SISTEMA DE PROCESAMIENTO DE DATOS DE SEGURIDAD PARA EL EJÉRCITO NACIONAL
No. JEMPP-CEDE6-DIPCO-ET-05715-COM-00



Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

SISTEMA DE PROCESAMIENTO DE DATOS DE SEGURIDAD PARA EL EJÉRCITO NACIONAL No. JEMPP-CEDE6-DIPCO-ET-05715-COM-00

CONTENIDO

1. OBJETO 3
2. DEFINICIONES Y APLICACIÓN 3
3. REQUISITOS 4
4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO: 20
5. MÉTODOS DE ENSAYO 20
6. APÉNDICE 20
7. ANEXOS 22
8. CONTROL DE REVISIONES 22

Elaboró	Revisó	Aprobó
TE. HUMBERTO MARTINEZ PORTELA Oficial de Respuesta Cibernética del Ejército Nacional	**MY. PABLO EDUARDO CORTES FORERO** Ejecutivo y Segundo Comandante del Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional **PS. OLGA LUCIA VILLALOBOS BACCA** Asesora Jurídica	**TC. ROGER JESUS BUELVAS NARVAEZ** Comandante Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional



COPIA NO CONTROLADA

1. OBJETO

La presente especificación técnica tiene por objeto fortalecer la infraestructura tecnológica del Ejercito Nacional con un sistema de procesamiento de datos de seguridad para el Ejército Nacional para optimizar el análisis y procesamiento de datos frente a las nuevas amenazas de naturaleza cibernética.

2. DEFINICIONES Y APLICACIÓN

2.1 DEFINICIONES

Ciberataque: cualquier acción que explota una vulnerabilidad en un sistema de información para causar daño o realizar una acción no autorizada. Estos ataques pueden variar en complejidad, desde simples intentos de adivinar contraseñas hasta operaciones altamente sofisticadas diseñadas para robar datos confidenciales o interrumpir servicios críticos.[1]

Correo electrónico (email): es un método para enviar mensajes digitales a uno o más usuarios mediante un computador o dispositivo móvil y recibir mensajes a través de una red. Es una de las formas más comunes de comunicación escrita en la actualidad, tanto para uso personal como profesional.[2]

DMARC o Domain-based Message Authentification Reporting and Conformance: es un protocolo de autenticación de correo electrónico de código abierto que suministra protección a nivel de dominio para el canal de correo electrónico.[3]

Inteligencia de Amenazas: es un proceso proactivo y continuo que busca identificar, analizar y comprender las amenazas potenciales que pueden afectar la seguridad de una organización. Esta disciplina se basa en la recopilación, el procesamiento y el análisis de una amplia variedad de datos, tanto internos como externos, para anticipar y responder a incidentes de seguridad.[4]

Malware: es un término general que se utiliza para describir cualquier tipo de software malicioso diseñado para infiltrarse en un dispositivo, sin el conocimiento del usuario y causar daños o interrupciones en el sistema o robar datos.[5]

---

[1] Tomado de IBM https://www.ibm.com/es-es/topics/cyber-attack

[2] Tomado de INCIBE https://www.incibe.es/ciudadania/blog/el-correo-electronico-una-herramienta-basica-para-comenzar-en-internet#:~:text=El%20correo%20electr%C3%B3nico%20o%20e,dispositivo%20con%20acceso%20a%20Internet.

[3] Tomado de PROOFPOINT https://www.proofpoint.com/es/threat-reference/dmarc#:~:text=puede%20ayudarle%20Proofpoint-,Definici%C3%B3n,el%20canal%20de%20correo%20electr%C3%B3nico.

[4] Tomado de KASPERSKY https://latam.kaspersky.com/resource-center/definitions/threat-intelligence?srsltid=AfmBOoreQhdGrvKWgsFGzdnOLeX7-stdLQIlvgwxDykvYB41VO5zyzXx

[5] Tomado de MICROSOFT https://support.microsoft.com/es-es/topic/c%C3%B3mo-impedir-y-eliminar-virus-y-otro-malware-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

Riesgo cibernético: es la probabilidad de que ocurra un evento negativo relacionado con la seguridad de los sistemas de información, lo que puede resultar en pérdidas financieras, interrupción de los negocios, daños a la reputación o pérdida de datos confidenciales.[6]

Vulnerabilidad: es una debilidad o fallo en un sistema informático, una aplicación o una configuración que puede ser explotada por un atacante para obtener acceso no autorizado, causar daño o interrumpir los servicios. Es como una puerta abierta en un sistema que los ciberdelincuentes pueden utilizar para infiltrarse.[7]

2.2 APLICACIÓN

La implementación de un sistema de procesamiento de datos de seguridad para el Ejército Nacional representa una inversión estratégica en la protección para el procesamiento de datos y los activos digitales de una organización. Al centralizar las comunicaciones y los datos en una plataforma de crecimiento seguro y escalable, se facilita la implementación de medidas de seguridad robustas, análisis de datos, respaldo de información, procesos de cifrado en el en tránsito y en reposo, la autenticación multifactor y la detección de amenazas en tiempo real. Además, esta solución permite al equipo técnico de seguridad colaborar de manera más eficiente y segura, independientemente de su ubicación geográfica, lo que se traduce en un aumento de la productividad, tiempos de respuesta e innovación.

Más allá de los beneficios en materia de ciberseguridad, la implementación de este sistema ofrece ventajas operativas significativas. Al eliminar la necesidad de gestionar appliance o equipos de propósito específico para la infraestructura tecnológica, reduciendo los costos asociados al hardware, software y mantenimiento. Así mismo, los sistemas de procesamiento suelen incluir un conjunto completo de administración para almacenamiento, procesamiento y respaldo de información, lo que permite a los usuarios acceder a todos los recursos que necesitan desde una única interfaz.

La seguridad y protección de la información es un pilar fundamental en cualquier solución de procesamiento, colaboración en la nube, la detección y prevención de amenazas, como el phishing y el malware, son esenciales para protegerse contra ataques cibernéticos.

3. REQUISITOS

3.1 REQUISITOS GENERALES

El Ejército Nacional brinda servicios informáticos de forma centralizada, por tal razón es fundamental garantizar la operatividad de las herramientas y plataformas de seguridad con

---

[6] Tomado de Hewllett packard https://www.hpe.com/lamerica/es/what-is/cybersecurity-threats.html

[7] Tomado de ORSYS-LEMANG.COM https://orsys-lemag.com/es/Glossaire/vulnerabilite-%F0%9F%9F%A5/#:~:text=Una%20vulnerabilidad%20de%20ciberseguridad%20es,la%20seguridad%20de%20ese%20sistema.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

una solución de procesamiento de datos de seguridad, evitando accesos no autorizados, unificando las comunicaciones y permitiendo la protección centralizada.

NÚM.	DESCRIPCIÓN DE REQUERIMIENTOS
3.1.1	**INSTALACIÓN, CONFIGURACIÓN Y PUESTA EN FUNCIONAMIENTO DE UNA INFRAESTRUCTURA DE HIPERCONVERGENCIA Y COPIA DE SEGURIDAD PARA EL BATALLON DE CIBERDEFENSA Y CIBERSEGURIDAD.**
3.1.1.1	La solución de hiperconvergencia y copias de seguridad requerida deberá quedar instalada y será utilizada por el BACCI en el Centro de Datos de Ejercito Nacional, en las instalaciones de la ciudad de Bogotá D.C, lo anterior con el fin de fortalecer la tecnología de servidores y adicional a ello maximizar la capacidad a nivel de espacio físico para albergar las diferentes máquinas virtuales y herramientas de ciberseguridad.
3.1.1.2	La solución de hiperconvergencia y sistema de copias de seguridad deberá proveer un crecimiento modular y escalable, garantizando el aprovisionamiento tanto de cómputo, memoria y almacenamiento. Por ello dentro de la oferta el proponente deberá suministrar detalladamente los equipos ofertados y el cumplimiento de las características técnicas requeridas.
3.1.1.3	El Oferente Adjudicatario dentro de la ejecución del Contrato y sin costo adicional, debe efectuar un levantamiento de información (nombres, IP, sistemas operativos, capacidades en procesamiento/almacenamiento y RAM, servicios), para la Migración de algunas herramientas de ciberseguridad (Alojadas en equipos de hardware on premise o en máquinas virtuales). De igual manera deberá parametrizar y configurar el almacenamiento de full backup y repositorio para los datos allí alojados. Para efectos de la migración el oferente debe suscribir el licenciamiento Microsoft a nombre del Batallón de ciberdefensa y ciberseguridad referente al Windows server Datacenter y/o sistema Operativo necesario a suministrar.
3.1.1.4	El Oferente Adjudicatario debe contemplar entre otros los siguientes servicios: • Instalación, Configuración y puesta en plena operación funcional para el BACCI la Infraestructura HIPERCONVERGENTE on Premise. • En general, contemplar sin costo adicional para el Ejército Nacional la totalidad de licenciamiento requerido, servicios de instalación y configuración de la nueva infraestructura suministrada por el Oferente Adjudicatario, con los servicios de migración de Particiones Lógicas y VM y puesta en operación final sin costo adicional; es decir todos los costos y servicios se deben contemplar dentro de la Oferta por parte del Oferente y el BACCI no deberá incurrir en costos adicionales. (No se deberán suministrar licenciamiento de ninguna herramienta de seguridad existente) Instalación y configuración de la solución de copias de seguridad.
3.1.1.5	• Se deberá garantizar todos los elementos necesarios para la instalación y puesta en funcionamiento de la solución de Hiperconvergencia y copias de seguridad.
3.1.1.6	Se debe proporcionar una solución hiperconvergente que ofrezca soporte y garantía integrados, con un único punto de contacto para la gestión tanto del hardware como del software

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.1.1.7	Garantizar el suministro e instalación de la última versión del firmware y software requerido para la hiperconvergencia y la solución de copias de seguridad de todos los elementos instalados. Debiendo calcular de acuerdo al número de CORE y servidores físicos y a virtualizar el licenciamiento requerido, sin incurrir en sub o sobre licenciamiento. Las penalidades por lo mismo o sobre costos serán asumidas por el contratista. Con el fin de asegurar una solución adecuada para la entidad y dada la importancia que tienen analistas como el Cuadrante Mágico de Gartner y Forrester en el análisis de las diferentes soluciones de tecnología, el software de Hiperconvergencia ofrecido deberá ser calificado como líder en los últimos reportes presentados por estas empresas.

3.2 REQUISITOS ESPECÍFICOS

ITEM	DESCRIPCIÓN
3.2.1	**INFRAESTRUCTURA DE HIPERCONVERGENCIA**
3.2.1.1	**CARACTERÍSTICAS GENERALES**
3.2.1.1.1	CANTIDAD La solución debe estar compuesta por mínimo tres (3) nodos, o con los nodos necesarios para la creación del clúster.
3.2.1.1.2	PROCESADOR Cada nodo de hiperconvergencia ofertado deberá incluir como mínimo dos (2) procesadores de la familia Intel Xeon Gold con CPU 2.0 GHz o superior de al menos 16 Cores físicos.
3.2.1.1.3	MEMORIA RAM La solución hiperconvergente debe contar con memoria RAM de mínimo 1.5 TB efectivas usables (total del clúster) en módulos DDR5 5600 MHz RDM o superior.
3.2.1.1.4	CONECTIVIDAD • Cada nodo deberá incluir como mínimo dos (2) puertos 10/25GbE y (2) puertos a 10G BaseT por nodo de hiperconvergencia o los necesarios para la interconexión de los nodos ofertados, con los conectores transceivers y fibras respectivas. • Se deben incluir los cables (poder, red, fibra óptica, entre otros), rieles de montaje y demás elementos requeridos para su instalación y puesta en funcionamiento.
3.2.1.1.5	La solución de hiperconvergencia debe soportar protocolo IPV4
3.2.1.1.6	La solución de hiperconvergencia debe soportar protocolo IPV6

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.1.1.7	Cada nodo deberá contar con mínimo dos (2) fuentes de alimentación AC, Voltaje 230V/115V, frecuencia 50/60 Hz redundantes, para cada uno de los nodos de hiperconvergencia ofertados.
3.2.1.1.8	ALMACENAMIENTO INTERNO • La solución de hiperconvergencia debe garantizar como mínimo (70) TB efectivos usables, antes de compresión, de-duplicación o algoritmos de optimización, en almacenamiento híbrido con discos SSD y HDD. • La solución de hiperconvergencia debe incluir compresión, sin licenciamiento adicional con las siguientes características: •Debe estar integrada de forma nativa. •Debe ser global tanto para clúster con almacenamiento híbridos (SSD y HDD)
3.2.1.2	**CARACTERÍSTICAS FUNCIONALES DE LA SOLUCIÓN DE HIPERCONVERGENCIA Y LICENCIAMIENTO O FIRMWARE REQUERIDO**
3.2.1.2.1	El soporte de la solución hiperconvergente debe ser gestionado a través de un único punto de contacto, proporcionado por el fabricante del software. Se deberá suscribir para el batallón de ciberdefensa y ciberseguridad el licenciamiento de software de la totalidad de los componentes funcionales de la solución de hiperconvergencia por mínimo 2 años.
3.2.1.2.2	El sistema debe contar con un nivel de aseguramiento (hardening) aplicado de fábrica y así mismo contar con un mecanismo nativo para automatizar la remediación de las desviaciones con respecto al hardening que puedan ocurrir durante todo el ciclo de vida de la solución, sin la ejecución de tareas manuales por parte de un administrador.
3.2.1.2.3	La solución debe poder ejecutar de-duplicación y compresión completamente en software, sin requerir el uso de ningún hardware especializado para esta funcionalidad. Estas deben poder activarse o desactivarse por parte del administrador del sistema ya sea que ambas estén activas o solo una de las dos en el clúster.
3.2.1.2.4	Debe ser una solución con capacidad de crecimientos modulares en el mismo clúster, incrementando el número de servidores; que podrán ser de diferente familia y modelo del fabricante de la solución de HCI, con diferentes capacidades de procesamiento (diferente generación de procesadores), diferente tamaño de memoria y diferente tipo de almacenamiento (nodos con almacenamiento híbrido y nodos con almacenamiento solo de estado sólido), para suplir futuras ampliaciones y requerimientos de la entidad, garantizando siempre los niveles de desempeño de la solución.
3.2.1.2.5	La solución debe soportar exportar almacenamiento por bloques a servidores externos por medio de ISCSI. (Internet Small Computer System Interface)
3.2.1.2.6	El sistema ofertado debe presentar el contenedor de almacenamiento virtualizado al hipervisor de manera automática por medio de NFS, SMB v3.0 o iSCSI (Internet Small Computer System Interface)

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.1.2.7	La solución debe incluir funcionalidades para el manejo de las nuevas tendencias denominadas "contenedores", de tal forma que permita según la necesidad de la entidad optimizar el rendimiento y el empaquetamiento de aplicaciones en ambientes de Cloud.
3.2.1.2.8	La solución debe soportar como mínimo Windows Guest Failover Clustering, funcionalidad que permite alta disponibilidad para las aplicaciones configuradas en clúster en una VM (Con sistema operativo Windows Server 2016 o Windows Server 2019 o Server 2022), para que transparentemente realice "failover" hacia otra VM ubicada en el mismo o en diferente host.
3.2.1.2.9	La solución deberá entregar alto rendimiento al presentar los recursos de almacenamiento desde el mismo nodo en el cual se encuentra la máquina virtual, haciendo los requerimientos de IOPS para cada máquina virtual de forma local en el mismo nodo.
3.2.1.2.10	La solución debe ser compatible para la virtualización de las plataformas (Windows Server 2016 o superior, Linux RedHat 8 o superior).
3.2.1.2.11	La solución debe detectar de manera proactiva el daño de un disco, removerlo automáticamente del clúster y reconstruir de manera inmediata los datos que ahí se alojaban en los otros discos del clúster.
3.2.1.2.12	La solución debe incluir la funcionalidad de replicación asincrónica que cumpla con los siguientes requerimientos básicos: - Replica a nivel de máquina virtual de forma granular. - Mecanismos de compresión y de-duplicación de los datos a ser replicados. - Replicación bidireccional entre dos centros de datos. - Posibilidad de limitar el ancho de banda usado por la replicación desde la - interfaz de administración de la solución hiperconvergente. - Replicar máquinas virtuales entre dos hipervisores diferentes. convirtiendo la máquina virtual de un hipervisor a otro de forma automática.
3.2.1.2.13	La solución debe soportar el respaldo y restauración de copias de las máquinas virtuales y archivos hacia la nube pública.
3.2.1.2.14	La solución hiperconvergente con el hipervisor propuesto, debe tener los drivers incluidos para la integración con Openstack, para mínimo los servicios de cómputo, imágenes, volúmenes y red.
3.2.1.2.15	El hipervisor ofrecido con la solución de hiperconvergencia, debe incluir la funcionalidad de ubicación inteligente de máquinas virtuales utilizando estadísticas de uso de CPU/RAM/almacenamiento del clúster en tiempo real de manera que se garantice a las cargas de trabajo el mejor acceso posible a los recursos. Esta funcionalidad debe venir habilitada por defecto.
3.2.1.2.16	El hipervisor ofrecido con la solución de hiperconvergencia, debe permitir la definición de redes virtuales (SDN) mediante un switch virtual con soporte y mapeo de vLans, Link Aggregation, y visualización sobre los puertos físicos.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.1.2.17	La solución debe soportar al menos 3 diferentes tipos de hipervisores tales como VMware ESXi, Microsoft Hyper-V Server y/o una distribución basada en KVM. Igualmente debe estar soportada la instalación del software en instancias de nube pública.
3.2.1.2.18	El hipervisor ofrecido con la solución de hiperconvergencia, debe proveer la capacidad de crear un camino directo de comunicación por cada vCPU hacia el almacenamiento sin implicar la instalación de ningún componente adicional.
3.2.1.2.19	El hipervisor ofrecido con la solución de hiperconvergencia, debe poder ser actualizado desde la misma consola gestión del sistema hiperconvergente a las últimas versiones sin disrupción del servicio.
3.2.1.3	**CARACTERÍSTICAS FUNCIONALES PARA LA ADMINISTRACIÓN Y MONITOREO DE LA SOLUCIÓN DE HIPERCONVERGENCIA**
3.2.1.3.1	La solución deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del clúster (servicios de almacenamiento, firmware de los nodos e hipervisor) directamente desde la consola web y de forma no disruptiva, es decir, sin necesidad de reinicio de las máquinas virtuales, ni solicitud de ventanas de mantenimiento ni indisponibilidad del servicio.
3.2.1.3.2	La solución propuesta debe incorporar la capa de software de gestión de la infraestructura de hiperconvergencia instalada como un servicio en cada uno de los nodos que componen la solución manteniendo una arquitectura de alta disponibilidad.
3.2.1.3.3	La solución de hiperconvergencia debe integrar herramientas de monitoreo y análisis predictivo de capacidad de cómputo, que permita determinar el análisis de crecimiento, de acuerdo con las necesidades de la entidad.
3.2.1.3.4	La interfaz de gestión debe estar construida sobre una interfaz HTML5 y ser administrado como mínimo a través de los navegadores Chrome, Firefox, Safari o Microsoft Edge.
3.2.1.3.5	La solución ofertada deberá incluir con el hipervisor propuesto un portal de auto aprovisionamiento que permita la creación de proyectos, perfiles, usuarios, máquinas virtuales, plantillas de máquinas virtuales, de tal forma que la permita al cliente la automatización en la creación de servicios a usuario internos sin la necesidad de intervención de los administradores de infraestructura.
3.2.1.3.6	La interfaz deberá permitir gestión global y federada, es decir, desde un solo panel de administración se deberán gestionar todos los componentes de la solución hiperconvergente.
3.2.1.3.7	La interfaz para el auto aprovisionamiento debe soportar la integración con el directorio activo y certificados firmados por SSL, para el manejo de la autenticación de los usuarios que acceden.
3.2.1.3.8	La interfaz para la administración debe permitir determinar en tiempo real el consumo de los recursos de CPU, Memoria RAM, y almacenamiento.
3.2.1.3.9	La interfaz de administración de solución de hiperconvergencia, deberá entregar estadísticas completas sobre las máquinas virtuales como consumos de vCPU, RAM, y discos, así como IOPS de lectura, IOPS de escritura y latencias.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.1.3.10	La interfaz para el auto aprovisionamiento debe contar con un catálogo donde se puedan configurar plantillas de máquinas virtuales y las imágenes que se deseen poner a disposición de los usuarios del portal.
3.2.1.3.11	La interfaz debe permitir la creación de diferentes roles de usuarios.
3.2.1.3.12	La interfaz de administración y monitoreo de la solución de hiperconvergencia deberá proveer accesos alternativos basados en SSH y/o interfaces seriales remotas, administración fuera de banda.
3.2.1.3.13	Soportar integración mediante el uso de REST API, a otras soluciones de administración para facilitar la integración con ambientes de monitoreo actuales.
3.2.1.3.14	La interfaz debe permitir el análisis de ancho de banda utilizado por la misma, así como el ancho de banda de una máquina virtual.
3.2.1.3.15	La solución debe distribuir los datos en el almacenamiento interno del clúster y adicionalmente replicarlos internamente para poder asegurar su disponibilidad, basados en Software y no en mecanismos legacy de hardware tipo RAID.
3.2.1.3.16	La solución debe incluir una funcionalidad que ejecute tareas de optimización automatizada de recursos, que permita realizar proyecciones de capacidad, tareas de planeación, basadas en tecnologías como machine learning.
3.2.1.3.17	La solución de hiperconvergencia debe incluir e integrar funcionalidades de aprovisionamiento, monitoreo y análisis predictivo de capacidad de cómputo, que permita determinar el análisis de crecimiento, de acuerdo con las necesidades de la entidad.
3.2.1.3.18	La solución debe incluir una funcionalidad que realice detección de anomalías, basadas en análisis de comportamiento para generar alertas tempranas.
3.2.1.3.19	La solución debe incluir un catálogo de acciones que se inicien automáticamente, ante la activación de una alerta específica.
3.2.1.3.20	La solución debe tener la capacidad de aprender el estado o condición normal de todos los elementos bajo su gestión, a lo largo del tiempo, y alertar cuando las condiciones son anormales, en lugar de esperar a que las condiciones estén violando alguna regla, política o umbral. Todo esto basado en análisis de comportamiento / machine learning.
3.2.1.3.21	La solución debe incluir una función que permita al personal crear tareas automatizadas para acciones de remediación o troubleshooting, basadas en alertas a través de un Wizard de Configuración.
ITEM	**DESCRIPCION**
3.2.2	**SISTEMA DE ALMACENAMIENTO PARA LAS COPIAS DE SEGURIDAD**
3.2.2.1	**CARACTERÍSTICAS GENERALES**
3.2.2.1.1	El oferente deberá demostrar el cumplimiento de los requerimientos con los enlaces web, catálogos o documentos técnicos que permitan validar el cumplimiento.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.1.	El oferente deberá entregar, instalar a la solución de hiperconvergencia, configurar y poner en funcionamiento, un servidor para el almacenamiento de copias de seguridad y recuperación de datos en entornos virtuales y físicos.
3.2.2.1.2	Debe ser un sistema inteligente de almacenamiento para copias de seguridad (backups) en disco, que se entiende como un dispositivo con el propósito específico de almacenamiento para copias de seguridad (backups) con cifrado, compresión, deduplicación y replicación de datos de-duplicados. Demostrando eso con los enlaces web, catálogos o documentos técnicos
3.2.2.1.3	El equipo o equipos propuestos deberán ser totalmente nuevos
3.2.2.1.4	El sistema para las copias de seguridad debe permitir el uso de todas las funcionalidades, tecnologías y recursos especificados, de forma perpetua, sin restricciones y sin necesidad de contemplar licencias adicionales. Es decir, los equipos deberán seguir funcionando normalmente incluso vencido el período de mantenimiento del fabricante
3.2.2.1.5	El sistema debe tener una arquitectura Scale-Out
3.2.2.1.6	Debe tener una interfaz WEB segura usando https con certificados tls para la administración del sistema de almacenamiento de respaldo
3.2.2.1.7	Debe llegar a tasas de de-duplicación de maximo 50:1 y en promedio máximo 15:1 dependiendo del cambio diario, tipos de datos y retenciones
3.2.2.1.8	Debe tener de-duplicación global identificando datos duplicados de copias de seguridad de diferentes fuentes dentro del mismo sistema para maximizar la tasa de optimización, esto incluyendo diferentes equipos o controladoras donde se almacenan los respaldos
3.2.2.1.9	Los crecimientos en el mismo sistema para las copias de seguridad deben permitir aumentar la capacidad de disco usable, así como la capacidad de cómputo para aumentar el desempeño de ésta, incluso cuando se requiera más almacenamiento por el crecimiento de los datos
3.2.2.1.10	Debe tener capacidades de tolerancia a fallas de discos, fuentes de alimentación y ventiladores
3.2.2.1.11	Los equipos del sistema de almacenamiento para las copias de seguridad deben tener mecanismos de protección contra la inconsistencia de los datos incluso en casos de interrupción abrupta o apagado accidental, esta protección debe ser adicional a la entregada por el RAID.
3.2.2.1.12	El sistema de almacenamiento para las copias de seguridad debe implementar mecanismos de validación de coherencia para los datos de-duplicados almacenados, lo que garantiza que estén en buen estado durante las copias de seguridad, las restauraciones y las replicaciones. La tecnología debe reparar automáticamente los datos que no son consistentes con las rutinas realizadas. El mecanismo debe ser nativo del equipo, y no se aceptan scripts para dar servicio a este artículo
3.2.2.1.13	El o los equipos del sistema incluidos en la propuesta deben ser entregados con 2 puertos de red de 1GbE para propósitos de administración

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.1.14	El o los equipos del sistema incluidos en la propuesta deben ser entregados con mínimo 2 puertos de red de 10 Gigabit Ethernet SFP+ Optical
3.2.2.1.15	El sistema de almacenamiento para las copias de seguridad debe soportar crecimientos y actualizaciones de equipos con configuraciones de red mínimo a 10 Gigabit Ethernet SFP+ Optical , 10 Gigabit Ethernet SFP+ TWINAX y/o 25Gbps Gigabit Ethernet SFP28 Optical , o Gigabit Ethernet SFP28 Twin Axial
3.2.2.1.16	Debe permitir la implementación de topologías de replicación, como 1 a 1, 1 para N, N a 1 y equipos en cascada. La solución debe permitir la replicación de los datos retenidos, a la nube pública
3.2.2.1.17	Cada equipo del sistema debe tener al menos un (1) puerto iLO/iDRAC/IPMI o similar
3.2.2.1.18	El sistema debe enviar soporte de alertas usando monitoreo de fabrica (Call home) y Syslog, SNMP, SMTP
3.2.2.1.19	El sistema debe soportar a IPV4 e IPV6
3.2.2.2	**CARACTERÍSTICAS ESPECIFICAS SOFTWARE DE COPIAS DE SEGURIDAD**
3.2.2.2.1	La solución debe proporcionar en una única consola capacidades de gestión para procesos de respaldo sin agentes para ambientes virtuales, replicación de máquinas virtuales on premises, gestión y distribución de agentes para maquinas físicas y gestión de respaldos y recuperación de máquinas virtuales sobre ambientes cloud
3.2.2.2.2	La solución debe proporcionar una copia de seguridad eficiente "incremental para siempre" e incluir opciones de copias de seguridad completas y ad-hoc para cualquiera que sea la carga objetivo (VM Onpremises, VM Cloud Publica, NAS, Servidor Físico).
3.2.2.2.3	La solución debe admitir la copia de seguridad de VM directamente para ambientes hyperconvergentes sin licenciamiento adicional.
3.2.2.2.4	La solución debe detectar automáticamente el espacio libre del datastore productivo y evitar la creación de snapshot para respaldo, si el espacio está por debajo del umbral definido.
3.2.2.2.5	La solución debe monitorear automáticamente la latencia del datastore productivo durante la copia de seguridad y reducir la velocidad de la copia de seguridad si la latencia del datastore supera un umbral definido.
3.2.2.2.6	La solución deberá permitir tomar respaldos a partir de los Snapshots generados por el almacenamiento de producción de forma integrada, es decir, no deberá ejecutar tareas personalizadas o tareas adicionales por fuera de la consola de administración de respaldos.
3.2.2.2.7	La solución debe permitir la recuperación de Máquinas virtuales, archivos granulares de sistema operativo y de aplicación desde los snapshot's generados por el almacenamiento de producción
3.2.2.2.8	La solución no debe requerir agentes implementados en máquinas virtuales para facilitar el respaldo de aplicaciones y la ejecución de tareas de recuperación granular de aplicaciones.
3.2.2.2.9	La solución debe permitir la recuperación de archivos y elementos de aplicaciones sin instalar Agentes en Máquinas Virtuales en ningún momento del proceso.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.2.10	En los procesos de respaldo se debe permitir truncar los registros de transacciones o archivos de aplicaciones como Microsoft SQLServer, Microsoft Exchange y Oracle Database sin el uso de agentes en las máquinas virtuales en ningún momento del proceso.
3.2.2.2.11	La solución debe utilizar la tecnología Changed Block Tracking para copias de seguridad incrementales de cargas de trabajo físicas o basadas en la nube.
3.2.2.2.12	La solución debe permitir la copia de seguridad de los servidores de Windows configurados como un clúster de conmutación por error.
3.2.2.2.13	La solución debe proporcionar una portabilidad completa en cualquier archivo de respaldo ejecutado por la solución y no debe depender de ninguna infraestructura de respaldo en un punto en el tiempo, por ejemplo, el catálogo central, para la recuperación.
3.2.2.2.14	La solución debe proporcionar tecnología de recuperación de respaldo de máquinas virtuales de forma instantánea (encendido en minimo de 11 minutos y automática) desde el repositorio de respaldos ya sea que se encuentren On premises o sobre un almacenamiento de Objetos en una nube publica
3.2.2.2.15	La solución debe poder utilizar la copia de seguridad o réplica de la máquina virtual para iniciar la máquina virtual en un entorno de red aislado para fines de prueba o certificación de respaldos, sin necesidad de realizar una recuperación completa de la VM o procesos de pre-aprovisionamiento de almacenamiento
3.2.2.2.16	La solución debe poder escanear los datos de la máquina virtual a recuperar con un software antivirus antes de iniciar la restauración de la máquina al entorno de producción de forma integrada y automática. La solución debe abortar la operación de recuperación si se detecta malware.
3.2.2.2.17	La solución debe proporcionar la capacidad de iniciar la máquina virtual en un entorno de red aislado durante el proceso de recuperación e inyectar un script que permita que el servidor se modifique para fines de cumplimiento antes de la recuperación.
3.2.2.2.18	La solución debe facilitar las operaciones de recuperación a nivel de archivo sin la necesidad de implementar un agente en el servidor destino
3.2.2.2.19	La solución debe permitir la recuperación de archivos de sistema operativo directamente sobre una máquina virtual incluso cuando no haya conexión de red entre el servidor de respaldo y la máquina virtual.
3.2.2.2.20	La solución debe proporcionar una interfaz de usuario de autoservicio basada en la web con la capacidad de buscar un archivo específico en todas las copias de seguridad.
3.2.2.2.21	La solución no debe usar un producto de terceros para la recuperación granular de elementos de la aplicación.
3.2.2.2.22	La solución debe proporcionar una interfaz de usuario de autoservicio basada en web con la capacidad de examinar y recuperar elementos de Microsoft Exchange, bases de datos.
3.2.2.2.23	La solución debe estar definida por software y ser capaz de ejecutarse localmente o en cualquier plataforma en la nube.
3.2.2.2.24	La solución debe ser independiente del almacenamiento y debe contar con tecnología integrada de de-duplicación y compresión.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.2.25	La solución debe poder escalar tanto horizontal como verticalmente
3.2.2.2.26	La solución debe proporcionar un mecanismo fácil para expandir o adicionar el almacenamiento de respaldo de destino.
3.2.2.2.27	La solución debe proveer la capacidad de implementar repositorio principal de respaldo de disco con características de Inmutabilidad, definiendo el número de días los cuales los archivos de respaldo no pueden ser modificados.
3.2.2.2.28	La solución debe admitir de forma nativa la copia de seguridad en cinta y no debe requerir software adicional.
3.2.2.2.29	La solución debe admitir medios de cinta y almacenamiento primario de disco tipo WORM.
3.2.2.2.30	La solución debe proporcionar una recuperación incremental y granular del almacenamiento de objetos basado en la nube.
3.2.2.2.31	La solución debe proporcionar soporte para el almacenamiento de objetos Onpremises
3.2.2.2.32	La solución debe ofrecer un movimiento incremental de datos hacia y desde el almacenamiento basado en objetos.
3.2.2.2.33	La solución debe ofrecer inmutabilidad en el almacenamiento de objetos S3
3.2.2.2.34	La solución debe tener la opción de copiar o mover datos al almacenamiento de objetos al finalizar la copia de seguridad. incluso, ambas opciones se pueden habilitar en una misma política.
3.2.2.2.35	La solución debe encriptar los archivos de respaldo usando el encriptado AES de 256 bits. El cifrado no debe depender de la plataforma de almacenamiento de respaldo.
3.2.2.2.36	La solución debe integrarse con SAML 2.0 para la autenticación extendida.
3.2.2.2.37	La solución debe proporcionar control de acceso basado en roles.
3.2.2.2.38	Deberá permitir la delegación de tareas de recuperación, a nivel de elementos de aplicación, hacia otros usuarios, de forma tal a poder descargar la cantidad de maniobras a ejecutar por el administrador de la plataforma
3.2.2.2.39	La solución debe leer y verificar automáticamente la consistencia de los datos de producción en el archivo de copia de seguridad una vez completada la copia de seguridad. En caso de que se detecte corrupción de datos, la solución debe reconstruir automáticamente el bloque dañado con datos de producción.
3.2.2.2.40	La solución deberá poder programar tareas de encendido automático de las máquinas virtuales a partir de los respaldos y ejecutar tareas de verificación de sistema operativo y la disponibilidad de aplicaciones. Esta prueba no debe tener impacto en la red de producción. La solución debe proporcionar un informe de verificación de recuperación.
3.2.2.2.41	La solución debe escanear automáticamente los datos de producción en busca de virus durante la verificación de respaldo.
3.2.2.2.42	La solución debe presentar la tecnología de replicación directa de máquina virtuales.
3.2.2.2.43	La solución debe alertar sobre trabajos de respaldo fallidos y trabajos que exceden la ventana de respaldo

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.2.44	La solución debe alertar por adelantado si el repositorio de los respaldos se acerca a la capacidad.
3.2.2.2.45	Las copias secundarias de respaldo deberán ser independientes de la copia principal y podrán seleccionar diferentes puntos de retención con soporte a estrategias GFS
3.2.2.2.46	La solución debe presentar tecnología de aceleración WAN incorporada para la replicación de datos con la capacidad de optimizar la utilización del ancho de banda.
3.2.2.2.47	La solución debe proporcionar alertas proactivas para eliminar problemas. Estos problemas deben detectarse automáticamente, abarcar la configuración y el rendimiento con actualización dinámicamente la detección.
3.2.2.2.48	La solución debe proporcionar un informe de autoevaluación. El informe debe detectar si la solución se implementa de acuerdo con las mejores prácticas.
3.2.2.2.49	La solución debe permitir el respaldo archivos a partir de los siguientes recursos: -CIFS -NFS -VSS Snapshot -SMB -Snapshot de dispositivos de almacenamiento Ontap Onpremises o Cloud
3.2.2.2.50	La solución debe permitir configurar en una única política la retención de corta duración en días o meses y movimiento de datos para retención de larga duración en meses y años para respaldo de datos no estructurados NAS
3.2.2.2.51	Para el item 3.2.6.50 las políticas de larga retención la solución podrá definir filtros de que tipo de datos respaldados desea mover a este nivel
3.2.2.2.52	La solución debe permitir la selección de cómo se debe gestionar el respaldo de los atributos de ACL, a nivel de carpeta o archivo y carpeta
3.2.2.2.53	La solución deberá poder seleccionar el nivel de compresión deseado por cada política de respaldo
3.2.2.2.54	La solución deberá permitir la encriptación de respaldo de NAS
3.2.2.2.55	La solución debe permitir la ejecución de tareas de revisión de salud de la cadena de respaldo de NAS para verificar la consistencia e integridad de forma programada o por demanda.
3.2.2.2.56	La solución deber permitir la inclusión de scripts personalizados en las tareas de respaldo de NAS
3.2.2.2.57	La solución debe permitir los siguientes procesos de recuperación granular a partir de los respaldos de NAS: -Recuperación de archivos granulares y carpetas de CIFS y NFS -Recuperación de archivos granulares y carpetas de servidores gestionados de sistemas operativos Windows.
3.2.2.2.58	La solución deberá proveer la capacidad de devolver en un instante del tiempo toda una carpeta o recurso compartido completo sobre el recurso compartido original o uno

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

	totalmente diferente de locación incluso de almacenamiento a partir de los respaldos de NAS
3.2.2.2.59	La solución deberá permitir la recuperación completa de un recurso compartido de los puntos disponibles de respaldo de NAS
3.2.2.2.60	La solución deberá permitir la recuperación granular desde el repositorio de larga retención para los respaldos de NAS
3.2.2.2.61	La solución deberá incluir la capacidad de recuperación instantánea de un respaldo de NAS en forma de recurso compartido para ser accedido por la organización, este proceso no debe estar limitado por el tamaño del respaldo o los datos a acceder.
3.2.2.2.62	La solución debe proveer la capacidad de realizar réplicas de máquinas virtuales sin necesidad de generar snapshots y sin dependencia de hardware en origen y destino. La réplica de máquinas virtuales debe ser basada en política de RPO (máxima pérdida de datos permitida en caso de desastre) en intervalos de ejecución en segundos.
3.2.2.2.63	La solución debe proporcionar un informe sobre máquinas virtuales que no están protegidas por copia de seguridad y un informe de cumplimiento de RPO (Objetivo del punto de recuperación) para las máquinas virtuales protegidas Onpremises y Cloud
3.2.2.2.64	La solución debe proporcionar planificación de capacidad y pronosticar la utilización del espacio de almacenamiento de respaldo.
3.2.2.2.65	La solución debe proporcionar un informe automatizado sobre todas las operaciones de recuperación para fines de auditoría.
3.2.2.2.66	La solución debe ofrecer la capacidad de generar alarmas y acciones de remedición en monitoreo de procesos y servicios de VM de ambientes Windows Onpremises
3.2.2.2.67	Se debe proveer la capacidad de generar reportes personalizados basados en datos de inventario y uso de recursos de la plataforma virtual, como también de la plataforma de respaldo
3.2.2.2.68	La solución debe proporcionar informes de uso por cada uno de los almacenamientos usados por la solución, Onpremises o cloud
3.2.2.2.69	La solución debe proporcionar informes históricos y actuales de las sesiones de respaldo para todos los tipos de cargas configurados en la solución (Cloud - Onpremises)
3.2.2.2.70	La solución debe proporcionar informes tipo chargeback del uso de recursos
3.2.2.2.71	Deberá ofrecer un conjunto de reportes capaces de presentar la siguiente información: -Reportes que permitan la planificación de la capacidad. -Reportes que permitan la determinación de inefectividad en el uso de recursos. -Reportes que faciliten la visibilidad de tendencias negativas y anomalías de respaldo y uso de almacenamiento. -Envió automático y programado de reportes de auditoria para operaciones de recuperación y modificaciones a políticas de respaldos o replicación. -Tableros de control claros, presentables e integrables en sitios web.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.3	**INTEGRACION**
3.2.2.3.1	El sistema de almacenamiento debe soportar integración para diferentes software o herramientas de copias de seguridad o backups utilizando CIFS, NFS y S3
3.2.2.3.2	El sistema de almacenamiento para las copias de seguridad debe poseer la función Veeam Data Mover y Veritas OST interna en el dispositivo de backup
3.2.2.3.3	El sistema debe soportar realizar copias de seguridad de aplicaciones y bases de datos como: Oracle y Microsoft SQL. Sin utilizar software de copia de seguridad para evitar el consumo de sus licencias y sin la necesidad de licenciar volúmenes (TB) o servidores de bases de datos (CPU, Tier, Core).
3.2.2.4	**ALMACENAMIENTO, CAPACIDAD Y ESPACIO EN RACK**
3.2.2.4.1	La capacidad del sistema de backup a disco propuesto debe ser de mínimo 160TB usables, (sin considerar desborde a la nube o cloud tier, tasas de de-duplicación, compresión).
3.2.2.4.2	El crecimiento mínimo del sistema de backup a disco debe ser de 1.5PB usables, (sin considerar desborde a la nube o cloud tier, tasas de de-duplicación, compresión y pérdidas de formato).
3.2.2.4.3	Debe suministrarse con discos duros conectables en caliente e intercambiables en caliente, lo que permite su reemplazo sin necesidad de interrumpir el funcionamiento de la solución
3.2.2.4.4	El o los equipos del sistema deben entregarse con arreglos de disco duro tipo RAID-6 por hardware con hot spare y protección ante interrupciones de energía
3.2.2.4.5	Debe tener licencia para replicar todo el sistema de almacenamiento de información de backup, incluida la capacidad de expansión
3.2.2.4.6	Debe ser instalado en rack estándar de 19 pulgadas, profundidad máxima de 36 pulgadas o 915mm
3.2.2.5	**DESEMPEÑO**
3.2.2.5.1	Debe llegar a tasas de transferencia de 15TB/hr. Desempeño sin requerir recursos (CPU, Memoria) de los clientes ni los servidores de respaldo.
3.2.2.5.2	El sistema de almacenamiento para las copias de seguridad propuesto debe escalar a tasas de transferencia mínimo de 90TB/hr.
3.2.2.6	**CIBER RECUPERACION Y SEGURIDAD**
3.2.2.6.1	El sistema de almacenamiento para las copias de seguridad debe tener protección ante ciberataques que puedan destruir los respaldos, borrándolos o cifrándolos.
3.2.2.6.2	Se debe entregar una arquitectura con Air-Gap o bóveda de seguridad para los datos protegidos en el sistema de almacenamiento, datos retenidos sin exposición a la red e independiente al software de respaldo para una mayor protección incluso cuando este ha sido comprometido

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.2.2.6.3	El sistema de almacenamiento para las copias de seguridad debe tener la capacidad de analizar los datos respaldados en sus repositorios y si ocurre un borrado de datos por arriba de un umbral definido, debe generar alertas para los administradores.
3.2.2.6.4	El sistema de almacenamiento para las copias de seguridad debe tener alertas ante posibles cifrados de los datos en el almacenamiento de producción o en el mismo sistema el almacenamiento para copias de seguridad o respaldo
3.2.2.6.5	El sistema de almacenamiento para las copias de seguridad debe soportar doble factor de autenticación para usuarios configurados en el equipo para el acceso a la gestión del sistema a través de la integración con sistemas de contraseñas desechables (contraseña de un solo uso - OTP), como Google Authenticator, Microsoft Authenticator o similares, característica soportada para usuarios locales del sistema de almacenamiento sin y con integración al directorio activo.
3.2.2.6.6	El sistema debe permitir configurar usuarios basado en roles y doble validación para actividades críticas en el sistema
3.2.2.6.7	El sistema de almacenamiento debe soportar cifrado para los datos respaldados en reposo basado en disco para no afectar el desempeño de la solución y validado por FIPS 140-2
3.2.2.6.8	El sistema debe soportar seguridad en WAN para la replicación cifrada usando AES de 256 bits, función de seguridad aprobada por FIPS PUB 140-2.
ITEM	**DESCRIPCION**
2.2.3	**INTERRUPTOR DE TRANSFERENCIA DE RACK HIBRIDO INTELIGENTE**
2.2.3.1	Para garantizar la continuidad de la operación, es necesario suministrar un interruptor de transferencia de Rack hibrido inteligente (Switch de transferencia), que permita mantener el suministro de energía hacia los equipos de la solución hiperconvergente en caso de fallos en las fuentes de alimentación (Energia eléctrica o UPS) que cumpla con las siguientes características:
2.2.3.2	Transferencias de carga ultrarrápidas entre 4 y 8 milisegundos, probadas para no interrumpir la carga de energía en condiciones reales.
2.2.3.3	Relés para manejar cargas grandes con alta fiabilidad
2.2.3.4	Evita las transferencias de cortocircuitos de salida, lo que podría llevar a una falla en cascada del segundo suministro de energía.
2.2.3.5	Suministro de energía redundante y arquitectura de controlador inteligente impulsada por firmware
2.2.3.6	Firmware Xerus con scripting
2.2.3.7	Umbrales configurables por el usuario para la calidad de la energía
2.2.3.8	Interfaz configurable basada en la web.
2.2.3.9	Seguridad de red robusta y protocolos de encriptación: AES128, SSH, SNMPv3, Smart TLS, FIPS 140-2.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

2.2.3.10	Tecnología híbrida (diseño de relé más SCR) para una mejor eficiencia energética y menos calor (arquitectura sin ventilador).
2.2.3.11	Precisión de medición de energía de grado de facturación (+/-1%).
2.2.3.12	Interruptor de transferencia de rack con medición de energía, monitoreo de calidad de energía y soporte para sensores ambientales opcionales
2.2.3.13	Pantalla local que muestra el estado del interruptor de transferencia y las condiciones de conmutación por falla de un vistazo.
2.2.3.14	Debe estar en la capacidad de operar a temperaturas de hasta 60° C (UL), 50° C (CE) en un entorno con 85% de humedad relativa (RH).
2.2.3.15	Compatible con SecureLock para prevenir desconexiones accidentales.
2.2.3.16	Componentes de estado sólido para transferencias rápidas
2.2.3.17	Elimina los arcos eléctricos que causan fallos en los relés de transferencia.
2.2.3.18	Identifica los cortocircuitos de salida y envía una alarma para que el cortocircuito pueda ser corregido antes de realizar la transferencia de energía manualmente.
2.2.3.19	Proporciona conmutación y medición a nivel de toma de corriente, así como energía confiable para dispositivos de un solo cable.
2.2.3.20	Sistema con diseño sin ventilador
2.2.3.21	Interfaz gráfica de usuario (GUI) intuitiva, SNMP, Modbus, TCP/IP, JSON-RPC para scripting, IPv4 / IPv6.
2.2.3.22	Acceso y control desde tabletas frontales y traseras a través de puertos USB.
2.2.3.23	Alertas por umbral y actualizaciones de estado a través de mensajes de texto GSM, correo electrónico y syslog.
2.2.3.24	Registra los tiempos de transferencia para informes.
2.2.3.25	Soporte para sensores ambientales plug-and-play.
2.2.3.26	Disponible en una unidad de rack
2.2.3.27	Deberá poderse conectar a los switch de transferencia inteligentes y las PDU inteligentes con las que cuenta actualmente el datacenter para gestionar de manera unificada.

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

3.3.1 Empaque.

Todos los equipos deberán venir correctamente empacados de acuerdo a la normatividad vigente para equipos tecnológicos.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

3.3.2 Rotulado.

Todos los elementos suministrados para la solución deben ser etiquetados, de acuerdo a la norma técnica internacional ANSI / TIA-606-C y previa aprobación del supervisor del contrato.

4. TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO:

4.1 TOMA DE MUESTRAS Y CRITERIO DE ACEPTACIÓN O RECHAZO PARA EVALUAR LOS REQUISITOS GENERALES Y REQUISITOS DE EMPAQUE Y ROTULADO

4.1.1 Muestreo.

Para verificar los requisitos generales, de empaque y rotulado se deben someter a evaluación todo el Sistema de procesamiento de datos de seguridad que se vaya a suministrar. Evaluando todos sus componentes.

4.1.2 Criterios de aceptación o rechazo para requisitos generales y requisitos de empaque y rotulado.

El criterio para aceptar o rechazar el producto depende del cumplimiento de todos los requisitos.

4.2 TOMA DE MUESTRAS Y CRITERIOS DE ACEPTACIÓN O RECHAZO PARA EVALUAR REQUISITOS ESPECÍFICOS.

4.2.1 Muestreo.

No aplica

4.2.2 Criterio de aceptación o rechazo para evaluar requisitos específicos.

No aplica

5. MÉTODOS DE ENSAYO

No aplica

6. APÉNDICE

6.1 NORMAS QUE DEBEN CONSULTARSE

- Constitución Política de Colombia.
- Código Civil.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

- Código General del Proceso.
- Código de Comercio.
- Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 80 de 1993 "Por la cual se expide el Estatuto General de Contratación de la Administración Pública" y las demás normas que la modifiquen o aclaren.
- Ley 816 de 2003 "Por medio de la cual se apoya a la industria nacional a través de la contratación pública" y las demás normas que la modifiquen o aclaren.
- Ley 1150 de 2007 "Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos" y las demás normas que la modifiquen o aclaren.
- Ley 1341 de 2009 "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones" y las demás normas que la modifiquen o aclaren.
- Ley 1474 de 2011 "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública" y las demás normas que la modifiquen o aclaren.
- Decreto Ley 19 de 2012 "Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública" y las demás normas que lo modifiquen o aclaren.
- 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" y las demás normas que la modifiquen o aclaren.
- Decreto 1082 de 2015 "por medio del cual se expide el Decreto Único Reglamentario del sector Administrativo de Planeación Nacional" y las demás normas que lo modifiquen o aclaren.
- Decreto 103 del 20 de enero de 2015 "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones" y las demás normas que lo modifiquen o aclaren.
- Resolución 2710 de 2017 del Ministerio de Tecnologías de la Información y las Comunicaciones "Por la cual se establecen lineamientos para la adopción del protocolo IPv6", modificada por la resolución No. 1126 de 2024 y las demás normas que la modifiquen o aclaren.
- Resolución 4223 de 2022 "Por la cual se delegan unas funciones y competencias relacionadas con la contratación de bienes y servicios con destino al Ministerio de Defensa nacional, unas funciones de carácter administrativo y se dictan otras" y las demás normas que la modifiquen o aclaren.
- Resolución 4130 de 2022 "MANUAL DE CONTRATACIÓN Y DE CONVENIOS" del Ministerio de Defensa Nacional y las demás normas que la modifiquen o aclaren.
- Resolución 7870 de 2022 del Ministerio de Defensa, Por la cual se emite y adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y Continuidad de los Servicios Tecnológicos en las Unidades

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial

Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa y se dictan otras disposiciones.

- Directiva permanente 00201 de 2017 "Lineamiento de Ciberseguridad y Ciberdefensa para el Ejército Nacional" y las demás normas que la modifiquen o aclaren.
- Directiva permanente 00221 de 2017 "Seguridad de la información para el Ejército Nacional" y las demás normas que la modifiquen o aclaren.
- Procedimiento documentos técnicos normativos P-JEMPP-CEDE4-348

6.2 ANTECEDENTES

Omitido

7. ANEXOS

Omitido.

8. CONTROL DE REVISIONES

Revisión y/o Actualización	Modificaciones	Fecha
00	Creación de especificación técnica SISTEMA DE PROCESAMIENTO DE DATOS DE SEGURIDAD PARA EL EJÉRCITO NACIONAL en cumplimiento a la circular 2023218017093013 del 03 de octubre del 2023 acogiéndose al numeral 20.1 "Citar el documento que motivo la creación o actualización de la Especificación Técnica" por medio del oficio No. 2025574001253173 de fecha 18 de enero de 2025 elaborado por el BACCI y oficio número 2025229001384313 del 20 de enero del 2025 elaborado por el CEDE6. El Batallón de Ciberdefensa y Ciberseguridad BACCI, en cumplimiento a la circular 2023218017093013 del 03 de octubre del 2023 acogiéndose al numeral 20.2 "La unidad en este documento técnico garantiza la pluralidad de oferentes" El Batallón de Ciberdefensa y Ciberseguridad BACCI, en cumplimiento a la circular 2023218017093013 del 03 de octubre del 2023 acogiéndose al numeral 20.3 "La unidad garantiza los requisitos generales y específicos, los cuales fueron revisados técnicamente y satisfacen las necesidades del Ejército Nacional" El Batallón de Ciberdefensa y Ciberseguridad BACCI, en cumplimiento a la circular 2023218017093013 del 03 de octubre del 2023 acogiéndose al numeral 20.4" La unidad garantiza que este documento técnico fue elaborado de manera profesional, con la mayor transparencia, siempre buscando enaltecer el nombre del Ejército Nacional.	28/01/2025

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial