1. OBJETO:

Definir los lineamientos e instrucciones para que el personal de soporte pueda brindar una asistencia efectiva a los usuarios de la UAESP y asegurar la disponibilidad de la infraestructura tecnológica de la Entidad manteniéndola en correcto funcionamiento y aumentando al máximo su vida útil.

2. ALCANCE:

El documento abarca los pasos, recomendaciones e instrucciones para resolver incidencias, realizar tareas de mantenimiento y configuración sobre el catalogo de servicios de la Oficina TIC. Aplica para los funcionarios y contratistas de la OTIC.

3. DEFINICIONES:

Data Center: Palabra en ingles que significa Centro de Datos y hace referencia a la infraestructura física o virtual usada para alojar los sistemas informáticos que procesan datos y centralizan los servidores de la Entidad.

Mantenimiento: Para propósitos del documento, el termino hace referencia a las acciones técnicas o administrativas enfocadas a la conservación en buen estado de la infraestructura tecnológica de la Entidad para evitar su deterioro.

Mantenimiento Preventivo: Acciones anticipadas y encaminadas a prever los fallos de maquinaria y equipos garantizando su correcto estado de funcionamiento.

Patch Cord: Se le llama así, al cable (UTP, F.O, etc) que se usa en una red para conectar un dispositivo electrónico con otro.

Servidor: Dispositivo físico o virtual que almacena, distribuye y suministra información.

Soporte: Acción focalizada en el usuario y en la ayuda que se le puede brindar para realizar un correcto uso de las herramientas tecnológicas y de la información.

Switch: Dispositivo de interconexión utilizado para conectar equipos en red formando lo que se conoce como una red de área local LAN.

UPS: Abreviación de la palabra en ingles Uninterruptable Power Supply que traduce Sistema de Alimentación Ininterrumpida. Este dispositivo permite un flujo de energía eléctrica mediante baterías cuando el suministro eléctrico principal falla y protege de picos altos o bajos de voltaje.

Usuario: Para propósitos de este documento, hace referencia a servidores (as) públicos (as) y contratistas que tienen asignado un equipo de cómputo o hacen uso de cualquier elemento de la infraestructura tecnológica de la Entidad.

4. GENERALIDADES DEL MANTENIMIENTO DE INFRAESTRUCTURA:

La Oficina de la Tecnologías de la Información y las Comunicaciones gestiona el mantenimiento preventivo de la infraestructura tecnológica a través de la administración de contratos dispuesto para ello.

Los servidores (as) públicos (as) o contratistas que apoyen la supervisión de los contratos de mantenimiento deberán:

- En la reunión inicial o Kick Off, elaborar el cronograma de mantenimiento de acuerdo con los contratos y fechas pactadas con el proveedor.
- Reportar en la Mesa de servicio, al correo mesa.servicios@uaesp.gov.co, las ventanas de mantenimiento y sesiones para informar al usuario fechas, tiempo estimado del mantenimiento y posibles afectaciones en el servicio.
- A través de la Mesa de Servicio, informar por correo electrónico a los usuarios y áreas correspondiente la realización del mantenimiento procurando que los escritorios se dejen libres de objetos personales y cualquier activo de información diferente al que será intervenido.

- Coordinar con el encargado en la Oficina TIC de las hojas de vida de los equipos, las acciones necesarias para el registro de las actividades de mantenimiento en sus respectivas hojas de vida.

- Asegurar el acompañamiento de los proveedores a la hora de realizar mantenimiento a los diferentes equipos o dispositivos de la infraestructura tecnológica, velando por la seguridad de los activos de información y cualquier bien de la Entidad en conformidad con el Manual de Políticas de Seguridad de la Información.

5. SOPORTE

Los agentes asignados por el administrador de la mesa de servicio para la atención de un caso de soporte o reportes realizados por el usuario deberán:

- Realizar diagnóstico: El agente deberá coordinar las acciones necesarias para realizar de forma presencial o remota, el diagnostico o análisis inicial de los equipos, herramientas o servicios que se encuentran dentro del catálogo de servicios de la OTIC, de acuerdo con la particularidad del caso reportado.

- Si el daño es sobre un dispositivo o herramienta se deberá revisar:

  - ❖ Garantía: Si está vigente la garantía, se deberá coordinar las acciones necesarias con el proveedor o fabricante para el envío del dispositivo y solicitar su reposición o arreglo.
  - ❖ Póliza de seguro: Si el daño no es cubierto por la garantía y tiene póliza de seguro, se deberá coordinar las acciones necesarias con la Oficina TIC y Apoyo Logístico o la persona encargada de los seguros de la Entidad, para iniciar el proceso respectivo.

- Si el daño no puede ser cubierto por garantía ni por el seguro, o no cuenta con ninguno de ellos, se deberá notificar al jefe de la Oficina TIC y seguir sus instrucciones.

- Software y elementos de configuración: Se deberá seguir las siguientes recomendaciones

6. MANTENIMIENTO PREVENTIVO

Siga las siguientes recomendaciones para llevar a cabo el mantenimiento preventivo de la infraestructura tecnológica de la Entidad, evitando traumatismo en la prestación de servicios u operación de esta.

6.1 Mantenimiento preventivo de equipos de cómputo de usuario y telefonía

Se debe procurar por programar los mantenimientos en horario no laboral a fin de no interrumpir la continuidad de la operación.

6.1.1 Sede Central

- Dividir la ejecución del mantenimiento por pisos, oficinas o áreas.

- informar a los usuarios la fecha programada para el mantenimiento procurando tomar las medidas necesarias para dejar el escritorio limpio.

- Cuando el mantenimiento se realice en horas nocturnas o no se supervise por parte de la Oficina TIC, se debe solicitar el acompañamiento del personal de seguridad física o vigilancia al proveedor, velando por la seguridad de los activos de información.

- El proveedor deberá realizar las acciones correspondientes y entregar un informe final, con el listado de equipos de cómputo y los hallazgos encontrados.

6.1.2 Archivo de Gestión, Archivo Central y otras sedes.

- El mantenimiento en el archivo de gestión y archivo central deberá realizarse en horario diurno y contar con supervisión del encargado en cada sede, para velar por la seguridad de los activos de información.

6.2 Mantenimiento de Impresoras

Las impresoras en la entidad son provistas bajo la modalidad de arriendo, por lo cual, el proveedor deberá informar las visitas para sus mantenimientos respectivos y se deberá coordinar su ingreso e informar a los usuarios.

6.3 Mantenimiento Escáneres propiedad de la UAESP

Con el propósito de no interrumpir las actividades de atención al ciudadano se programará el mantenimiento de los escáneres de la siguiente forma:

- Coordinar las actividades necesarias para que se realice el mantenimiento en horario no laboral.
- Informar a los usuarios la fecha programada para el mantenimiento procurando tomar las medidas necesarias para dejar el escritorio limpio.
- Cuando el mantenimiento se realice en horas nocturnas o no se supervise por parte de la Oficina TIC, se debe solicitar el acompañamiento del personal de seguridad física o vigilancia al proveedor, velando por la seguridad de los activos de información.
- El encargado de las hojas de vida de los equipos en la Oficina TIC realizará la actualización de estas.

6.4 Mantenimiento Aires Acondicionados

La Oficina TIC velará por el mantenimiento de los aires acondicionados ubicados en el Data Center y el cuarto de UPS, para lo cual se deberá:

- Realizar el mantenimiento en horario diurno.
- El mantenimiento a los aires acondicionados ubicados en el Data Center se hará uno a la vez, para garantizar la redundancia del control de temperatura dentro del Data Center.
- El mantenimiento a los aires acondicionados ubicados en el cuarto de UPS se hará uno a la vez, para garantizar la redundancia del control de temperatura.
- La Oficina TIC deberá realizar acompañamiento al proveedor para velar por la seguridad de los activos de información.
- En caso de encontrar fallas, el proveedor realizara el mantenimiento correctivo necesario.
- El proveedor deberá realizar las acciones correspondientes y entregar en el informe final las acciones y cambios correctivos realizados, si los hubiera.
- El encargo de las hojas de vida de los equipos en la Oficina TIC realizará la actualización de estas.

6.5 Mantenimiento UPS

A estos equipos de misión crítica deberán realizárseles mantenimiento tenido en cuenta los siguientes lineamientos:

- El mantenimiento se realizará a 1 UPS a la vez para minimizar el impacto a la continuidad de la operación.
- La Oficina TIC deberá realizar acompañamiento al proveedor para velar por la seguridad de los activos de información.

- En caso de encontrar fallas, el proveedor realizará el mantenimiento correctivo necesario.

- El proveedor deberá realizar las acciones correspondientes y entregar en el informe final las acciones y cambios correctivos realizados, si los hubiera.

- El encargo de las hojas de vida de los equipos en la Oficina TIC realizará la actualización de estas.

6.6 Mantenimiento Centro de cableado

Este mantenimiento incluye, los switches, patch cord, entre otros, y deberán seguirse los siguientes lineamientos.

- El mantenimiento se realizará en horario no laboral, por las afectaciones al servicio.

- Cuando el mantenimiento se realice en horas nocturnas o no se supervise por parte de la Oficina TIC, se debe solicitar el acompañamiento del personal de seguridad física o vigilancia al proveedor, velando por la seguridad de los activos de información.

- El proveedor deberá realizar las acciones correspondientes y entregar en el informe final las acciones y cambios correctivos realizados, si los hubiera.

- El encargo de las hojas de vida de los equipos en la Oficina TIC realizará la actualización de estas.

6.7 Mantenimiento del Data Center

Para el mantenimiento del Data Center se seguirán los siguientes lineamientos:

- El mantenimiento se realizará en horario no laboral para minimizar el impacto en la continuidad de la operación.

- Coordinar las actividades y servicios críticos para intervenir los servidores.
- Dividir el mantenimiento en 2 sesiones, o las necesarias, de acuerdo con las actividades críticas de la Entidad.
- Intervenir 1 nodo a la vez, trasladando las cargas de trabajo a un segundo nodo.
- Distribuir cargas y poner el servicio en funcionamiento normal.
- Los servidores de baja disponibilidad se programarán en un fin de semana y deberá informarse que el servicio se verá afectado.
- Para el mantenimiento del firewall se usará la misma estrategia, de nodos, basada en la alta disponibilidad.
- El proveedor deberá realizar las acciones correspondientes y entregar en el informe final las acciones y cambios correctivos realizados, si los hubiera.
- El encargo de las hojas de vida de los equipos en la Oficina TIC realizará la actualización de estas.

6.8 Mantenimiento Planta Eléctrica

Se realizará el mantenimiento de la planta eléctrica de acuerdo con los siguientes lineamientos:

- Programar el mantenimiento en horario no laboral y diurno, de ser posible en un fin de semana.
- Una vez realizado el mantenimiento, se realizará una prueba controlada con el acompañamiento de la Oficina TIC, verificando que la planta realice su encendido correctamente en conjunto con las UPS, de la siguiente forma:
  - ❖ Verificar el funcionamiento de las UPS.

- ❖ Desconectar el suministro principal de energía.
- ❖ Verificar si la planta realiza el encendido y monitorear por 10 minutos el suministro de energía.
- ❖ Si la planta no realiza el encendido, automático o manual, no se debe esperar más de 10 minutos hasta conectar el suministro de energía principal, para no afectar la operación continua del Data Center.

6.9 Mantenimiento de Drones

Se deberán seguir las recomendaciones y lineamientos dados en el MN-03 Manual Operación y Mantenimiento de Aeronaves no Tripuladas, en su última versión vigente o el que haga sus veces.

7. BORRADO SEGURO DE LA INFORMACIÓN

El borrado seguro de la información y la destrucción de los soportes no solo buscan proteger contra la divulgación no autorizada de la información confidencial o reservada de la Entidad, sino también, proteger la fuga de datos personales de la ciudadanía.

Importante: Antes de realizar el borrado seguro de la información, se debe tener autorización del responsable del activo de información. Salvo los casos, donde los equipos o dispositivos electrónicos de almacenamiento que son devueltos a almacén o a la OTIC.

Para realizar el proceso de borrado seguro, siga las siguientes instrucciones.

7.1 Verificación

Se debe verificar el soporte o dispositivo de almacenamiento de la información para:

- Determinar el método de borrado seguro adecuado.

- De ser requerido, realizar el respaldo de la información de acuerdo con los lineamientos del procedimiento GTI-PC-11 Gestión de Respaldos o el que haga sus veces.

7.2 Borrado Seguro

El método más eficaz es la destrucción física, no obstante, se debe realizar un borrado por sobreescritura para dispositivos de almacenamiento como Discos Duros u otros similares, previo a la destrucción física. Para esto, realice lo siguiente.

SOBREESCRITURA:

Ejecute la acción de borrado seguro, usando la suite de herramientas de Hiren´s Boot empleando un método de 3 pasadas como el DoD 5220 o cualquier equivalente, para los dispositivos que aplique. En caso de no contar con la herramienta descrita, use cualquier otra disponible en la Oficina TIC, luego realice una destrucción física.

Nota: El formateo de un dispositivo de almacenamiento no es un método eficiente y parte o toda la información puede llegar a ser recuperada.

DESTRUCCIÓN FISICA:

- Trituración: Use una trituradora de papel para destruir medios flexibles como CD/DVD o la misma información impresa, de forma que el fragmento sea tan pequeño que sea casi imposible recuperar la información o los datos.

- Desintegración, pulverización, fusión o incineración: Métodos que no se emplean directamente en la UAESP, pero que pueden ser usados por los proveedores autorizados para la disposición final de medios de almacenamiento como HD, SSD, USB u otros. No obstante, antes de enviarlos con el proveedor se debe realizar un proceso de borrado digital como la sobreescritura y solicitar el certificado de disposición final.

8. LNEAMIENTOS DE SEGURIDAD PARA TELETRABAJO

Se deberá verificar las siguientes condiciones para el visto bueno de la Oficina TIC en relación con la modalidad de teletrabajo.

8.1 Equipo de computo

Equipo de la Entidad:

- Sistema de autenticación: Usuario y contraseña.
- Otro: Cierre de sesión por inactividad.
- Conectividad:
  - ❖ Recomendado, mínimo, la banda ancha definido para Colombia.
  - ❖ Conexión VPN o Remota, cuando sea necesario.
- Software Antimalware: Agente antivirus o EndPoint actualizado.
- Software Aplicación, utilitario y aplicación:
  - ❖ Agente antivirus o EndPoint actualizado
  - ❖ Sistema Operativo licenciado y actualizado.
  - ❖ Suite ofimática licenciada, cuando aplique.
  - ❖ Compresor de archivos.
  - ❖ Revisión de software no autorizado en la Entidad.

Equipo personal:

- Sistema de autenticación: Usuario y contraseña.

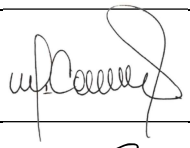
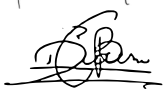
- Otro: Cierre de sesión por inactividad.
- Conectividad:
  - ❖ Recomendado, mínimo, la banda ancha definido para Colombia.
  - ❖ Conexión VPN o Remota, cuando sea necesario.
- Hardware:
  - ❖ Procesador Intel Core i3, equivalente o superior.
  - ❖ Memoria RAM 8 GB o superior.
- Software Antimalware: Agente antivirus o EndPoint actualizado.
- Software Aplicación, utilitario y aplicación:
  - ❖ Agente antivirus o EndPoint actualizado
  - ❖ Sistema Operativo licenciado y actualizado.
  - ❖ Suite ofimática licenciada, cuando aplique.
  - ❖ Compresor de archivos.
  - ❖ Revisión de software no autorizado en la Entidad.

9. CONTROL DE CAMBIOS:

Versión	Fecha	Descripción de la modificación
1	06/08/2021	Creación del documento.
2	10/07/2023	Se ajustó el nombre del instructivo pasando de "Mantenimiento preventivo" a "Soporte técnico", el

Versión	Fecha	Descripción de la modificación
		objetivo y su alcance. se adiciona las instrucciones para el borrado seguro de la información y lineamientos de seguridad para teletrabajo.

10. AUTORIZACIONES:

	NOMBRE	CARGO	FIRMA
Elaboró	Juan Sebastián Perdomo Méndez	Profesional Universitario – Oficina TIC	
	Maria Consuelo Torres Pinto	Contratista – Oficina TIC	
	Daniel Contreras Bolaños	Contratista – Oficina TIC	
Revisó	Cesar Mauricio Beltran Lopez	Jefe - Oficina TIC	
	Luz Mary Palacios Castillo	Profesional Universitario – Oficina Asesora de Planeación	
Aprobó	Yesly Alexandra Roa	Jefe Oficina Asesora de Planeación	Alexandra Roa Mendoza Firmado digitalmente por Alexandra Roa Mendoza Fecha: 2023.07.07 19:06:55 -05'00'