MINISTERIO DE LA DEFENSA NACIONAL

UNIDAD DE INFORMÁTICA

PROCEDIMIENTO OPERATIVO NORMAL (PON) DE LA UNIDAD DE INFORMÁTICA DEL MINISTERIO DE LA DEFENSA NACIONAL.

JUL 2020

COPIA N° ___ DE _6_ COPIAS
HOJA N° _1_ DE _27_ HOJAS
UNIDAD DE INFORMÁTICA
SAN SALVADOR (7585)
JUL020
JEFATURA
B2e-065B

PROCEDIMIENTO OPERATIVO NORMAL (PON) DE LA UNIDAD DE INFORMÁTICA DEL MINISTERIO DE LA DEFENSA NACIONAL.

1.- OBJETO Y ALCANCE.

a.- Objeto.

El presente Procedimiento Operativo Normal (PON), tiene como objetivo regular las actividades que se realizan en los diferentes puestos funcionales que conforman la Unidad de Informática del Ministerio de la Defensa Nacional.

b.- Alcance.

1) Disponer de un documento que defina los procedimientos que se realizan en cada uno de los puestos funcionales de la Unidad de Informática, basados en experiencia y buenas prácticas.

2) Dar cumplimiento a la normativa que regula la documentación interna del Ministerio de la Defensa Nacional.

2.- JEFATURA DE LA UNIDAD DE INFORMÁTICA.

a.- Diseñar y proponer políticas de ciberseguridad.

b.- Proponer sistemas para la simplificación de procesos administrativos.

c.- Asesorar al Mando en la actualización y adquisición de nuevas tecnologías para la Secretaría de Estado.

d.- Supervisar el cumplimiento de los planes de mantenimiento a los equipos informáticos de la Secretaría de Estado.

e.- Asistir a reuniones programadas y no programadas.

3.- SECRETARIA.

a.- Atender llamadas.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

1) Atender llamadas telefónicas.

2) Transferir las llamadas a las áreas correspondientes.

3) Tomar recados o notas de las llamadas recibidas en caso que sea necesario.

b.- Libro de Control de Entradas y Salidas del Personal de esta Unidad.

1) Elaborar el formato del Libro de Control de Entradas y Salidas del Personal de esta Unidad.

2) Verificar que todo el personal registre su hora de entrada y salida en el libro.

3) Pasar a Firma el libro al Jefe de la Unidad y al Encargado de Personal.

4) Escanear libro y remitir a la Dirección de Administración, en la primera semana de cada mes.

c.- Recibir, registrar y distribuir documentos de entrada.

1) Recibir y revisar la documentación procedente de las diferentes dependencias de esta cartera de estado, unidades militares y de instituciones externas.

2) Registrar los documentos recibidos en el libro de control de correspondencia.

3) Entregar documentación al Jefe de la Unidad para su respectiva marginación.

4) Escanear documentación marginada y enviarla a través del Sistema Cero Papeles.

d.- Elaborar, registrar y distribuir documentos de salida.

1) Elaborar documentos requeridos (memorándum, mensajes, oficios, informes, entre otros).

2) Asignar número al documento de salida de acuerdo al control de numeración anual de esta Unidad.

3) Asignar código de asunto al documento de salida de acuerdo a la tabla de clasificación.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

4) Registrar la salida del documento en el libro de control de correspondencia.

5) Enviar por medio del Sistema Cero Papeles el documento elaborado para su revisión.

6) Cuando el documento se encuentre firmado, entregarlo al ordenanza de esta Unidad para su distribución.

e.- Brindar seguimiento al trámite de los requerimientos de información recibidos de la Unidad.

f.- Agendar fecha de contestación de los documentos que lo requieren y dar seguimiento a estos.

g.- Verificar si la documentación de entrada o salida está vinculada a documentos o proyectos a los que se le está dando seguimiento o están en ejecución.

h.- Llevar el control del archivo de documentos de la unidad,

1) Recodificar documentos de entrada y salida de la unidad, en caso que lo amerite.

2) Escanear la documentación de entrada y salida de la unidad.

3) Elaborar expedientes con la documentación recibida y enviada.

4) Archivar la documentación en físico ordenada por clasificación LAIP, asunto y fecha de envío o recepción de información.

5) Respaldar el archivo de forma digital de acuerdo al procedimiento del sistema integrado de archivo.

6) Subir documentación al Sistema de Gestión de Documentos Institucional (SGDI).

i.- Agendar reuniones o actividades del personal de la Unidad.

1) Llevar control de los días y horas en el que el personal de la Unidad tiene reuniones o actividades programadas.

2) Colaborar en orientar al personal que visita la unidad.

3) Brindar atención al personal que visita la unidad.

j.- Control de permisos del personal.

1) Elaborar permisos del personal.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

2) Llevar control de horas de permisos personales y consultas médicas.

3) Remitir permisos autorizados a la Dirección de Administración, según programación establecida.

4) Archivar permisos en expedientes personales.

4.- ORDENANZA.

a.- Hacer aseo en toda la oficina.

1) Barrer y trapear aplicando desinfectante de piso, todos los días.

2) Limpiar el escritorio del jefe

3) Lavar lavamanos dos veces al día como mínimo.

4) Lavar taza de inodoro, con lejía o detergente, como mínimo dos veces al día.

5) Botar la basura hasta el depósito que se encuentra en el predio del EMCFA.

6) Cambiar a diario las toallas de mano, y llevarlas a lavar cada semana.

7) Apoyar en otras actividades de la unidad según lo requiera el jefe.

b.- Entregar la documentación.

1) Estar pendiente de la documentación.

2) Entregar toda la documentación producida en el día.

c.- Realizar turnos.

1) Hacer los turnos correspondientes, según el rol de servicio de ordenanzas, estos turnos son días de semanas y fines de semanas.

2) Hacerle limpieza a los lugares designados, los cuales son:

a) El auditórium

b) Los baños del auditórium

c) El edificio de los pabellones de oficiales.

d.- Mantener limpio el DATA CENTER.

1) Por ser una área delicada hay que hacerle limpieza con mucho cuidado ya que se encuentran equipos informáticos que se pueden dañar

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

fácilmente, por eso con cuidado se barre y se trapea con una franela húmeda se limpian los gabinetes por fuera.

e.- Lavar el auto de la unidad.

1) Lavar por fuera.

2) Limpiar y aspirar por dentro.

3) Aplicar silicon al tablero.

4) Limpiar vidrios con papel periódico.

5) Lavar llantas y aplicar silicón.

f.- Limpiar el pabellón del jefe de la unidad.

1) Barrer y trapear aplicando desinfectante.

2) Lavar lavamanos y taza del inodoro con lejía o detergente, dos veces a la semana.

g.- Mantenimiento preventivo de aires acondicionados de la oficina, datacenter y pabellón, cada dos meses.

1) Limpiar por fuera.

2) Sacar y lavar los filtros.

5.- JEFATURA DE LA SECCIÓN DE INVESTIGACIÓN Y DESARROLLO.

a.- Proponer la implementación de sistemas que simplifique los procesos administrativos de la Secretaría de Estado.

b.- Supervisar la implementación de sistemas.

c.- Proponer políticas orientadas a sistematizar y estandarizar las plataformas informáticas.

d.- Proponer nuevas aplicaciones.

1) Realizar investigación de campo en las diferentes dependencias de esta Cartera de Estado, con el objetivo de identificar los procesos administrativos rutinarios que puedan ser automatizados mediante un sistema informático.

2) Recibir por escrito los requerimientos de los nuevos sistemas por parte de los usuarios a través del conducto regular correspondiente.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

3) Elaborar documento con la propuesta para la creación de nuevos sistemas.

6.- ANALISTA-PROGRAMADOR.

a.- Modificación de aplicaciones existentes.

1) Recibir requerimientos por escrito de los usuarios a través del conducto regular correspondiente.

2) Realizar el análisis de los requerimientos recibidos.

3) Determinar la factibilidad de las modificaciones solicitadas.

4) Realizar el diseño de las nuevas modificaciones y/o funcionalidades.

5) Llevar a cabo la programación del diseño basados en buenas prácticas.

6) Realizar las pruebas con los usuarios finales y las correcciones necesarias.

7) Implementar las nuevas modificaciones.

8) Documentar técnicamente las funcionalidades adicionadas.

b.- Proponer nuevas aplicaciones.

1) Realizar investigación de campo en las diferentes dependencias de esta Cartera de Estado, con el objetivo de identificar los procesos administrativos rutinarios que puedan ser automatizados mediante un sistema informático.

2) Recibir por escrito los requerimientos de los nuevos sistemas por parte de los usuarios a través del conducto regular correspondiente.

3) Elaborar documento con la propuesta para la creación de nuevos sistemas.

c.- Ejecución del ciclo de vida de un sistema informático.

1) Fase de análisis.

a) Recopilar y analizar la información obtenida mediante visita de campo, entrevistas, encuestas, entre otras.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

b) Determinar el lenguaje de programación y motor de base de datos a utilizar, de acuerdo a las necesidades identificadas, tratar de homogenizar con los lenguajes que han sido diseñado los sistemas existentes.

c) Determinar los posibles procesos de migración de datos existentes.

d) Elaborar el documento de análisis respectivo.

2) Fase de diseño.

a) Crear un diseño que satisfaga las necesidades de las entradas, salidas y controles del sistema, basado en estándares de lenguaje unificado de modelado (UML).

b) Diseñar los flujos de trabajo.

c) Modelar la base de datos.

d) Diseño de pantallas y reportes.

3) Fase de desarrollo y documentación.

a) Configurar los entornos de desarrollo y producción, así como el control de versiones a fin de poder realizar las integraciones opciones y/o módulos asignados a los desarrolladores.

b) Escribir las líneas de código en el lenguaje de programación definido, utilizando buenas prácticas.

c) Realizar las pruebas de funcionamiento del código generado en el entorno de desarrollo.

d) Realizar las pruebas de migración de los datos y verificar la integridad de los mismos.

e) Elaborar documentación técnica (manuales de usuario y ficha técnica).

4) Fase de implementación.

a) Presentar el sistema a los usuarios finales, con el fin de que sea evaluada su funcionalidad y resultados requeridos.

b) Realizar migración de datos existentes previamente determinados en la fase de análisis.

c) Capacitar al usuario.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

d) Instalar sistema.

5) Fase de depuración

a) Identificar anomalías y corregir funcionalidades a fin de optimizar el código fuente.

b) Documentar correcciones realizadas y actualizar los manuales de usuario y ficha técnica.

6) Respaldos (adicionado)

a) Crear respaldos periódicamente del código fuente y binario.

7.- WEBMASTER.

a.- Instalaciones de infraestructura de servidores de producción.

1) Instalación y configuración de servidor web.

2) Instalación y configuración de motor de base de datos.

3) Instalación y configuración de servidor de Sistema de Nombres de Dominio (DNS).

b.- Programación de sitios web y desarrollo de nuevos módulos.

1) Configurar el entorno de desarrollo.

2) Instalación y configuración de plataformas de gestión de contenidos (CMS), como pueden ser WordPress) para implementar los sitios web institucionales o utilizar un CMS de terceros.

3) Elegir el motor de base de datos a utilizar.

4) Diseñar, crear e instalar la base de datos que utilizarán los sitios web.

5) Diseñar y crear la estructura del sitio web.

6) Aplicar y combinar de manera dinámica los diferentes elementos que forman parte de un sitio web: colores, tipografías, menú, botones, etc.

7) Instalación de plugins o complementos que sean necesarias para la creación de la página web solicitada.

8) Vinculación con los servicios complementarios, tales como las herramientas online como Google Analytics o Search Console de ser necesario.

9) Diseñar las imágenes que se usarán en el sitio web.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

10) Creación de usuarios correspondientes, los cuales actualizaran el contenido de los diferentes sitios web creados, con sus respectivos privilegios.

11) Innovar constantemente la forma de presentar o integrar las redes sociales en los sitios web.

12) Instalar el sitio o sitios desarrollados en el servidor de producción.

c.- Implementar políticas de seguridad para evitar daños o intrusiones.

1) Políticas de seguridad desde la aplicación.

a) Crear usuarios administradores o editores (accesos limitados) según sea la necesidad.

b) Investigar constantemente las vulnerabilidades de aquellos módulos, plugins, fragmentos de código, archivos flash entre otros, que utiliza el sitio web, para posteriormente depurarlos.

c) Auditar constantemente las bitácoras de accesos a los sitios web.

d.- Políticas de seguridad del lado del servidor

1) Configurar el sistema operativo que brinde la seguridad adecuada.

2) Asignar privilegios de lectura o escritura a los directorios de la aplicación web.

3) Restringir el acceso por IP al área de administración a los usuarios que serán encargados de administrar el sitio web.

4) Configurar directivas o módulos que brinden la protección de ataques hacia las aplicaciones.

5) No permitir que se listen los archivos en los directorios.

e.- Realizar respaldos de las bases de datos de cada sitio web que se tienen en producción.

1) Realizar respaldo diario, semanal y mensualmente de las bases de datos de los sitios que están en producción.

2) Realizar respaldo periódico de la aplicación web.

3) Mantener los respaldos de forma local y remota (sitio de contingencia).

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

f.- Proponer cambios para la implementación de mejoras en los sitios web.

1) Asesorar en cambios en los sitios web para actividades especiales como son Dia del Soldado, 15 de septiembre, Navidad, entre otros.

2) Apoyar en el diseño de imágenes que se usarán para los sitios web para las actividades mencionadas.

g.- Dar cumplimiento a nuevos estándares y/o requerimientos del Gobierno Central, referentes a los sitios web.

1) Coordinar con la autoridad competente que designe el Gobierno Central los requerimientos hechos y verificar si es posible cumplirlos si no riñen con los principios institucionales.

h.- Configuración del servidor para la realización de la transmisión en vivo de eventos importantes a través de Internet en donde participen los miembros del Alto Mando y otros que se requieran por disposición legal (Ejemplo rendición de cuentas).

1) Coordinar con DCP para que asignen equipo.

2) Activar el canal para realizar transmisión en vivo.

3) Realizar prácticas o ensayos previos al evento.

i.- Arte y diseño de imágenes ya sea de temas principales de los sitios web o de otra índole.

1) Emplear herramientas de diseño asistido por computadora (CAD) para crear imágenes, diseños y gráficos.

2) Realizar todo lo relacionado a diseño gráfico de los sitios web que se desarrollan e implementan.

3) Utilizar bancos de imágenes, previa coordinación con la Dirección de Comunicaciones y Protocolo, que son los encargados de las tomas de fotografías y videos.

4) Desarrollar iconos estándares e imágenes para las aplicaciones que se desarrollan en la Unidad de Informática.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

5) Coordinar con personal de las diferentes Dependencias de esta Secretaria de Estado que haya solicitado algún tipo de diseño gráfico para conocer sus necesidades, previa solicitud con el Jefe de la Unidad de Informática.

6) Supervisar la producción y entrega del producto final, en caso de impresiones con empresas particulares.

7) Desarrollo de portadas y contraportadas graficas de Informes, Revistas, etc.

8.- JEFATURA DE LA SECCIÓN DE SOPORTE Y MANTENIMIENTO.

a.- Centralizar el mantenimiento de los equipos y sistemas informáticos de la Secretaría de Estado.

b.- Desarrollar el plan de mantenimiento preventivo anual a los equipos informáticos.

c.- Aprobar la opinión técnica para la adquisición y descargo de equipo informático.

d.- Analizar los sistemas de comunicación y proponer medidas preventivas para fortalecer la ciberseguridad de la Secretaría de Estado.

9.- TÉCNICO EN MANTENIMIENTO DE HARDWARE Y SOFTWARE.

a.- Instalación, mantenimiento y actualización de software.

1) Instalación de controladores para periféricos (DRIVERS)

a) Verificación de funcionamiento del periférico, hacer las pruebas de su funcionamiento y determinar fallas en los controladores en caso de no lograr un buen funcionamiento se realizaría la reinstalación de drivers según los siguientes pasos.

b) Desinstalación del driver dañado.

c) Verificación de la media de los drives correspondiente al equipo.

d) Instalación de nuevo drivers.

e) Reinicio de equipo para determinar que este bien instalado el driver.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

f) Verificar el buen funcionamiento del driver.

2) Software. (Sistemas Operativos).

a) En casos que la computadora este presentando fallas en el sistema operativo, tales como (virus, instalar y desinstalar programas una y otra vez, drivers incorrectos entre otros) hacer las pruebas necesarias en tal equipo para posteriormente hacer una reinstalación de dicho sistema operativo.

b) Realizar una copia de seguridad de los datos antes de hacer una estación de un sistema operativo.

c) Arranque, encender el ordenador rápidamente para entrar al menú BIOS, presionando la tecla configurada de tu equipo.

d) Pasos:

(1) Tener la Pc lista conectada a la corriente eléctrica y reconocer sus características (Procesador, D. Duro, Memoria RAM, etc.)

(2) Reconocer sus características para descargar los drivers o controladores enfocados al Sistema Operativo que se le instalar. (Ejemplo: mi pc es Compac Presario y la serie que sea) los drivers serán instalados después de la instalación del S. Operativo.

(3) Respaldar Archivos de la PC.

(4) Tener el S.O listo en un DVD o en una memoria USB listo para ser ejecutado.

(5) Introducir el DVD antes de encender para que el sistema lo reconozca y lo ejecute, en el caso de la USB puede colocarse cuando está encendida y ejecutarlo.

(6) Aparecerá una pantalla de Sistema y continuará apareciéndole una Interfaz gráfica donde le dará la opción de instalas el S.O.

(7) Seguir los pasos que le indica, le dará opciones como idioma, le dará opciones de formatear el disco duro y de hacerle particiones (según lo que el usuario desee).

(8) El sistema se reiniciará un par de veces esto es normal, ATENCION: no retire el disco ni desconecte su equipo.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

(9) Después de la instalación, le dará opciones de nombre del usuario y colocar contraseña.

(10) Enseguida podrá entrar a la Interfaz Gráfica del Usuario donde podrá interactuará con la PC.

(11) Instalará los drivers o controladores que tiene en una USB o en un CD-R dependiendo donde los haya colocado, de esta forma trabajara mejor su máquina.

3) Software (seguridad, antivirus)

a) Todas las computadoras de uso personal y propiedad del Ministerio, que accedan a la red del Ministerio, deberán de tener instalado el antivirus institucional.

b) Verificación del buen funcionamiento del antivirus, en caso de falla o de mala instalación, hay que proceder a desinstalar el programa, (antivirus) y posteriormente la nueva instalación del programa para mantener en óptimas condiciones nuestro equipo.

c) El primer paso, y quizá el más obvio, es la instalación. Los antivirus, al igual que la mayoría de aplicaciones para los ordenadores, se instalan a través de sencillos pasos donde se nos pregunta dónde queremos instalarlo, el proceso es sencillo por lo que no encontraremos problemas.

d) Una vez hemos instalado el antivirus nos dará la opción de abrirlo. Cuando estemos dentro de él lo más posible es que nos pida una configuración rutinaria para escanear nuestro equipo. Lo más conveniente es hacerlo, para localizar cualquier amenaza que tuviéramos en nuestro ordenador.

e) El siguiente paso es el corta fuegos, el sistema operativo también cuenta con su propio sistema.

f) Por último, y no por ello menos importante, tenemos que revisar las actualizaciones automáticas. Por defecto, suelen venir activadas, pero es conveniente asegurarse de que es así. De tal modo, nuestro ordenador estará al día de todas las amenazas que vayan saliendo.

b.- Mantenimiento preventivo y correctivo al hardware.

1) Realizar pruebas de funcionamiento de Baterías de UPS.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

a) Voltaje de fuente de alimentación

b) Voltaje de entrada y salida

c) Corriente de entrada y salida

d) Pruebas con carga

e) Pruebas para verificar con bancos de baterías

f) Revisión, limpieza y pruebas de transformadores de aislamiento

g) Limpieza general del entorno de la UPS

h) Pruebas del UPS con el tablero de transferencia automática.

i) En caso de resultados negativos se recomienda al usuario que sea revisado por el Técnico en Electrónica.

2) Verificar el buen estado de los Periféricos, Mouse, Teclado y Monitor, en caso de fallas se remitirá al Técnico en Electrónica.

a) Mouse.

(1) Haga clic con todos los botones de su mouse y compruebe si se iluminan en la ilustración del mouse.

(2) Apunte el cursor de su mouse a la ilustración de mouse y gire la rueda central de su mouse hacia arriba y abajo.

(3) Compruebe si las flechas en la ilustración también se Iluminan.

(4) En caso de resultados negativos se recomienda al usuario que sea revisado por el Técnico en Electrónica.

b) Teclado.

(1) Normalmente cuando las teclas de un teclado no funcionan se debe a una falla mecánica. Los motivos pueden ser varios, pero entre los más comunes se encuentran las acumulaciones de suciedad, contacto con el agua (u otros líquidos) y golpes. Esto puede derivar en que determinadas teclas no funcionan como antes, teniendo que presionarlas más fuertes o varias veces seguidas, o en el peor de los casos que dejen de funcionar directamente.

(2) Revisión del normal funcionamiento de las teclas.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

(3) En caso de resultados negativos se recomienda al usuario que sea revisado por el Técnico en Electrónica.

c) Monitor.

(1) Cuando una computadora falla en mostrar su salida a un monitor conectado a ella, hay dos posibles causas: el monitor o su cable están fallando, el subsistema de visualización de video de la computadora está fallando. Ambos problemas pueden pasar al mismo tiempo. Desafortunadamente, los monitores típicamente no facilitan demostraciones de su información de estado en la computadora, así que un software no puede diagnosticar con certeza cuál es su condición.

(a) Apaga y luego desconecta el monitor que está conectado en este momento a la computadora.

(b) Conecta el mismo monitor a una computadora que sepas que funciona apropiadamente. La computadora de estar encendida. Si se obtiene una buena imagen en la pantalla, entonces tu computadora original tiene la falla en su subsistema de visualización de video.

(c) Conectar un monitor que se sepa que funciona bien a la computadora original. Enciende el monitor. Si se ve una buena imagen en la pantalla, entonces es el monitor original el que tiene la falla.

(d) En caso de resultados negativos se recomienda al usuario que sea revisado por el Técnico en Electrónica.

d) CPUs:

(1) Realizar procedimiento de limpieza del CPU de los equipos las partes internas las cuales constan de Memoria RAM, Microprocesador, Tarjetas grafica expandibles entre otras.

(2) Desmontaje, limpieza interna, aspirado, verificación de tarjetas, limpieza de drivers, limpieza externa.

(3) Limpieza y revisión de teclado.

(4) Limpieza y revisión de monitor.

3) Pruebas y diagnóstico.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

a) Al momento de encontrar una falla tales como (acumulación de polvo, corto circuito, fuente quemada entre otros) en cualquier dispositivo posteriormente se realizan pruebas tales como:

(1) En caso de una fuente de poder se hace la prueba con multímetro, también con un clic haciendo la unión del cable negro con el cable verde para saber si enciende la fuente de poder, de no ser así pasar al Técnico en Electrónica.

(2) En las memorias RAM, tendríamos que hacer las pruebas en una tarjeta madre diferente para descargar que sean los slot donde se colocan las memorias.

(3) En los microprocesadores, se hace la revisión del estado de la pasta térmica, para determinar que sea por eso la falla, y caliente demasiado el microprocesador.

(4) En caso de que sea la tarjeta madre, hacer la revisión de capacitores que no estén dañados o cualquier otro componente el cual este haciendo que la tarjeta madre falle.

(5) En caso de encontrar un daño o desperfecto que amerite remplazo o compra de piezas y/o accesorio en la ejecución del mantenimiento será necesario realizar un mantenimiento correctivo. Para esto el personal Técnico en electrónica levantará un reporte de diagnóstico que justifique la compra de las partes o accesorios dañados o en mal estado.

4) Configuración cuentas de usuarios agregados a directorio activo.

a) Verificar que el responsable del equipo haya creado en el Disco Local (C:) las carpetas con los archivos Institucionales y Personales.

b) Habilitar la cuenta predefinida Administrador del equipo y ponerle la contraseña que deben de tener todos los equipos institucionales.

c.- Habilitar y deshabilitar la cuenta predefinida Administrador.

1) Usar la consola MMC Usuarios y grupos locales

a) Ir al menú “Ejecutar” (una forma rápida de hacerlo es pulsando las teclas WINDOWS + R simultáneamente).

b) Escribir el comando lusrmgr.msc y pulsar INTRO.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

c) Seleccione en Usuarios y grupos locales la carpeta Usuarios (Doble Click).

d) Haga clic con el botón secundario en la cuenta Administrador y seleccione Propiedades. (Aparecerá la ventana Propiedades de administrador).

e) En la ficha General, active la casilla La cuenta está deshabilitada. (Con esto quedara habilitada la cuenta).

f) Vuelva a hacer clic con el botón secundario en la cuenta Administrador y seleccione establecer contraseña. (Dar click en continuar y luego asigne y confirme la contraseña para administrador local: Contraseña Administrador)

g) Cierre la consola MMC

2) Cambiar nombre de Equipo y Agregarlo al Dominio MDN.MIL

a) Todas las computadoras que tengan acceso a la red del Ministerio, deberán de ser agregadas al Directorio Activo.

b) Todas las computadoras del Ministerio que se incorporen a la red deberán de ser identificadas con su respectivo número de inventario (hostname).

c) Las computadoras propiedad del Ministerio que no posean número de inventario, cada oficina responsable de deberá de reservarle el respectivo número y realizar el tramite de cargo respectivo posteriormente.

d) Para cambiar el nombre de un equipo o unirse a un dominio, utilice la ficha Nombre de equipo del cuadro de diálogo Propiedades del sistema. Para buscar esta ficha, utilice uno de los métodos siguientes:

e) Haga clic con el botón secundario del mouse (ratón) en Mi PC y, a continuación, haga clic en Propiedades.

f) Haga clic en Inicio y en Ejecutar, escriba sysdm.cpl y haga clic en Aceptar.

g) Haga clic en Inicio y en Panel de control y, después, haga clic en Sistema.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

h) Ingresar al nuevo usuario de dominio con las credenciales correspondientes. (Los responsables de cada equipo ya tienen acceso a su cuenta en Cero Papeles, por lo tanto esas serán las mismas credenciales a utilizar.)

i) Una vez dentro del perfil del usuario de dominio, hacer el traslado de la documentación en la carpeta Mis documentos, es decir Mover la carpeta Institucionales hacia Mis documentos y verificar en la Barra de direcciones del Explorador de Windows que este apuntando hacia la siguiente dirección:

j) \\mdn-repo02\MDN\Usuarios\<UsuariodeDominio>\Mis documentos\Institucionales

3) Emitir opinión técnica para la adquisición y descargo de equipo informático.

a) Revisión de equipo informático.

b) Toma de características de la máquina incluyendo fecha de adquisición para tener un parámetro del tiempo de vida dado por el fabricante.

c) Prueba de diagnóstico para estado operacional del equipo.

d) Se completa Informe de Mantenimiento de Equipo de Computación para presentar al Jefe de cada Departamento o Unidad que lo solicite.

4) Soporte en instalación de software.

a) Se brindará apoyo a los usuarios en la instalación de software destinado al cumplimiento de las tareas asignadas, en ningún momento se podrá instalar software para la realización de tareas personales o de ocio.

b) En caso de software restringido por el uso de una licencia, el usuario deberá de presentar la respectiva licencia de autenticidad del software.

c) En el caso de software de uso libre, se deberá de solicitar una comprobación previa del funcionamiento de dicho software a fin de evitar que el mismo cause daños a la red o vulnere la seguridad de la información.

d) Se reportará al Técnico en Seguridad de Redes en nuevo software instalado a fin de que se autorizado su ejecución en el Directorio Activo.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

10.- TÉCNICO EN ELECTRÓNICA.

a.- Brindar soporte Técnico en diversas dependencias

1) Recibir Solicitud de soporte por parte de los usuarios para brindar servicio y atención de mantenimiento en los diferentes escalones a todo equipo relacionado con la parte electrónica fallas comunes y específicas de manera eficiente.

2) Informar a la secretaria de la oficina, el número de extensión y la dependencia en la que se saldrá a brindar soporte técnico.

3) En la dependencia que se brindará soporte se debe informar al más antiguo el motivo de la presencia en ese sitio.

4) Apersonarse al solicitante y en presencia del mismo hacer inspección al equipo

5) Verificar si el equipo cuenta con garantía, en caso de ser así el departamento al que pertenece dicho equipo se encarga de gestionar la garantía.

6) Realizar diagnóstico al equipo y emitir opinión técnica

7) Realizar reparación, y en caso de no solventar en el sitio la falla, informar al usuario y jefe inmediato que el equipo solo puede ser desarmado en el lugar por lo que será necesario trasladarlo al taller.

b.- Equipo trasladado al Taller de la Unidad de Informática por el Técnico.

1) Para efectos de orden y control deberá completarse el formulario respectivo. (Ver ANEXO “B” **INFORME DE MANTENIMIENTO DE EQUIPO DE COMPUTACIÓN**).

2) Se genera una orden de ingreso del equipo al taller.

3) Se procede a diagnosticar la falla del equipo.

4) Se determina si el equipo se puede reparar sin reemplazo de piezas, y en caso de ser necesario adquirir repuestos, estos se cotizan y se le da parte al usuario para que gestionen la compra.

5) Al obtener los repuestos se procede a reparar el equipo, y cuando este se encuentre listo se entrega al usuario junto con su respectiva hoja de

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

evaluación técnica, en la cual debe detallarse el procedimiento realizado, cambio y/o reparación de partes y el estado operacional.

6) En caso que no se autorice la compra de los repuestos necesarios, se arma el equipo y se le devuelve al usuario junto con su respectiva hoja de evaluación técnica y la cotización. Finalizando de esta manera el proceso.

c.- Equipo trasladado al Taller de la Unidad de Informática por el Usuario.

1) Para efectos de orden y control deberá completarse el formulario respectivo. (Ver ANEXO “B” **INFORME DE MANTENIMIENTO DE EQUIPO DE COMPUTACIÓN**)

2) Se genera una orden de ingreso del equipo al taller.

3) Se procede a diagnosticar la falla del equipo.

4) Verificar si el equipo posee garantía vigente, si es afirmativa la garantía del equipo se devuelve a la dependencia o Unidad Militar a la que pertenece para que realicen las coordinaciones pertinentes a fin de que esta se haga efectiva en la brevedad posible.

5) Si el equipo no cuenta con garantía, debe efectuarse evaluación y revisión técnica.

6) Se determina si el equipo se puede reparar sin reemplazo de piezas, y en caso de ser necesario adquirir repuestos, estos se cotizan y se le da parte al usuario para que gestionen la compra.

7) Al obtener los repuestos se procede a reparar el equipo, y cuando este se encuentre listo se entrega al usuario junto con su respectiva hoja de evaluación técnica, en la cual debe detallarse el procedimiento realizado, cambio y/o reparación de partes y el estado operacional

8) En caso que no se autorice la compra de los repuestos necesarios, se arma el equipo y se le devuelve al usuario junto su respectiva hoja de evaluación técnica y la cotización. Finalizando de esta manera el proceso.

d.- Avalar solicitudes de descargo de equipo.

1) El personal de las diversas dependencias solicita diagnóstico de equipo para avalar descargo del bien.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

2) Realizar el diagnóstico del equipo y emitir hoja de evaluación técnica, en la cual debe detallarse el estado operacional de dicho equipo.

3) Se entrega a la dependencia propietaria el equipo revisado junto con el informe de la evaluación técnica.

e.- Solicitud de habilitación de punto de red.

1) Se recibe la solicitud de las diversas dependencias o Unidades Militares para habilitación de punto de red.

2) Contar con las herramientas idóneas para realizar el procedimiento de canaleteo, crimpado y certificación de puntos.

3) Realizar mediciones exactas, cantidad de materiales y accesorios presentando presupuesto a la unidad o dependencia solicitante.

4) Constatar la numeración asignada al punto de red debiendo informar dependencia, ubicación y usuario al administrador de red a fin que asigne lo pertinente en dicho usuario.

5) Verificar junto al usuario el buen funcionamiento del punto de red habilitado.

11.- JEFATURA DE LA SECCIÓN DE TELECOMUNICACIONES.

a.- Proponer estudios para mejorar la estructura de redes físicas.

b.- Supervisar la estructura de redes a fin de mantener la conectividad en los sistemas.

c.- Recomendar la implementación de medidas de seguridad y políticas para los usuarios, a fin de evitar la vulnerabilidad de las redes.

12.- ADMINISTRADOR DE REDES.

a.- Recepción de equipo de comunicación nuevo.

1) Para el caso de la Adquisición un Equipo de Comunicación Nuevo, sean estos Conmutadores, Enrutadores, Cortafuegos, Servidores, Puntos de Acceso Inalámbricos y cualquier otro Equipo Periférico Administrable por Red, se dispone de hacer la recepción de dicho equipo verificando mediante

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

documentación que éste se encuentre en buen estado físico, y cumpla con los requerimientos antes solicitados.

2) Agregando al punto anterior, se debe supervisar la instalación física en la Sala de Servidores, la cual el proveedor debe realizar, dejando listo el equipo para su debida configuración o uso.

3) Luego de la inducción proporcionada por los proveedores, realizar las pruebas de funcionamiento de los equipos con las primeras configuraciones, hasta que quede en producción, la implementación.

b.- Administración de Infraestructura de Red.

1) Documentar licenciamientos del software legal adquirido.

2) Llevar control de credenciales para la administración y Direcciones IP asignadas a todos los equipos y servidores físicos y virtuales de red.

3) Definir todos los aspectos de topología e infraestructura física de la red en un esquema bajo nomenclatura estándar, para dimensionar el nivel de escalabilidad de la red.

4) Llevar el control de direcciones IP Estáticos para dispositivos terminales, como Impresores, Plotters, Consolas para cámaras de video vigilancia, entre otros.

5) Configurar en los equipos de conmutación las diferentes VLAN's a manera de separar segmentos de red a nivel lógico y llevar el listado de control de todas ellas.

6) Llevar el control de los puertos de los Switches, para la concordancia con los Puntos de red y poder gestionar la Seguridad de Puertos de manera eficiente.

7) Configurar rutas, NAT, VPN, entre otros, para lograr integrar redes externas de manera segura a servicios y políticas de nuestra red.

c.- Autenticación y Autorización de Servicios.

1) Crear nuevos usuarios según nomenclatura y estructura definida en el Directorio Activo.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

2) Coordinar con el Técnico de Mantenimiento de Hardware y Software para comprobar que el nuevo usuario una vez ingresado al dominio, adquiera las políticas y servicios correspondientes.

3) Proceder al desbloqueo de un usuario, por demanda del mismo, cuando este haya bloqueado su usuario por intentos fallidos de inicio de sesión, el cual obedece a una política de seguridad.

4) Reestablecer contraseña, en caso que por demanda del usuario haya olvidado dicha contraseña y sea necesario hacer el cambio desde el servidor para que, este pueda colocarle a su conveniencia una nueva contraseña a su usuario.

5) Configurar cualquier otra política que conceda o deniegue algún tipo permiso o servicio para los usuarios.

6) Llevar el control de dispositivos autorizados y agregados en los Puntos de Acceso de Red Inalámbrica, considerando ya sea el nivel de prioridad, la jerarquía y/o autorización escrita o verbal del jefe de la Unidad.

7) Se procederá a obtener la dirección física MAC del dispositivo que se desee agregar, ya que los puntos de acceso inalámbricos están previamente configurados para que todo aquel equipo que se añada a la red, establezca un nivel de autenticación por lista de filtrado MAC;

8) En cuanto esta MAC sea agregada, se coordina con el Técnico de Mantenimiento de Hardware y Software para que ingrese en el dispositivo las configuraciones correspondientes para la conectividad vía Wifi.

d.- Mantenimiento de la Infraestructura de Red.

1) Programar Mantenimiento Preventivo y Limpieza a los equipos ubicados en la Sala de Servidores.

2) Realizar la gestión con los proveedores en caso que un equipo presente una falla y sea necesaria la visita técnica o el cambio de alguna pieza, para el Reclamo por Garantía.

3) Hacer uso de las distintas herramientas de monitoreo en la red y acceso remoto al sitio de contingencia para detectar tráfico malicioso, problemas causados por la sobrecarga y/o fallas en los servidores, o cualquier otro problema

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

físico o lógico de la infraestructura de red (u otros dispositivos), estableciendo procesos y mecanismos de defensa y reacción ante fallas o ataques

13.- TÉCNICO EN REDES.

a.- Instalación de puntos de red.

1) Realizar el estudio de las necesidades de materiales.

2) Determinar el recorrido del cableado de la red.

3) Instalar el cableado de conformidad a las normas.

4) Realizar las pruebas de conectividad respectivas.

b.- Instalación, cambio y mantenimiento de los accesorios de red tales como switches y routers.

1) Detectar en que equipos se están ocasionando fallos de comunicación.

2) Determinar la necesidad de limpieza, sustitución o cambio del equipo que está presentando fallos.

3) Coordinar con los técnicos en mantenimiento de hardware y software y con el técnico en electrónica según sea la falla del equipo.

4) Instalar nuevo equipo y coordinar con el administrador de la red, para su correcta configuración.

5) Realizar las pruebas de comunicaciones respectivas.

c.- Verificación de la conectividad de la red informática.

1) Realizar revisión constante del funcionamiento de la conectividad en la red.

2) Detección y corrección de problemas físicos de conectividad de las redes locales.

3) Revisar los enlaces de conexiones externas, mediante prueba de conectividad.

14.- TÉCNICO EN SEGURIDAD DE REDES.

a.- Analizar los sistemas existentes para determinar sus vulnerabilidades y limitar las amenazas existentes.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

1) Buscar en bases de datos preexistentes reportes de vulnerabilidades a tecnologías de elaboración de sistemas informáticos.

2) Someter los sistemas al escaneo de herramientas de software libre para detección de vulnerabilidades.

b.- Definir e implementar medidas de ciberseguridad que eviten las vulnerabilidades.

1) Medidas de seguridad perimetral.

a) Configuración de reglas de firewall a nivel de contenido web y aplicaciones.

b) Configuración de reglas de antivirus centralizados.

c) Configuración de reglas de conexión de redes externas.

2) Medidas de seguridad de infraestructura de servidores.

a) Actualizaciones de seguridad de software.

b) Políticas de acceso físico al centro de datos.

3) Medidas de seguridad de equipos de usuarios finales

a) Restricción en instalación y ejecución de software.

b) Restricción en conexión de dispositivos de almacenamiento externo.

c) Control de actualizaciones de seguridad de software.

d) Monitoreo del comportamiento del tráfico de los equipos en la red interna.

e) Escaneo del tráfico de la red.

f) Análisis del tráfico de la red.

c.- Sensibilizar y capacitar a los usuarios sobre vulnerabilidades existentes.

1) Investigar surgimiento de nuevas vulnerabilidades.

2) Preparar material para capacitación.

3) Elaborar plan y programación de sensibilización y capacitación de usuarios.

4) Elaborar calendario de capacitaciones.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

5) Realizar la capacitación.

6) Llevar control de personal sensibilizado.

d.- Analizar el funcionamiento, la efectividad y el cumplimiento de las políticas de ciberseguridad, asi como proponer correcciones y reportar violaciones a su cumplimiento.

1) Monitoreo del comportamiento del tráfico de los equipos en la red interna.

2) Escaneo del tráfico de la red.

3) Análisis del tráfico de la red.

4) Investigación de equipos con tráfico sospechoso.

5) Preparación de informe de hallazgos y recomendación de medidas correctivas.

e.- Analizar el nuevo hardware y software a instalarse para determinar su fortaleza o vulnerabilidad antes de ser instalado.

1) Análisis de nuevo hardware.

a) Búsquedas en bases de datos de reportes de hardware vulnerable.

b) Actualización de drivers del software instalado.

2) Análisis de software.

a) Control de software libre, parches, etc., a ser instalado.

b) Aplicación de técnicas de ingeniería inversa, a fin de determinar los procesos que ejecuta el software desconocido.

f.- Mantener coordinación permanente con el administrador de redes con el objetivo de reducir vulnerabilidades.

1) Alertar al administrador de redes sobre el surgimiento de nuevas vulnerabilidades en los sistemas de redes.

2) Proponer buenas prácticas de aseguramiento de la red y los sistemas.

15.- DISPOSICIONES GENERALES.

a.- Toda adición o eliminación de procedimientos en cada uno de los cargos se informará en su debida oportunidad.

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

b.- Todo cambio en el Manual de Puestos de la Unidad de Informática, ocasionará modificaciones al PON.

c.- Cualquier recomendación al presente PON debe ser dirigida a la Jefatura de la Unidad.

JOSÉ NAPOLEÓN MORÁN HERNÁNDEZ
CNEL. Y LIC.
JEFE DE LA UNIDAD DE INFORMÁTICA

ANEXO "A" **ORGANIGRAMA DE LA UNIDAD DE INFORMATICA.**
"B" **INFORME DE MANTENIMIENTO DE EQUIPO DE COMPUTACIÓN.**

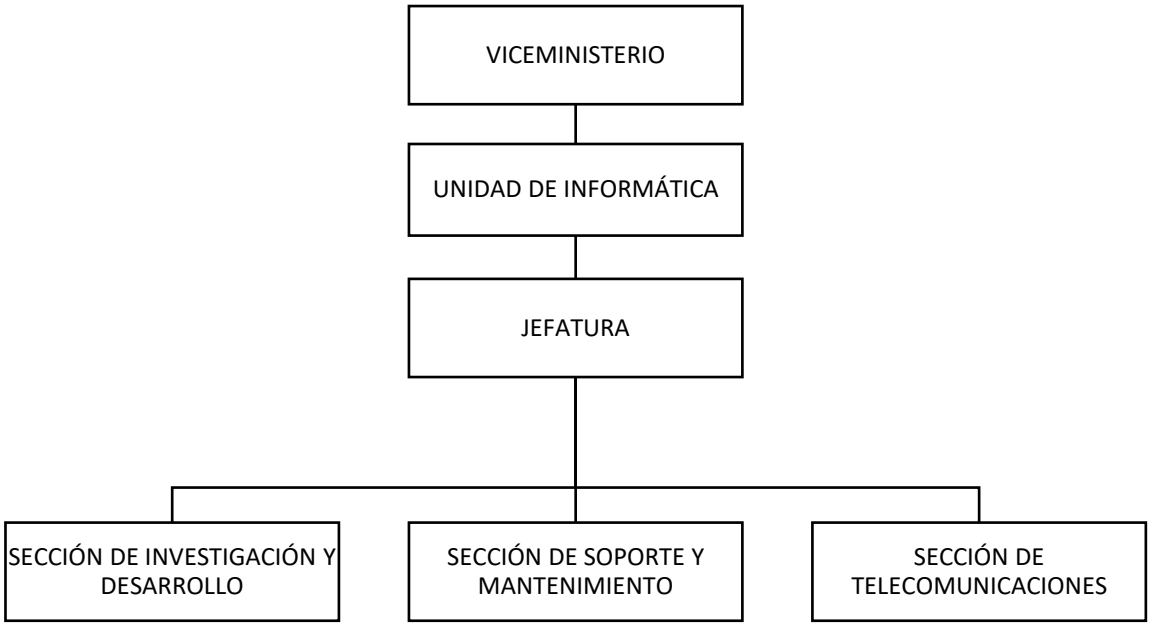
DISTRIBUCIÓN	**N° DE COPIA**
DIRECCIÓN DE ADMINISTRACION	1
UNIDAD DE INFORMÁTICA	2
SECCION DE INVESTIGACION Y DESARROLLO	3
SECCION DE SOPORTE Y MANTENIMIENTO	4
SECCION DE TELECOMUNICACIONES	5
ARCHIVO	6
TOTAL	**6**

AUTENTICADO

MAYE
JEFE SECCIÓN

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

ANEXO “A” **ORGANIGRAMA DE LA UNIDAD DE INFORMATICA**



AUTENTICADO

MAYE
JEFE SECCIÓN

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.

ANEXO "B" **INFORME DE MANTENIMIENTO DE EQUIPO DE COMPUTACIÓN**

MINISTERIO DE LA DEFENSA NACIONAL
Unidad de Informática
República de El Salvador, C.A.

INFORME DE MANTENIMIENTO DE EQUIPO DE COMPUTACION REALIZADO EN LAS DIFERENTES DIRECCIONES Y DEPENDENCIAS DE ESTA CARTERA DE ESTADO

San Salvador, ____ de _____ de 2018.

DIRECCION O UNIDAD : _____

DEPARTAMENTO SECCION: _____

EQUIPO :
PARTICULAR ☐ **INSTITUCIONAL** ☐

EQUIPO :

- CPU ☐
- MONITOR ☐
- TECLADO ☐
- IMPRESOR ☐
- UPS ☐
- LAPTOP/PORTATIL ☐
- MOUSE ☐
- OTRO: _____

DATOS DEL EQUIPO:

N° INVENTARIO _____ MARCA _____
MODELO _____ SERIE _____

ASIGNADO A: _____

TRABAJO TÉCNICO REALIZADO:

_____
_____
_____
_____
_____
_____
_____
_____

_____ _____
NOMBRE DEL TECNICO
UNIDAD DE INFORMATICA
EXT. 8105

USUARIO DE EQUIPO

AUTENTICADO

MAYE
JEFE SECCIÓN

NOTA CONFIDENCIAL: La información contenida en este documento o correo-electrónico originado en la FUERZA ARMADA DE EL SALVADOR, C.A. contiene información confidencial y sólo puede ser utilizada por la persona, entidad o compañía a la cual está dirigido. Si no es el destinatario autorizado, cualquier retención, difusión, distribución o copia total o parcial de este documento o su información es prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenviarlo o entréguelo a su remitente y borrarlo inmediatamente.