MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

MANUAL GENERAL DE OPERACIONES DE INFRAESTRUCTURA DE TI

PROCESO

Gestión de Servicios de Información y Soporte Tecnológico

Versión 1

15/02/2023

MADSIG
Sistema Integrado de Gestión

TABLA DE CONTENIDO

MADSIG Sistema Integrado de Gestión

1. INTRODUCCIÓN

El Ministerio de Ambiente y Desarrollo Sostenible en el proceso de implementación de los lineamientos de la Política de Gobierno y Seguridad Digital continúa haciendo esfuerzos para garantizar la prestación de los servicios al ciudadano, a otras entidades y sectores y mediante los procesos de mejora continua se proponen nuevos retos para lograrlo. En este sentido, las Tecnologías de la Información y las Comunicaciones (TIC) constituyen solo un eslabón sobre el que está construido el andamiaje de los servicios del Estado. En el presente, las TIC y otras tecnologías hacen posible que se realicen comunicaciones internacionales, tales como, transacciones bancarias, de comercio electrónico con aerolíneas, hoteles a nivel global entre otros. Todos los ciudadanos del mundo interactuamos digitalmente con empresas y personas, y de esa misma forma, el ciudadano con las entidades públicas.

¿Qué pasaría si por algún motivo los servicios digitales a nivel local, nacional o mundial sufren un retraso en minutos, horas o días? Ni imaginarlo. Por esta razón, la Oficina de Tecnologías de la Información y las Comunicaciones como custodio de los servicios tecnológicos del Ministerio, además de administrar técnicamente, mantiene información documentada que pueda facilitar y garantizar la continuidad de las operaciones para que ninguna parte interesada se vea afectada significativamente.

En este sentido, pensando en reducir los riesgos de que información sensible de las operaciones de TI y seguridad de los servicios y sistemas de información pueda quedar expuesta en manos de terceros, se crea este documento en cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad del Ministerio TIC.

MADSIG Sistema Integrado de Gestión

2. OBJETIVO

Establecer los lineamientos técnicos generales que permita estandarizar los criterios operativos de cada uno de los elementos de la infraestructura tecnológica para su gestión, configuración y control de conformidad con las políticas de TI establecidas al interior de la entidad. Cada componente de la infraestructura de TI está relacionado, mediante manuales técnicos que sirvan como instrumento de apoyo a la continuidad de las operaciones y a la seguridad de la información, recopilando las mejores prácticas, estándares y marcos de referencia para soportar su debida administración.

3. ALCANCE

Incluye cada uno de los manuales básicos operativos respecto a la operación existente de infraestructura de TI, que de acuerdo con los componentes que se referencian como documentos ANEXOS, contienen información técnica detallada. En este sentido, el acceso a esta información (ANEXOS) se encuentra en clasificación restringida por tratarse de información de la configuración de los servicios de red, seguridad perimetral, acceso y operación de TI del Ministerio, la cual se encuentra centralizada en el repositorio de información de la oficina TIC.

4. CLASIFICACION DE INFORMACIÓN

El acceso a los manuales de operación descritos en los numerales a continuación identificados como ANEXOS, son documentos técnicos que por su naturaleza tienen acceso restringido y que, en manos equivocadas o no autorizadas, pueden causar daño parcial o total al normal funcionamiento de las operaciones de TI o seguridad y de la continuidad del negocio, afectación de los servicios tecnológicos del Ministerio, afectación reputacional, alteración en los tiempos de respuesta al ciudadano, en los procesos internos y externos, etc.

Con el propósito de minimizar el riesgo de exposición de los Manuales de operación (ANEXOS) y su contenido no esté disponible a personal, procesos o terceros no autorizados, estos documentos se clasifican según su confidencialidad como Información Pública Reservada, según su integridad como Alta y disponibilidad Baja, a partir de la aprobación y publicación de este documento. También serán incluidos este manual y sus anexos en el inventario de activos de información del proceso correspondiente.

5. REDES (NETWORKING)

5.1 ANEXO 1. Manual de operaciones de redes.

Este manual contiene información relacionada con la administración de los equipos de red que forman parte de la red LAN y WLAN de toda la entidad y cuya gestión se centraliza desde la consola de NAC (Network Access Control) dado que en los últimos tres años se ha venido controlando poco a poco la manera en que los usuarios acceden a los recursos de red de la entidad.

La red LAN de la entidad se encuentra bajo una arquitectura de dos capas CORE y ACCESO, las cuales se han reestructurado luego de un largo estado de obsolescencia, permitiendo tener equipos de última generación y tecnologías emergentes que faciliten la integración e interoperabilidad de diferentes fabricantes. En este sentido, se dimensionó el crecimiento de la LAN acorde a la alta demanda de servicios de red cableados aumentando el desempeño desde los usuarios con puertos de operación compatibles a 1Gbps.

Los enlaces de alta velocidad fueron migrados de 1Gbps en fibra y dimensionados a 20 y 30 Gbps reduciendo notablemente los cuellos de botella en tráfico.

La WLAN ha venido sufriendo una serie de cambios sustanciales ante la alta demanda de servicios inalámbricos por lo que se encuentra en un proceso de migración y optimización dado los últimos estándares en uso. En el momento, se están administrando dos soluciones de dos fabricantes que vienen coexistiendo, permitiendo hacer un desmonte gradual de la solución más limitada en capacidad, operación y recursos.

Esta administración, si bien es separada se encuentra integrada a la herramienta de control de acceso pues dadas las mejores prácticas, fue imperativo controlar la manera en que los usuarios empleaban los recursos de red inalámbricos. Es así como el uso de 802.1x, MAC y claves pre compartidas hacen parte del tipo de acceso. Este último, para un segmento definido de usuarios.

En razón al estado de obsolescencia y las vulnerabilidades que esto conlleva y en aras de aprovechar el mayor desempeño de los equipos recientemente adquiridos, con sus nuevas características y de mayor desempeño, se implementó el NAC. Esta herramienta controla todo acceso de dispositivo a la red de datos de la entidad y visualiza con granularidad los datos como IP, puerto, hora, tipo de dispositivo que el usuario emplea en su conexión alámbrica e inalámbrica. Esta herramienta genera mucho valor para la administración de la red pues no interactúa sola, sino vincula de forma directa el uso del directorio activo por lo que hace más seguro los ambientes de operación TI.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto.*

6. SEGURIDAD PERIMETRAL Y PUNTO FINAL

6.1 ANEXO 2. Manual de operaciones de firewall de perímetro.

Este manual contiene información asociada a los equipos de seguridad que controlan y protegen el acceso a la red de accesos no autorizados. Estos permiten monitorear el tráfico de red entrante y saliente permitiendo o bloqueando un tráfico específico en función de un conjunto de reglas de seguridad. Establecen además una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como internet.

Los dispositivos perimetrales cuentan con un número específico de políticas creadas de seguridad, así como perfiles de antivirus, IPS, filtrado web, control de aplicaciones, VPN´s, entre otros. Diariamente se crean requerimientos en la red que pasan por allí y que permiten aumentar la disponibilidad de servicios en TI.

Estos dispositivos cuentan con un roadmap vigente teniendo como característica principal que son NGFW (Next Generation Firewall) que además de garantizar funcionalidades tradicionales de permiso o bloqueo de tráfico, emplean tecnología de SDWAN, análisis de reputación, indicadores de compromiso, protección contra ataques de DNS, etc.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) Jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto.*

6.2 ANEXO 3. Manual de operaciones de firewall de aplicaciones.

Este manual contiene la información asociada a los equipos que protegen las aplicaciones web contra ataques maliciosos y tráfico de internet no deseado, como bots, inyección y denegación de servicio (denial of service, DoS) de capa de aplicación mediante una serie de políticas diseñadas para decidir si se deben bloquear o permitir las comunicaciones hacia o desde estas.

Estos controlan la ejecución de archivos o código por parte de aplicaciones concretas. De este modo, aunque un intruso acceda a la red o servidor, no puede ejecutar código malicioso. En este sentido, la entidad a medida que implementa aplicaciones según su necesidad crece la necesidad de protegerlas ante riesgos de seguridad digital.

En la actualidad, la entidad cuenta con más de 20 publicaciones protegidas y con solicitudes para proteger las que se encuentran en desarrollo permitiendo garantizar tanto el acceso, la seguridad y la operación en sus aplicativos. Así las cosas, la oficina TIC siendo consciente de la responsabilidad que tiene a cargo por el desempeño tecnológico de sus aplicaciones ha venido implementando el uso de buenas prácticas tanto en el

desarrollo de sus aplicaciones como en la actualización de su plataforma de seguridad para garantizar el buen desempeño de esta.

Estos equipos brindan protecciones complementarias tales como: Escaneo, análisis y detección de vulnerabilidades en aplicaciones web, protección antidefacement y balanceo de tráfico HTTP y HTTPS, entre otras.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto.*

6.3 ANEXO 4. Manual de operaciones de administrador de registros.

Este manual contiene la información asociada al administrador de registros, análisis e informes que se proporciona a la entidad mediante una única consola para gestionar, automatizar, orquestar y responder, lo que permite operaciones de seguridad simplificadas, identificación proactiva y corrección de riesgos, y visibilidad completa de todo el panorama de ataques.

Este equipo se encuentra integrado con los firewalls, WAF, DDoS mediante ADOMs creados con la finalidad de tener visibilidad y conocimientos críticos de la red mediante un grupo importante de reportes personalizados de acuerdo con la información de interés.

La plataforma cuenta con la última versión actualizada en firmware y liberada por fabricante de acuerdo con el plan de mantenimiento aprobado por la jefatura.

NOTA: *Esta documentación está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) Jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto.*

6.4 ANEXO 5. Manual de operaciones de solución antivirus.

Este manual contiene la información asociada a la plataforma de administración de antivirus implementada en la entidad con el proveedor Kaspersky. Se cuenta con un numero específico de licencias para los endpoints del ministerio el cual protege, controla y brinda protección en tiempo real contra ataques de virus. Esta solución está diseñada para evaluar datos como páginas web, archivos, software y aplicaciones, a fin de encontrar y erradicar malware tan pronto como sea posible.

Un software antivirus comienza comparando archivos y programas informáticos con una base de datos de tipos de malware conocidos. Debido a que los hackers crean y distribuyen nuevos virus constantemente, también hará un escaneo de los equipos en la búsqueda de un tipo nuevo o desconocido de amenaza de malware.

Generalmente, la mayoría de los programas usará tres dispositivos de detección diferentes: detección específica, la cual identifica el malware conocido; detección genérica, la cual busca partes o tipos de malware conocido, o patrones que se relacionan en virtud de una base de código común; y detección heurística, la cual escanea virus desconocidos al identificar estructuras de archivos sospechosas conocidas. Cuando el programa encuentra un archivo que contiene un virus, generalmente lo pone en cuarentena y/o lo aparta para eliminarlo, lo que lo hace inaccesible.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto.*

7. INFRAESTRUCTURA DE SERVIDORES

7.1 ANEXO 6. Manual de operaciones de plataforma hiperconvergente.

Este manual contiene la información del sistema hyperconvergente donde se pueden realizar tareas de administración, movimiento de máquinas y recursos entre los mismos nodos. Los hosts de HPE se administran dentro de una interfaz, que es un contenedor virtual que representa un grupo de hosts de HPE en red. La interfaz permite administrar la infraestructura hiperconvergente implementada en varios sitios como un solo dispositivo. El Clúster proporciona alta disponibilidad (HA) y permite que una máquina virtual realice un *fail over* de un host HPE a otro host.

MADSIG Sistema Integrado de Gestión

Utiliza estas interfaces de red:

- Gestión: gestiona la infraestructura y el tráfico de red de máquinas virtuales.
- Almacenamiento: gestiona el acceso de la máquina virtual a los datastores de HPE.
- Interfaz: maneja el tráfico entre los controladores virtuales en un clúster, incluidas las comunicaciones de heartbeat y las comunicaciones HA (alta disponibilidad) para cada máquina virtual en el clúster.

De forma predeterminada, el dispositivo virtual de administración utiliza la interfaz de red de administración.

Nutanix ofrece una solución de infraestructura hiperconvergente especialmente diseñada para virtualización y entornos en la nube. Esta solución brinda el rendimiento y los beneficios económicos de la arquitectura a escala web a través de la plataforma de nube Nutanix.

Los atributos de esta solución incluyen:

- Almacenamiento y recursos informáticos hyperconvergente en servidores x86.
- Inteligencia del sistema ubicada en el software.
- Datos, metadatos y operaciones totalmente distribuidos en todo el clúster de servidores x86.
- Auto-curación para tolerar y ajustarse a las fallas de los componentes.
- Automatización basada en API y análisis enriquecido.

Nutanix Acrópolis se puede dividirse en tres componentes fundamentales: *Distributed Storage Fabric*

(DSF), *App Mobility Fabric* (AMF) y *AHV. Prism* ofrece administración de infraestructura con un solo clic para entornos virtuales que se ejecutan en Acrópolis. Acrópolis es independiente del hipervisor y admite dos hipervisores de terceros, *ESXi* e *Hyper*-V, además del hipervisor nativo de Nutanix, AHV.

La estructura de almacenamiento distribuido (DSF) *Distributed Storage Fabric* (DSF) proporciona almacenamiento de datos como un servicio bajo demanda, al emplear una arquitectura de software altamente distribuida. Nutanix elimina la necesidad de soluciones SAN y NAS tradicionales y genera un amplio conjunto de servicios definidos por software centrados en VM. Específicamente, DSF maneja la ruta de datos de características tales como instantáneas, clones, alta disponibilidad, recuperación de desastres, de duplicación, compresión y codificación de borrado.

El DSF opera a través de una red interconectada de Controladoras VM (CVM) que forman un clúster de Nutanix, y cada nodo del clúster tiene acceso a datos de SSD compartidos, HDD y recursos de la nube. Los hipervisores y DSF se comunican utilizando los protocolos NFS, iSCSI y SMB3 estándar de la industria.

***NOTA**: La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto.*

7.2 ANEXO 7. Manual de operaciones de plataforma de virtualización

La virtualización de servidores consiste en el proceso de creación de servidores, infraestructuras, servicios y múltiples recursos informáticos en una plataforma virtual. Inicialmente, el software y el hardware de los ordenadores estaban diseñados para soportar aplicaciones individuales. Como resultado, los servidores se veían obligados a procesar una sola tarea a la vez, lo que provocaba un desperdicio de capacidad de memoria y de procesadores no utilizados.

Entonces, a medida que se desplegaban aplicaciones y servicios adicionales en la infraestructura de red, el número de servidores crecía exponencialmente. Los centros de datos estaban al límite por el aumento de los precios y la mayor demanda de espacio, energía, refrigeración y mantenimiento.

Un servidor físico se divide en numerosos espacios virtuales individuales y remotos, cada uno de los cuales sirve a varios usuarios. En otras palabras, la virtualización añade una capa extra de software a un ordenador y controla sus recursos virtualizados, dividiéndolos en instancias lógicas capaces de funcionar de forma independiente que reciben el nombre de máquinas virtuales. Esto minimiza los costes informáticos porque reduce el número de servidores, alivia la carga de los recursos del centro de datos y mejora la flexibilidad informática.

El presente anexo relaciona los lineamientos correspondientes a la descripción de actividades para la instalación de software y creación de máquinas virtuales en el ambiente de producción que ejecuta el Ministerio de Ambiente y Desarrollo Sostenible, con el propósito de establecer un estándar para la gestión de las operaciones en los servidores, mejorar los tiempos de respuesta a los requerimientos presentados, mejorar la disponibilidad de los servicios así como documentar una arquitectura estandarizada.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto.*

7.3 ANEXO 8. Manual de operaciones de plataforma de almacenamiento (storage).

Este documento contiene información técnica respecto a la instalación, configuración, administración y puesta en marcha de la solución de almacenamiento HPE StoreOnce 3640 y 2 dispositivos SAM de almacenamiento Qnap, los cuales representan la plataforma de almacenamiento externo para backups y copias de respaldo del Ministerio de Ambiente y Desarrollo Sostenible, los cuales son administrados por el software nativo HP StoreOnce y Veritas NetBackup/Backup Exec, cuyo tipo de licenciamiento es perpetuo para su funcionamiento.

Desde la plataforma HP StoreOnce son realizados los Backups de tipo full y granular con las políticas de creación de respaldos de máquinas virtuales y desde las SAM Qnap de almacenamiento. La información es salvaguardada de acuerdo con políticas de retención establecida por el Ministerio.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto*

7.4 ANEXO 9. Manual de operaciones de solución de copias de respaldo (Backup).

El manual referenciado en este ítem proporciona información del software utilizado para la programación, administración, creación y restauración (software nativo *HP StoreOnce* y *Veritas NetBackup/Backup Exec*), el cual cuenta con licenciamiento de tipo perpetuo adquirido por el Ministerio de Ambiente y Desarrollo Sostenible

La generación de copias de seguridad se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas. Este software no solamente es capaz de realizar la tarea básica de hacer copias de bits en una media de respaldo, sino que también proporciona funcionalidades tales como:

- ✓ Planificar respaldos para que se ejecuten en el momento adecuado
- ✓ Maneja la ubicación, rotación y uso de la media de respaldo
- ✓ Funciona con operadores (y/o cargadores robóticos) para asegurarse de que la media apropiada está disponible
- ✓ Asistencia para ubicar la media que contiene un respaldo específico de un archivo dado

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto*

7.5 ANEXO 10. Manual de operaciones de servidores y servicios de Active Directory.

El presente manual contiene información relacionada con el diseño, implementación y configuración de un sistema basado en Windows Server 2012 R2, en especial el sistema de directorio Active Directory. Toda la configuración queda reflejada en la memoria de la solución.

El Directorio Activo o *Active Directory* (AD) es una base de datos de información sobre usuarios, estaciones de trabajo, impresoras entre otros. Ofrece a los usuarios el acceso a diferentes recursos de una red mediante un único inicio de sesión. Esto reduce considerablemente el número de contraseñas y facilita la administración de usuarios por parte del administrador.

No obstante, cualquier objeto de la red solo puede existir dentro de un dominio. Los dominios se usan para agrupar objetos relacionados con el fin de reflejar la red. El acceso a los objetos dentro de cada dominio se controla mediante entradas de control de acceso (ACE, *Access Control Entries*) contenidas en listas de control de acceso (ACL, *Access Control Lists*).

El Sistema de Nombres de Dominio (DNS) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a una red. Este sistema asocia información variada con nombres de dominios asignados a cada uno de los participantes. Su función más importante es traducir (resolver) nombres en identificadores binarios asociados a los equipos con el propósito de poder localizarlos y direccionarlos.

Las consultas DNS se resuelven de diferentes formas. A veces, un cliente responde a una consulta localmente mediante la información almacenada en la cache obtenida de una consulta anterior. Un servidor DNS también puede consultar o ponerse en contacto con otros servidores DNS en nombre del cliente solicitante para resolver el nombre por completo y, a continuación, enviar una respuesta al cliente. DNS utiliza los protocolos TCP y UDP en el puerto 53 para servir las peticiones. Generalmente la mayoría de las consultas DNS consisten en un solo paquete UDP enviado por el cliente seguido de un paquete UPD de respuesta generado por el servidor. TCP se utiliza en los casos en que la respuesta excede de los 512 bytes.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto*

7.6 ANEXO 11. Manual de operaciones de servidores Windows (otros servicios).

Este anexo contiene información relacionada con los diferentes roles a nivel del sistema operativo Microsoft, como lo son, el DA, DNS, DHCP, *File Server*, Plataformas como *Docker*, *PrintServe*r, etc., como también los Sistemas en H-A y otros instalados en los sistemas operativos *Microsoft Windows Server*. Como se mencionó anteriormente en otros tipos de software el licenciamiento Microsoft para servidores es perpetuo y se encuentra a nombre del Ministerio De Ambiente y Desarrollo Sostenible.

El servidor utiliza una consola de administración de Windows Server que permite aprovisionar y administrar servidores locales y remotos basados en Windows desde sus escritorios, sin necesidad de tener acceso físico a los servidores o la necesidad de habilitar conexiones de protocolo de Escritorio remoto (rdP) a cada servidor.

El administrador del servidor en Windows Server 2016, Windows Server 2012 R2 y Windows Server 2012 se pueden usar para administrar hasta 100 servidores, en función de las cargas de trabajo que ejecutan los servidores. El número de servidores que puede administrar mediante una única consola del Administrador del servidor, puede variar en función de la cantidad de datos que solicite de los servidores administrados y los recursos de hardware y red disponibles para el equipo que se ejecuta. A medida que la cantidad de datos que desea mostrar se aproxima a la capacidad de recursos del equipo, puede experimentar respuestas lentas del administrador del servidor y retrasos en la finalización de las actualizaciones. Para ayudar a aumentar el número de servidores que puede gestionar mediante el administrador del servidor, se recomienda limitar los datos de eventos que obtiene los servidores administrados mediante la configuración del cuadro de diálogo configurar.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto*

7.7 ANEXO 12. Software colaborativo y ofimática (Office 365)

El Ministerio de Ambiente y Desarrollo Sostenible cuenta con la suite completa y actualizada de Office 365 asociada a Microsoft 365 E5, la cual se estableció como trabajo colaborativo en nube y cada usuario puede contar con 58 aplicaciones asociadas a la licencia previamente mencionada. Este trabajo colaborativo en la nube tiene niveles de seguridad establecidos por el proveedor Microsoft, con la finalidad de salvaguardar la información y evitar perdida de datos accidentales.

Así mismo estas herramientas le permiten a los usuarios de la entidad, crear, acceder y compartir documentos online entre distintos usuarios en Word, Excel, PowerPoint y OneNote, entre otros; así mismo permite a la entidad centralizar una serie de herramientas colaborativas para que sean administradas desde una misma

plataforma, controlando el manejo, uso y la apropiación, además de evitar los reprocesos y desgaste administrativos del recurso humano, puesto que se generaban varios procesos contractuales para la adquisición de todos ellos.

Es por ello, por lo que ahora el correo electrónico y la ofimática (word, Excel, PowerPoint) y las demás aplicaciones que conforman esta suite en la nube, las cuales se sincronizan con el Directorio activo (AD), permiten una mejor experiencia de usuario al poder ser accedidas desde cualquier parte del mundo, con solo contar con datos en un dispositivo.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto*

8. Servicios de Mesa de Ayuda (GEMA)

8.1 ANEXO 13. Service Desk.

El propósito principal de este de manual consiste en orientar al usuario sobre el procedimiento a seguir para solicitar la atención técnica del Proceso de Gestión de Servicios e Infraestructura Tecnológica, ante inconvenientes en la operación de los sistemas de información, software, hardware y equipos que utiliza en sus actividades diarias. De igual forma permite establecer los lineamientos para gestionar los servicios que se prestan a través del punto único de gestión de servicios de TI.

La razón de ser de la mesa de ayuda es prestar al usuario una atención rápida y eficiente, además de asegurar que los procesos de la estrategia y gobierno de TI y Gestión de Servicios e Infraestructura Tecnológica, cuenten con la información clara y concisa de la necesidad del usuario con el propósito de asignar al analista o especialista idóneo para su atención de acuerdo con el componente requerido. La herramienta tecnológica de mesa de ayuda utiliza un conjunto de servicios que se ofrecen para gestionar y solucionar todos los posibles requerimientos e incidencias de manera integral, junto con la atención de los casos relacionados con las TIC (Tecnologías de Información y las Comunicaciones).

La herramienta tecnológica permite procesar los trámites y solicitudes que se realicen a los procesos, estrategia, gobierno de TI y Gestión de Servicios e infraestructura Tecnológica del Ministerio de Ambiente y Desarrollo Sostenible; así como hacer seguimiento, generar estadísticas e indicadores, en aras de ofrecer un buen servicio a la entidad. En este manual se explica cómo un usuario puede acceder y usar las principales características de la mesa de Ayuda.

Todo requerimiento o incidencia tecnológica debe ser reportada por el usuario a mesa de ayuda para su respectiva atención.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto.*

8.2 ANEXO 14. Creación de usuarios

El presente manual contiene las directrices mediante el cual se busca generar el mecanismo de protección, límites y procedimientos frente a la administración y responsabilidad relacionada con los accesos a la información.

- Control de acceso con usuario y contraseña: El control de acceso a las redes, aplicaciones, y/o sistemas de información de la entidad, es solicitado por los jefes de cada oficina mediante la herramienta de gestión TI, adjuntando el debido contrato o documentos que permitan evidenciar el vínculo contractual con la entidad, el área en que se desempeña y las aplicaciones o herramientas a que acedera, así mismo por cada servidor público se establece el acceso y su respectiva contraseña.
- Suministro del control de acceso: Esta política debe determinar los procedimientos formales y directrices que se deben construir para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, también deben tenerse en cuenta en esta política los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad.
- Gestión de contraseñas: define los lineamientos y criterios mínimos para el establecimiento de las contraseñas, tiempo duración y la manera de ser utilizadas en los accesos a la red, aplicaciones y sistemas de información de la entidad.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto*

MADSIG Sistema Integrado de Gestión

9. SISTEMAS DE INFORMACIÓN

9.1 ANEXO 15. Manual de operaciones de servidores de Bases de Datos.

El presente documento establece los lineamientos para la administración de las bases de datos de los servidores, mediante el cual se define la gestión en el monitoreo, aplicación de los ajustes necesarios para garantizar su debida operación, optimización de desempeño, verificación de logs, estandarización de nombramiento y codificación de las mismas entre otros.

El servidor de base de datos tiene como finalidad almacenar, recuperar y administrar los datos, mediante el uso de tablas, índices y registros para acceder a la información que se gestiona desde diferentes servidores, permitiendo generar acciones dependiendo del nivel de privilegios que se posea. En cuanto a los motores de las bases de datos se generan diferentes consultas, lo que permite escribir en determinada tabla, mientras que en otra solo se genera lectura de datos.

Dentro de las definiciones que se establecen en el manual, se describen algunas funcionalidades que se encuentran implementadas en los servidores de bases de datos para la indexación de los sitios web, servidor de contenido dinámico, administración de documentos, así como el registro de usuarios. De igual forma se describe la arquitectura implementada en la entidad de forma general como soporte a la gestión de las operaciones y continuidad del servicio.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto*

9.2 ANEXO 16. Manual de operaciones de servidores de aplicaciones

El servidor de aplicaciones constituye el motor de las bases de datos de las aplicaciones que se han implementado en él. En el presente manual anexo se describe la arquitectura implementada al interior de la entidad, con el propósito de facilitar la gestión sobre la misma y proporcionar la información necesaria para responder en la continuidad de las operaciones de la infraestructura tecnológica. El servidor de aplicaciones proporciona la lógica del negocio y el entorno de ejecución de la red distribuida en un programa de aplicación, lo que significa que es donde realmente se ejecutan las aplicaciones a través de diferentes niveles: el Front end representa la interfaz gráfica para los usuarios basado en el navegador web; interfaz para programación de aplicaciones (API) como intermediario entre la comunicación de la interfaz del front end y las bases de datos en el back end; y el Back end destinada para el almacenamiento y transacciones de datos.

NOTA: *La documentación detallada anexa está clasificada como confidencial, cualquier solicitud de acceso deberá ser autorizado por el (la) jefe de la Oficina TIC, del Ministerio o un delegado debidamente autorizado con roles y responsabilidades específicas en este contexto*

10. ROLES Y RESPONSABILIDADES

Para los fines correspondientes al cumplimiento de salvaguarda y custodia se establecen los siguientes roles y responsabilidades para todos los documentos a los que se hace referencia en este Manual general de operaciones. El modelo de operación y administración de infraestructura tecnológica incluye todos los elementos de operación y servicios requeridos para garantizar la disponibilidad y operación de la plataforma tecnológica.

COMPONENTE	RESPONSABLE	ACTIVIDADES PRINCIPALES
Planificación de TI	Jefe Oficina TIC	Definir e implementar los planes, proyectos y programas relacionados con la gestión de la Tecnología y sistemas de información para garantizar una gestión, eficiente, eficaz y transparente en el marco de la normatividad vigente para la Entidad.
		Gestión de la seguridad y cumplimiento normativo
		Gestión estratégica (Evaluación de tecnologías emergentes)
		Plan estratégico de TI
		Definición, seguimiento y evaluación de políticas de TI
Gestión de infraestructura de TI	Líder infraestructura de TI	Aplicar en concordancia con el plan estratégico, políticas, procesos y procedimientos de la entidad, vigentes, garantizando el servicio y el desarrollo de planes, proyectos y programas de infraestructura tecnológica.
		Definición y actualización de la arquitectura de la infraestructura tecnológica
		Desarrollo de planes de capacidad para proyectar los crecimientos de la infraestructura (Gestión de la capacidad)
		Gestión de la continuidad de los servicios de TI
		Seguimiento y control respecto a los procedimientos de administración y control sobre los requerimientos de cambios que surgen a partir de la actualización de las plataformas
		Desarrollo de planes de disponibilidad para garantizar las necesidades teniendo en cuenta los planes de mantenimiento (Gestión de la disponibilidad)
		Gestión y seguimiento plan de mantenimiento
	Administrador de Infraestructura	Administración de las soluciones de almacenamiento
		Administración de sistemas de backup
		Monitoreo de la infraestructura
		Administración del licenciamiento de software datacenter
		Garantizar el respaldo, custodia y la recuperación de la información de la infraestructura tecnológica
		Administración del directorio activo
	Administrador de redes y comunicaciones	Gestión de la conectividad (redes e internet)
		Gestión de la red local
		Seguimiento de la operación de los dispositivos activos
		Seguimiento de la operación del canal de internet
		Garantizar el respaldo, custodia y la recuperación de la información de la infraestructura tecnológica
		Administración de los servicios de comunicaciones unificadas
	Administrador de aplicaciones	Solución de novedades para mantener el uso de los sistemas de información con base en la plataforma tecnológica
		Administración técnica de las aplicaciones
		Administración de los componentes de capa media que soportan las aplicaciones

		Administración de base de datos
		Garantizar el respaldo, custodia y la recuperación de las bases de datos y aplicaciones
	Administrador de seguridad	Administración de firewalls
		Administración antivirus
		Administración sistema de seguridad perimetral
		Monitoreo y seguimiento disponibilidad de servicios
Gestión de servicios tecnológicos	Líder de servicios tecnológicos	Dirigir, gestionar, evaluar y controlar el cumplimiento de los objetivos institucionales en concordancia con, plan estratégico, políticas, procesos y procedimientos de la entidad, vigentes, garantizando el servicio y el desarrollo de los planes, proyectos y programas de infraestructura tecnológica
		Gestión de la disponibilidad
		Gestión de niveles de servicio
		Gestión de problemas
	Equipo de soporte mesa de ayuda	Detectar, clasificar y dimensionar los eventos que se presenten en los servicios TI
		Registro de solicitudes y seguimiento a la atención
		Solución de consultas sobre el uso de las aplicaciones
		Solución de incidentes con equipos y software de oficina
		Atención de requerimientos de servicios informáticos
		Diagnóstico inicial y escalamiento de incidentes y requerimientos a los siguientes niveles de atención
		Seguimiento y gestión de hardware y software de estaciones de trabajo

Tabla 1. Modelo de operación y administración de infraestructura tecnológica Minambiente. Tomado de: Versión propia de acuerdo con el MODELO DE GESTIÓN IT4+ MINTIC

REFERENCIAS

Incibe_. (s.f.). *CONTRASEÑAS*. Obtenido de Instituto Nacional De Ciberseguridad: https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf

MinTic. (29 de Julio de 2016). *Modelo de Seguridad y Privacidad de la Información*. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Pinzón Serrano, L. C. (s.f.). *Política de escritorio limpio y pantalla limpia*. Obtenido de MinTIC: https://www.mineducacion.gov.co/1780/articles-407695_galeria_02.pdf

Serrano, P. C. (s.f.). *Política sobre el uso de controles criptográficos*. Obtenido de MinTIC: https://www.mineducacion.gov.co/1759/articles-407695_galeria_07.pdf

MADSIG Sistema Integrado de Gestión