad digital incluyen actos dirigidos, o deliberados, ejemplo los realizados por Hackers y sucesos no dirigidos, aleatorios o impredecibles (como puede ser un rayo).
- **Análisis de riesgo:** Proceso para comprender la naturaleza del riesgo y para determinar el nivel de riesgo. (ISO 27000, Glosario de términos y definiciones**).**
- **Apetito al riesgo:** Magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener. (Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018.).
- **Asumir el Riesgo:** Medida de tratamiento del riesgo, en la cual se aceptan las consecuencias del riesgo por considerar muy baja la probabilidad de su ocurrencia, o leves sus consecuencias.
- **Causas:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. (Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018.).
- **Comunicación y consulta de riesgos:** Conjunto de procesos continuos e iterativos que una organización lleva a cabo para proporcionar, compartir u obtener información, y para dialogar con las partes interesadas con respecto a la gestión de riesgos. (ISO 27000, Glosario de términos y definiciones)**.**
- **Compartir o Transferir el riesgo:** Forma de reducir los efectos de un riesgo como medida de tratamiento que permita disminuir las pérdidas originadas por un riesgo trasladándolas o compartiéndolas con un tercero, frente a una probabilidad de ocurrencia de éste.
- **Confidencialidad:** Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. (ISO 27000, Glosario de términos y definiciones).
- **Consecuencias:** Resultado del evento que puede ser cierto o incierto y tener efectos positivos o negativos para la organización y que puede expresarse en términos cualitativos o cuantitativos. Una consecuencia inicial puede tener mayor impacto considerando los efectos secundarios**.** (ISO 31000).
- Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas. ([1] Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018).
- **Control:** Medida que modifica el riesgo (procesos, políticas, dispositivos, prácticas u otras acciones). (Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018.).

- **Controles Detectivos:** Diseñados para identificar un evento o resultado no previsto. Y así detectar la situación no deseada para que se tomen las acciones correctivas, oportunamente. (Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018).
- **Controles Preventivos:** Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos. (Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018).
- **Descripción del Riesgo:** Presentación con el nivel de detalle suficiente para entender el escenario donde una amenaza aprovecha una vulnerabilidad de la seguridad de la información para causar un impacto negativo en la entidad.
- **Disponibilidad**: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.
- **Dueño de proceso**: Rol encargado de la gestión operativa de un proceso. (ITIL® glosario).
- **Efectos:** Constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad, generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos y fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.
- **Efectividad:** La efectividad es el equilibrio entre eficacia y eficiencia.
- **Equipos de Gerencia:** Responsables a nivel de gerencia frente a los riesgos en la primera Línea de defensa.
- **Evaluación de riesgo:** Proceso de comparar los resultados del análisis de riesgo con los criterios de riesgo para determinar si el riesgo y / o su magnitud es aceptable o tolerable. La evaluación de riesgos ayuda en la decisión sobre el tratamiento de riesgos. (ISO 27000, Glosario de términos y definiciones).
- **Evento:** Incidente o situación que ocurre en un lugar determinado durante un período determinado y éste puede ser cierto o incierto y su ocurrencia puede ser única o parte de una serie.
- **Evitar el riesgo:** Emprender acciones que impidan la materialización misma del riesgo.
- **Frecuencia del Riesgo:** Medida estadística del número de veces que se presenta un riesgo en un periodo de tiempo determinado.
- **Gestión de riesgos:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (ISO 27000, Glosario de términos y definiciones).
- **Herramienta del Sistema de Gestión:** (Isolucion) Contiene la caracterización de los procesos y los documentos generales de cada proceso.
- **Identificador del Activo:** Número consecutivo único que identifica el Activo de Información, este identificador es la unión de Código del Macroproceso, el Código del Proceso y el número consecutivo del Activo de información.
- **Identificación de riesgo:** Proceso de búsqueda, reconocimiento y descripción de riesgos. La identificación del riesgo implica la identificación de las fuentes de riesgo, los eventos sus causas y sus posibles consecuencias. La identificación del riesgo puede incluir datos históricos, análisis teóricos, opiniones informadas y de expertos, y las necesidades de los interesados. (ISO 27000, Glosario de términos y definiciones).

- **Infraestructura Crítica Cibernética:** Son las infraestructuras estratégicas soportadas por Tecnologías de Información y Comunicaciones (TIC) o Tecnologías de Operación (TO), cuyo funcionamiento es indispensable, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales. **(**Ministerio de Defensa de Colombia**).**
- **Impacto:** se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo. (Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018).
- **Integridad:** Propiedad de exactitud y completitud de la información. (ISO 27000, Glosario de términos y definiciones).
- **Líder de proceso:** Individuo capaz de motivar, liderar e implementar el cambio organizacional, inspirando en el personal a su cargo confianza, compromiso y conocimiento de los procesos productivos existentes, y de las mejores prácticas en el cumplimiento de las metas.
- **Mapa de riesgos**: Documento con la información resultante de la gestión del riesgo. **(**Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018).
- **Mitigación:** Son todas las medidas y planes que se llevan a cabo ante la posible ocurrencia de un riesgo, permitiendo a su vez esclarecer el panorama de amenazas y la planificación de las acciones a seguir, con el fin de reducir el riesgo futuro.
- **Monitorear**: Verificar, supervisar o medir regularmente el progreso de una actividad, es la acción establecida para identificar los cambios en cada uno de los riesgos.
- **Nivel de riesgo**: Magnitud de un riesgo expresada en términos de la combinación de consecuencias y su probabilidad. (ISO 27000, Glosario de términos y definiciones).
- **Nivel de riesgo aceptable:** Cantidad de riesgo, a nivel global, que la organización está dispuesta a aceptar en el cumplimiento de su misión. (COBIT 5 for Risk).
- **Parte interesada:** Persona u organización que puede afectar, verse afectada o percibirse afectada por una decisión o actividad. (ISO 27000, Glosario de términos y definiciones).
- **Probabilidad:** La posibilidad de ocurrencia del riesgo, esta puede ser medida con criterios de frecuencia o factibilidad.
- **Proceso:** Procesos que realiza una organización que se clasifican en procesos estratégicos, misionales, apoyo, control, de evaluación, entre otros.
- **Propietario de Riesgo:** Persona o entidad con la responsabilidad y autoridad para gestionar un riesgo. (ISO 27000, Glosario de términos y definiciones).
- **Reducción del Riesgo:** Aplicación de controles para reducir las probabilidades de ocurrencia de un evento.
- **Riesgo:** Posibilidad de incurrir en pérdidas económicas, operativas o de imagen, por deficiencias, fallas o por acontecimientos externos que afecten la integridad, disponibilidad o confidencialidad de los Activos de Información.
- **Riesgo Residual**: Riesgo que permanece aún después de aplicados los controles o las acciones de tratamiento y que la Entidad está dispuesta a aceptar, tolerar o asumir en un momento dado.
- **Riesgo Inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. ([1]Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018).

- **Riesgo emergente:** Manifestación novedosa que no se ha experimentado previamente. (Guía de implementación de RIMS Strategic Risk Management).
- **Tolerancia al riesgo:** Son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable. (Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018).
- **Tratamiento de riesgos:** El proceso de selección e implementación de las medidas o controles encaminados a modificar el nivel de los riesgos. (ISO 31000).
- **Usuarios:** aquella persona que utiliza un dispositivo o un ordenador y realiza múltiples operaciones con distintos propósitos.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotado por una o más amenazas. (ISO 27000, Glosario de términos y definiciones).

SIGLAS

CICCI: Comité Institucional de Coordinación de Control Interno.
CIGDI: Comité Institucional de Gestión y Desempeño.
MIPG: Modelo Integrado de Planeación y Gestión.
MECI: Modelo Estándar de Control Interno.
OAP: Oficina Asesora de Planeación.
SG: Sistema de Gestión.

BIBLIOGRAFÍA

- Guía de implementación de RIMS Strategic Risk Management
- Guía para la administración del riesgo y diseño de controles en entidades públicas DAFP, versión 2018.
- NTC/ISO 31000
- NTC/ISO 27000

ANEXOS

ANEXO A NTC/ISO 27001:2013

Dominio	Dominio	Ob. De Control	Ob. De Control	Control	Control
A.5	Política de Seguridad	A.5.1	Política de Seguridad de la Información	A.5.1.1	Políticas para la seguridad de la información.
				A.5.1.2	Revisión de la política de seguridad de la información.
A.6	Organización de la Seguridad de la	A.6.1	Organización interna	A.6.1.1	Seguridad de la información roles y responsabilidades.
				A.6.1.2	Separación de deberes.
				A.6.1.3	Contacto con las autoridades.

Dominio	Dominio	Ob. De Control	Ob. De Control	Control	Control
	Información			A.6.1.4	Contacto con grupos de interés especial.
				A.6.1.5	Seguridad de la información en gestión de proyectos.
		A.6.2	Dispositivos móviles y teletrabajo	A.6.2.1	Política para dispositivos móviles.
				A.6.2.2	Teletrabajo.
A.7	Seguridad de los Recursos Humanos	A.7.1	Antes de asumir el empleo	A.7.1.1	Selección.
				A.7.1.2	Términos y condiciones del empleo.
		A.7.2	Durante la ejecución del empleo	A.7.2.1	Responsabilidades de la dirección.
				A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.
				A.7.2.3	Proceso disciplinario.
		A.7.3	Terminación o cambio de empleo	A.7.3.1	Terminación o cambio de responsabilidades de empleo.
A.8	Gestión de Activos	A.8.1	Responsabilidad por los activos	A.8.1.1	Inventario de activos.
				A.8.1.2	Propiedad de los activos.
				A.8.1.3	Uso aceptable de los activos.
				A.8.1.4	Devolución de activos.
		A:8.2	Clasificación de la información	A.8.2.1	Clasificación de la información.
				A.8.2.2	Etiquetado de la información.
				A.8.2.3	Manejo de activos.
		A.8.3	Manejo de Medios	A.8.3.1	Gestión de medios de soporte removibles.
				A.8.3.2	Disposición de los medios de soporte.
				A.8.3.3	Transferencia de medios de soporte físicos.
A.9	Control de Acceso	A.9.1	Requisitos del Negocio para Control de Acceso	A.9.1.1	Política de control de acceso.
				A.9.1.2	Acceso a redes y a servicios en red.
		A.9.2	Gestión de acceso de usuarios	A.9.2.1	Registro y cancelación del registro de usuarios.
				A.9.2.2	Suministro de acceso de usuarios.

Dominio	Dominio	Ob. De Control	Ob. De Control	Control	Control
				A.9.2.3	Gestión de derechos de acceso privilegiado.
				A.9.2.4	Gestión de información de autenticación secreta de usuarios.
				A.9.2.5	Revisión de los derechos de acceso de usuarios.
				A.9.2.6	Retiro o ajuste de los derechos de acceso.
		A.9.3	Responsabilidades de los usuarios	A.9.3.1	Uso de información de autenticación secreta.
		A.9.4	Control de Acceso a Sistemas y Aplicaciones	A.9.4.1	Restricción de acceso a información.
				A.9.4.2	Procedimiento de ingreso seguro.
				A.9.4.3	Sistema de gestión de contraseñas.
				A.9.4.4	Uso de programas utilitarios privilegiados.
				A.9.4.5	Control de acceso a códigos fuente de programas.
A.10	Criptografía	A.10.1	Controles Criptográficos	A.10.1.1	Política sobre el uso de controles criptográficos.
				A.10.1.2	Gestión de Llaves.
A.11	Seguridad Física y del Entorno	A.11.1	Áreas Seguras	A.11.1.1	Perímetro de seguridad física.
				A.11.1.2	Controles de acceso físico.
				A.11.1.3	Seguridad de oficinas, recintos e instalaciones.
				A.11.1.4	Protección contra amenazas externas y ambientales.
				A.11.1.5	Trabajo en áreas seguras.
				A.11.1.6	Áreas de carga, despacho y acceso público.
		A-11.2	Equipos	A.11.2.1	Ubicación y protección de los equipos.

Dominio	Dominio	Ob. De Control	Ob. De Control	Control	Control
				A.11.2.2	Servicios públicos de soporte.
				A.11.2.3	Seguridad del cableado.
				A.11.2.4	Mantenimiento de los equipos.
				A.11.2.5	Retiro de activos.
				A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.
				A.11.2.7	Disposición segura o reutilización de equipos.
				A.11.2.8	Equipos de usuario desatendido.
				A.11.2.9	Política de escritorio limpio y pantalla limpia.
A.12	Seguridad de las Operaciones	A.12.1	Procedimientos Operacionales y Responsabilidades	A.12.1.1	Documentación de los procedimientos de operación.
				A.12.1.2	Gestión de cambios.
				A.12.1.3	Gestión de la capacidad.
				A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.
		A.12.2	Protección Contra Códigos Maliciosos	A.12.2.1	Controles contra códigos maliciosos.
		A.12.3	Copias de Respaldo	A.12.3.1	Copias de respaldo de la información.
		A.12.4	Registro y Seguimiento	A.12.4.1	Registro de eventos.
				A.12.4.2	Protección de la información de registro.
				A.12.4.3	Registros del administrador y del operador.
				A.12.4.4	Sincronización de relojes.

Dominio	Dominio	Ob. De Control	Ob. De Control	Control	Control
		A12.5	Control de Software Operacional	A.12.5.1	Instalación de software en sistemas operativos.
		A.12.6	Gestión de la Vulnerabilidad Técnica	A.12.6.1	Gestión de las vulnerabilidades técnicas.
				A.12.6.2	Restricciones sobre la instalación de software.
		A.12.7	Consideraciones sobre Auditorias de Sistemas de Información	A.12.7.1	Controles de auditorías de sistemas de información.
A.13	Seguridad de las Comunicaciones	A.13.1	Gestión de la Seguridad de las Redes	A.13.1.1	Controles de redes.
				A.13.1.2	Seguridad de los servicios de red.
				A.13.1.3	Separación en las redes.
		A.13.2	Transferencia de Información	A.13.2.1	Políticas y procedimientos de transferencia de información.
				A.13.2.2	Acuerdos sobre transferencia de información.
				A.13.2.3	Mensajes electrónicos
				A.13.2.4	Acuerdos de confidencialidad o de no divulgación.
A.14	Adquisición, Mantenimiento y Desarrollo de Sistemas	A.14.1	Requisitos de seguridad de los sistemas de información	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información.
				A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas.
				A.14.1.3	Protección de transacciones de servicios de aplicaciones.
		A.14.2	Seguridad en los procesos de desarrollo y soporte	A.14.2.1	Política de desarrollo seguro.
				A.14.2.2	Procedimientos de control de cambios en sistemas.
				A.14.2.3	Revisión técnica de aplicaciones después de

Dominio	Dominio	Ob. De Control	Ob. De Control	Control	Control
					cambios en la plataforma de operaciones.
				A.14.2.4	Restricciones en los cambios a los paquetes de software.
				A.14.2.5	Principios de construcción de los sistemas seguros.
				A.14.2.6	Ambiente de desarrollo seguro.
				A.14.2.7	Desarrollo contratado externamente.
				A.14.2.8	Pruebas de seguridad de sistemas.
				A.14.2.9	Prueba de aceptación de sistemas.
		A.14.3	Datos de prueba	A.14.3.1	Protección de datos de prueba.
A.15	Relaciones con los Proveedores	A.15.1	Seguridad de la información en las relaciones con los proveedores	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores.
				A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.
				A.15.1.3	Cadena de suministro de tecnología de información y comunicación.
		A.15.2	Gestión de la prestación de servicios de proveedores	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores.
				A.15.2.2	Gestión de cambios a los servicios de los proveedores.
A.16	Gestión de Incidentes de Seguridad de la Información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1	Responsabilidades y procedimientos.
				A.16.1.2	Reporte de eventos de seguridad de la información.
				A.16.1.3	Reporte de debilidades de seguridad de la información.
				A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
				A.16.1.5	Respuesta a incidentes de seguridad de la información.

Dominio	Dominio	Ob. De Control	Ob. De Control	Control	Control
				A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.
				A.16.1.7	Recolección de evidencia.
A.17	Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio	A.17.1	Continuidad de Seguridad de la Información	A.17.1.1	Planificación de la continuidad de la seguridad de la información.
				A.17.1.2	Implementación de la continuidad de la seguridad de la información.
				A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
		A.17.2	Redundancias	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.
A.18	Cumplimiento	A.18.1	Cumplimiento de requisitos legales y contractuales	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.
				A.18.1.2	Derechos de propiedad intelectual.
				A.18.1.3	Protección de registros.
				A.18.1.4	Privacidad y protección de información de datos personales.
				A.18.1.5	Reglamentación de controles criptográficos.
		A.18.2	Revisiones de seguridad de la información	A.18.2.1	Revisión independiente de la seguridad de la información.
				A.18.2.2	Cumplimiento con las políticas y normas de seguridad.
				A.18.2.3	Revisión del cumplimiento técnico.

- **Instrumento para el diligenciamiento de la matriz de riesgos:** Instructivo que describe las instrucciones para facilitar el diligenciamiento del instrumento “Matriz de Riesgos de Seguridad Digital”.

OBJETIVO

Describir las instrucciones para facilitar el diligenciamiento del instrumento “Matriz de Riesgos de Seguridad Digital”.

RESPONSABLES

Los funcionarios responsables del desarrollo de las actividades del instructivo son:

Proceso	Responsable
TODOS LOS PROCESOS	Líderes de Proceso – Responsables de la Información
ADMINISTRACIÓN DEL SISTEMA INTEGRADO DE GESTIÓN	Jefe Oficina Asesora de Planeación Coordinador Grupo Organización y Calidad Aeronáutica
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Director de Informática Coordinador Grupo Seguridad de la Información

Tabla 16. Responsables.
Fuente: Elaboración propia

FRECUENCIA

La frecuencia de diligenciamiento de la Matriz de Riesgos de Seguridad Digital se lleva a cabo al menos (3) veces por año o cuando se requiere, por ejemplo: Cuando se presenta un incidente grave o un cambio significativo en el proceso.

FUENTE DE INFORMACIÓN

Las fuentes de información requeridas para diligenciamiento de la Matriz de Riesgos de Seguridad Digital son:

- Los Activos de información.
- La información del sistema de gestión.
- Las entrevistas con los responsables de los procesos.
- Las normas.
- El marco legal y regulatorio.

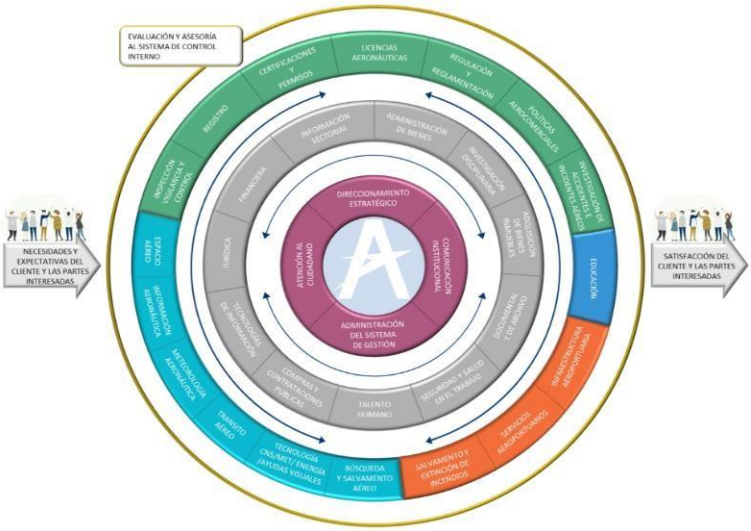
PUNTOS IMPORTANTES

El Líder del Proceso es el responsable del diligenciamiento de la Matriz de Riesgos de Seguridad Digital, esta actividad será apoyada por el Coordinador del Grupo Organización

y Calidad Aeronáutica y cuando sea requerido se solicitará apoyo al Responsable de Seguridad de la Información.

CONTENIDO

A continuación, en la siguiente tabla se detalla la instrucción para el diligenciamiento de la matriz de riesgos de seguridad digital:

ÍTEM	NOMBRE	DESCRIPCIÓN
IDENTIFICACIÓN DEL RIESGO		
1	IDENTIFICADOR DEL ACTIVO	Número consecutivo único que identifica el Activo de Información. Combinación del código del macroproceso, el código del proceso y un número consecutivo, Ejemplo: GSAN-2.2/001.
2	NOMBRE DEL ACTIVO	Nombre del archivo, documento, registro, otros, que identifica el Activo de Información.
3	PROCESO	Se identifica el nombre del Proceso según el mapa de procesos de la UAEAC. 
4	PROPIETARIO DEL RIESGO	Rol encargado de la gestión operativa de un proceso. Es una parte designada de la Entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de la gestión del riesgo.
5	PROPIEDAD AFECTADA	Posibilidad de incurrir en pérdidas económicas, operativas o de imagen, por deficiencias, fallas o por acontecimientos externos si el riesgo se origina en la afectación de la

ÍTEM	NOMBRE	DESCRIPCIÓN
		confidencialidad, la integridad o la disponibilidad de los activos de Información. Selección del tipo de propiedad afectada del riesgo: • Pérdida de confidencialidad del activo de información. • Pérdida de la integridad del activo de información. • Pérdida de la disponibilidad del activo de información.
6	AMENAZAS	Todo elemento o acción capaz de atentar contra la seguridad digital. El anexo No. 2 presenta las amenazas más comunes. Seleccione una opción de la lista sugerida o incluya la amenaza que aplique.
7	CAUSAS	Son todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo. Puede existir más de una causa, razón por la cual se numera cada una. El anexo No. 1 presenta las causas más comunes. Seleccione una opción de la lista sugerida o incluya la causa que aplique.
8	CONSECUENCIAS	Son efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la Entidad, sus grupos de valor y demás partes interesadas. Las consecuencias pueden ser por ejemplo una pérdida, un daño, un perjuicio o un detrimento, entre otros.
9	DESCRIPCIÓN DEL RIESGO	Detalla la información referente al riesgo. Campo de diligenciamiento manual donde se explica cómo se afecta la UAEAC. La descripción del riesgo puede incluir los siguientes campos del registro: • Nombre del activo. • Propiedad afectada. • Causa. • Amenaza. • Consecuencia.
VALORACIÓN DEL RIESGO		
10	PROBABILIDAD	Es la posibilidad de ocurrencia del riesgo durante un cierto período de tiempo. Se debe hacer la selección de las opciones desplegadas. La siguiente Tabla detalla el análisis por probabilidad: **ANÁLISIS POR PROBABILIDAD**

<table>
<tr><th>ÍTEM</th><th>NOMBRE</th><th colspan="3">DESCRIPCIÓN</th></tr>
<tr><td></td><td></td><td>Rara vez</td><td>1</td><td>No se ha presentado en los últimos cinco años.</td></tr>
<tr><td></td><td></td><td>Improbable</td><td>2</td><td>Al menos una vez en los últimos cinco años.</td></tr>
<tr><td></td><td></td><td>Posible</td><td>3</td><td>Al menos una vez en los últimos dos años.</td></tr>
<tr><td></td><td></td><td>Probable</td><td>4</td><td>Al menos una vez en el último año.</td></tr>
<tr><td></td><td></td><td>Casi seguro</td><td>5</td><td>Más de una vez al año.</td></tr>
<tr><td>11</td><td>IMPACTO</td><td colspan="3">Consecuencias que puede ocasionar a la UAEAC la materialización del riesgo. Se debe hacer la selección de las opciones desplegadas:
5. CATASTRÓFICO
4. MAYOR
3. MODERADO
2. MENOR
1. INSIGNIFICANTE
El anexo No.4 detalla el análisis por impacto.</td></tr>
<tr><td>12</td><td>ZONA DE RIESGO</td><td colspan="3">Campo automático. Mapa de calor del riesgo, se muestra la calificación dada para la probabilidad y la calificación dada al impacto, es decir, la evaluación del riesgo. La siguiente tabla detalla el mapa de calor del riesgo.
<table>
<tr><th colspan="7">MAPA DE CALOR DEL RIESGO</th></tr>
<tr><td rowspan="6">PROBABILIDAD DE OCURRENCIA</td><td>5
Casi seguro</td><td>Alto
-5</td><td>Alto
-10</td><td>Extremo
-15</td><td>Extremo
-20</td><td>Extremo
-25</td></tr>
<tr><td>4
Probable</td><td>Moderado
-4</td><td>Alto
-8</td><td>Alto
-12</td><td>Extremo
-16</td><td>Extremo
-20</td></tr>
<tr><td>3
Posible</td><td>Bajo
-3</td><td>Moderado
-6</td><td>Alto
-9</td><td>Extremo
-12</td><td>Extremo
-15</td></tr>
<tr><td>2
Improbable</td><td>Bajo
-2</td><td>Bajo
-4</td><td>Moderado
-6</td><td>Alto
-8</td><td>Extremo
-10</td></tr>
<tr><td>1
Rara vez</td><td>Bajo
-1</td><td>Bajo
-2</td><td>Moderado
-3</td><td>Alto
-4</td><td>Alto
-5</td></tr>
<tr><td colspan="2">IMPACTO</td><td>1
Insignificante</td><td>2
Menor</td><td>3
Moderado</td><td>4
Mayor</td><td>5
Catastrófico</td></tr>
</table></td></tr>
<tr><td>13</td><td>TRATAMIENTO DEL RIESGO</td><td colspan="3">Campo Automático. Establece el tratamiento del riesgo con base en el Nivel de Riesgo Aceptable:

Aceptar o asumir el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo.</td></tr>
</table>

<table>
<tr><th>ÍTEM</th><th>NOMBRE</th><th>DESCRIPCIÓN</th></tr>
<tr><td></td><td></td><td>Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo.
Reducir o Mitigar el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles.
Compartir o transferir el riesgo: Se reduce la probabilidad o el impacto del riesgo, transfiriendo o compartiendo una parte del riesgo.

La siguiente tabla detalla las opciones para el tratamiento del riesgo.

<table>
<tr><th colspan="2">TRATAMIENTO DEL RIESGO</th></tr>
<tr><td>Nivel de riesgo</td><td>Tratamiento a seguir</td></tr>
<tr><td>Bajo</td><td>Asumir</td></tr>
<tr><td>Moderado</td><td>Asumir</td></tr>
<tr><td>Alto</td><td>Reducir – Evitar - Compartir</td></tr>
<tr><td>Extremo</td><td>Reducir – Evitar - Compartir</td></tr>
</table>
</td></tr>
<tr><td colspan="3">VALORACIÓN DE CONTROLES</td></tr>
<tr><td>13</td><td>IDENTIFICADOR DEL CONTROL</td><td>Número de control puede haber uno (1) o varios controles.</td></tr>
<tr><td>14</td><td>DESCRIPCIÓN DEL CONTROL</td><td>Controles que mitigan de manera adecuada los riesgos. Se debe hacer la descripción del control teniendo en cuenta aspectos como:

• Debe indicar cuál es el propósito del control.
• Debe establecer el cómo se realiza la actividad del control.
• Debe indicar que pasa con las observaciones o desviaciones resultantes de ejecutar el control.</td></tr>
<tr><td>15</td><td>Control del Anexo A, de la NTC/ISO 27001:2013</td><td>Lista desplegable de los controles correspondientes al Anexo A, de la norma NTC: ISO/IEC 27001. Contiene los Controles de Seguridad que podrían implementarse para mitigar o minimizar el riesgo. El anexo No.3 detalla la lista despegable de los controles del Anexo A, de la norma NTC: ISO/IEC 27001.</td></tr>
<tr><td>16</td><td>OTROS CONTROLES</td><td>Control definido por la Entidad, que se encuentra por fuera de lo contemplado en el Anexo A, de la norma NTC: ISO/IEC 27001.</td></tr>
</table>

ÍTEM	NOMBRE	DESCRIPCIÓN
17	CARGO RESPONSABLE DEL CONTROL	Indicar el cargo del responsable de la ejecución del control.
18	PERIODICIDAD DEL CONTROL	Lista desplegable que indica el periodo de tiempo en el que se ejecuta el control.
19	EVIDENCIA	Evidencia o rastro de la ejecución del control. Refleja los resultados de su aplicación y la efectividad de su desarrollo.
20	OBSERVACIONES O DESVIACIONES RESULTANTES DE EJECUTAR EL CONTROL.	Descripción de los resultados de la aplicación y la efectividad de los controles.
21	NATURALEZA DEL CONTROL	Lista desplegable que indica la naturaleza del control: PREVENTIVOS: Diseñados para evitar un evento no deseado en el momento en que se produce. DETECTIVOS: Diseñados para identificar un evento o resultado no previsto después de que se haya producido.
22	CRITERIOS PARA LA EVALUACIÓN DEL CONTROL	Se deben determinar las cualidades y características de cada control, que tienen la posibilidad de disminuir el nivel de riesgo. Dependiendo de la efectividad de los controles existentes asociados a la gestión de cada riesgo, se obtiene un nuevo valor de probabilidad y un nuevo valor de impacto. El anexo No.5 detalla los criterios para la evaluación del Control donde se determinarán los parámetros de evaluación de efectividad del control existente.
23	EL CONTROL SE EJECUTA DE MANERA CONSISTENTE POR LOS RESPONSABLES (EJECUCIÓN)	Campo automático. Para su cálculo, toma el resultado del campo Valoración de los controles.
24	SOLIDEZ INDIVIDUAL DE CADA CONTROL	Campo automático. Para su cálculo, toma los valores de los campos Valoración de los controles y El control se ejecuta de manera consistente por los responsables (Ejecución). NOTA:

ÍTEM	NOMBRE	DESCRIPCIÓN
		Dependiendo del resultado del cálculo de este campo, puede tomar algunos de las siguientes opciones: **Controles Fuertes**: El control se ejecuta de manera consistente por parte del responsable. **Controles Moderados**: El control se ejecuta algunas veces por parte del responsable. **Controles Débiles**: El control no se ejecuta por parte del responsable.
25	APLICA PLAN DE ACCIÓN PARA FORTALECER EL CONTROL (SI/NO)	Campo automático. Para su cálculo, toma los valores de los campos Valoración de los controles y El control se ejecuta de manera consistente por los responsables (Ejecución). El campo indica si se debe aplicar un plan de acción para fortalecer el control.
26	SOLIDEZ DEL CONJUNTO DE LOS CONTROLES	Campo automático. Promedia el contenido del campo Solidez individual de cada control.
27	CONTROLES QUE AYUDAN A DISMINUIR LA PROBABILIDAD	Campo automático. Toma el contenido de los campos de, Naturaleza del control y Solidez individual de cada control.
28	CONTROLES QUE AYUDAN A DISMINUIR IMPACTO	Campo automático. Toma el contenido de los campos Naturaleza del control y Solidez individual de cada control.
VALORACIÓN DEL RIESGO RESIDUAL		
29	PROBABILIDAD	Campo automático. Promedia la solidez de los controles. Dependiendo de la efectividad de los controles existentes a la gestión de cada riesgo, se obtiene un nuevo valor de la probabilidad.
30	IMPACTO	Campo automático. Promedia la solidez de los controles. Dependiendo de la efectividad de los controles existentes a la gestión de cada riesgo, se obtiene un nuevo valor del impacto.
31	NIVEL DEL RIESGO	Campo automático. Se muestra la calificación dada para la probabilidad y la calificación dada al impacto "Evaluación del riesgo".
ACCIONES ASOCIADAS AL CONTROL		

ÍTEM	NOMBRE	DESCRIPCIÓN
31	ACCIONES	Establecer las acciones de mejora para los controles definidos en el tratamiento de riesgos. Estas acciones permiten elevar los indicadores de efectividad. Ejemplo: Control: Definir un procedimiento de gestión de parches que cubra toda la plataforma tecnológica. Acciones: Socializar el procedimiento a los funcionarios de la Entidad.
32	RESPONSABLE	Es una parte designada de la Entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad y autoridad para gestionar las acciones de mejora del control.
33	INDICADOR	Establecer el indicador que permita monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control.

Tabla 2. Instrucciones para el diligenciamiento de la matriz de riesgos de seguridad digital.
Fuente: Elaboración propia.

ANEXOS

Anexo No.1 Causas comunes
Anexo No.2 Amenazas más comunes
Anexo No.3 Anexo A Norma NTC: ISO/IEC 27001
Anexo No.4 Análisis por impacto
Anexo No.5 Parámetros de evaluación de efectividad del control existente

LISTADO DE VERSIONES

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
V.1.0	30/07/2020	Se libera la primera versión del presente documento.

Grupo que participó en la elaboración de este documento	Seguridad de la Información.

ELABORADO POR	REVISADO POR	APROBADO POR
Nombre: Responsable:	Nombre: Responsable:	Nombre: Responsable:

Fecha:	Fecha:	Fecha:

Anexo No. 1

CAUSAS COMUNES		
TIPO	ID	ITEM
1. Recurso Humano	**1.1**	No se hace gestión de vulnerabilidades de la plataforma tecnológica.
	1.2	Ausencia de personal idóneo.
	1.3	Debilidades en las políticas de retiro de personal.
	1.4	Ausencia de capacitaciones periódicas en el uso de los Sistemas de Información.
	1.5	Ausencia de Políticas, Normas, Roles o Procedimientos de Seguridad de la Información.
	1.6	Falta de conciencia en el reporte de incidentes de Seguridad de la Información.
	1.7	Incumplimiento de Políticas, Normas, Estándares o Procedimientos de Seguridad de la Información.
	1.8	Falta de conciencia en Seguridad de la Información.
	1.9	Ausencia o incumplimiento de políticas para el buen uso de los servicios informáticos (Red, Correo, Internet, Sistemas de Información, Chat, Skype, Redes Sociales, etc.).
	1.10	Incumplimiento de Procedimientos y Protocolos operativos.
	1.11	Uso inadecuado de software y hardware.
	1.12	Personal inconforme.
	1.13	Ausencia de capacitación o entrenamiento a los Servidores Públicos.
	1.14	Incorrecta asignación de funciones.
	1.15	Ausencia del personal en las capacitaciones o entrenamientos.
	1.16	Falta de capacitación al personal de soporte técnico sobre la operación o funcionamiento de los Sistemas de Información.
	1.17	Falta de documentación técnica sobre los componentes tecnológicos.
	1.18	Enfermedades Pandémicas.
2. Procesos	**2.1**	Almacenamiento de información, medios o documentos sin adecuadas medidas de protección.
	2.2	Ausencia de procedimiento formal para la divulgación de información al público.
	2.3	Ausencia de procedimientos para clasificar y/o gestionar información.
	2.4	Ausencia de lineamientos de seguridad de la información durante todo el ciclo de vida de la relación contractual entre la Entidad y sus Servidores Públicos sean directos, contratistas, estudiantes en pasantía, terceros o proveedores.
	2.5	Ausencia de pruebas de vulnerabilidad regulares.
	2.6	Ausencia de procedimientos de gestión de parches.
	2.7	Ausencia de rastros de auditoría.
	2.8	Falta de revisión de rastros de auditoría.
	2.9	Inexistencia de la validación de los planes de vuelo registrados en el Sistema de Información.

CAUSAS COMUNES		
TIPO	ID	ITEM
3. Infraestructura Física	**3.1**	Insuficiencia o mal funcionamiento de controles de acceso físico.
	3.2	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y recintos.
	3.3	Falta de mantenimiento a la infraestructura física.
	3.4	Ubicación en un área susceptible de inundación.
	3.5	Susceptibilidad a la humedad, polvo y suciedad.
	3.6	Susceptibilidad a caída de avión.
	3.7	Susceptibilidad a terremoto o ventisca.
	3.8	Ausencia o deficiencia en los controles para prevención de incendios.
	3.9	Falta de mantenimiento de la planta eléctrica, de las UPS o del aire acondicionado.
4. Sistemas de Información / Servicios informáticos / Información	**4.1**	Gestión deficiente de contraseñas.
	4.2	Asignación errada de privilegios de acceso.
	4.3	Ausencia de mecanismos de identificación y autenticación de usuario.
	4.4	Inadecuada segregación de funciones, roles y perfiles de usuario.
	4.5	Ausencia de un proceso formal para la revisión periódica de los permisos de acceso de los usuarios.
	4.6	Notificación inoportuna de novedades de usuario a Seguridad de la Información.
	4.7	Ausencia de documentación actualizada de los Sistemas de Información.
	4.8	Imposibilidad de actualización de los Sistemas de Información por integración con otros.
	4.9	Ausencia de protección a los datos de producción en los ambientes de prueba.
	4.10	Uso de software desactualizado o que no cumple con los requerimientos de los usuarios.
	4.11	Falta de control en el cumplimiento de estándares de actualización de software.
	4.12	Ausencia o insuficiencia de pruebas de software.
	4.13	Conexiones a redes públicas sin mecanismos de protección.
	4.14	Configuraciones por defecto.
	4.15	Los ambientes de pruebas, desarrollo y producción no se encuentran separados.
	4.16	Incapacidad del sistema para atender un alto volumen de conexiones.
	4.17	Ejecución de sesiones simultáneas del mismo usuario en el sistema de información o servicio.
5. Tecnología	**5.1**	Mantenimiento inadecuado o inoportuno de los componentes tecnológicos.
	5.2	Ausencia de mantenimientos preventivos programados.
	5.3	Ausencia o deficiencia en los procedimientos de control de cambios.
	5.4	Ausencia o deficiencia en los procedimientos de notificación de cambios técnicos y operativos al personal y grupos de trabajo.
	5.5	Falta de antivirus y/o antivirus desactualizado.
	5.6	Falta o fallas de sincronización de reloj del servidor.

CAUSAS COMUNES		
TIPO	ID	ITEM
	5.7	Debilidades en la seguridad perimetral de la red de datos.
	5.8	Arquitectura de red de datos interna insegura.
	5.9	Falta de separación de capas de red (presentación, aplicación, datos).
	5.10	Ausencia de documentación de los puertos que utilizan los Sistemas de Información o Servicios Informáticos.
	5.11	Acceso directo a las Bases de datos de producción.
	5.12	Difusión SSID.
	5.13	Tráfico sensible sin protección o sin cifrado.
	5.14	Ausencia de líneas base para la instalación de los Componentes Tecnológicos.
	5.15	Puertos abiertos a internet con servicios innecesarios.
	5.16	Habilitación de servicios innecesarios.
	5.17	Ausencia de control para "terminar sesión" luego de un tiempo determinado de inactividad.
	5.18	Ausencia de control sobre dispositivos móviles.
	5.19	Ausencia o deficiencia en los procedimientos de monitoreo a los recursos de procesamiento de información.
	5.20	Ausencia de auditorías regulares.
	5.21	Ausencia de Planes de Continuidad o Planes de Recuperación de Desastres (DRP).
	5.22	Ausencia de sistemas redundantes (Alta Disponibilidad).
	5.23	Tener un solo proveedor de Internet.
	5.24	Ausencia de pruebas de los Planes de Continuidad y/o los Planes de Recuperación de Desastres (DRP).
	5.25	Ausencia o insuficiencia de ANS (Acuerdos de Niveles de Servicio).
	5.26	Susceptibilidad a las variaciones de temperatura.
	5.27	Susceptibilidad a las variaciones de voltaje.
	5.28	Versión desactualizada de software y medios de almacenamiento para las copias de respaldo.
	5.29	Falta de pruebas de verificación de las copias de respaldo.
	5.30	Ausencia de almacenamiento externo de los medios de almacenamiento para las copias de respaldo.
	5.31	Obsolescencia de medios de respaldo y recuperación de información.
	5.32	Obsolescencia tecnológica.
	5.33	Ausencia de alertas de seguridad en los componentes tecnológicos.
	5.34	Uso de protocolos inseguros.
	5.35	Deficiencia en la capacidad de almacenamiento del correo electrónico.

Anexo No. 2

AMENAZAS MAS COMUNES

	ID	Amenazas
1. Recurso Humano	1.1	Empleados inconformes.
	1.2	Sobrecarga laboral.
	1.3	Ingeniería social.
	1.4	Hurto información o medios de soporte.
	1.5	Alta rotación de personal.
	1.6	Errores Humanos en la operación.
2. Infraestructura Física	2.1	Contaminación, Polvo, Corrosión.
	2.2	Temperatura o humedad extremas.
	2.3	Fallas de electricidad.
	2.4	Señales de interferencia.
	2.5	Daño en instalaciones físicas.
	2.6	Fallas en el aire acondicionado.
	2.7	Fallas en las UPS.
	2.8	Fallas en la planta eléctrica.
	2.9	Desastres naturales.
	2.10	Fuego / Incendio.
	2.11	Agua / Inundación.
	2.12	Asonada/Conmoción civil / Terrorismo.
	2.13	Desastre accidental.
3. Sistemas de Información / Servicios informáticos / Información	3.1	Divulgación no autorizada o robo de Información.
	3.2	Errores Humanos en la operación.
	3.3	Ingeniería social.
	3.4	Interceptación de información o Espionaje Remoto.
	3.5	Recuperación de información de componentes tecnológicos reciclados o desechados.
	3.6	Acceso físico no autorizado.
	3.7	Acceso no autorizado a la información o a componentes tecnológicos.
	3.8	Alteración de la información.
	3.9	Corrupción de los datos.
	3.10	Suplantación de usuarios o Falsificación de derechos de acceso.
	3.11	Uso indebido de la información o los componentes tecnológicos.
	3.12	Abuso de privilegios.
	3.13	Dependencia de servidores públicos críticos.
	3.14	Dependencia de terceras partes.
	3.15	Ausencia de Información.

AMENAZAS MAS COMUNES

	ID	Amenazas
1. Recurso Humano	1.1	Empleados inconformes.
	1.2	Sobrecarga laboral.
	1.3	Ingeniería social.
	1.4	Hurto información o medios de soporte.
	1.5	Alta rotación de personal.
	1.6	Errores Humanos en la operación.
	3.16	Errores Humanos en el soporte de los Sistemas de Información.
4. Tecnología	4.1	Código malicioso o virus.
	4.2	Denegación de servicios.
	4.3	Fallas en los componentes tecnológicos.
	4.4	Software defectuoso.
	4.5	Plataforma computacional con múltiples vulnerabilidades.
	4.6	Datos incorrectos.
	4.7	Falla de medios de respaldo y recuperación.
	4.8	Fallas en el aire acondicionado.
	4.9	Actos malintencionados.
	4.10	Ataques o Intrusiones a los componentes tecnológicos.
	4.11	Ejecución de código remoto.
	4.12	Hurto de equipos, medios magnéticos o documentos.
	4.13	Ciberdelincuencia en conexiones de Teletrabajo.

Anexo No. 3

Anexo A Norma NTC: ISO/IEC 27001

ID Dominio	Dominio	ID Control	Ob. De Control	ID Control	Control
A.5	Política de Seguridad	A.5.1	Política de Seguridad de la Información	A.5.1.1	Políticas para la seguridad de la información.
				A.5.1.2	Revisión de la política de seguridad de la información.
A.6	Organización de la Seguridad de la Información	A.6.1	Organización interna	A.6.1.1	Seguridad de la información roles y responsabilidades.
				A.6.1.2	Separación de deberes.
				A.6.1.3	Contacto con las autoridades.
				A.6.1.4	Contacto con grupos de interés especial.
				A.6.1.5	Seguridad de la información en gestión de proyectos.
		A.6.2	Dispositivos móviles y teletrabajo	A.6.2.1	Política para dispositivos móviles.
				A.6.2.2	Teletrabajo.
A.7	Seguridad de los Recursos Humanos	A.7.1	Antes de asumir el empleo	A.7.1.1	Selección.
				A.7.1.2	Términos y condiciones del empleo.
		A.7.2	Durante la ejecución del empleo	A.7.2.1	Responsabilidades de la dirección.
				A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.

Anexo A Norma NTC: ISO/IEC 27001

ID Dominio	Dominio	ID Control	Ob. De Control	ID Control	Control
				A.7.2.3	Proceso disciplinario.
		A.7.3	Terminación o cambio de empleo	A.7.3.1	Terminación o cambio de responsabilidades de empleo.
A.8	Gestión de Activos	A.8.1	Responsabilidad por los activos	A.8.1.1	Inventario de activos.
				A.8.1.2	Propiedad de los activos.
				A.8.1.3	Uso aceptable de los activos.
				A.8.1.4	Devolución de activos.
		A:8.2	Clasificación de la información	A.8.2.1	Clasificación de la información.
				A.8.2.2	Etiquetado de la información.
				A.8.2.3	Manejo de activos.
		A.8.3	Manejo de Medios	A.8.3.1	Gestión de medios de soporte removibles.
				A.8.3.2	Disposición de los medios de soporte.
				A.8.3.3	Transferencia de medios de soporte físicos.
A.9	Control de Acceso	A.9.1	Requisitos del Negocio para Control de Acceso	A.9.1.1	Política de control de acceso.
				A.9.1.2	Acceso a redes y a servicios en red.
		A.9.2	Gestión de acceso de usuarios	A.9.2.1	Registro y cancelación del registro de usuarios.
				A.9.2.2	Suministro de acceso de usuarios.
				A.9.2.3	Gestión de derechos de acceso privilegiado.
				A.9.2.4	Gestión de información de autenticación secreta de usuarios.
				A.9.2.5	Revisión de los derechos de acceso de usuarios.
				A.9.2.6	Retiro o ajuste de los derechos de acceso.
		A.9.3	Responsabilidades de los usuarios	A.9.3.1	Uso de información de autenticación secreta.
		A.9.4	Control de Acceso a Sistemas y Aplicaciones	A.9.4.1	Restricción de acceso a información.
				A.9.4.2	Procedimiento de ingreso seguro.
				A.9.4.3	Sistema de gestión de contraseñas.
				A.9.4.4	Uso de programas utilitarios privilegiados.
				A.9.4.5	Control de acceso a códigos fuente de programas.
A.10	Criptografía	A.10.1	Controles Criptográficos	A.10.1.1	Política sobre el uso de controles criptográficos.
				A.10.1.2	Gestión de Llaves.
A.11	Seguridad Física y del Entorno	A.11.1	Áreas Seguras	A.11.1.1	Perímetro de seguridad física.
				A.11.1.2	Controles de acceso físico.
				A.11.1.3	Seguridad de oficinas, recintos e instalaciones.
				A.11.1.4	Protección contra amenazas externas y ambientales.
				A.11.1.5	Trabajo en áreas seguras.
				A.11.1.6	Áreas de carga, despacho y acceso público.
		A-11.2	Equipos	A.11.2.1	Ubicación y protección de los equipos.
				A.11.2.2	Servicios públicos de soporte.
				A.11.2.3	Seguridad del cableado.
				A.11.2.4	Mantenimiento de los equipos.
				A.11.2.5	Retiro de activos.
				A.11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.

Anexo A Norma NTC: ISO/IEC 27001

ID Dominio	Dominio	ID Control	Ob. De Control	ID Control	Control
				A.11.2.7	Disposición segura o reutilización de equipos.
				A.11.2.8	Equipos de usuario desatendido.
				A.11.2.9	Política de escritorio limpio y pantalla limpia.
A.12	Seguridad de las Operaciones	A.12.1	Procedimientos Operacionales y Responsabilidades	A.12.1.1	Documentación de los procedimientos de operación.
				A.12.1.2	Gestión del cambio.
				A.12.1.3	Gestión de la capacidad.
				A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación.
		A.12.2	Protección Contra Códigos Maliciosos	A.12.2.1	Controles contra códigos maliciosos.
		A.12.3	Copias de Respaldo	A.12.3.1	Copias de respaldo de la información.
		A.12.4	Registro y Seguimiento	A.12.4.1	Registro de eventos.
				A.12.4.2	Protección de la información de registro.
				A.12.4.3	Registros del administrador y del operador.
				A.12.4.4	Sincronización de relojes.
		A12.5	Control de Software Operacional	A.12.5.1	Instalación de software en sistemas operativos.
		A.12.6	Gestión de la Vulnerabilidad Técnica	A.12.6.1	Gestión de las vulnerabilidades técnicas.
				A.12.6.2	Restricciones sobre la instalación de software.
		A.12.7	Consideraciones sobre Auditorias de Sistemas de Información	A.12.7.1	Controles de auditorías de sistemas de información.
A.13	Seguridad de las Comunicaciones	A.13.1	Gestión de la Seguridad de las Redes	A.13.1.1	Controles de redes.
				A.13.1.2	Seguridad de los servicios de red.
				A.13.1.3	Separación en las redes.
		A.13.2	Transferencia de Información	A.13.2.1	Políticas y procedimientos de transferencia de información.
				A.13.2.2	Acuerdos sobre transferencia de información.
				A.13.2.3	Mensajes electrónicos.
				A.13.2.4	Acuerdos de confidencialidad o de no divulgación.
A.14	Adquisición, Mantenimiento y Desarrollo de Sistemas	A.14.1	Requisitos de seguridad de los sistemas de información	A.14.1.1	Análisis y especificación de requisitos de seguridad de la información.
				A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas.
				A.14.1.3	Protección de transacciones de servicios de aplicaciones.
		A.14.2		A.14.2.1	Política de desarrollo seguro.

Anexo A Norma NTC: ISO/IEC 27001

ID Dominio	Dominio	ID Control	Ob. De Control	ID Control	Control
			Seguridad en los procesos de desarrollo y soporte	A.14.2.2	Procedimientos de control de cambios en sistemas.
				A.14.2.3	Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones.
				A.14.2.4	Restricciones en los cambios a los paquetes de software.
				A.14.2.5	Principios de construcción de los sistemas seguros.
				A.14.2.6	Ambiente de desarrollo seguro.
				A.14.2.7	Desarrollo contratado externamente.
				A.14.2.8	Pruebas de seguridad de sistemas.
				A.14.2.9	Prueba de aceptación de sistemas.
		A.14.3	Datos de prueba	A.14.3.1	Protección de datos de prueba.
A.15	Relaciones con los Proveedores	A.15.1	Seguridad de la información en las relaciones con los proveedores	A.15.1.1	Política de seguridad de la información para las relaciones con proveedores.
				A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores.
				A.15.1.3	Cadena de suministro de tecnología de información y comunicación.
		A.15.2	Gestión de la prestación de servicios de proveedores	A.15.2.1	Seguimiento y revisión de los servicios de los proveedores.
				A.15.2.2	Gestión de cambios a los servicios de los proveedores.
A.16	Gestión de Incidentes de Seguridad de la Información	A.16.1	Gestión de incidentes y mejoras en la seguridad de la información	A.16.1.1	Responsabilidades y procedimientos.
				A.16.1.2	Reporte de eventos de seguridad de la información.
				A.16.1.3	Reporte de debilidades de seguridad de la información.
				A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
				A.16.1.5	Respuesta a incidentes de seguridad de la información.
				A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información.
				A.16.1.7	Recolección de evidencia.
A.17	Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio	A.17.1	Continuidad de Seguridad de la Información	A.17.1.1	Planificación de la continuidad de la seguridad de la información.
				A.17.1.2	Implementación de la continuidad de la seguridad de la información.
				A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
		A.17.2	Redundancias	A.17.2.1	Disponibilidad de instalaciones de procesamiento de información.
A.18	Cumplimiento	A.18.1	Cumplimiento de requisitos legales y contractuales	A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales.
				A.18.1.2	Derechos de propiedad intelectual.
				A.18.1.3	Protección de registros.
				A.18.1.4	Privacidad y protección de información de datos personales.

Anexo A Norma NTC: ISO/IEC 27001					
ID Dominio	**Dominio**	**ID Control**	**Ob. De Control**	**ID Control**	**Control**
				A.18.1.5	Reglamentación de controles criptográficos.
		A.18.2	Revisiones de seguridad de la información	A.18.2.1	Revisión independiente de la seguridad de la información.
				A.18.2.2	Cumplimiento con las políticas y normas de seguridad.
				A.18.2.3	Revisión del cumplimiento técnico.

Anexo No. 4

ANÁLISIS POR IMPACTO		
Nivel	**Impacto (consecuencias) Cuantitativo**	**Impacto (consecuencias) Cualitativo**
CATASTRÓFICO (5)	- Impacto que afecte la ejecución presupuestal en un valor ≥50%. - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥50%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥50%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥50% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por más de cinco (5) días. - Intervención por parte de un ente de control u otro ente regulador. - Pérdida de Información crítica para la Entidad que no se puede recuperar. - Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. - Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.
MAYOR (4)	- Impacto que afecte la ejecución presupuestal en un valor ≥20%. - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥20%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥20%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥20% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por más de dos (2) días. - Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. - Sanción por parte del ente de control u otro ente regulador. - Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. - Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.

ANÁLISIS POR IMPACTO		
Nivel	**Impacto (consecuencias) Cuantitativo**	**Impacto (consecuencias) Cualitativo**
MODERADO (3)	- Impacto que afecte la ejecución presupuestal en un valor ≥5% - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥10%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥5% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por un (1) día. - Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la Entidad. - Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. - Reproceso de actividades y aumento de carga operativa. - Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. - Investigaciones penales, fiscales o disciplinarias.
MENOR (2)	- Impacto que afecte la ejecución presupuestal en un valor ≥1% - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥5%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥1% - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥1% del presupuesto general de la Entidad.	- Interrupción de las operaciones de la Entidad por algunas horas. - Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. - Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
INSIGNIFICANTE (1)	- Impacto que afecte la ejecución presupuestal en un valor ≥0,5% - Pérdida de cobertura en la prestación de los servicios de la Entidad ≥1%. - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la Entidad en un valor ≥0,5%. - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador, las cuales afectan en un valor ≥0,5%del presupuesto general de la Entidad.	- No hay interrupción de las operaciones de la Entidad. - No se generan sanciones económicas o administrativas. - No se afecta la imagen institucional de forma significativa.

Anexo No. 5

PARÁMETROS DE EVALUACIÓN DE EFECTIVIDAD DEL CONTROL EXISTENTE			
CRITERIO DE EVALUACIÓN	**ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL**	**OPCIÓN DE RESPUESTA AL CRITERIO DE EVALUACIÓN**	**PESO EN LA EVALUACIÓN DEL DISEÑO DEL CONTROL**

1.1 Asignación del responsable	¿Existe un responsable asignado a la ejecución del control?	Asignado	15
		No Asignado	0
1.2 Segregación y autoridad del responsable	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?	Adecuado	15
		Inadecuado	0
2. Periodicidad	¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?	Oportuna	15
		Inoportuna	0
3. Propósito	¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo?, Ej.: verificar, validar, cotejar, comparar, revisar, etc.	Prevenir	15
		Detectar	10
		No es un control	0
4. Cómo se realizó la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable	15
		No confiable	0
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven oportunamente	15
		No se investigan y resuelven oportunamente	0
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa	10
		Incompleta	5
		No existe	0

- **Matriz para la gestión de riesgos de Seguridad Digital:** Es un formato en Excel para la gestión de riesgos de seguridad Digital.

Pestaña: Riesgos de Seguridad Digital

AERONÁUTICA CIVIL
UNIDAD ADMINISTRATIVA ESPECIAL

FORMATO

MATRIZ PARA LA GESTIÓN DE RIESGOS

Principio de Procedencia: 3403-20 **Clave:** XXXXXXX **Versión:** 1.0

IDENTIFICACIÓN DEL RIESGO								
IDENTIFICADOR DEL ACTIVO	NOMBRE DEL ACTIVO	PROCESO	PROPIETARIO DEL RIESGO	PROPIEDAD AFECTADA	AMENAZAS	CAUSAS	CONSECUENCIAS	DESCRIPCIÓN DEL RIESGO

VALORACIÓN DE CONTROLES																								
Identificador del Control	Descripción del Control	Control del Anexo A, de la NTC/ISO 27001:2013	Otros Controles	Cargo Responsable del Control	Periodicidad del Control	Evidencia	Observaciones o desviaciones resultantes de ejecutar el control	Naturaleza del control	CRITERIOS PARA LA EVALUACIÓN DEL CONTROL							Valoración de los Controles		El control se ejecuta de manera consistente por los responsables (Ejecución)		Solidez individual de cada control		Aplica plan de acción para fortalecer el control (SI/NO)	Solidez del conjunto de los controles	Controles que ayudan a disminuir la probabilidad	Controles que ayudan a disminuir impacto
									1.1	1.2	2	3	4	5	6										

VALORACIÓN DEL RIESGO RESIDUAL			ACCIONES ASOCIADAS AL CONTROL		
PROBABILIDAD	IMPACTO	NIVEL DEL RIESGO	ACCIONES	RESPONSABLE	INDICADOR

- **Matriz de Riesgos GINF 6.0:** En este instrumento se gestionan los riesgos de los Activos de Información del proceso Gestion de Tecnologías de la Información - GINF 6.0.

Principio de Procedencia: 3403-20	**Clave:** XXXXXXX	**Versión:** 01

PROCESO	PROPIETARIO DEL RIESGO	ACTIVOS AFECTADOS	AMENAZAS	CAUSAS	CONSECUENCIAS	NOMBRE DEL RIESGO	DESCRIPCIÓN DEL RIESGO	ANÁLISIS DEL RIESGO INHERENTE						Descripción del Control	Cargo Responsable del Control	Periodicidad del Control
								PROBABILIDAD		IMPACTO		ZONA DE RIESGO	TRATAMIENTO DEL RIESGO			
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Toda la Información del proceso de Gestión de tecnologías de la Información	Incumplimiento en el establecimiento de políticas y reglas de seguridad de la información	Falta de participación en la creación y actualización de las políticas de seguridad de la información	Sanciones legales por el incumplimiento ante los entes de control por la divulgación de información. Retraso	Confidencialidad	Perdida de confidencialidad de la información debido a la incapacidad de implementar adecuadament	3	Posible	4	Mayor	Extremo	Reducir	Incluir a TI. En la definición y actualización de las políticas de seguridad de la información		

					en las operaciones		e los controles técnicos para garantizar el cumplimiento de las políticas debido a la falta de participación en la definición de las políticas									
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Toda la Información del proceso de Gestión de tecnologías de la Información	Compromiso de la información soportada por los activos de información	Falta de contacto con grupos de interés enfocados en temas de seguridad de la información	Retraso en las operaciones por el compromiso de los activos de información	Confidencialidad	Perdida de confidencialidad de la información, debido a la falta de implementación de actualizaciones	4	Probable	3	Moderado	Alto	Reducir	Establecer contacto con los grupos de interés y fabricantes de los sistemas de informa		

							, parches de seguridad, nuevas configuraciones y controles adicionales reportados por los grupos de interés enfocados a seguridad de la información							ción, enfocados en temas de seguridad de la información con el fin de recibir información oportuna acerca de actualizaciones, parches de seguridad, nuevas configuraciones y controles adicionales para mitigar vulnerabilidades		

														emergentes		
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Toda la Información del proceso de Gestión de tecnologías de la Información	Divulgación de información Clasificada o reservada	Desconocimiento del proceso disciplinario en caso de tener responsabilidad en un incidente de seguridad	Sanciones legales por el incumplimiento ante los entes de control por la divulgación de informaci ón.	Confidencialidad	Perdida de confidencialidad de la información, debido a la divulgación de información clasificada y reservada por desconocimiento de las sanciones disciplinarias por parte de los colaboradores	3	Posible	4	Mayor	Extremo	Reducir	Realizar campañas de concientización y divulgación acerca del proceso disciplinario y las sanciones disciplinarias a las que se ve expuesto un colaborador que tenga responsabilidad en un incidente de seguridad de la información		

GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Información	Compromiso de la información soportada por los activos de información	El inventario de activos de información no se actualiza en sincronía con la adquisición de nuevos equipos o sistemas de información	Sanciones legales por el incumplimiento ante los entes de control por la divulgación de información. Retraso en las operaciones	Confidencialidad	Perdida de confidencialidad de la información soportada por los activos de información, que no son incluidos ni actualizados en el inventario de activos de información cuando son adquiridos o implementados nuevos activos impidiendo tener	3	Posible	3	Moderado	Alto	Reducir	Actualizar el inventario de activos de información cada vez que se adquiera o modifique un activo de información		

							un control sobre los controles implementados									
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Toda la Información del proceso de Gestión de tecnologías de la Información	Compromiso de la información soportada por los activos de información	Ausencia de pruebas de seguridad Informática a los nuevos sistemas de información y las actualizaciones antes de ser llevados a producción	Sanciones legales por el incumplimiento ante los entes de control por la divulgación de información. Retraso en las operaciones	Confidencialidad	Perdida de confidencialidad de la información soportada por los sistemas de información y las nuevas actualizaciones de estos, al presentar vulnerabilidades de seguridad que no fueron	3	Posible	3	Moderado	Alto	Reducir	Incluir una cláusula en los contratos con proveedores de software que permita el derecho a auditar los sistemas de información desarrollados por terceros. Incluir la entrega		

							identificadas por medio de pruebas de seguridad informáticas						de los resultados de pruebas de seguridad de la información para nuevos sistemas de información y nuevas funcionalidades		
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Toda la Información del proceso de Gestión de tecnologías de la Información	Divulgación de información Clasificada o reservada	No se realiza el etiquetado de la información de acuerdo a su clasificación	Sanciones legales por el incumplimiento ante los entes de control por la divulgación de información.	Confidencialidad	Perdida de la confidencialidad de la información debido al tratamiento inadecuado de esta, por el desconocimiento del nivel de	3	Posible	3	Moderado	Alto	Reducir	Establecer un procedimiento de etiquetado de la información Etiquetar la información en medios físicos o digitales, con		

							clasificación que tiene debido a la falta de etiquetas visuales						etiquetas visuales de la clasificación del nivel de confidencialidad de la información		
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Toda la Información del proceso de Gestión de tecnologías de la Información	Divulgación de información Clasificada o reservada	Almacenamiento de información de la UAEAC en discos duros locales de equipos de cómputo personales de los colaboradores de la entidad	Sanciones legales por el incumplimiento ante los entes de control por la divulgación de información.	Confidencialidad	Perdida de la confidencialidad de la información debido al almacenamiento en discos duros locales en equipos de cómputo personales que pueden ser accedid	3	Posible	3	Moderado	Alto	Reducir	Establecer un repositorio de información centralizado accesible para todos los colaboradores con una gestión de acceso basada en roles y perfiles de acuerdo al nivel de		

							os por terceros						acceso que debe tener cada colaborador		
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Toda la Información del proceso de Gestión de tecnologías de la Información	Eliminación o perdida de la información	Almacenamiento de información en discos duros locales de los equipos de cómputo asignados por la UAEAC y equipos de cómputo personales de los colaboradores	Retraso en las operaciones Perdida reputacional	Disponibilidad	Pérdida de la disponibilidad de la información por eliminación o daño de los discos duros locales de equipos de cómputo asignados por la UAEAC	3	Posible	3	Moderado	Alto	Reducir	Restringir el almacenamiento de información en los discos duros locales.		

GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Toda la Información del proceso de Gestión de tecnologías de la Información	Incumplimiento el tratamiento de la información	Todos los colaboradores de la UAEAC no cuentan con VPN para acceder a la red y la información centralizada de la entidad	Retraso en las operaciones	Disponibilidad	Perdida de la disponibilidad de la información debido a la imposibilidad de almacenarla en un repositorio centralizado ya que no se tiene acceso vía VPN a la red de la UAEAC	4	Probable	3	Moderado	Alto	Reducir	Configurar y entregar un manual y las claves de acceso vía VPN a todos los colaboradores de la entidad		
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Activos de tipo hardware del proceso de Gestión de tecnol	Eventos naturales	Las alarmas de incendio del Datacenter no funcionan Fallas	Retraso en las operaciones	Disponibilidad	Perdida de la disponibilidad de la información debido a un evento natural	3	Posible	3	Moderado	Alto	Reducir	Datacenter certificado mínimo como TIER III o certificaciones		

		ogías de la Información		en la UPS del Data Center			que afecte los activos de información del Data Center							similares		
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Toda la Información del proceso de Gestión de tecnologías de la Información	Abuso de los derechos de acceso	No se cuenta con una gestión de roles y perfiles de acceso a la información y a los sistemas de información centralizada, basada en las labores que desempeña cada uno de los colabor	Sanciones legales por el incumplimiento ante los entes de control por la divulgación de información. Perdida reputacional por la divulgación de información clasificada y reservada	Confidencialidad	Perdida de la confidencialidad de la información debido al acceso no autorizado, por la deficiencia en la identificación en el perfil y los niveles de acceso a la información que	4	Probable	4	Mayor	Extremo	Reducir	Establecer un listado de perfiles y roles y los niveles de acceso a la información, que debería tener cada uno de los colaboradores de acuerdo con sus labores dentro de la entidad		

				adores, ni se ha establecido el nivel de acceso que debería tener cada colaborador definidos por los dueños de la información			debe tener cada colaborador							definido por los dueños de la información Solución de gestión de identidades y acceso centralizada		
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Activos de tipo software y servicios del proceso de Gestión de tecnologías de la Información	Mal funcionamiento del software	No se aplica ni se tiene documentado el ciclo de vida para los diferentes sistemas de información	Sanciones legales por el incumplimiento ante los entes de control por la divulgación de informacion. Perdida reputacional por la divulgación de	Confidencialidad	Perdida de la confidencialidad de la información tratada por los sistemas de información, debido a la falta de identificación de los	3	Posible	3	Moderado	Alto	Reducir	Documentar y aplicar el ciclo de vida de los sistemas de información contemplando aspectos de seguridad de la información en cada		

					información clasificada y reservada		controles de seguridad adecuados en cada una de las fases del ciclo de vida de los sistemas de información							una de sus fases		
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Activos de tipo software y servicios del proceso de Gestión de tecnologías de la Información	Mal funcionamiento del hardware o software	No se tiene formalizado y documentado un procedimiento de gestión de la capacidad, para planificar el aumento o	Retraso en las operaciones Perdida reputacional	Disponibilidad	Perdida de disponibilidad de la información tratada por los activos de información, debido al exceso de las capacid	3	Posible	3	Moderado	Alto	Reducir	establecer un procedimiento documentado para la gestión de las capacidades tecnológicas		

	Coordinador Grupo Proyectos de Tecnología de Información			disminución de las capacidades tecnológicas, Los administradores realizan las solicitudes a su discreción.			ades tecnológicas	4	Probable	3	Moderado	Alto	Reducir	Realizar la revisión a intervalos planificados de las capacidades tecnológicas y realizar las estimaciones adecuadas en crecimiento o decrecimiento.		
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Activos de tipo software y servicios del proceso de Gestión de tecnologías de la	Corrupción de datos	No existen restricciones de acceso a los logs para los administradores de los sistemas de información	Pérdida reputacional	Integridad	Pérdida de la integridad de los registros de auditoria (Logs) de los diferentes sistemas de	3	Posible	3	Moderado	Alto	Reducir	Implementar restricciones de modificación a los logs de los diferentes sistemas de información.		

		Información					información, debido a que estos pueden ser accedidos y modificado por los Administradores									
GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Exchange Online (Correo electrónico)	Suplantación de usuarios	Para el correo electrónico se asigna una clave de acceso por defecto y no se obliga al usuario a realizar el cambio en su primer inicio de sesión	Sanciones legales por el incumplimiento ante los entes de control por la divulgación de información.	Confidencialidad	Perdida de la confidencialidad de la información del correo electrónico por el acceso de un tercero debido al uso de credenciales por defecto	3	Posible	3	Moderado	Alto	Reducir	Configurar el correo electrónico para que fuerce al usuario a cambiar su contraseña después del primer inicio de sesión		

GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN	Coordinador Grupo Proyectos de Tecnología de Información	Exchange Online (Correo electrónico)	Suplantación de usuarios	No se tiene habilitados los protocolos y políticas para el correo electrónico: SPF, DKIM y DMARC	Retraso en las operaciones Perdida reputacional	Integridad	Perdida de la integridad de la información del correo electrónico por la suplantación de un tercero debido a la falta de vinculación de un nombre de dominio a una dirección de correo y mensaje electrónicos especifico	3	Posible	4	Mayor	Extremo	Reducir	Habilitar y configurar los estándares SPF, DKIM y DMARC para todos los mensajes de correo electrónico		

CONCLUSIONES

Para realizar el diagnóstico del estado actual de la Entidad frente al SGSI y diseñar un modelo de gestión de seguridad de la información, se basó en las principales herramientas y en las mejores prácticas a nivel internacional como lo son las normas ISO/IEC 27001, ISO/IEC 27002 e ISO/27005 y las guías de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI de MinTic, lo cual permitió evidenciar que la Aerocivil se encuentra en un 20% de madurez en la gestión de seguridad de la información frente a lo establecido por MinTic, a su vez permitió descubrir puntos vulnerables de la entidad y proveer herramientas valiosas para diseñar procedimientos fuertes de seguridad.

El diseño de la política general y las políticas específicas del SGSI, fueron basadas en los lineamientos dados en las guías de implementación del Modelo de seguridad y privacidad de la información (MSPI) de MinTic, específicamente en la Guía No. 2 - Elaboración de la política general de seguridad y privacidad de la información, estas políticas han sido definidas para establecer el comportamiento que debe tener cada uno de los funcionarios responsables de la información y usuarios de Activos de Información, en el manejo de la información y de los componentes tecnológicos de la Entidad.

Se logró una metodología de Gestión de Activos de Información basada en la Guía No. 5 de MinTic. Guía para la Gestión y Clasificación de Activos de Información, con la cual se establecen las actividades para la identificación, actualización, clasificación y valoración del inventario de Activos de Información de la UAEAC, a fin de salvaguardar su confidencialidad, integridad y disponibilidad.

Con el fin de gestionar los riesgos de seguridad de la información, se diseñó una metodología basada en la Guía No. 7 - Guía de gestión de riesgos de MinTic y la Guía para la administración del riesgo y el diseño de controles en entidades públicas del Departamento Administrativo de la Función Pública – DAPF.

La gestión de seguridad de la información logra sus objetivos si se basa en una aplicación exitosa de la metodología de gestión de riesgos en todos los procesos, de esta forma es fundamental que todos los colaboradores de la UAEAC entiendan y apliquen estas técnicas para una identificación, clasificación, valoración, evaluación y tratamiento efectivo de los riesgos que pueden causar incertidumbre en el cumplimiento de los objetivos de la organización.

RECOMENDACIONES

Para el diseño de un Sistema de Gestión de Seguridad de la Información – SGSI, se recomienda basarse en los lineamientos de MinTic sobre el Modelo de Seguridad y Privacidad de la Información – MSPI ya que presenta 21 guías que permiten abordar de manera detallada cada una de las fases del modelo.

Se debe realizar una evaluación de seguridad de la información mínimo cada año con el fin de identificar el nivel de madurez en la implementación del Modelo de seguridad y privacidad de la información, permitiendo así establecer el estado de la gestión y adopción de controles técnicos y administrativos al interior de las Entidades.

Es necesario tener un inventario de los activos de información, lo cual permite clasificarlos y estar al tanto de a cuáles se les debe brindar mayor protección, pues se identifican claramente sus características y rol al interior de un proceso, este inventario debe ser actualizado cada que ingrese o que se decida eliminar un nuevo activo o por lo menos actualizarlo cada año, dado que es un insumo para la evaluación de riesgos en seguridad de la información siendo una buena práctica realizar esta gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA.

BIBLIOGRAFÍA

ALCALDIA DE BOGOTÁ. [www.alcaldiabogota.gov.co]. Bogotá: ALCALDIA DE BOGOTÁ, documentos para TELECOMUNICACIONES. Tecnologías de la Información y las Comunicaciones-TIC. [Consulta realizada en mayo del 2020]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/listados/tematica2.jsp?subtema=28474&cadena=t.

COLOMBIA. CORTE CONSTITUCIONAL. Constitución Política de Colombia. Actualizada con los Actos Legislativos a 2015. Artículo 15.2003. Bogotá: La Corte. Disponible en: https://www.corteconstitucional.gov.co/inicio/Constitucion%20politica%20de%20Colombia%20-%202015.pdf.

COLOMBIA. DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. [www.funcionpublica.gov.co]. Bogotá: DAFP, Guía para la Administración del Riesgo. Dirección de control interno y racionalización de trámites. Colombia. Cuarta edición. 2011. [Consulta realizada en mayo del 2020]. Disponible en: https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba.

COLOMBIA. FUNCIÓN PÚBLICA. Decreto 1499 de 2017. (11, septiembre, 2017). Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015. Bogotá: La Función Pública. Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=83433.

COLOMBIA. MINISTERIO DE LAS TECNOLOGIAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [www.mintic.gov.co]. Bogotá: MINTIC, Guía para la Implementación de Seguridad de la Información en una MIPYME. [Consulta realizada en mayo del 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-5482_Guia_Seguridad_informacion_Mypimes.pdf.

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [www.mintic.gov.co]. Bogotá: MINTIC. Fortalecimiento de la Gestion TI en el estado. [Consulta realizada en mayo del 2020]. Disponible en: https://mintic.gov.co/portal/inicio/Iniciativas/Servicios/Fortalecimiento-de-las-TI-de-la-informacion-en-la-gestion-del-Estado-y-la-informacion-publica/.

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [www.mintic.gov.co]. Bogotá: MINTIC, Guía para la Gestión y

Clasificación de Activos de Información. [Consulta realizada en mayo del 2020]. Disponible en: https://www.mintic.gov.co/gestionti/615/articles-482_G5_Gestion_Clasificacion.pdf.

COLOMBIA. MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. [estrategia.gobiernoenlinea.gov.co]. Bogotá: MINTIC, Manual de Gobierno Digital. Implementación de la Política de Gobierno Digital. [Consulta realizada en mayo del 2020]. Disponible en: https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf.

COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Decreto 1078 de 2015. (26, mayo, 2015). Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Bogotá: La Presidencia. Disponible en: http://wp.presidencia.gov.co/sitios/normativa/decretos/2015/Decretos2015/DECRETO%201078%20DEL%2026%20DE%20MAYO%20DE%202015.pdf.

COLOMBIA. PRESIDENCIA DE LA REPÚBLICA. Ley estatutaria 1581 de 2012. (17, octubre, 2012). Por el cual se dictan disposiciones generales para la protección de datos personales. Bogotá: La Presidencia. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf.

COLOMBIA. SECRETARÍA DEL SENADO. Ley estatutaria 1266 de 2008. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. En: Diario Oficial. Diciembre, 2019. No. 47.219. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html.

COLOMBIA. SECRETARÍA DEL SENADO. Ley estatutaria 1273 de 2009. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. En: Diario Oficial. Diciembre, 2019. No. 47.223. Bogotá: La Secretaría. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html.

COLOMBIA. SECRETARÍA DISTRITAL DE HACIENDA. Ley 1712 de 2014. (6, marzo, 2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Bogotá: La Secretaría. Disponible en: http://www.shd.gov.co/shd/transparencia-y-acceso-a-informacion-publica-secretaria-hacienda.

CÓRDOBA SUÁREZ, Alba Elisa. [en línea]. Proyecto de Grado para optar al título de Especialista en Seguridad Informática. Universidad Nacional Abierta y A Distancia “UNAD”. 2015. [Consulta realizada el 14 de abril de 2020]. Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/3627/59650050.pdf?sequence=1&isAllowed=y.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. [www.iso.org]. STANDARD. [Consulta realizada el 14 de abril de 2020]. Disponible en: https://www.iso.org/home.html.

MORÁN DELGADO, Pedro Enrique. [en línea]. Tesis de grado previa a la obtención del título de ingeniero en sistemas e informática. Universidad Regional Autónoma de los Andes Uniandes, 2016. [Consulta realizada en mayo del 2020]. Disponible en: http://dspace.uniandes.edu.ec/bitstream/123456789/4222/1/TUSDSIS030-2016.pdf.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS. [www.oas.org]. INTERNET SECURITY ALLIANCE BOARD OF DIRECTORS. Manual de supervisión de riesgos cibernéticos para juntas corporativas. 2017. [Consulta realizada en mayo del 2020]. Disponible en: https://www.oas.org/es/sms/cicte/docs/ESP-Manual-de-Supervision-de-riesgos-ciberneticos-para-juntas-coporativas.pdf.

UNIDAD ADMINISTRATIVA ESPECIAL DE AERONAUTICA CIVIL DE COLOMBIA. [www.aerocivil.gov.co]. Bogotá: AEROCIVIL, [Consulta realizada en mayo de 2020]. Disponible en: http://www.aerocivil.gov.co/.

UNIVERSIDAD AUTONOMA DEL ESTADO DE MEXICO; Gestión de la Seguridad de la Información ISO / IEC 27000; [Blog]; [Consulta realizada en mayo del 2020]. Disponible en: https://www.academia.edu/19056080/GESTION_DE_LA_SEGURIDAD_DE_LA_INFORMACIO.

ANEXOS

ANEXO 1. ACUERDO DE CONFIDENCIALIDAD

ACUERDO DE CONFIDENCIALIDAD ENTRE SIXTA ALEXANDRA QUIROGA CASTILLO Y LA UNIDAD ADMINISTRATIVA ESPECIAL DE AERONÁUTICA CIVIL - AEROCIVIL

Por la **parte reveladora**
Nombre: Unidad Administrativa Especial de Aeronáutica Civil - Aerocivil
Dirección: Av. Eldorado 103-15
Teléfono: 2962311
E-mail: nicolas.ortiz@aerocivil.gov.co

Por la parte **receptora de la información**
Nombre: Sixta Alexandra Quiroga Castillo
Dirección: Conjunto Residencial El Trébol Kra 3E No. 11-60 Mz. 6 Int. 11 casa 34 – Mosquera Cundinamarca
Teléfono: 3102687802
E-mail: aquiroga1969@gmail.com

Identificación del proyecto

Entre los firmantes, identificados anteriormente, hemos convenido en celebrar el presente acuerdo de confidencialidad previa las siguientes **CONSIDERACIONES**

1. Que la información compartida en virtud del presente acuerdo pertenece a la ***Unidad Administrativa Especial de Aeronáutica Civil - Aerocivil,*** y la misma es considerada sensible y de carácter restringido en su divulgación, manejo y utilización. Dicha información es compartida en virtud del desarrollo del proyecto aplicado con el título: Diseño del SGSI en la Aerocivil para el proceso de Gestión de Tecnologías de Información (GINF 6.0).

2. Que la información de propiedad de ***Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil*** ha sido desarrollada u obtenido legalmente, como resultado de sus procesos, programas o proyectos y, en consecuencias abarca documentos, datos, tecnología y/o material que considera único y confidencial, o que es objeto de protección a título de secreto industrial.

3. Que el presente acuerdo se realiza por un lado entre la parte receptora de la información como integrante del proyecto de investigación ***Diseño del***

SGSI en la Aerocivil para el Proceso de Gestión de Tecnologías de Información (GINF 6.0)., Sixta Alexandra Quiroga Castillo que, para el presente caso actúa como **revelador, guarda y administrador** de la información de propiedad de ***Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil.***

En consecuencia, **las partes** se suscriben a las siguientes cláusulas:

Primera. Objeto: en virtud del presente **acuerdo de confidencialidad,** la **parte receptora**, se obliga a no divulgar directa, indirecta, próxima a remotamente, ni a través de ninguna otra persona o de sus subalternos o funcionarios, asesores o cualquier persona relacionada con ella, la **información confidencial** perteneciente al ***Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil*****,** así como también a no utilizar dicha

información en beneficio propio ni de terceros, sólo con fines estadísticos y de mejoramiento de la ***Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil*****.**

Segunda. Definición de información confidencial: se entiende como **Información Confidencial**, para los efectos del presente acuerdo:

1. La información que no sea pública y sea conocida por la **parte receptora** con ocasión de del proyecto de investigación y/ extensión.

2. Cualquier información societaria, técnica, jurídica, financiera, comercial, de mercado, estratégica, de productos, nuevas tecnologías, patentes, modelos de utilidad, diseños industriales,

   modelos de negocios, información del personal de la organización y/o cualquier otra relacionada con el proyecto ***Diseño del SGSI en la Aerocivil para el Proceso de Gestión de Tecnologías de Información (GINF 6.0).,*** lograr tales fines, y/o cualquier otro ente relacionado con la estructura organizacional, bien sea que la misma sea escrita, oral o visual, o en cualquier forma tangible o no, incluidos los mensajes de datos (en la forma definida en la ley), de la cual, la **parte receptora** tenga conocimiento o a la que tenga acceso por cualquier medio o circunstancia en virtud de las reuniones sostenidas y/o documentos suministrados.

3. La que corresponda o deba considerarse como tal para garantizar el derecho constitucional a la intimidad, la honra y el buen nombre de las personas y deba guardarse la debida diligencia en su discreción y manejo en el desempeño de sus funciones.

Tercera. Origen de la información confidencial: provendrá de documentos suministrados en el desarrollo del proyecto y que tiene que ver con las creaciones del intelecto, a la naturaleza, medios, formas de distribución, comercialización de productos o de prestación de servicios, transmitida verbal, visual o materialmente, por escrito en los documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mail u otros elementos similares suministrados de manera tangible o intangible, independiente de su fuente o soporte y sin que requiera advertir su carácter confidencial.

Cuarta. Obligaciones de la parte receptora: Se considerará como **parte receptora** de la **información confidencial** a la persona que recibe la información, o que tenga acceso a ella. La parte receptora se obliga a:

De ser necesario o conveniente según la necesidad del titular de la información, se adicionarán las obligaciones que se consideren pertinentes:

1. Mantener la **información confidencial** segura, usarla solamente para los propósitos relacionados con él, en caso de ser solicitada, devolverla toda (incluyendo copias de esta) en el momento en que ya no requiera hacer uso de la misma o cuando termine la relación, caso en el cual, deberá entregar dicha información antes de la terminación de la vinculación.

2. Proteger la **información confidencial**, sea verbal, escrita, visual, tangible, intangible o que por cualquier otro medio reciba, siendo legitima poseedora de la misma ***Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil*****,** restringiendo su uso exclusivamente a las personas que tengan absoluta necesidad de conocerla.

3. Abstenerse de publicar la **información confidencial** que conozca, reciba o intercambie con ocasión de las reuniones sostenidas.

4. Usar la **información confidencial** que se le entregue, únicamente para los efectos señalados al momento de la entrega de dicha información.

5. Mantener la **información confidencial** en reserva hasta tanto adquiera el carácter de pública.

6. Responder por el mal uso que le den sus representantes a la **información confidencial.**
7. Guardar la reserva de la **información confidencial** como mínimo, con el mismo cuidado con la que protege la **información confidencial.**

8. La **parte receptora** se obliga a no transmitir, comunicar revelar o de cualquier otra forma divulgar total o parcialmente, pública o privadamente, la

información confidencial sin el previo consentimiento por escrito por parte de ***Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil*****.**

9. La **parte receptora** se compromete a establecer que los datos a utilizar son documentación relacionada con seguridad informática y de la información como: formatos, procedimientos, instructivos, manuales, políticas, activos de información del proceso GINF-6.0 Gestión de Tecnologías de Información.

10. La información capturada por la **parte receptora** se observará como cifras para estudio estadístico, comparativo, información cualitativa, no existirá ningún tipo de ganancia económica, es netamente educativo.

11. La identidad de todo personal de la ***Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil,*** no será revelada, dado que no se capturará sus nombres completos ni algún otro tipo de información que revele su identidad física o digital.

12. Las pruebas realizadas por la **parte receptora** nunca pondrán en peligro los activos tecnológicos de la ***Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil*****,** ni violentará la ley de delitos informáticos colombiana 1273 de 2009 estando en el margen de las buenas prácticas y los procesos legales pertinentes.

13. El estudiante ***Sixta Alexandra Quiroga Castillo*** se compromete a difuminar, bloquear y ocultar toda información que revele la identidad de la empresa la ***Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil*****,** para salvaguardar la confidencialidad e identidad de la empresa en el documento final del proyecto el cual será publicado en el repositorio institucional y de acceso público.

14. El título del proyecto no podrá contener el nombre de la empresa u organización con la que se firma el presente acuerdo de confidencialidad, este nombre deberá ser reemplazado.

Parágrafo: Cualquier divulgación autorizada de la **información confidencial** a terceras personas estará sujeta a las mismas obligaciones de confidencialidad derivadas del presente **Acuerdo** y la **parte receptora** deberá informar estas restricciones incluyendo la identificación de la información cono confidencial.

Quinta. Obligaciones de la parte reveladora: Son obligaciones de la parte reveladora:

1. Mantener la reserva de la **información confidencial** hasta tanto adquiera el carácter de pública.

2. Documentar toda la **información confidencial** que transmita de manera escrita, oral o visual, mediante documentos, medios electrónicos, discos ópticos, microfilmes, películas, e-mails u otros elementos similares o en cualquier forma tangible o no, incluidos los mensajes de datos, como registro de la misma para la determinación de su alcance, e indicar específicamente y de manera clara e inequívoca el carácter confidencia de la información suministrada de la **parte receptora**.

Sexta. Exclusiones a la confidencialidad: La **parte receptora** queda relevada o eximida de la obligación de confidencialidad, únicamente en los siguientes casos:

1. Cuando la **información confidencial** haya sido o sea de dominio público. Si la información se hace de dominio público durante el plazo del presente acuerdo, por un hecho ajeno a la **parte receptora,** esta conservará su deber de reserva sobre la información que no haya sido afectada.

2. Cuando la **información confidencial** deba ser revelada por sentencia en firme de un tribunal o autoridades competentes en desarrollo de sus funciones que ordenen el levantamiento de la reserva y soliciten el suministro de esta información. No obstante, en este caso la parte reveladora será la encargada de dar cumplimiento a la orden, restringiendo la divulgación a la información estrictamente necesaria, y en el evento de que la confidencialidad se mantenga, no eximirá a la parte receptora del deber de reserva.

3. Cuando la **parte receptora pruebe** que la **información confidencial** ha sido obtenida por otras fuentes.

4. Cuando la **información confidencial** ya la tenía en su poder la parte receptora antes de la entrega de la información reservada.

Séptima. Responsabilidad: la parte que contravenga el acuerdo será responsable ante la otra parte o ante los terceros de buena fe sobre los cuales se demuestre que se han visto afectados por la inobservancia del presente **acuerdo**, por los perjuicios morales y económicos que estos puedan sufrir como resultado del incumplimiento de las obligaciones aquí contenidas.

Octava. Solución de controversias: Las partes ***Sixta Alexandra Quiroga Castillo*** – la ***Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil*****,** se comprometen a esforzarse en resolver mediante los mecanismos alternativos de solución de conflictos cualquier diferencia que surja con motivo de la ejecución del presente **acuerdo.** En caso de no llegar a una solución directa para la controversia planteada, someterán la cuestión controvertida a las leyes colombianas y a la jurisdicción competente en el momento de presentarse la diferencia. La Universidad

Nacional Abierta y a Distancia como institución educativa no se hace responsable del no cumplimiento de las cláusulas del presente acuerdo de confidencialidad por parte de ***Sixta Alexandra Quiroga Castillo***.

Novena. Legislación aplicable: Este **acuerdo** se regirá por las leyes de la República de Colombia y se interpretará de acuerdo con las mismas.

Décima. Aceptación del Acuerdo: Las partes han leído y estudiado de manera detenida los términos y el contenido del presente **Acuerdo** y por tanto manifiestan estar conformes y aceptan todas las condiciones.

Firman en Bogotá D.C., a los (04) días del mes de (mayo) de 2020

Como Parte Receptora: **Por la parte reveladora:**

Sixta Alexandra Quiroga Castillo
Estudiante UNAD
No.63.434.979 de Vélez

Nicolás Ortiz Espitia
Unidad Administrativa Especial de Aeronáutica Civil – Aerocivil
C.C. No.79.399.957 de Bogotá

ANEXO 2. AUTORIZACIÒN

Bogotá, 04 de mayo de 2020

Señor:
NICOLAS ORTIZ ESPITIA
Coordinador Grupo Seguridad de la Información

Asunto: Autorización para la ejecución del proyecto titulado: DISEÑO DEL SGSI EN LA AEROCIVIL PARA EL PROCESO DE GESTION DE TECNOLOGIAS DE INFORMACIÓN (GINF 6.0).

Cordial saludo estimado Gerente,

Como es de su conocimiento, actualmente me encuentro adelantando estudios de posgrado en la Especialización en Seguridad Informática ofertado por la Universidad Nacional Abierta y a Distancia “UNAD”. Para finalizar mi proceso académico es mi objetivo desarrollar un trabajo de grado aplicado a Unidad Administrativa Especial de Aeronáutica Civil - AEROCIVIL, de manera que pueda aportar mis conocimientos adquiridos y generar un impacto positivo en la empresa, relacionado con los temas de Seguridad Informática, motivo por el cual, muy comedidamente solicito su autorización y aprobación para la ejecución del proyecto titulado: DISEÑO DEL SGSI EN LA AEROCIVIL PARA EL PROCESO DE GESTION DE TECNOLOGIAS DE INFORMACIÓN (GINF 6.0).el cual se encuentra avalado por parte la Institución de educación superior “UNAD”.

El proyecto en su objetivo general describe lo siguiente: “Diseñar el SGSI en la Unidad Administrativa Especial de Aeronáutica Civil - AEROCIVIL, con el fin de realizar un comparativo de los procesos actuales que tiene la Entidad con los lineamientos de cumplimiento de la norma ISO/IEC 27001 y establecer en qué áreas o procesos se debería priorizar y enfocar los esfuerzos y así incrementar la seguridad de la información”; al mismo tiempo será apoyado por los objetivos específicos: “Diagnosticar el estado actual de la Entidad frente al SGSI y diseñar un

Modelo de Gestión de Seguridad de la Información para el proceso de Gestión de Tecnologías de Información (GINF. 6.0).
Diseñar la Política General y las específicas del SGSI
Diseñar la metodología de Activos de Información y Riesgos para el proceso GINF. 6.0 Gestión de Tecnologías de Información, bajo los lineamientos de MinTic" para obtener como resultado un alto impacto en la seguridad de la empresa Unidad Administrativa Especial de Aeronáutica Civil - AEROCIVIL.

De obtener esta autorización, se elaborará un acuerdo de confidencialidad para proteger la identidad la empresa y sus activos de información; a su vez se destacan los siguientes procesos para ser garantes en la transparencia de la ejecución del proyecto:

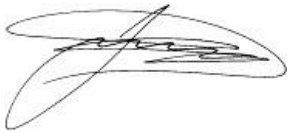
- Se prohíbe la ejecución de cualquier tipo de pruebas de seguridad que no estén autorizadas expresamente por Unidad Administrativa Especial de Aeronáutica Civil - AEROCIVIL.
- La empresa Unidad Administrativa Especial de Aeronáutica Civil - AEROCIVIL deberá establecer qué tipo de información es privada y cuál es pública para delimitar el acceso de pruebas en la ejecución del proyecto.
- La solicitud de información al igual que ejecución de pruebas deben quedar por escrito y se genera un informe de resultados semanalmente el cual será compartido con el gerente de la organización o empresa.
- La persona autorizada siempre debe operar dentro de la ley 1273 de 2009 y de las demás regulaciones establecidas en la empresa.
- Respetar la privacidad de todos los individuos y mantener su privacidad en los reportes. Se encuentra prohibida la divulgación de información personal en tales reportes.

El resultado del proyecto se verá reflejado en un documento el cual será cargado al repositorio institucional de la Universidad Nacional Abierta y a Distancia "UNAD". El documento ampara la confidencialidad y anonimato de la empresa, estos aspectos se encuentran estipulados en el acuerdo de confidencialidad; agradezco el apoyo prestado en esta etapa de mi carrera profesional.

Firman en Bogotá D.C., a los (04) días del mes de (mayo) de 2020

Cordialmente,

Sixta Alexandra Quiroga Castillo
Estudiante UNAD.



Nicolás Ortiz Espitia
Coordinador Grupo Seguridad de la Información