ANEXO ESPECIFICACIONES TECNICAS DE OBLIGATORIO CUMPLIMIENTO

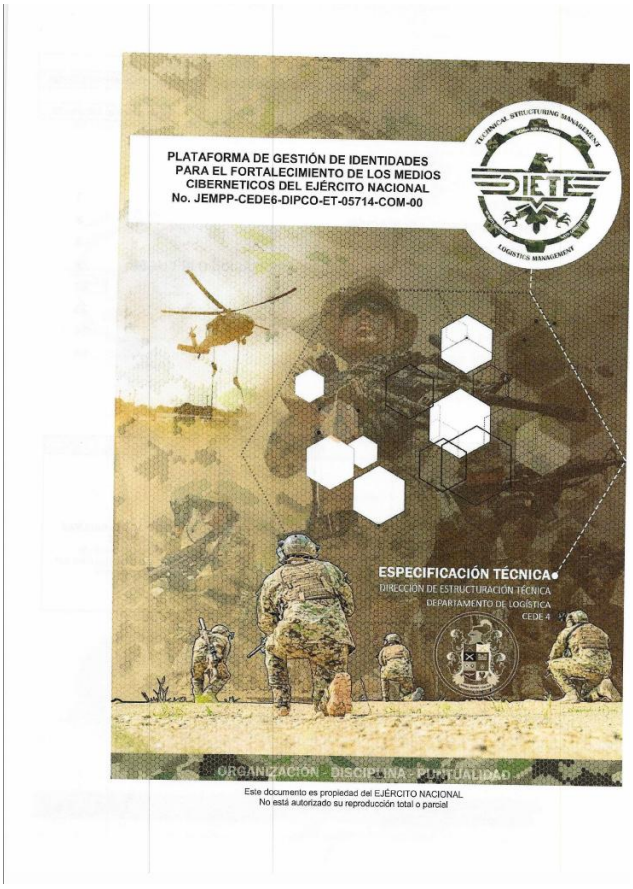
Facatativá XX de XXXXX de 2025

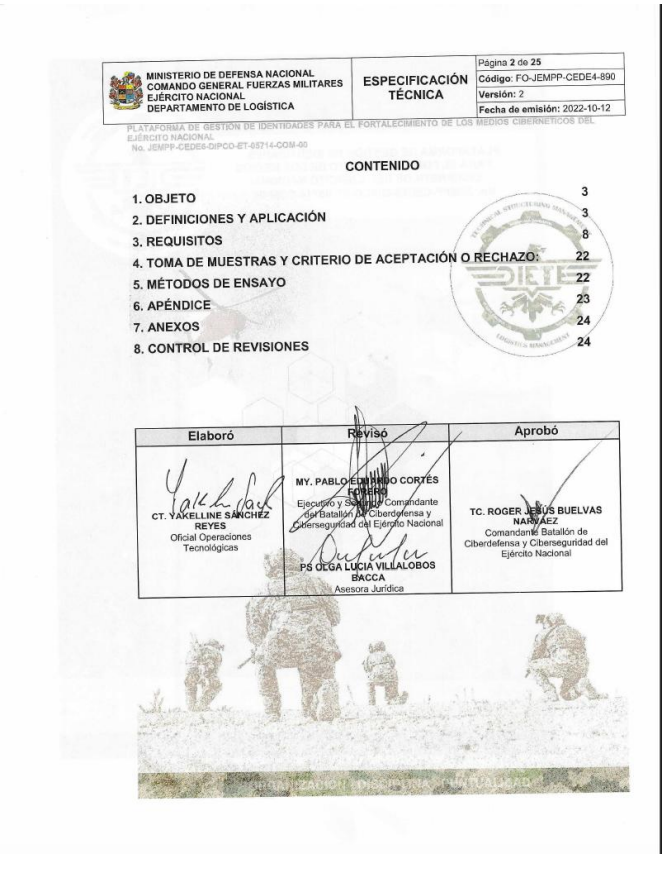
(El apoderado o representante legal), obrando en nombre y representación de conformidad con lo establecido en la Invitación a ofertar, ofertó de forma irrevocable, los siguientes bienes o servicios objeto del presente proceso de contratación, con las siguientes características técnicas:

CUMPLIMIENTO

Para efectos de establecer las especificaciones técnicas del presente proceso, cuyo objeto es la **"ADQUISICIÓN, INSTALACIÓN Y CONFIGURACIÓN DE UNA PLATAFORMA DE GESTIÓN DE IDENTIDADES PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNÉTICOS DEL EJÉRCITO NACIONAL, A EJECUTAR EN LA VIGENCIA 2025"** se debe dar aplicabilidad a la Ficha Técnica **No. JEMPP-CEDE6-DIPCO–ET-05714-COM–00 PLATAFORMA DE GESTIÓN DE IDENTIDADES PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNETICOS DEL EJÉRCITO NACIONAL**, y a las **ESPECIFICACIONES TECNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO**, las cuales contienen los parámetros técnicos que deben cumplir los oferentes y el contratista en la acreditación de la adquisición de los bienes, los cuales se describen a continuación:

FICHA TÉCNICA JEMPP-CEDE6-DIPCO–ET-05714-COM–00





1. OBJETO

Establecer los requisitos mínimos para la protección de la infraestructura tecnológica del Ejercito Nacional, garantizando la identidad de los usuarios que cuentan con acceso a los recursos informáticos de las plataformas del Ejército Nacional.

2. DEFINICIONES Y APLICACIÓN

2.1 DEFINICIONES

Amenaza Cibernética: es una indicación de que un hacker o actor malicioso está intentando obtener acceso no autorizado a una red para lanzar un ataque cibernético[1].

Aplication-to-Aplication: arquitectura de integración de sistemas en la que dos o más aplicaciones se comunican directamente entre sí, sin la intervención de una interfaz de usuario. Es decir, las aplicaciones intercambian datos y comandos de manera automatizada, siguiendo protocolos y formatos de datos predefinidos[2].

Aplication-to-DataBase: describe la interacción directa entre un software de aplicación y una base de datos. Esta conexión permite que la aplicación pueda leer, escribir, modificar y eliminar datos almacenados en la base de datos. Esencialmente, la aplicación sirve como interfaz entre el usuario y los datos subyacentes[3].

Autenticación: es el proceso que usan las empresas para confirmar que solo las personas, servicios y aplicaciones adecuados con los permisos correctos pueden acceder a recursos de la organización. Es una parte importante de la ciberseguridad porque la mayor prioridad de un infiltrado es obtener acceso no autorizado a los sistemas. Para llevar esto a cabo, roban el nombre de usuario y las contraseñas de los usuarios que sí tienen acceso[4].

Backup: copia de seguridad, respaldo o copia de reserva es una réplica exacta de los datos originales, creada con el propósito de recuperarlos en caso de pérdida o daño[5].

[1] Tomado de https://www.ibm.com/mx-es/think/topics/cyberthreats-types#:~:text=IBM%20Cloud%20Team&text=En%20el%20sentido%20m%C3%A1s%20sencillo,para%20lanzar%20un%20ataque%20cibern%C3%A9tico.
[2] Tomado de https://www.ibm.com/think/topics/application-integration
[3] Tomado de https://learn.microsoft.com/es-es/dotnet/framework/data/adonet/sql/linq/communicating-with-the-database
[4] Tomado de https://www.microsoft.com/es-co/security/business/security-101/what-is-authentication
[5] Tomado de https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

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

Certificado Digital: documento electrónico emitido por una autoridad de certificación de confianza que vincula una identidad a una clave pública[6].

Ciberataque: es cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos a través del acceso no autorizado a una red, sistema informático o dispositivo digital[7].

DevOps: metodología que combina las prácticas de desarrollo de software (Dev) y las operaciones de tecnología de la información (Ops). Su objetivo principal es acortar el ciclo de vida del desarrollo de software y proporcionar una entrega continua de alta calidad[8].

Endpoints: cualquier dispositivo que se conecta a una red y puede servir como punto de entrada o salida de datos[9].

Fail-Over: conmutación por error, es una estrategia de alta disponibilidad que permite a un sistema continuar funcionando sin interrupciones significativas en caso de una falla[10].

Gateway: un dispositivo o software que conecta dos o más redes con diferentes protocolos o arquitecturas. Actúa como un traductor, permitiendo que los dispositivos en una red puedan comunicarse con dispositivos en otra red[11].

Gestión de Acceso e Identidades (Identity and Access Management IAM): es la disciplina de ciberseguridad que se ocupa de cómo los usuarios acceden a los recursos digitales y qué pueden hacer con esos recursos. Los sistemas IAM mantienen alejados a los hackers al mismo tiempo que garantizan que cada usuario individual tenga los permisos exactos que necesita para hacer su trabajo y no más que eso[12].

Gestión de Acceso Privilegiado (Privileged Access Management PAM): hace referencia a la gestión y protección de cuentas que tienen permisos de acceso a

[6] Tomado de https://www.aepd.es/
[7] Tomado de https://www.ibm.com/es-es/topics/cyber-attack
[8] Tomado de https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-devops
[9] Tomado de https://www.cyberark.com/es/what-is/endpoint-security/
[10] Tomado de https://www.ansys.es/blog/failover-failback
[11] Tomado de https://www.adaptixnetworks.com/puerta-de-enlace/
[12] Tomado de https://www.ibm.com/es-es/topics/identity-access-management

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

sistemas y datos altamente sensibles, como las cuentas de administración de TI, los sistemas de liquidación de sueldos y los repositorios de códigos[13].

Gobernanza: se refiere a uno o varios marcos que gestionan la forma en que las organizaciones optimizan el uso de las operaciones de 00para lograr los objetivos de negocio[14].

GPO: Group Policy Object u Objeto de Directiva de Grupo, es una herramienta fundamental dentro del entorno de Active Directory de Microsoft que permite a los administradores de sistemas aplicar de forma centralizada configuraciones a los equipos y usuarios de una red[15].

HelpDesk: mesa de ayuda, es un servicio que ofrece soporte técnico a los usuarios de una organización. Es el primer punto de contacto para cualquier consulta, problema o solicitud relacionada con la tecnología[16].

HTML: se conoce como Hyper Text Markuo Languaje o Lenguaje de Marcado de Hipertexto. Es el fundamento o lenguaje sobre el que se construye toda página web, se utiliza para estructurar el contenido de forma sencilla para que cualquier usuario pueda acceder a la información de forma sencilla y útil[17].

Identidad digital: es el conjunto de información que sumado proyecta una imagen o reputación acerca de nosotros en Internet. Está conformada, en gran parte, por nuestra huella digital y de aquellos datos que constantemente generamos de forma consciente o inconsciente[18].

In-House: Se refiere a la metodología en la que la propia Entidad desarrolla su software con sus desarrolladores y analistas quienes conocen el negocio[19].

[13] Tomado de https://www.keepersecurity.com/es_ES/resources/glossary/what-is-privileged-access-management/#:~:text=La%20gesti%C3%B3n%20de%20acceso%20privilegiado%20(PAM)%20hace%20referencia%20a%20la,y%20los%20repositorios%20de%20c%C3%B3digos.
[14] Tomado de https://www.ibm.com/mx-es/think/topics/it-governance
[15] Tomado de https://learn.microsoft.com/es-es/windows-server/identity/ad-ds/manage/group-policy/group-policy-overview
[16] Tomado de https://www.zendesk.com.mx/blog/como-funciona-un-help-desk/
[17] Tomado de https://universidadeuropea.com/blog/que-es-html/
[18] Tomado de https://www.santander.com/es/stories/que-es-la-identidad-digital
[19] Tomado de https://sigi.sic.gov.co/SIGI/portal/view_term.php?idTermino=1090

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

LDAP: Lightweight Directory Access Protocol, o Protocolo Ligero de Acceso a Directorios) es un protocolo de red que se utiliza para acceder y gestionar información de manera centralizada en un entorno de red[20].

Man In the Middle: hombre en el medio" en español, es una técnica de hacking en la que un atacante se interpone en una comunicación entre dos partes, como un usuario y un servidor web. El atacante puede interceptar, leer, modificar o incluso retransmitir los datos que se envían entre ambas partes, sin que estas se den cuenta[21].

Multi-Tenant: es un modelo arquitectónico de software donde una sola instancia de una aplicación sirve a múltiples clientes o inquilinos de forma simultánea[22].

NTFS: New Technology File System o "Sistema de Archivos de Nueva Tecnología". Es el sistema de archivos principal utilizado en las versiones modernas de Windows, desde Windows NT 3.1 en adelante[23].

PKI: Public Key Infrastructure o Infraestructura de Clave Pública, es un sistema complejo que utiliza criptografía de clave pública para garantizar la seguridad en las comunicaciones digitales[24].

Políticas de grupos: herramienta fundamental dentro de los sistemas operativos Windows Server que permite a los administradores de sistemas configurar de manera centralizada y unificada los equipos y usuarios de una red[25].

RADIUS: Remote Authentication Dial-In User Service, es un protocolo de red estándar que se utiliza para gestionar la autenticación, autorización y contabilidad de usuarios que se conectan a una red[26].

RDP: Remote Desktop Protocol, Protocolo de Escritorio Remoto, es una tecnología desarrollada por Microsoft que permite acceder y controlar un ordenador de forma remota, como si estuvieras sentado frente a él, a través de una conexión de red[27].

[20] Tomado de https://salesystems.es/protocolo-ldap/
[21] Tomado de https://www.kaspersky.com/resource-center/threats/man-in-the-middle-attack
[22] Tomado de https://www.ibm.com/mx-es/topics/multi-tenant
[23] Tomado de https://learn.microsoft.com/es-es/windows-server/storage/file-server/ntfs-overview
[24] Tomado de https://www.certsuperior.com/pki/
[25] Tomado de https://otoiuiu.com/blog/que-son-y-para-que-sirven-las-gpo/
[26] Tomado de https://www.ibm.com/docs/es/i/7.5?topic=authentication-remote-dial-in-user-service-overview
[27] Tomado de https://www.splashtop.com/es/blog/remote-desktop-protocol-rdp

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

Riesgo cibernético: son los posibles ataques o fallos en el sistema de información digital que pueden ocasionar daños y consecuencias[28].

SAML: *Security Assertion Markup Language* o *Lenguaje de Marcado de Aserciones de Seguridad*, es un estándar abierto basado en XML que permite el intercambio de información de autenticación y autorización entre diferentes sistemas de seguridad[29].

SIEM (Security Information and Event Management): solución de seguridad que permite a las organizaciones recopilar, analizar y correlacionar datos de seguridad de diversas fuentes en tiempo real[30].

SSH: Secure Shell es un protocolo de red que permite establecer conexiones seguras y cifradas entre dos dispositivos, como una computadora y un servidor remoto[31].

VNC: *Virtual Network Computing* (Computación de Red Virtual en español), es una tecnología que permite controlar un ordenador de forma remota a través de una red[32].

Vulnerabilidad: es una debilidad existente en un sistema que puede ser utilizada por una persona malintencionada para comprometer su seguridad[33].

Workflow: secuencia ordenada de pasos, actividades o tareas necesarias para completar un proceso o alcanzar un objetivo específico[34].

XSS: Cross-Site Scripting, es una de las vulnerabilidades más comunes en aplicaciones web. Consiste en la inyección de código malicioso (generalmente JavaScript) en páginas web legítimas, con el objetivo de robar información confidencial de los usuarios o manipular su navegador[35].

Zero Trust: Confianza Cero, es un modelo de seguridad cibernética que se basa en la premisa de que no se debe confiar en ningún usuario, dispositivo o sistema, ya sea interno o externo a la red de una organización. En lugar de confiar implícitamente en

[28] Tomado de https://www.deltaprotect.com/blog/riesgos-de-ciberseguridad-ejemplos-y-prevencion
[29] Tomado de https://www.microsoft.com/es-co/security/business/security-101/what-is-security-assertion-markup-language-saml
[30] Tomado de https://www.ibm.com/es-es/topics/siem
[31] Tomado de https://www.siteground.es/kb/que-es-ssh/
[32] Tomado de https://www.realvnc.com/es/
[33] Tomado de https://www.bancosantander.es/glosario/vulnerabilidad-informatica
[34] Tomado de https://www.ibm.com/es-es/topics/workflow
[35] Tomado de https://www.cloudflare.com/es-es/learning/security/how-to-prevent-xss-attacks/

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

todo lo que se encuentra dentro del perímetro de la red, Zero Trust exige una verificación continua de la identidad y la autorización para acceder a los recursos[36].

2.2 APLICACIÓN

Esta plataforma permite asegurar el ingreso únicamente de personal autorizado a información sensible, lo cual brinda mayor seguridad, aumento de la eficiencia, mayor experiencia del usuario y escalabilidad, esto a través de la protección de cuentas, lo cual minimiza la superficie de ataque, al controlar el acceso y privilegios de los usuarios.

Permite gestionar la identidad de los usuarios, autenticarlos y autorizar el acceso a los recursos informáticos, esto incluye la creación de cuentas, la asignación de roles y permisos, y el control de acceso basado en roles. También se enfoca específicamente en la gestión de cuentas con privilegios elevados. Estas cuentas tienen acceso a sistemas y datos críticos, por lo que requieren una protección adicional.

3. REQUISITOS

3.1 REQUISITOS GENERALES

Item	DESCRIPCIÓN DE REQUERIMIENTOS
3.1.1	INSTALACIÓN Y CONFIGURACIÓN DE UNA PLATAFORMA DE GESTIÓN DE IDENTIDADES PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNÉTICOS DEL EJÉRCITO NACIONAL
3.1.1.1	Se debe garantizar que la plataforma no requiera licenciamiento adicional de terceros para el funcionamiento o implementación de esta, por tal razón la plataforma debe ser autónoma en el manejo de identidades.
3.1.1.2	Se debe garantizar que se cumpla el objetivo de "una única identidad para un solo usuario", por lo cual, al terminar la implementación, se debe garantizar que no van a quedar usuarios repetidos, ni que un usuario tenga varias cuentas.

[36] Tomado de https://www.ibm.com/es-es/topics/zero-trust

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

3.1.1.3	Se debe garantizar que en la implementación e integración de la plataforma se realicen todos las API necesarias para cumplir el objetivo de "una única identidad para un solo usuario", al igual que configuraciones y demás que sean requeridas.
3.1.1.4	Se debe garantizar que se integren todas las aplicaciones que usa el ejército nacional, por lo cual el contratista debe realizar el desarrollo, implementación, integración que sean necesarias para cumplir con el objetivo de "una única identidad para un solo usuario".
3.1.1.5	Personalización de los reportes: Exportar, ordenar y modificar las columnas del reporte según las necesidades.

3.2 REQUISITOS ESPECÍFICOS

ÍTEM	DESCRIPCIÓN
3.2.1	GESTIÓN DE ACCESO PRIVILEGIADO
3.2.1.1	CARACTERÍSTICAS GENERALES
3.2.1.1.1	La herramienta debe contar con la posibilidad de crear, modificar y eliminar roles específicos según las necesidades de la organización, dichos roles deben permitir configurar la visibilidad, la edición, la gestión, y el uso de las contraseñas de la organización.
3.2.1.1.2	La herramienta debe contar con la posibilidad de importar usuarios desde el directorio activo o por medio del protocolo LDAP.
3.2.1.1.3	Debe contar con opciones que permitan la creación y administración de grupos de usuarios, con el fin de facilitar las operaciones de manera masiva.
3.2.1.1.4	Debe permitir la integración con diferentes servicios de directorio (Active Directory, eDirectory y LDAP en general) se debe realizar de forma simultánea y transparente, sin requerimiento de plugins o extensiones sobre el servicio de directorio.
3.2.1.1.5	La herramienta debe permitir la autenticación por medio del servidor RADIUS.

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

3.2.1.1.6	Debe permitir la autenticación de manera nativa.
3.2.1.1.7	Debe soportar los siguientes protocolos: TCP/IP, UDP/IP, HTTP, HTTPS, SMB, HTML5 RDP Client, SAML 2.0, SSL/TLS, XML, WEB-Services, PKI, OPEN VPN, HTML, HTML5, OCSP, LDAP, LDAPS, NTLMv1, OATH, TOTP, OpenID Connect, OpenID RP. Todo de forma integral, sin módulos o componentes externos y sin costos adicionales.
3.2.1.1.8	Se debe contar con la opción para autenticarse en la herramienta por medio de SAML 2.0 que le permita actuar como proveedor de servicio (SP) o de identidad (IdP) bajo el modelo de Identidad Federada de forma simultánea. Sin módulos externos para generar este alcance.
3.2.1.1.9	La herramienta debe permitir realizar el doble factor de autenticación por medio de otras aplicaciones.
3.2.1.1.10	Se debe soportar la restricción de acceso basado en el rol que tenga el usuario.
3.2.1.1.11	La herramienta debe contar con la opción de la creación de un Super Administrador, con acceso a toda la gestión de las contraseñas, recursos, llaves y certificados de la organización.
3.2.1.1.12	Se debe contar con la posibilidad de limitar la cantidad de usuarios con rol de Super Administrador a más de uno.
3.2.1.1.13	Se debe contar con opciones para la gestión de cuentas privilegiadas para herramientas de DevOps.
3.2.1.1.14	Debe contar con la funcionalidad de proxy inverso para la publicación de aplicaciones además de cifrar la comunicación brindando mayor nivel de seguridad evitando el uso de VPN.
3.2.1.1.15	La herramienta debe contar con autenticación a través de sus credenciales de usuario de proveedores de servicios que soporten OpenID Connect y OpenID RP.
3.2.1.1.16	La herramienta debe contar con la capacidad de monitorear todos los intentos de loguin fallidos a la herramienta.
3.2.1.1.17	La herramienta debe contar con la posibilidad de implementar la metodología de Zero Trust (Confianza Cero) para los usuarios y recursos de la herramienta.
3.2.1.1.18	La herramienta debe contar con la posibilidad de configurar parámetros de confianza para usuarios y recursos de la misma.
3.2.1.1.19	La herramienta debe contar con la capacidad de crear y configurar políticas de acceso que se alineen a la metodología Zero Trust planteada

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

	con los parámetros de puntuación de confianza.
3.2.1.1.20	El componente de seguridad debe soportar el protocolo FIDO2.
3.2.1.1.21	Debe permitir la creación de múltiples portales de acceso a través de instancias basadas en subdominios, las cuales puedan conectarse de forma independiente a directorios de usuarios externos de forma simultánea. Debe soportar dominios y subdominios múltiples sobre la misma instalación.
3.2.1.1.22	La herramienta debe soportar conexiones de tipo RDP, SSH, Telnet, SQL y VNC.
3.2.1.1.23	La herramienta debe contar con acceso basado en la web para la misma herramienta.
3.2.1.1.24	La herramienta debe contar con la posibilidad de realizar la conexión directa a recursos remotos de en u data center por medio de la configuración de un servidor de aterrizaje.
3.2.1.1.25	La herramienta debe contar con la posibilidad de brindar acceso a los recursos (permitir el uso de una contraseña) por un tiempo limitado.
3.2.1.1.26	La herramienta debe contar con la capacidad de autenticar usuarios mediante mecanismos sólidos (autenticación doble factor): soft- token, hard-token, email-token, matriz de coordenadas, kerberos.
3.2.1.1.27	La herramienta debe contar con capacidad de autenticar usuarios mediante mecanismos sólidos (autenticación doble factor): soft- token, hard-token, email-token, matriz de coordenadas, kerberos.
3.2.1.1.28	La herramienta debe contar con la posibilidad de utilización de HSTS (HTTP Strict Transport Security).
3.2.1.2	**GESTIÓN DE RECURSOS Y CONEXIONES**
3.2.1.2.1	Se debe contar con la opción de implementar la elevación de privilegios.
3.2.1.2.2	La herramienta debe contar con la opción de brindar acceso exclusivo para el uso de las contraseñas.
3.2.1.2.3	La herramienta debe contar con opciones para iniciar sesiones remotas con un solo click, sin la necesidad de revelar las credenciales de acceso en texto plano.
3.2.1.2.4	La herramienta debe contar con varias opciones al momento de abrir una conexión de manera automática. Tales como conexión por RDP, Windows Remote Desktop, VNC, entre otras.
3.2.1.2.5	La herramienta debe contar con la opción de configurar el control de

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

	acceso por aplicación en los recursos deseados.
3.2.1.2.6	La herramienta debe contar con configuración Single Sign On para las aplicaciones web y/o escritorios remotos sin requerir la modificación o ajuste a las bases de datos de usuarios y/o de repositorios de usuarios.
3.2.1.2.7	La herramienta debe contar con la posibilidad de conexión a dos recursos e implementar la transferencia bidireccional de archivos.
3.2.1.2.8	Se debe tener la opción de grabar todas las conexiones a los recursos gestionados en la herramienta.
3.2.1.2.9	La herramienta debe contar con la posibilidad de monitorear en tiempo real la sesión de un usuario.
3.2.1.2.10	La herramienta debe contar con la posibilidad de terminar la sesión de un usuario en caso de detectar actividad sospechosa en su comportamiento.
3.2.1.2.11	La herramienta debe contar con acceso seguro a la misma de manera Off-Line.
3.2.1.2.12	La herramienta debe contar con la opción de implementar una extensión en el buscador para facilitar el acceso a los recursos y a las aplicaciones.
3.2.1.2.13	La herramienta debe poder soportar aplicaciones nativas (In-House).
3.2.1.2.14	La herramienta debe ofrecer la posibilidad de realizar sesiones remotas para dispositivos Tablet como Ipad.
3.2.1.2.15	La herramienta debe tener la capacidad de realizar una conexión directa a todos los dispositivos y sitios web gestionados.
3.2.1.2.16	Se debe contar con la posibilidad de terminar las sesiones del usuario por inactividad.
3.2.1.2.17	Todas las conexiones realizadas por medio de la herramienta deben ser completamente seguras ante ataques como XSS o Man In the Middle.
3.2.1.3	**GESTIÓN DE CONTRASEÑAS**
3.2.1.3.1	La herramienta debe contar con la posibilidad de ser un repositorio seguro y centralizado de todas las contraseñas privilegiadas de la organización.
3.2.1.3.2	Posibilidad de almacenamiento y gestión de cuentas compartidas.
3.2.1.3.3	La herramienta debe tener la capacidad de autenticar usuarios mediante mecanismos sólidos (autenticación doble factor): soft- token, hard-token, email-token, matriz de coordenadas, kerberos.

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

3.2.1.3.4	Debe contar con opciones para realizar la gestión de las contraseñas para las cuentas de servicio en Windows.
3.2.1.3.5	La herramienta debe tener la capacidad de actuar como cliente Radius y como Servidor Radius simultáneamente.
3.2.1.3.6	Capacidad de conectarse a un cliente Radius para consulta de usuarios y posterior autorización de acceso.
3.2.1.3.7	Capacidad actuar como Servidor Radius, permitiendo la consulta de los usuarios creados localmente para autorización de acceso.
3.2.1.3.8	La herramienta debe contar con la posibilidad de reestablecer la contraseña de un recurso remoto, bien sea con la necesidad de agente o sin agente.
3.2.1.3.9	Debe contar con la posibilidad de programar la rotación automática de las contraseñas de manera periódica.
3.2.1.3.10	Garantiza la protección de las credenciales de usuario dentro del sistema, durante su transporte hacia y desde la aplicación, utilizando conexión segura fuerte, mediante el protocolo SSL –TLS 1,2 como mínimo.
3.2.1.3.11	Se debe contar con el aprovisionamiento de acciones, con el fin de dar seguimiento a cualquier acción posterior a haber restablecido la contraseña.
3.2.1.3.12	Control y configuración de requerimientos para contraseñas y llaves SSH.
3.2.1.3.13	La herramienta debe tener soportadas múltiples plataformas para realizar el restablecimiento de contraseña de manea remota.
3.2.1.3.14	La herramienta debe contar con controles para la aprobación del uso de una contraseña por parte de un usuario.
3.2.1.3.15	La herramienta debe contar con políticas de contraseña predefinidas para variar la fortaleza de las contraseñas dentro de la organización.
3.2.1.3.16	Debe contar con la posibilidad de crear nuevas políticas de contraseña según las necesidad y gustos de la organización.
3.2.1.3.17	Se debe contar con la posibilidad de obligar a los usuarios a emplear las políticas de contraseña definidas.
3.2.1.3.18	Se debe contar con la opción de verificar que las contraseñas cumplen con los estándares de las políticas de cumplimiento.

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

3.2.1.3.19	Se debe contar con la opción para importar contraseñas.
3.2.1.3.20	Se debe contar con la opción de exportar contraseñas en múltiples formatos, tales como xslx o HTML.
3.2.1.3.21	La herramienta debe contar con la opción de generar contraseñas sugeridas según las políticas de contraseña definidas.
3.2.1.3.22	Se debe contar con el acceso a todo el historial de contraseñas administradas por la herramienta.
3.2.1.3.23	La herramienta debe contar con un espacio para la gestión y almacenamiento de contraseñas personales de cada usuario.
3.2.1.3.24	La herramienta debe contar con la opción para realizar el restablecimiento de la contraseña posterior a un único uso por parte de un usuario.
3.2.1.4	**AUDITORÍA Y REPORTE**
3.2.1.4.1	La herramienta debe contar con la posibilidad de acceder a los registros de acceso a todas las contraseñas, es necesario conocer quien, que y cuando se accede a una contraseña o llave SSH.
3.2.1.4.2	Posibilidad de tener un registro completo de todas las operaciones de gestión de contraseñas, llaves (claves SSH) y certificados de la herramienta.
3.2.1.4.3	Posibilidad de contar con el registro de toda la actividad de los usuarios.
3.2.1.4.4	Posibilidad de obtener reportes sobre el inventario de las contraseñas, certificados, llaves SSH, políticas de cumplimiento, contraseñas expiradas, etc.
3.2.1.4.5	La herramienta debe contar con la capacidad de programar reportes de manera periódica.
3.2.1.4.6	La herramienta debe contar con la posibilidad de enviar los reportes generados por correo electrónico.
3.2.1.4.7	Debe contar con la posibilidad de exportar reportes en formato PDF o Excel.
3.2.1.4.8	Posibilidad de personalizar el reporte conforme las necesidades y gustos de la organización.
3.2.1.4.9	La herramienta debe contar con reportes por defecto para consulta sin necesidad de ser creados.
3.2.1.4.10	Debe contar con la posibilidad de realizar un Backup de la base de datos.

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

3.2.1.4.11	La herramienta debe contar con la opción de reproducir todas las sesiones grabadas, incluyendo las sesiones privilegiadas.
3.2.1.4.12	La herramienta debe permitir el enmascaramiento de la URL original de acceso a las aplicaciones para no revelar la ubicación final de las mismas.
3.2.1.5	**ALERTAS Y NOTIFICACIONES**
3.2.1.5.1	La herramienta debe enviar notificaciones o alertas a los usuarios a través de correo electrónico con el fin de enviar información relevante cuando sea necesario.
3.2.1.5.2	La herramienta debe contar con la posibilidad de implementar alertas y/o notificaciones sobre la recuperación, restablecimiento, caducidad, cambio de titularidad y demás aspectos afines a una contraseña de la organización.
3.2.1.6	**INTEGRACIONES**
3.2.1.6.1	La herramienta debe contar con la posibilidad de integrarse con herramientas de SIEM (Security Information and Event Management).
3.2.1.6.2	La herramienta debe contar con la capacidad de integrarse con herramientas de gestión de Tickets.
3.2.1.6.3	La herramienta debe contar la capacidad de integración para almacenamiento en nube.
3.2.1.6.4	La herramienta debe contar con la posibilidad de Integrarse con escáneres de vulnerabilidades.
3.2.1.6.5	La herramienta debe ser capaz de integrarse con herramientas para la automatización de procesos robóticos (RPA).
3.2.1.6.6	La herramienta debe contar con la capacidad de realizar integraciones con plataformas de contenedores.
3.2.1.6.7	La herramienta debe contar con la capacidad de realizar integraciones con herramientas de análisis de comportamiento de usuarios y entidades.
3.2.1.6.8	La herramienta debe contar con la capacidad de integrarse con herramientas de Gestión de Identidades.
3.2.1.6.9	La herramienta debe permitir el Re- direccionamiento de todo el tráfico a través de un único puerto seguro 443 (SSL/TLS).
3.2.1.6.9.10	La herramienta debe garantizar la protección de las credenciales de

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

	usuario dentro del sistema, durante su transporte hacia y desde la aplicación, utilizando conexión segura fuerte, mediante el protocolo SSL –TLS 1,2 como mínimo.
3.2.1.7	**ARQUITECTURA**
3.2.1.7.1	Indicar a detalle el funcionamiento de la herramienta, con énfasis primordial en la Arquitectura de la misma.
3.2.1.7.2	La herramienta debe contar con la posibilidad de realizar configuraciones para el acceso ininterrumpido a los datos.
3.2.1.7.3	La herramienta debe contar con la posibilidad de funcionar bajo el servicio de Fail-Over.
3.2.1.7.4	La herramienta debe contar con la posibilidad de implementar varias instancias en el servidor, ante cualquier eventualidad de falla.
3.2.1.7.5	La herramienta debe contar con mecanismos de prestación del servicio en clúster de alta disponibilidad activo-activo, activo-pasivo.
3.2.1.7.6	La herramienta debe contar con un sistema integrado para el balanceo de carga automático a través de los nodos en una instalación tipo clúster.
3.2.1.7.7	La herramienta debe contar con una arquitectura Multi- Tenant (Capacidad de manejar una sola instancia en un solo servidor para múltiples clientes y peticiones).
3.2.1.7.8	Detallar cual es el modelo para el licenciamiento de la herramienta, por ejemplo, por cantidad de usuarios totales, cantidad de usuarios administradores, cantidad de conexiones recurrentes, entre otros.
ÍTEM	**DESCRIPCION**
3.2.2	**GESTIÓN DE IDENTIDAD Y ACCESO**
3.2.2.1	**CARACTERÍSTICAS GENERALES**
3.2.2.1.1	Informes de inicio de sesión de usuarios en Directorio Activo.
3.2.2.1.2	Informes sobre el tiempo de inicio de sesión de los usuarios, sesiones fallidas, inactividad, entre otros.
3.2.2.2	**REPORTES**
3.2.2.2.1	Informes de objetos del Directorio Activo sobre usuarios de AD, computadores, grupos, unidades organizacionales (OUs), políticas de grupos (GPOs).
3.2.2.2.2	Programar la generación de informes con una duración determinada y el

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

	envío vía correo electrónico a direcciones especificadas.
3.2.2.2.3	Informes de cumplimiento: Debera contar con capacidad de generar informes de cumplimiento o integrarse a una plataforma de terceros para protocolos comom FISMA, GLBA, SOX, GDPR, HIPAA, y regulaciones en PCI- DSS.
3.2.2.3	**ADMINISTRACIÓN**
3.2.2.3.1	Gestión de usuarios en bloque: Agregar, modificar, activar, desactivar, mover y eliminar usuarios.
3.2.2.3.2	Desbloquear las cuentas de usuario: Realizar restablecimientos masivos de las contraseñas y desbloqueo de cuentas de usuario.
3.2.2.3.3	Gestión de grupos a gran escala: Agregar, modificar, mover y eliminar grupos de forma masiva.
3.2.2.3.4	Gestión masiva de computadores y contactos: Agregar, modificar, activar, desactivar, mover y eliminar computadores y contactos.
3.2.2.3.5	Integraciones con terceros: La herramienta debe estar en la capacidad de integrarse con herramientas de terceros con las cuales cuenta la Fuerza.
3.2.2.3.6	Gestión de file server: Gestionar los permisos de NTFS de los recursos compartidos.
3.2.2.3.7	Administración de GPO: Gestionar y administrar GPO asociadas a las unidades organizacionales del sitio y dominio.
3.2.2.4	**AUDITORÍA**
3.2.2.4.1	La plataforma debe permitir generar informes para la gestión de usuarios, Workstations, grupos y OU. La plataforma debe permitir generar informes para auditar otros objetos de Directorio Activo, incluidos: DNS, Contactos, Esquema, Permisos, Configuración, Cambios de dominio. La plataforma debe permitir generar informes para visualizar cambios de valor de los atributos (antes y después). La plataforma debe tener informes de auditoría de GPO.
3.2.2.4.2	Auditoria de servidores: La plataforma debe permitir generar un reporte que permita visualizar los cambios realizados en los servidores de archivos.

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

	La plataforma debe tener reportes de lo siguiente: • Cambios de política. • Eventos del sistema. • Gestión de objetos. • Tareas programadas.
3.2.2.4.3	Auditoria de todas las acciones: Generar reportes sobre el Directorio Activo, donde se evidencien modificaciones, usuarios que las realizan, fecha, hora y ubicación.
3.2.2.4.4	Auditoria de inicio de sesión de usuarios: Ver la hora exacta de entrada y salida de usuario junto con la duración de sesión.
3.2.2.4.5	Auditoria de cambios en los atributos: Obtener informes sobre los atributos antes y después de un objeto.
3.2.2.4.6	Informes de la auditoria de las GPO: Reportes sobre los cambios en los objetos de las políticas de grupo.
3.2.2.4.7	Personalización de informes de auditoría: Crear reportes personalizados o en función de las necesidades de la Fuerza.
3.2.2.4.8	Auditoria a nivel de objetos: Auditar todas las acciones de los usuarios, computadores, grupos y unidades organizacionales.
3.2.2.4.9	Análisis del comportamiento de los usuarios: Detectar comportamientos anómalos de los usuarios basándose en sus patrones de actividad anteriores.
3.2.2.4.10	La herramienta debe contar con un portal seguro único de administración.
3.2.2.4.11	Auditoria de failover: Auditar y monitorear el clúster de failover por error de Windows FileServer.
3.2.2.4.12	Historial de auditorías: Obtener informes sobre Directorio Activo de un periodo de tiempo determinado.
3.2.2.4.13	Programar informes de auditoría: Programar la entrega de informes de Directorio Activo para su visualización.
3.2.2.4.14	Búsquedas rápidas: Buscar rápidamente informes de auditoría y registros específicos.
3.2.2.4.15	Acceso a través del navegador web: Permite el acceso mediante navegadores web.

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

3.2.2.4.16	Acceso basado en roles: Acceso seguro a los informes esenciales en función de sus roles.
3.2.2.4.17	Soporte de múltiples dominios: Auditar la información de múltiples dominios con una sola instalación.
3.2.2.4.18	La herramienta debe contar con capacidad para la Des-habilitación de protocolos considerados no seguros (TLS 1.0 / TLS 1.1).
3.2.2.4.19	Registros de auditoría de los eventos: Obtener un informe completo sobre la secuencia de eventos que dieron lugar a un cambio en particular.
3.2.2.4.20	Servidor de Gateway remoto: Auditoria del servidor Gateway remoto.
3.2.2.4.21	Analizador de bloqueo de cuentas: Analizar las razones de los bloqueos de las cuentas de dominio.
3.2.2.4.22	Integración con SIEM: Integrar los registros en bruto en sus sistemas de gestión de eventos e información de seguridad (SIEM) locales.
3.2.2.5	**ALERTAS**
3.2.2.5.1	Perfiles de alertas: Programar alertas en función de un determinado nivel de umbral o del horario de trabajo.
3.2.2.5.2	Avisos personalizados: Programar alertas personalizadas para eventos e informes importantes que se enviaran automáticamente a sus direcciones de correo electrónico.
3.2.2.6	**AUTOGESTIÓN Y GESTIÓN DE CONTRASEÑAS**
3.2.2.6.1	Restablecimiento de la contraseña y desbloqueo de la cuenta en autoservicio.
3.2.2.6.2	Gestión de contraseñas de autoservicio con opciones de autenticación: Admitir métodos de autenticación diferentes para el restablecimiento de contraseñas en autoservicio y el desbloqueo de cuentas.
3.2.2.6.3	Sincronizaciones contraseñas en tiempo real: Sincroniza automáticamente las contraseñas de Directorio Activo de los usuarios con las aplicaciones en la nube y otros sistemas locales.
3.2.2.6.4	Notificación de expiración de la contraseña: Envía recordatorios periódicos de caducidad de las contraseñas a los usuarios de Directorio Activo mediante correo electrónico y notificaciones push.
3.2.2.6.5	Restablecimiento de la contraseña desde la pantalla de inicio de sesión: Permite a los usuarios restablecer sus contraseñas desde las pantallas de inicio de sesión de sus equipos Windows, macOS o Linux.

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

3.3 REQUISITOS DE EMPAQUE Y ROTULADO

3.3.1 Empaque.

No aplica, toda vez que la plataforma es intangible.

3.3.2 Rotulado.

No aplica, toda vez que la plataforma es software, no se entregan equipos.

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.

No aplica, toda vez que la plataforma es software, no se entregan equipos.

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

No aplica, toda vez que la plataforma es software, no se entregan equipos.

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.

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

3.2.2.6.6	Algoritmos de cifrado: cifrado DES, 3DES, RC4, AES, Hashes:MD5 y SHA, cumpliendo con la normativa internacional. No permite la exposición directa de los recursos.
3.2.2.7	**SINGLE SIGN-ON (SSO)**
3.2.2.7.1	Proporcionar un acceso seguro con un solo clic a las aplicaciones de la Fuerza.
3.2.2.7.2	Posibilidad de configurar el SSO para las aplicaciones internas.
3.2.2.7.3	Proporcionar a los usuarios de Directorio Activo acceso SSO a las aplicaciones utilizando sus credenciales de dominio.
3.2.2.7.4	Admite las normas SSO: Soporta SAML, OAuth y OIDC SSO.
3.2.2.7.5	Reportes en aplicaciones: Proporcionar informes integrados para ver quién ha accedido a qué aplicaciones.
3.2.2.8	**AUTENTICACIÓN MULTI-FACTOR (MFA)**
3.2.2.8.1	MFA de Acceso a Windows: Añadir una capa adicional de autenticación a los inicios de sesión locales interactivos y RDP de Windows.
3.2.2.8.2	MFA de Acceso a macOS: Añadir una capa adicional de autenticación a los inicios de sesión de macOS.
3.2.2.8.3	MFA de Acceso a Linux: Añadir una capa adicional de autenticación a los inicios de sesión en Linux.
3.2.2.8.4	Utilizar diferentes conjuntos de factores de autenticación para los intentos de inicio de sesión de alto y bajo riesgo.
3.2.2.8.5	Utilizar factores de autenticación más fuertes para iniciar la sesión en las aplicaciones.
3.2.2.9	**COPIA DE SEGURIDAD Y RESTAURACIÓN**
3.2.2.9.1	Restaurar todos los atributos de un usuario o algunos, incluyendo su pertenencia a un grupo, y la última contraseña establecida.
3.2.2.9.2	Hacer una copia de seguridad de todos los objetos informáticos de su dominio, es decir, cuando se restaura una cuenta de equipo, también se restaura la última contraseña establecida de la cuenta de equipo, reincorporando el equipo al dominio instantáneamente.
3.2.2.9.3	Hacer una copia de seguridad de todos los cambios realizados en los grupos, incluyendo la adición o eliminación de miembros del grupo y las modificaciones de los derechos y permisos.
3.2.2.9.4	Realizar una copia de seguridad y restaurar todos los objetos de directiva de grupo de su dominio, también debe permitir realizar un seguimiento de cada cambio realizado en los GPO, deshacer cualquier modificación

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

	especifica, o revertir todos los cambios a la vez.
3.2.2.9.5	Realiza una copia de seguridad de todos los atributos de un contacto, restaurar los atributos vinculados, como la pertenencia al grupo de distribución del contacto, el gerente y los informes directos, todo de una vez.
3.2.2.9.6	Hacer una copia de seguridad de todos los objetos de Directorio Activo presentes en una OU o contenedor con un solo clic. Restaurar los permisos de delegación que se asignaron previamente al restaurar OUs o contenedores eliminados.
3.2.2.9.7	Hacer una copia de seguridad de las zonas DNS y de los nodos DNS en el dominio. Realizar un seguimiento de los cambios de configuración de DNS en su dominio y Hacer una copia de seguridad para facilitar su restauración.
3.2.2.9.8	Gestión de cambios, copias de seguridad y recuperación: Revierta hasta el más mínimo cambio de valor de los atributos para deshacer cualquier modificación no deseada.
3.2.2.9.9	Hacer una copia de seguridad sólo de los cambios realizados después del último ciclo de copia de seguridad para acelerar el proceso de copia de seguridad.
3.2.2.9.10	Definir un período de conservación de las copias de seguridad y eliminar la información de las copias de seguridad que ya no sean necesarias.
3.2.2.9.11	Realizar operaciones de recuperación sin tener que reiniciar sus controladores de dominio para garantizar una alta disponibilidad continua.
3.2.2.9.12	Mantener varias versiones de una copia de seguridad para cada objeto. Restaurar o retroceder a la versión que necesite.
3.2.2.9.13	Creación de políticas de automatización personalizadas añadiendo tareas para realizar un proceso.
3.2.2.9.14	Aceptar archivos CSV, informes de productos y ubicaciones compartidas como entrada para las tareas automatizadas.

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

6. APÉNDICE

6.1 NORMAS QUE DEBEN CONSULTARSE

- Constitución Política de Colombia.
- Código Civil.
- 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

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

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 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 PLATAFORMA DE GESTIÓN DE IDENTIDADES PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNÉTICOS DEL EJÉRCITO NACIONAL en cumplimiento a la circular 2023218017093013 del 03 de octubre del 2023	28/01/2025

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

acogiéndose al numeral 20.1 "Citar el documento que motivo la creación o actualización de la Especificación Técnica" por medio del oficio N° 2025574001405103 del 20 de enero de 2024 elaborado por el BACCI y oficio 2025229001384313 de fecha 20 enero 2025 elaborado por CEDE 6.

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" por medio del Oficio N° 2025574001413183 del 20 de enero del 2024 elaborado por el BACCI.

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.

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

Especificaciones técnicas No. JEMPP-CEDE6-DIPCO–ET-05714-COM–00 PLATAFORMA DE GESTIÓN DE IDENTIDADES PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNETICOS DEL EJÉRCITO NACIONAL, la cual contiene los parámetros técnicos que deben cumplir los oferentes y el contratista en la acreditación de la adquisición del bien, así mismo, el contenido es el mismo del ANEXO ESPECIFICACIONES TÉCNICAS se encuentra firmada y avalada.



Elaboró	Revisó	Aprobó
CT. YAKELLINE SÁNCHEZ REYES Oficial Operaciones Tecnológicas	MY. PABLO EDUARDO CORTÉS FORERO Ejecutivo y Segundo Comandante del Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional PS OLGA LUCIA VILLALOBOS BACCA Asesora Jurídica	TC. ROGER JESÚS BUELVAS NARVAEZ Comandante Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional

ANEXO TÉCNICO ESTUDIO PREVIO

ESPECIFICACIONES TÉCNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO

ANEXO TÉCNICO ESTUDIO PREVIO

ESPECIFICACIONES TÉCNICAS ADICIONALES DE OBLIGATORIO CUMPLIMIENTO

	ADQUISICIÓN DE UNA PLATAFORMA DE GESTIÓN DE IDENTIDADES PARA EL FORTALECIMIENTO DE LOS MEDIOS CIBERNÉTICOS DEL EJÉRCITO NACIONAL
1	**OBLIGACIONES GENERALES DEL CONTRATISTA:** • **Confidencialidad de la Información** El contratista se obliga a no suministrar ni publicar ninguna información que obtenga o conozca con ocasión de la ejecución del contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo y sea revelada información marcada como confidencial. El contratista deberá diligenciar el formulario Anticorrupción “acuerdo de confidencialidad”. La empresa adjudicataria, así como todos los miembros del equipo de trabajo objeto del proceso deberán guardar secreto profesional sobre toda la información, documentos y asuntos, independientemente de su naturaleza (técnica, comercial, financiera, operacional o de otro tipo), a los que tenga acceso o conocimiento durante la vigencia del contrato, independientemente de la forma o

soporte (verbal, escrita, grabado o de cualquier otro tipo), por la que haya adquirido la información. En tal virtud, está obligado y se adoptarán todas las medidas necesarias para no hacer público, sustraer, duplicar, alterar, ocultar, ceder o enajenar cuanto dato conozca como consecuencia o con ocasión de la ejecución del contrato. Esta obligación no se limita al tiempo de ejecución del contrato, sino que deberá ser respetada aún después de su finalización.

A tal efecto todos los miembros del equipo prestador del servicio deberán tener un completo conocimiento del deber de secreto de la información durante la ejecución del contrato y en el supuesto de producirse algún cambio en la composición del equipo prestador del servicio, los nuevos integrantes asumirán las obligaciones contenidas en este ítem. Con esta finalidad el contratista se compromete a formar e informar al personal de tales obligaciones asumiendo, en el caso contrario, las responsabilidades que pudieran devenirse por su incumplimiento.

Por lo anterior, es indispensable que el contratista se comprometa a conocer, aceptar y ajustarse a las políticas de seguridad informática del Comando General de las Fuerzas Militares y del Ejército Nacional y firmar al inicio del contrato una promesa de reserva donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere, como producto de la ejecución del contrato y la de estos pliegos técnicos, y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros.

El contratista y los recursos humanos que formaran parte del grupo de trabajo deberán firmar al inicio de la ejecución del contrato, el acuerdo de confidencialidad donde garantizan la confidencialidad de la información institucional a la cual tengan acceso directamente o por intermedio de terceros, así como la que genere como producto de la ejecución del contrato y por tanto en ningún caso podrá divulgarla, copiarla, reproducirla o suministrarla a terceros; así mismo.

- **Propiedad Intelectual**

Todos los estudios y documentos elaborados por el contratista como consecuencia de la ejecución del contrato serán de propiedad del Ejército Nacional, quien podrá reproducirlos, publicarlos y divulgarlos, sin que pueda oponerse a ello el adjudicatario autor material de los trabajos, en cumplimiento de los términos establecidos en la Ley 23 de 1982, modificada por la Ley 44 de 1993 y la Ley 1915 de 2018.

En particular, toda aquella documentación generada por intervenciones del personal asignado al servicio en el Ejército será propiedad de la institución, por tanto, no podrá ser facilitada a otra persona o entidad sin consentimiento expreso del Ejército.

El adjudicatario renuncia expresamente a cualquier derecho que sobre los trabajos realizados como consecuencia de la ejecución del contrato pudiera corresponderle, y no podrá hacer ningún uso o divulgación de los estudios y documentos utilizados o elaborados en base a este pliego de condiciones, bien sea en forma total o parcial, directa o extractada, original o reproducida, sin autorización expresa y por escrito del Ejército Nacional.

Por lo anterior al finalizar la ejecución del proceso toda la información y documentos entregados por el Comando del Ejército, deberán ser retornados y no podrá quedarse con la información que se genere.

- **Documentación**

El contratista deberá entregar al Ejército Nacional la documentación necesaria para la Instalación,

	configuración, implementación y parametrización. Esta documentación debe incluir el detalle del plan de trabajo completo para efectuar la instalación y configuración de las plataformas adquiridas, además se debe especificar: - Los recursos necesarios para la instalación. - Cada uno de los pasos que se deben efectuar. - Los tiempos de ejecución de cada uno de los pasos. - Para el desarrollo de la instalación se deberá presentar un cronograma de tareas después de firmada el acta de inicio del contrato. - Después cada configuración se debe entregar un manual de procedimiento de las configuraciones realizadas en cada una de las soluciones. - Informe final donde se describa el total de las soluciones, configuraciones y procesos realizados en la ejecución del contrato - Entrega de topología - Informe de cada visita, documentando los procedimientos realizados. • **<u>Otros</u>** El contratista se debe comprometer a conocer, aceptar y ajustarse a las políticas de seguridad de la Directiva de Seguridad Informática del Ministerio de Defensa - Comando General de las Fuerzas Militares Directivas Permanentes de Ciberdefensa y Seguridad de la Información.
2	**<u>El contrato debe ser tratado como un proyecto llave en mano.</u>** Para todos los efectos de funcionalidad e interoperabilidad, el contratista debe instalar, configurar, dar soporte y acompañamiento de las soluciones adquiridas y el software instalado, garantizando al Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad el correcto funcionamiento de acuerdo a las especificaciones técnicas requeridas. ***Nota:*** *"Sera considerado un proyecto llave en mano, aquel que asegure el resultado final de manera satisfactoria, cumpliendo las especificaciones. La optimización de costo, logística, mejores prácticas de implementación serán potestad del contratista, siempre y cuando cumplan con el objetivo final de suministrar una solución que garantice las especificaciones técnicas requeridas; de ser necesario el oferente asumirá costos adicionales de servicios, accesorios, componentes de software, hardware, cableado y elementos adicionales requeridos para la óptima implementación de esta solución e integración con todas las soluciones tecnológicas del Ejercito Nacional."* Se debe suministrar por parte del contratista la logística necesaria para el desarrollo del contrato como: portátiles, desplazamientos, hospedajes, alimentación, discos duros extraíbles, papelería y software para el desarrollo del contrato, sin que esto genere costo adicional para el Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad; una vez finalizado el contrato, a estos elementos se les debe realizar un procedimiento de borrado seguro por parte de la Batallón de Ciberdefensa y Ciberseguridad del Ejército Nacional para posteriormente ser retirados de las instalaciones del Ministerio de Defensa Nacional – Ejército Nacional – Batallón de Ciberdefensa y Ciberseguridad.

3	**SOPORTE PROVEEDOR:** El proveedor debe brindar un soporte en horario de 24x7 (24 horas del día, los 7 días de la semana) remoto o presencial según lo solicite la entidad a partir de la firma del contrato, el proveedor debe asumir todos los costos por desplazamiento, instalaciones, configuraciones y demás que sean necesarios en sitio y esto no incurrirá en ningún costo para el Ejército Nacional, por la vigencia de la solución a adquirir. TIPO DE ATENCIÓN o Soporte Nivel 1: De manera presencial un día a la semana con duración de 8 horas laborales (5x8) en las instalaciones Ejército del Cantón Militar "Caldas" Cra 46 # 20c -01 Bogotá o donde se encuentre el sistema, el horario de trabajo será de acuerdo al requerimiento del supervisor del contrato. o Soporte Nivel 2: Cuando se requiera remotamente a través de herramientas web online; en horario 7x24 (7 días a la semana las 24 horas del día) durante la vigencia de la solución a adquirir, para prestar este servicio el ingeniero de soporte debe contar con equipo de cómputo suministrado por el contratista. o Estarán a cargo del contratista todos los costos en que deba incurrir en el cumplimiento de su deber de garantía. NOTA: Los términos de garantía técnica y el tiempo de respuesta de esta, deberán ser aportados en documento independiente debidamente suscrito por el oferente.
4	**SOPORTE FABRICANTE:** • El fabricante debe brindar un soporte en horario de 24x7 (Las 24 horas del día, los 7 días a la semana) desde la firma del contrato, por la vigencia de la solución a adquirir. • Acceso al portal de soporte (base de conocimiento, Escalamiento de Tickets) • 7x24x365 soporte telefónico • Priorización de Caso • Asignación de un TAM (especialista de producto) para revisión y evaluación periódica • Healtcheck de la solución de forma trimestral • Reportes trimestrales • Gestión de casos proactivos • Acompañamiento en nuevas funcionalidades y actualizaciones
5	**<u>Cumplimiento de Normatividad Gubernamental en Materia de Tics</u>** Todas las soluciones deben ser compatibles con los protocoles IPV4 e IPV6 CUMPLIMIENTO DE NORMATIVIDAD GUBERNAMENTAL EN MATERIA DE TICS Los bienes y servicios TICS contemplados en el presente anexo técnico, deben brindar soporte al protocolo de internet versión seis (IPv6) de conformidad con la Resolución 2710 del 03 de octubre de 2017 de MINTIC, que en su Artículo 5. "Contratación", estipula: "A partir de la entrada en vigencia de la presente resolución, todos los procesos de selección que inicien las entidades públicas deberán, desde los mismos pliegos de condiciones o lo que haga sus veces, exigir soporte IPv6 nativo en coexistencia con IPv4, en la contratación de bienes y servicios relacionados con las TICS." **<u>Cumplimiento Normas Técnicas</u>**

	El Contratista debe cumplir o exceder en las siguientes especificaciones de instalación, documentación, componentes y sistemas de la industria según sea el caso: NIST CSF 2.0 ISO/IEC 27001
6	Al finalizar la implementación el contratista debe entregar un diagrama técnico detallado donde sea representado gráficamente cada uno de los componentes de Software con sus correspondientes conexiones de red de dato con el propósito de proporcionar información suficiente para facilitar su análisis, mantenimiento e integración con las demás herramientas con las que cuenta el Ejército Nacional.
7	Las soluciones por implementar deben ser compatibles con las plataformas actuales del Ejército Nacional y cumplir con el protocolo IPv4 e IPV6.
8	El Contratista debe contar con personal técnico especializado, capacitado y certificado en cada una de las herramientas relacionadas en la presente especificación técnica para atender y solucionar los incidentes reportados durante la ejecución del contrato y el tiempo de soporte de todas las soluciones.
9	**Término de Respuesta de la Garantía Técnica** Para el presente proceso de selección, el proponente junto con la oferta deberá presentar el termino de respuesta de la garantía técnica, el cual cubrirá lo siguiente: ○ El Contratista deberá garantizar el normal funcionamiento de la solución después del funcionamiento y puesta en marcha, de no ser así el contratista deberá cubrir los gastos (configuraciones, horas ingenieros) que se generan hasta restablecer el funcionamiento de la solución en un tiempo no mayor a 24 horas. ○ Soporte a la garantía disponible los 365 días del año en horario 7x24 (7 días a la semana las 24 horas del día). ○ El servicio de garantía debe ser atendido de manera inmediata de acuerdo con los niveles de servicio. ○ Si en un lapso de cuatro (04) horas después de haber reportado el incidente no se da solución al mismo, el contratista deberá enviar personal técnico especializado a sitio en un tiempo máximo de dos (02) horas. ○ Estarán a cargo del contratista todos los costos en que deba incurrir en el cumplimiento de su deber de garantía. NOTA1: Los términos de garantía técnica y el tiempo de respuesta, deberán ser aportados en documento independiente debidamente suscrito por el oferente. NOTA 2: El término de respuesta de la garantía técnica debe ser por la vigencia de la solución a adquirir. NOTA 3: El Oferente deberá incluir con la oferta los canales o medios de comunicación a través de los cuales será atendido el servicio de garantía (número de línea, correo electrónico, forma remota, etc).
10	**Garantía** El Contratista durante los primeros 15 días posteriores a la reunión de inicio deberá indicar el procedimiento que se deberá seguir para solicitar el servicio de garantía de software de los servicios implementados.

	El término de la garantía técnica por parte fabricante será de mínimo cuatro (04) años. El término de la garantía técnica por parte del contratista será de mínimo cuatro (04) años para cada elemento, desde la firma del acta de recibo a satisfacción. **NOTA:** El Oferente deberá incluir con la oferta el procedimiento que se deberá seguir para solicitar el servicio de garantía del software de los servicios implementados.
11	**Certificación de Fabricante** El oferente debe adjuntar en documento independiente en la oferta, certificado de fábrica que indique que es canal certificado en la herramienta y que está autorizado para distribuir y dar soporte de los productos adquiridos. El oferente deberá presentar carta del fabricante de la solución propuesta la cual avale la solución ofertada para el cumplimiento de todas las características técnicas. El contratista durante los primeros cinco (5) días después de formalizado el contrato se compromete a entregar al supervisor una certificación o documento que soporte la compra de la solución propuesta expedido por el fabricante.
12	**SERVICIO DE MIGRACIÓN E IMPLEMENTACIÓN:**
12.1	**Implementación del Proyecto** El contratista junto con el supervisor debe realizar un plan de trabajo de la propuesta de implementación del proyecto garantizando la integración de cada una de las capacidades y herramientas que se deben integrar. El contratista debe brindar acompañamiento en el Kick Off del proyecto. El Contratista debe contar con personal técnico especializado, capacitado y certificado en las herramientas relacionadas en la presente especificación técnica para atender y solucionar los incidentes reportados durante la ejecución del contrato y el tiempo de soporte de todas las soluciones. Antes de realizar una implementación el contratista debe garantizar compatibilidad con la infraestructura y arquitectura tecnológica actual e indicar que el presente proceso es para fortalecer e integrar la seguridad perimetral con la que cuenta actualmente el Ejército Nacional. El contratista asumirá los costos que genere las integraciones con las tecnologías que posee el Ejército Nacional que sean necesarias para el óptimo funcionamiento de todas las tecnologías. El fabricante realizara un acompañamiento durante la implementación de la herramienta, ateniendo los requerimientos del Ejercito Nacional.
12.2	**Caso de Fallas** Los daños ocasionados por la implementación, desarrollo y puesta en marcha del contrato a cualquier elemento o sistema existente en la entidad serán asumidos por el contratista sin costo alguno para la entidad. En caso de presentarse fallas en cualquiera de los elementos que componen el sistema, se deberán efectuar los soportes todas las veces que se requiera; estos soportes deben incluir como mínimo:

	Instalación de software. • Configuraciones, puesta en producción y funcionamiento En caso de falla el fabricante deberá proporcionar los materiales y/o piezas para su reparación o reemplazo de características iguales o superiores. En caso de presentarse fallas ocasionadas por las actividades efectuadas como producto de la ejecución del contrato por parte del contratista, este debe garantizar el perfecto funcionamiento y la continuidad de los procesos y servicios prestados.
12.3	**Integración:** Realizar una correcta instalación: Es importante realizar una correcta instalación de la solución, siguiendo las instrucciones proporcionadas por el fabricante y verificando que se cumplan los requisitos de hardware y software. Configuración adecuada: La configuración de la solución debe realizarse de manera adecuada, considerando las políticas de seguridad existentes en la organización y las necesidades de la red. Pruebas de integración: El contratista en conjunto con el supervisor del contrato debe realizar pruebas de integración para comprobar la eficacia de la solución en la infraestructura existente y asegurarse de que la solución esté proporcionando el servicio esperado.
13	**RECURSOS HUMANOS**
13.1	Implementación: La implementación debe ser realizada por el contratista de acuerdo a los siguientes perfiles, de la cual el oferente deberá presentar junto con la oferta los siguientes requerimientos: Líder o gerente del Proyecto: Profesional responsable de coordinar y supervisar la ejecución del contrato, así como de comunicarse con el supervisor del contrato para garantizar el cumplimiento de los objetivos y las obligaciones establecidas, encargado de la implementación de la tecnología a adquirir y con quien se gestionará el cumplimiento del objeto del contrato, debe cumplir con los siguientes requisitos. ✓ Se requiere que el rol del líder o gerente del proyecto, la realice como mínimo un (01) ingeniero con el siguiente perfil: Ingeniero de sistemas y/o electrónico y/o telecomunicaciones o afines, con fecha de expedición en tarjeta profesional igual o superior a ocho (8) años. ✓ Deberá demostrar experiencia por medio de mínimo cinco (5) certificaciones en proyectos de ciberseguridad similares, no se aceptan auto certificaciones. ✓ Especialista en Gerencia de Proyectos con certificado PMP vigente. Responsabilidades:

- ✓ El Gerente del Proyecto desempeña un papel crucial en la supervisión y coordinación de todas las actividades relacionadas con la implementación de la solución. Su trabajo se enfoca en garantizar el cumplimiento de los objetivos del proyecto, la eficiencia en la gestión y la mejora continua de la seguridad de la entidad.
- ✓ Generación de informes para la mejora: El Gerente del Proyecto debe generar informes que identifiquen áreas de mejora en la implementación y administración de la solución a implementar. Estos informes deben contener recomendaciones y sugerencias para optimizar el desempeño y la efectividad de las soluciones.
- ✓ Informe ejecutivo de la gerencia del proyecto: El Gerente del Proyecto debe elaborar y entregar mensualmente un informe ejecutivo que brinde una visión general del estado del proyecto. Este informe debe incluir: porcentaje de avance, actividades realizadas, actividades pendientes, línea de tiempo con el avance y lo pendiente, riesgos identificados y acciones preventivas o correctivas tomadas en respuesta a esos riesgos.

Implementación: Se requiere del recurso como Ingeniero Implementación, quien será el responsable de realizar las configuraciones relacionadas con la solución ofertada, integración con la infraestructura existente, instalación de la herramienta, así como de las actividades que se planeen y desarrollen en la ejecución del contrato y demás actividades y servicios indicado en el proyecto.

- ✓ Se requiere que la implementación de la solución y despliegue de la solución a adquirir, la realice como mínimo un (01) ingeniero con el siguiente perfil: Ingeniero de sistemas y/o electrónico y/o telecomunicaciones o afines, con fecha de expedición en tarjeta profesional igual o superior a cinco (05) años.
- ✓ Deberá demostrar experiencia por medio de mínimo cinco (5) certificaciones en proyectos de sistema de gestión de identidades, no se aceptan autocertificaciones.
- ✓ Deberá contar con las siguientes certificaciones:
- ✓ Certificación en instalación y administración de sistema para gestión de identidades y acceso seguro.
- ✓ Certificación o constancia de entrenamiento en la solución ofertada, emitido por el fabricante o por un ente certificador autorizado por el fabricante.
- ✓ Certificación en auditoria en el sistema para gestión de identidades y acceso seguro.

Analista de seguridad: Profesional responsable de realizar las actividades propias a las pruebas de seguridad posteriores a la implementación de la solución garantizando el cumplimiento de los objetivos y las obligaciones establecidas, encargado de corroborar el cumplimiento del objeto del contrato, debe cumplir con los siguientes requisitos.

- ✓ Se requiere que las pruebas de seguridad de la solución a implementar, las realice como mínimo un (01) ingeniero con el siguiente perfil: Ingeniero electrónico y/o de sistemas y/o telecomunicaciones o afines, con fecha de expedición en tarjeta profesional igual o superior a cinco (05) años.
- ✓ Deberá contar con las siguientes certificaciones:
- ✓ Certified Ethical Hacker vigente.

Soporte: Profesional encargado de garantizar la continuidad operativa de la solución, resolver incidencias técnicas, realizar mantenimiento preventivo y correctivo, y asegurar la disponibilidad y el rendimiento óptimo de la solución durante el termino de garantía técnica, por la vigencia de solución adquirir.

- ✓ Se requiere que el soporte, la realice como mínimo uno (01) Profesional o Tecnólogo electrónico y/o de sistemas y/o telecomunicaciones o afines, con fecha de expedición en tarjeta profesional igual o superior a tres (3) años.
- ✓ Certificación o constancia de entrenamiento en la solución ofertada, emitido por el fabricante o por un ente certificador autorizado por el fabricante.
- ✓ Debe acreditar al menos dos (2) certificaciones o más de experiencia relacionada con la implementación o soporte u operación o administración de la solución implementada, no se aceptan auto certificaciones.
- ✓ Deberá contar con certificación de troubleshooting en el sistema para gestión de identidades y acceso seguro.

Nota 1: Los ingenieros deben ser de nacionalidad colombiana.

Nota 2: El oferente deberá presentar junto con la oferta las hojas de vida con sus respectivas certificaciones académicas y de experiencia laboral en las funciones requeridas para los anteriores perfiles:

Para realizar la validación correspondiente del personal requerido, el oferente debe aportar la siguiente documentación del personal encargado de estas actividades.

- Copia legible del diploma de pregrado como ingeniero de sistemas, o electrónico, o de telemática, o comunicaciones y/o afines conforme al SNIES a estas profesiones.
- Copia legible de la tarjeta profesional
- Copia de cédula de ciudadanía que verifique la nacionalidad colombiana.
- La experiencia se deberá certificar considerando los siguientes aspectos que se relacionan a continuación:
  - Nombre o razón social del contratante
  - Descripción de las actividades realizadas
  - Fecha de iniciación del contrato
  - Fecha de terminación del contrato
  - Dirección y teléfono de quién expide la certificación

Otras obligaciones del contratista:

El Contratista, durante la ejecución del contrato, acepta que el Ejército Nacional evalúe el desempeño profesional de la(s) persona(s) asignadas para el proyecto y estará(n) en facultad de solicitar su reemplazo, si esta(s) no cumple(n) con las expectativas del supervisor del contrato.

Durante la ejecución del contrato, si se requiere reemplazar un funcionario por otro, éste deberá tener un perfil profesional igual o superior al que va a ser reemplazado, y cumplir con los requerimientos estipulados en esta especificación técnica.

En caso de que el contratista requiera realizar un cambio de personal, este deberá informar al supervisor del contrato de tal situación con mínimo diez (10) días hábiles de antelación, anexando la hoja de vida del nuevo funcionario que debe cumplir con las especiaciones requeridas.

El supervisor evaluará el desempeño laboral del profesional asignado para el soporte y estará en facultad de solicitar su remplazo si lo considera necesario, en dado caso el oferente adjudicatario

	deberá reemplazarlo en un tiempo no mayor a cinco (5) días luego de la solicitud formal por parte del supervisor del contrato.
14	**APLICACIONES POR INTEGRAR**

14.1

N°	APLIACIONES	DESCRIPCIÓN
1	Acreedores varios	Sistema que permite a tesorería realizar pagos a terceros
2	INFODIAN	Reporte Exógenas DIAN
3	Nómina reintegros	Liquidación personal de Soldados Profesionales
4	Pasajes Viáticos	Liquida conceptos de pasajes y viáticos a pagar a empleados
5	Prestaciones sociales	Liquidar nómina correspondiente cesantías, liquidaciones por muerte e indemnizaciones
6	Retenciones Militares	Pago de retenciones militares efectuadas a los empleados
7	SILAE	Sistema de lecciones aprendidas del Comando de Educación y Doctrina
8	Mesa de Ayuda	Sistema que permite el registro de requerimientos de tipo tecnológicos y la atención por parte del personal designado
9	DICCO	Software Mando y Control Convenios de Colaboración
10	ESPRO	Sistema de incorporación de Soldados Profesionales
11	SIWEP - DIPER	Sistema de Información WEB de personal Ejército
12	SICOE	Sistema de Información del Centro de Operaciones del Ejército Nacional
13	SIGE	Sistema de Información Geográfico
14	RA	Sistema de Información de Traslados
15	Estudio de Seguridad	Sistema de Información de Estudio de Seguridad Militar para soldados
16	Cibercultura	Plataforma de alfabetización digital
17	SIJEN	Sistema de Información Jurídico
18	FOVID	Sistema de Folios de Vida Digital del Ejército Nacional
19	SICOI	Sistema de Información de Control de Inspecciones
20	ORFEO	Sistema de Gestión Documental
21	Directorio Activo	Base de datos y conjunto de servicios que conectan a los usuarios con los recursos de red.

15	**DOBLE FACTOR DE AUTENTICACIÓN**
15.1	Aplicaciones permitidas para realizar la integración para el doble factor de autenticación: • Google authenticator • Microsoft authenticator • Matriz enigma • Zoho OneAuth • Authy • LastPass Authenticator • Duo Mobile • FreeOTP • Yubico Authenticator

16	**HERRAMIENTAS TIPO RPA**
16.1	Herramientas tipo RPA a integrar en la solución: • Soluciones de seguridad de la marca Checkpoint • Soluciones de seguridad de la marca Crowdstrike
17	**INTEGRACIÓN CON HERRAMIENTAS DE GESTIÓN DE IDENTIDADES**
17.1	La solución por adquirir debe tener la capacidad de integrarse con OneAuth.
18	**USUARIOS**
18.1	Usuarios por licenciar: 15.000 usuarios internos
19	**AMBIENTES REQUERIDOS**
19.1	**Ambiente de construcción:** Permite crear y configurar las personalizaciones, integraciones y adaptaciones de la solución a adquirir a la infraestructura tecnológica del Ejército Nacional, para pruebas iniciales, desarrollo de flujos de trabajo, configuración de políticas, entre otros. **Usuarios principales**: Personal de implementación, infraestructura, redes, servidores y seguridad. **Ambiente de pruebas:** Permite validar la funcionalidad e integración de la solución a adquirir con los sistemas existentes del Ejército Nacional antes de pasar a producción, probar flujos de autenticación, autorizaciones, pruebas de carga, rendimiento y seguridad. **Usuarios principales**: Personal de implementación y Analista de seguridad. **Ambiente de producción:** Es el ambiente real dentro de Ejército Nacional donde será desplegada la solución a adquirir, contiene datos reales, opera 24/7 en alta disponibilidad y respaldo. **Usuarios principales**: Personal de soporte, usuarios finales y administradores. Volumen de usuarios por ambiente: **Ambiente de construcción:** 15 usuarios aproximadamente **Ambiente de pruebas:** 15 usuarios aproximadamente **Ambiente de producción:** 15.000 usuarios aproximadamente
20	**MATRIZ DE COORDENADAS**
20.1	La matriz de coordenadas será una herramienta de autenticación fuerte para uso en aplicaciones core donde no se hará uso de sistemas OTP, Soft Token o Hard Token.
21	**TIPO DE SOLUCIÓN**
21.1	La solución requerida es SaaS 100% redundante.

22	**PRUEBAS DE INTEGRACIÓN FUNCIONAL**
22.1	A continuación, se detallan los mínimos alcances de las pruebas de integración funcional: a. Verificación de autenticación y autorización • Confirmar que los usuarios puedan autenticarse correctamente en todas las aplicaciones integradas. • Validar que los roles y permisos configurados en la solución a adquirir se apliquen de forma efectiva en las aplicaciones vinculadas. b. Integración • Asegurar que la solución a adquirir se comunique correctamente con la fuente de identidades. • Validar la sincronización de usuarios, grupos y atributos. c. Flujo de provisión y desprovisión • Verificar que la creación, modificación o eliminación de usuarios se replica adecuadamente en todos los sistemas integrados. • Confirmar que las cuentas quedan inmediatamente inactivas cuando un usuario sale de la organización. d. Funcionalidad de SSO (Single Sign-On) • Validar que los usuarios puedan iniciar sesión una sola vez para acceder a todas las aplicaciones autorizadas. • Probar que las políticas de sesión y tiempo de expiración funcionen correctamente. e. Gestión de contraseñas • Probar la gestión segura de contraseñas. • Verificar que los cambios de contraseña se reflejen en todos los sistemas vinculados. f. Monitoreo y auditoría • Confirmar que la solución a adquirir registre y reporte todas las acciones críticas (inicio de sesión, cambios de privilegios, acceso privilegiado, etc.). • Validar la integridad y disponibilidad de los registros. g. Gestión de cuentas privilegiadas • Verificar que los accesos privilegiados solo se habiliten con las aprobaciones y controles configurados. • Confirmar que las sesiones privilegiadas se graban y se pueden revisar posteriormente. h. Escenarios de error y recuperación • Simular fallos o caídas de sistemas para confirmar que la plataforma responde

	adecuadamente. • Validar la continuidad operativa y la recuperación de datos.
23	**AUDITORÍAS**
23.1	Dentro de los registros o eventos de auditoría requeridos están: Autenticación y acceso • Registros de inicio de sesión exitoso y fallido. • Información del dispositivo, ubicación y método de autenticación. • Horario y duración de la sesión. Creación y gestión de cuentas • Creación, modificación o eliminación de cuentas de usuario. • Cambios en roles o privilegios. • Provisión y desprovisión de cuentas en sistemas integrados. Acciones administrativas • Configuración y cambios en políticas de acceso o en la plataforma. • Creación y gestión de grupos de usuarios o perfiles. • Cambios en las credenciales de cuentas privilegiadas. Accesos privilegiados • Uso de cuentas privilegiadas. • Grabación y/o supervisión de sesiones privilegiadas. • Comandos o acciones ejecutadas en sesiones con privilegios elevados. Actividad de usuarios • Acciones relevantes durante la sesión. • Comportamientos inusuales. Alertas y eventos de seguridad • Eventos relacionados con la detección de amenazas o violaciones de políticas. • Alarmas generadas automáticamente por la solución. • Respuestas automáticas o manuales ante incidentes.
24	**INTEGRACIÓN CON ESCÁNERES DE VULNERABILIDADES**
24.1	La solución por adquirir deberá está en capacidad de integrarse por medio de protocolos como LDAP, Syslog, RESTful APIs SAML, entre otros.

El OFERENTE

_____

REPRESENTANTE LEGAL O APODERADO
Nombre
Identificación Razón social
C.C. / NIT XXXXXXX