FUERZAS MILITARES DE COLOMBIA
EJERCITO NACIONAL

GUÍA DE GESTIÓN DE ACTIVOS

Código: G-JEMPP-CEDE6-3	**Versión:** 1	**Fecha de emisión:** 2021-11-12	**Pág.** 1 de 12

Elaboró	Revisó	Aprobó
Equipo de trabajo CEDE6/CEDE2	**TC. JULIO CESAR VILLANUEVA MÉNDEZ** Director Planeación y Políticas C5 **MY. ANDRÉS FELIPE ARIZA SAAVEDRA** Director Protección de Datos y Archivos	**CR. OSCAR MAURICIO ORTIZ GUZMAN** Jefe Departamento de Comunicaciones **CR. ANDRÉS QUINTERO ARIAS** Jefe Departamento de Inteligencia y Contrainteligencia

TABLA DE CONTENIDO

1. ALCANCE:

La presente guía define los criterios que se deben seguir, para poner en marcha la gestión y clasificación de activos de información que son responsabilidad del Ejército Nacional, con el fin de determinar que activos de información poseen, cuáles son sus propiedades, su clasificación y valoración, esto permite construir y mantener un inventario de activos de información actualizado con la información requerida, con el fin de aplicar los controles de seguridad de la información apropiados de acuerdo a su importancia o criticidad.

Los lineamientos establecidos en esta guía aplican a todos los activos de información del Ejército Nacional.

2. IDENTIFICACIÓN, CLASIFICACIÓN Y VALORACIÓN DEL ACTIVO DE INFORMACIÓN:

Para realizar la identificación, clasificación y valoración de los activos de información se deben realizar las siguientes actividades en el orden que a continuación se especifica para documentar el inventario de activos, registrando los valores en la "***Matriz Gestión de Activos de información FO-JEMPP-CEDE6-1358***", así:

1. Identificación del activo de información
2. Clasificación del activo de información
3. Valoración del activo de información.

Los cuales se detallan a continuación, así:

2.1 Identificación del activo de información:

La identificación de los activos de información del proceso a analizar se realiza a partir de la caracterización de los procesos y sus procedimientos y demás documentación asociada, analizando el porqué, como, cuando, donde, de los elementos, equipos, información, personas, y lugares relacionados con la ejecución de las actividades de dicho proceso.

Dentro de la ***"Matriz Gestión de Activos de información FO-JEMPP-CEDE6-1358"***, en la sección ***"Inventario de Activos"***, se indican los campos de propiedades que debe tener cada activo y que se detallan a continuación, así:

- **ID:** Número consecutivo único que identifica al activo en el inventario.
- **Nombre del activo:** Identificación formal del activo de información.
- **Tipo de activo:** Define el tipo al cual pertenece el activo. Para este campo

se utilizan los siguientes valores:

TIPO DE ACTIVO	DESCRIPCIÓN
PERSONAS	Aquellos roles que, por su conocimiento, experiencia y criticidad para el proceso, son considerados activos de información.
SOFTWARE	Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
INFRAESTRUCTURA	Infraestructura física que soporta el funcionamiento del proceso.
INFORMACIÓN	Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
HARDWARE	Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
SERVICIO	Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet, entre otros.
DATOS PERSONALES	De acuerdo con lo estipulado en la Ley 1581, cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

- **Proceso:** Nombre del proceso al que pertenece el activo.
- **Ubicación:** especificación del lugar físico o lógico según corresponda al tipo de activo de información.
- **Propietario (Responsable):** 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 el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.
- **Custodio Técnico:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el

proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

2.2 Clasificación del Activo de información:

La clasificación de activos de información tiene como objetivo asegurar que la información recibe los niveles de protección adecuados, ya que con base en su valor y de acuerdo con otras características particulares, requiere un tipo de manejo especial. Para la clasificación de los activos se toma como referencia la guía "***Gestión y Clasificación de Activos de Información***" del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Dentro de la ***"Matriz Gestión de Activos de información FO-JEMPP-CEDE6-1358"***, en la sección "***Clasificación de Activos***", se indican los campos de clasificación que debe tener cada activo y que se detallan a continuación, así:

- **Valor:** Para la propiedad *Confidencialidad* es el número entre 1, 2 ,3, 4, 5, 6 y 7, donde 1 tiene el valor más bajo y 7 el más alto, y para las propiedades *Integridad* y *Disponibilidad* es el número entre 1, 2 y 3, donde 1 tiene el valor más bajo y 3 el más alto en la calificación del criterio a evaluar, el cual se escoge del combo que se despliega en esta celda.
- **Nivel:** Es la descripción del nivel de calificación de acuerdo a lo que se haya escogido en la columna "*Valor*", para los criterios de Confidencialidad, Integridad y Disponibilidad.

A continuación, se relaciona el valor con el nivel de criticidad que puede tomar para cada uno de los valores, así:

CONFIDENCIALIDAD	
VALOR	**NIVEL**
7	ULTRASECRETO
6	SECRETO
5	CONFIDENCIAL
4	RESTRINGIDO
3	INFORMACIÓN PUBLICA RESERVADA
2	INFORMACIÓN PÚBLICA CLASIFICADA
1	INFORMACIÓN PÚBLICA

INTEGRIDAD	
VALOR	NIVEL
3	ALTA
2	MEDIA
1	BAJA

DISPONIBILIDAD	
VALOR	NIVEL
3	ALTA
2	MEDIA
1	BAJA

A continuación, se presenta una definición de los tres criterios a tener en cuenta para elegir el valor para cada propiedad:

CRITERIO	DESCRIPCIÓN
Confidencialidad	Se establece para que roles o funcionarios o grupos está permitido acceso al activo de información, y que impacto tendría el incumplimiento de esta condición.
Integridad	Establecer cuál es el efecto de la modificación no autorizada de los datos del activo de información, que impacto tendría en los procesos donde se encuentra involucrado y a su vez que consecuencias tendría para la entidad.
Disponibilidad	Cuál es el efecto que se genera para la entidad cuando el activo de información no puede estar cuando se requiere; esto se determina por el tiempo que se puede esperar para que dicho activo de información pueda ser utilizado.

Luego de identificar el valor para las tres propiedades de seguridad (confidencialidad, integridad y disponibilidad), éste se debe registrar en la columna "VALOR" de cada propiedad, teniendo en cuenta los niveles que a continuación se detallan:

2.2.1 Clasificación de acuerdo con la Confidencialidad

CONFIDENCIALIDAD		
VALOR	**NIVEL**	**DESCRIPCIÓN**
7	ULTRASECRETO	Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al exterior del país los intereses del Estado o las relaciones internacionales.
6	SECRETO	Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar al interior del país los intereses del Estado.
5	CONFIDENCIAL	Es el nivel de clasificación que se debe dar a todos los documentos de inteligencia y contrainteligencia que contengan información sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar directamente las instituciones democráticas.
4	RESTRINGIDO	Es el nivel de clasificación que se debe dar a todos los documentos que contengan información de las instituciones militares, de la Policía Nacional o de los organismos y dependencias de inteligencia y contrainteligencia, sobre posibles amenazas, riesgos, oportunidades o capacidades, que puedan afectar en las citadas instituciones y organismos, su seguridad, operaciones, medios, métodos, procedimientos, integrantes y fuentes.
3	INFORMACIÓN PUBLICA 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 de transparencia.
2	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 de transparencia.
1	INFORMACIÓN PÚBLICA	Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

La confidencialidad se refiere a que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados, para esto se definieron siete (7) niveles alineados con los niveles de clasificación de la información declarados en la

"*Directiva Permanente 1016 Instrucciones para la aplicación del proceso de gestión documental en el Ejército Nacional*" en el Anexo B, literal F. Niveles de clasificación de seguridad de los documentos, de Gestión Documental, y el "*REGLAMENTO GENERADOR DE FUERZA DEL EJÉRCITO GESTIÓN DOCUMENTAL PARA EL EJÉRCITO RGE 4-0.1*" en el *"CAPITULO III PROCESOS DE LA GESTIÓN DOCUMENTAL"*, ítem *"B. PRODUCCIÓN"*, numeral "*10. Niveles de clasificación de seguridad de la información*", pagina 15, así:

2.2.2 Clasificación de acuerdo con la Integridad:

La integridad se refiere a la exactitud y completitud de la información (ISO 27000), esta propiedad es la que permite que la información sea precisa, coherente y completa desde su creación hasta su destrucción, para esto se definieron tres (3) niveles:

INTEGRIDAD		
VALOR	**NIVEL**	**DESCRIPCIÓN**
3	ALTA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas de la entidad.
2	MEDIA	Información cuya pérdida de exactitud y completitud puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado a funcionarios de la entidad.
1	BAJA	Información cuya pérdida de exactitud y completitud conlleva un impacto no significativo para la entidad o entes externos.

2.2.3 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, para esto se definieron tres (3) niveles:

DISPONIBILIDAD		
VALOR	**NIVEL**	**DESCRIPCIÓN**
3	ALTA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdidas de imagen severas a entes externos.
2	MEDIA	La no disponibilidad de la información puede conllevar un impacto negativo de índole legal o económica, retrasar sus funciones, o generar pérdida de imagen moderado de la entidad.

DISPONIBILIDAD		
1	BAJA	La no disponibilidad de la información puede afectar la operación normal de la entidad o entes externos, pero no conlleva implicaciones legales, económicas o de pérdida de imagen.

2.3 Valoración del activo de Información:

El valor del activo de información determina la importancia o criticidad del activo de información.

Dentro de la ***"Matriz Gestión de Activos de información FO-JEMPP-CEDE6-1358"***, en la sección "***Valoración del Activo***", se indican los campos de la valoración del activo, los cuales se detallan a continuación, así:

- **Valor:** Número entre 3 y 13, donde 3 indica que tiene el menor valor y 13 el valor más alto en cuanto a importancia o criticidad, el cual se obtiene sumando los valores de los tres criterios: Confidencialidad, Integridad y Disponibilidad.
- **Nivel:** Es la calificación de criticidad del activo, la cual se obtiene dependiendo de las diferentes combinaciones de valores obtenidos en cada una de las propiedades, así:

CRITICIDAD DEL ACTIVO	
ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta. Considerando que para la propiedad de confidencialidad se valora en alta los niveles secreto, ultrasecreto y confidencial.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio. Considerando que para la propiedad de confidencialidad se valora en medio el nivel restringido e información pública reservada.
BAJA	Activos de información en los cuales la clasificación de la información en las propiedades integridad y disponibilidad es baja, y en la propiedad confidencialidad es información pública clasificada e información pública.

La siguiente tabla muestra la relevancia de un activo de información de acuerdo con su criticidad:

NIVEL DE CRITICIDAD	DESCRIPCIÓN
ALTA	La entidad se ve seriamente afectada y puede generar sanciones elevadas y afectar la credibilidad de la entidad y sus procesos.
MEDIA	El activo puede afectar de forma parcial una operación o un proceso. Las pérdidas o afectación pueden ser moderadas.

NIVEL DE CRITICIDAD	DESCRIPCIÓN
BAJA	El activo puede afectar una tarea aislada de la operación o del proceso. Las pérdidas o afectación serían menores y no incurrirían en sanciones.

El propósito de la identificación, clasificación y valoración de los activos permitirá definir la criticidad e importancia del activo dentro del Modelo de Seguridad y Privacidad de la Información, de tal manera que se garantice los controles de seguridad apropiados, protegiéndolo de los riesgos asociados.

3. REVISIÓN:

La revisión se refiere a la verificación que se lleva a cabo para determinar si un activo de información continua o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.

En general, el inventario de activos puede ser revisado o validado en cualquier momento en que el líder del proceso (o quien haga sus veces) así lo solicite, o si el propietario (responsable) lo requiere.

Las razones por las cuales debería realizar una revisión o validación son:

- Actualizaciones al proceso al que pertenece el activo.
- Adición de actividades al proceso.
- Inclusión de nuevos registros de calidad, nuevos registros de referencia o procesos y procedimientos.
- Inclusión de un nuevo activo.

4. GLOSARIO:

Activo: Cualquier cosa que tenga valor para un individuo, una organización o un gobierno. (ISO/IEC 27032:2012)

Confidencialidad: Propiedad de que la información no se pone a disposición o se divulga a personas, entidades o procesos no autorizados. (ISO/IEC 27000:2018)

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada. (ISO/IEC 27000:2018)

Integridad: Propiedad de la información relativa a su exactitud y completitud. (ISO/IEC 27000:2018)

5. NORMATIVIDAD APLICABLE:

- Ley 1621 de 17 de abril de 2013 "por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones"
- Ley 1712 de 6 de marzo 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 1008 de 14 de junio de 2018 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"
- Directiva Permanente 1016 Instrucciones para la aplicación del proceso de gestión documental en el Ejército Nacional.
- REGLAMENTO GENERADOR DE FUERZA DEL EJÉRCITO GESTIÓN DOCUMENTAL PARA EL EJÉRCITO RGE 4-0.1
- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, Tecnología de la Información, Técnicas de Seguridad, Sistemas de Gestión de la Seguridad de la Información, Requisitos.
- Norma Técnica Colombiana NTC-ISO-IEC 27002:2013, Guía de Implementación Sistemas de Gestión de la Seguridad de la Información.

6. REFERENCIAS:

- Manual del Sistema Integrado de Gestión MC-JEMPP-CEDE5-002, https://www.ejercito.mil.co/s_i_g/manual_calidad
- Directiva Permanente 1016 "Instrucciones para la aplicación del proceso de gestión documental en el Ejército Nacional"
- Reglamento Generador de Fuerza del Ejército Gestión Documental para el Ejército Nacional REG 4-0.1 de enero de 2018.
- Ministerio de Tecnologías de la Información y las Comunicaciones, Guía para la Gestión y Clasificación de Activos de Información, http://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf
- Norma Técnica Colombiana NTC-ISO-IEC 27001:2013, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

- Norma Técnica Colombiana NTC-ISO-IEC 27002:2013, http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

7. CONTROL DE CAMBIOS:

Actualización a la Versión No.	Actualización realizada	Fecha de emisión
0	Guía Inicial	2019-11-19
1	Se agrega el código de la Matriz Gestión de Activos de información (FO-JEMPP-CEDE6-1358), para facilitar identificación del documento que se referencia para las actividades.	2021-11-13