INSTITUTO DE PREVISIÓN SOCIAL DE LA FUERZA ARMADA

MANUAL DE ORGANIZACIÓN Y FUNCIONAMIENTO DEL DEPARTAMENTO DE INFORMÁTICA

GERENCIA ADMINISTRATIVA

UNIDAD DE DESARROLLO ORGANIZACIONAL

2018

Contenido

Objetivo

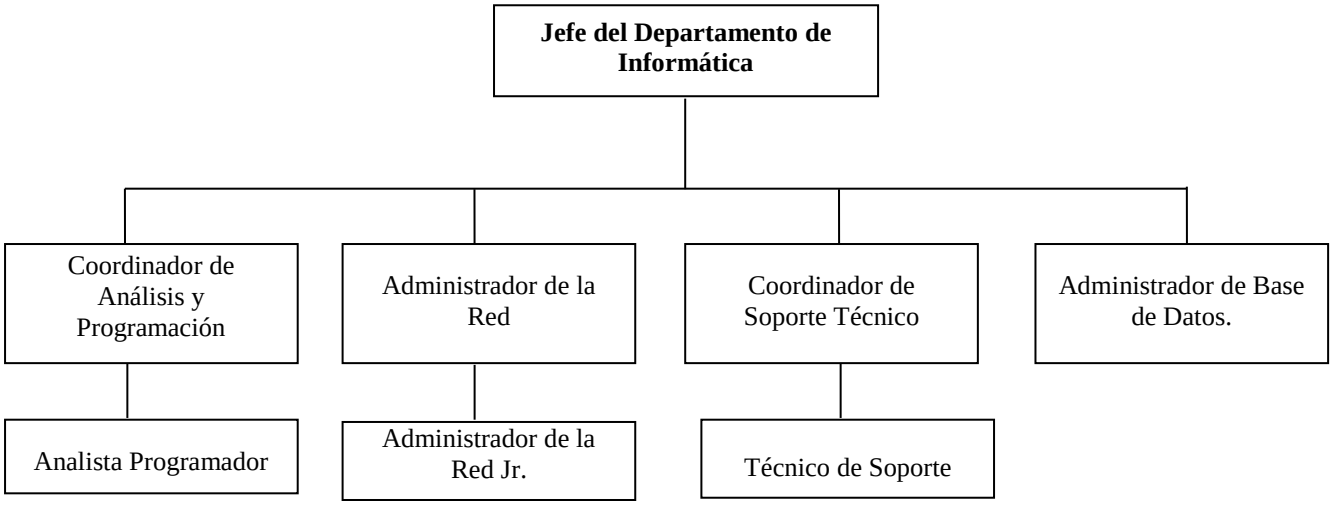
Documentar la estructura organizativa y funcional del Departamento de Informática, como guía de orientación interna y externa, que permita conocer la operatividad, regulaciones y procedimientos necesarios, para el cumplimiento de los objetivos del Departamento en coherencia con los institucionales.

I. GENERALIDADES

A. Identificación de la Oficina

Nombre de la Oficina:	Departamento de Informática
Código de Oficina:	111270
Depende Organizativa:	Gerencia Administrativa

B. Estructura Organizativa



C. Objetivos de la Oficina

1. General

Ser los responsables ante el IPSFA del diseño de los nuevos sistemas de información y mantenimiento óptimo de los actuales como también de la plataforma tecnológica informática Institucional.

2. Específicos

2.1 Brindar servicios informáticos a nuestros clientes internos (usuarios-IPSFA) y externos promoviendo así una cultura informática a nivel Institucional.

2.2 Velar por el seguimiento de las políticas establecidas por y para el Departamento de Informática.

2.3 Dar cumplimiento a lo establecido en el Plan Operativo Anual, Plan Estratégico y a las prioridades informáticas Institucionales.

2.4 Desarrollar nuevas soluciones informáticas acorde a las necesidades de las diferentes áreas del IPSFA y sus Unidades de Negocio.

D. Funciones del Departamento

1. Generales

1.1 Desarrollar aplicaciones informáticas acorde a las necesidades de las diferentes áreas del IPSFA y sus Unidades de Negocio.

1.2 Proporcionar mantenimiento a las diferentes aplicaciones informáticas de todas las áreas del IPSFA y sus Unidades de Negocio.

1.3 Proporcionar el mantenimiento preventivo al equipo de cómputo del IPSFA y sus Unidades de Negocio.

1.4 Planear y ejecutar el plan de mantenimiento preventivo y correctivo de los servidores y el resto de dispositivos de la red informática Institucional.

1.5 Ejecutar y controlar la realización de los respaldos de la información procesada por las diferentes áreas del Instituto.

1.6 Analizar y determinar los requerimientos informáticos a nivel Institucional tanto de hardware como de software.

1.7 Dar soporte técnico a las áreas usuarias sobre la utilización de las diferentes aplicaciones en función, sistemas operativos, utilitarios y así como también en el uso de los diferentes periféricos que están inmersos en la funcionalidad de los equipos informáticos.

2. Específicas de la red institucional

2.1 Mantener en buenas condiciones las comunicaciones de la red institucional, unidades descentralizadas y de negocio.

2.2 Velar por mantener la alta disponibilidad en los Data Center Institucional.

2.3 Velar por la seguridad de la red y los Data Center Institucional.

3. Específicas de base de datos Oracle

3.1 Se generan dos respaldos completos y diarios realizados a la base de datos Oracle de producción mediante utilitarios nativos del sistema operativo y utilitario de Oracle como lo es el utilitario Export y Rman.

3.2 Se mantienen en el disco duro del servidor de base de datos de producción 2 meses de respaldos diarios completos generados por el utilitario Export (.dmp) dado que la demanda de restauraciones generalmente es en ese período. Luego de dos meses se van eliminando del disco y ante una petición de recuperación se suben del tape o RDX numerado con dicha fecha, adicionalmente los archivos generados desde el utilitario Rman se mantienen 1 día en el servidor.

3.3 Estos están en unidades de disco duro RDX o tape

3.4 Transmisión del .dmp's al sitio de contingencia.

3.5 Dar apoyo a los analistas programadores en el tuning del código pl/sql.

3.6 Monitoreo a la base de datos.

4. Específicas de soporte técnico

Los respaldos de información se realizan bajo dos ambientes: File Server y productos Oracle.

4.1 Se refieren a respaldos de las carpetas institucionales compartidas y propias de cada área de la red Institucional.

4.2 Se realizan diariamente en discos locales del servidor y en dura RDX bajo el formato utilizado por los utilitarios de los sistemas operativos Windows y Linux.

4.3 Los tipos de respaldos de información que se realizan son:

a. Respaldos incrementales, se actualizan únicamente los cambios que la data ha experimentado durante el día, se realizan a diario al final de la jornada laboral cuando no hay usuarios en el sistema.

b. Respaldos completos, la información respaldada contenida en ellos, es el 100% de la data, éstos se realizan de forma trimestral.

c. Respaldos y restauración a demanda, estos respaldos se realizan sólo a solicitud de un usuario.

4.4 Control de tape y RDX en el sistema y control de backup.

4.5 El resguardo y traslado de los respaldos en tapes y RDX es exclusiva función del Área de Soporte Técnico.

4.6 Control y envío de tapes y RDX al sitio de contingencia.

E. Legislación Relacionada y Documentos

1. Ley del IPSFA.
2. Reglamento de la Ley IPSFA.
3. Ley de Corte de Cuentas de la República.
4. Reglamento para el Uso y Control de las Tecnologías de Información y Comunicación en las Entidades del Sector Público.
5. Normas Técnicas de Control Interno Específicas del IPSFA (NTCIE-IPSFA).
   a. Capítulo III Normas Relativas a las Actividades de Control: Definición de Políticas y Procedimientos de los Controles Gerenciales de los Sistemas de Información (Arts. 110 y 111); Definición de Políticas y Procedimientos de los Controles de Aplicación (Art. 112).
   b. Capítulo IV Normas Relativas a la Información y Comunicación: Adecuación de los sistemas de información y comunicación (Art. 113); Proceso de Identificación, registro y recuperación de la información (Art. 114); y Características de la Información (Art. 115).

II. MARCO REGULATORIO

A. Políticas

1. Generales

1.1 Promover y mantener una cultura informática estableciendo mecanismos de comunicación interna y externa a nivel Institucional.

1.2 Desarrollar e implementar herramientas informáticas, dotando a la Institución de una estructura y soporte tecnológico de calidad.

1.3 Solventar las necesidades de actualización tecnológica, tanto en hardware como en software

1.4 Proveer calidad en la atención a los usuarios, mediante una adecuada solución a sus requerimientos; manteniendo así una constante certificación, capacitación y actualización de conocimientos para los miembros del Departamento de Informática.

1.5 Crear, reestructurar y brindar mantenimiento a las bases de datos necesarias para optimizar los procesos.

2. Específicas de seguridad física

2.1 El Departamento de Informática, será la única responsable de realizar movimientos y traslados de cualquier equipo computacional en las instalaciones de la Torre El Salvador, relacionadas con el IPSFA, Unidades descentralizadas y dependencias externas mediante el formulario respectivo.

2.2 El Departamento de Informática es delimitada como área restringida, por lo que el acceso de personal ajeno al Departamento, deberá ser canalizado a través de la Jefatura de Informática o Coordinación de Área.

2.3 En caso de cancelación o traslado del personal en forma temporal o definitiva, y que hiciese uso del sistema computacional, deberá ser reportado en forma escrita e inmediatamente al Departamento de Informática por las áreas respectivas.

2.4 El área reservada para la granja de servidores es catalogada como área restringida de máxima seguridad, por lo que el acceso de personal ajeno al Departamento, deberá canalizarse a través de la jefatura de Informática y deberá ser acompañado por el Administrador de la Red y llenar el formato de control de entradas y salidas.

2.5 El área de granja de Servidores tiene clima artificial para mantener la temperatura adecuada a estos equipos. Este Aire acondicionado se opera de forma separada de los equipos centrales del IPSFA.

2.6 La alimentación eléctrica de todos los equipos del IPSFA, incluyendo Granja de Servidores y Sistema es alimentada por medio de una estructura eléctrica separada del resto del edificio y alimentada en caso de falla en el suministro de energía por un esquema de UPS redundante (doble UPS, si uno falla entra el otro en operación) mientras la planta eléctrica entra en funcionamiento.

3. Específicas de seguridad lógica

3.1 El acceso a los recursos de informática (a nivel del sistema) se limitará a las personas con la debida autorización a los niveles correspondientes.

3.2 El Administrador de Red, mantendrá un control por escrito de las definiciones de usuario y privilegios, que contenga: Nombre de la persona que autoriza, cargo, fechas y tiempo que tuvo la responsabilidad.

3.3 Las claves de acceso serán creadas por el propio usuario en forma individual, personal y exclusiva, y no de manera generalizada para la utilización de varios usuarios.

3.4 Si un usuario olvida su clave secreta (password) éste deberá solicitar nueva clave al administrador de red, ya que el administrador no podrá en ningún momento ver la clave en el archivo de seguridad, porque contraviene la disposición anterior.

3.5 Los niveles de acceso al sistema serán asignadas de acuerdo a las funciones y necesidades de información del usuario.

3.6 El uso de las claves de acceso al sistema computacional es de responsabilidad exclusiva del usuario. Los accesos a las unidades lógicas institucionales, serán asignados por el administrador de la red de acuerdo a la estructura del organigrama institucional.

3.7 Los respaldos de información (Back-up), estarán resguardados de forma que estén libres de cualquier riesgo y almacenados de forma que sea fácil de localizar.

3.8 Se establece que los respaldos de información (Back-up) se estarán haciendo diariamente el respaldo incremental y trimestralmente un respaldo definitivo.

3.9 Se establece que los respaldo de información a la base de datos se estarán realizando diariamente (estos son respaldos definitivos o totales).

3.10 El Departamento de Informática deberá, evaluar y clasificar la información para backup tomando en consideración los términos de riesgo siguientes:

a. Archivos de Datos y programas que contienen información difícil de recuperar.
b. Información que tenga un alto costo financiero en caso de pérdida o pueda provocar un gran impacto en la toma de decisiones.
c. Información cuya pérdida pueda provocar la posibilidad de que no pueda sobrevivir sin esa información.

4. Específicas de acceso en los aplicativos

4.1 Sistema de base de datos Oracle: Acceso al sistema operativo del servidor

4.1.1 Se ingresa al sistema operativo en base a un usuario registrado y a una contraseña que se definen al momento de la creación de los usuarios y su ambiente de trabajo (tales como directorios de inicio de sesión, scripts de inicio, y otras variables de entorno), siendo de uso exclusivo del Administrador de red, de base de datos y Jefe de la Departamento de Informática.

4.1.2 Se creará el usuario para la instalación y mantenimiento de la base de datos, no para su utilización como tal, es decir, se crea el usuario Oracle con todos los privilegios sobre el software de base de datos y para la creación de respaldos.

4.1.3 El usuario Oracle es utilizado únicamente por el Administrador de Base de Datos y Jefe del Departamento de Informática y el usuario Root por el Administrador de Red y Jefe del Departamento de Informática.

4.2 Sistema de base de datos Oracle: Acceso a la base de datos Oracle

4.2.1 La base de datos Oracle debe permitir la creación y mantenimiento de seguridad propia y completamente independiente del sistema operativo además de mostrar portabilidad. La seguridad está basada en usuarios, roles y perfiles:

a. **Usuarios:** Son creados por el Administrador de Base de datos por requerimiento de las Jefaturas de las áreas usuarias. Existe un usuario

único asignado a un empleado, es decir, nadie comparte un usuario aunque tenga funciones afines.

b. **Roles:** Son accesos específicos que se permiten a los objetos de la base de datos, por ejemplo: accesos de sólo lectura a ciertas tablas, privilegios de inserción, de actualización, de borrado, etc. Los roles se asignan a usuarios. Múltiples usuarios pueden compartir roles.

c. **Perfiles:** Son características en el modo de conexión a la base de datos, esto es, que van desde el tiempo ocioso que un usuario puede estar a los sistemas, la forma como expiran los passwords, etc. Se crean perfiles acorde a los tipos de usuarios.

4.2.2 Es función del Administrador de la base de datos el configurar dicha seguridad de acuerdo con la funcionabilidad de los sistemas.

4.2.3 El acceso a los aplicativos será basado en asignación de roles solicitados por los responsables de cada módulo.

4.3 Acceso a los programas fuentes y ejecutables

4.3.1 Los programas tanto ejecutables como fuentes se encuentran almacenados en un servidor distinto al de base de datos.

4.3.2 El acceso a las carpetas que contienen los programas fuentes y ejecutables, se configuran en base a la seguridad propia del Dominio implementado bajo Windows, es decir, en base a usuarios, y privilegios de lectura, escritura y ejecución establecidos a través de la seguridad proveída por el sistema operativo de red.

4.3.3 La administración de las programas fuentes lo realiza el encargado de la administración del NEO-IPSFA, cada analista tiene acceso a una copia de los programas fuentes, para disminuir los tiempos de respuesta ante requerimientos.

5. Mantenimiento de software y hardware

5.1 El software al que se le provee mantenimiento se puede dividir en:

a. **Software Aplicativo:** Consiste en el software desarrollado en el Departamento de Informática o adquirido externamente mediante el cual se da soporte informático a las diferentes áreas usuarias del Instituto.

b. **Sistemas Operativos:** Se refiere a los diferentes sistemas operativos utilizados en: Computadoras Personales, Servidores y equipos de comunicación.

c. **Software de Base de Datos y Desarrollo de Aplicaciones:** El software de base de datos utilizado es Oracle y para el desarrollo de las aplicaciones es Oracle Developer Suite manteniendo un estándar para la totalidad de desarrollos de aplicaciones.

d. **Software Aplicativo:** El área de análisis y el Departamento de Informática del IPSFA da apoyo técnico a las diferentes áreas del Instituto:

5.2 Creando nuevos aplicativos

5.3 Proporcionando mantenimiento a los ya existentes.

5.4 Automatizando procesos administrativos y financieros para las diferentes áreas del Instituto.

5.5 Los requerimientos deberán ser solicitados por medio de correo electrónico ó en un formato especialmente diseñado para ello, el cual contiene todo el detalle del trabajo a realizar.

6. Mantenimiento y control en los cambios de software de los sistemas de información del NEO IPSFA.

6.1 Todo requerimiento y modificación a los diferentes aplicativos deberá ser solicitado a la Unidad e Informática a través del responsable del mismo, apoyándose del formulario Solicitud y Análisis de Requerimientos. (FORM-08-GG-INF-01) o por medio de correo electrónico dirigido a helpdesk@ipsfa.com, ningún usuario podrá solicitar modificaciones a los aplicativos si no es por medio del responsable del mismo.

6.2 Todo requerimiento de acceso a los diferentes aplicativos deberá ser solicitado a la Unidad e Informática a través del responsable del mismo, apoyándose del formulario Solicitud y Análisis de Requerimientos. (FORM-08-GG-INF-01) o por medio de correo electrónico dirigido a helpdesk@ipsfa.com, ningún usuario podrá solicitar accesos a los aplicativos si no es por medio del responsable del mismo.

6.3 Para reducir la necesidad de mantenimiento:

a. Para mayor precisión los requerimientos deberán ser solicitados a través del formato específico.

b. Hacer buen uso de las herramientas y técnicas existentes (principios de diseño de software: modularidad, acoplamiento, cohesión, control, tamaño, uso compartido).

6.4 Actualmente clasificamos los tipos de mantenimiento al Software que utilizamos así :

a. **Mantenimiento correctivo.** Involucra el diagnóstico y corrección de uno o más errores. Ocurren errores en el sistema que el usuario reporta al desarrollador.

b. **Mantenimiento Adaptivo.** Modifica el sistema para adaptarlo a los cambios del medio ambiente. Esto se debe a los cambios rápidos que ocurren en cualquier aspecto computacional. Por ejemplo, nuevas versiones del software de desarrollo, de sistemas operativos, de equipo periférico, etc. El mantenimiento de los sistemas también implica adaptaciones de versiones anteriores, adecuar cambios de reportes, archivos y procesos.

c. **Mantenimiento Perfectivo.** Conforme el sistema es usado, nuevas recomendaciones para satisfacer nuevos requerimientos, modificaciones a las funciones existentes, y mejoras en general son recibidas por parte de los usuarios. La mayor parte del tiempo de mantenimiento se convierte en perfectivo conforme pasa la vida del sistema. Este tipo de mantenimiento trata de cumplir las nuevas peticiones de los usuarios, mejorar la documentación o decodificar para mejorar la eficiencia (tiempo de respuesta).

d. **Mantenimiento Preventivo**. Ocurre cuando hay cambios en el software para mejorar la facilidad de mantenimiento del sistema o proveer mejores bases para un mejor desempeño. Este tipo de mantenimiento usualmente es sugerido por la misma área de desarrollo.

6.5 Mantenimiento de hardware

6.5.1 El Hardware Informático utilizado al cual se le provee de mantenimiento se puede dividir en:

a. **Computadoras Personales y Laptops.** Consiste en el lote de PC's y computadoras portátiles que se encuentran en uso en el Instituto, sus oficinas de negocio y sucursales, generalmente constan de cpu, pantalla, teclado, Mouse, disqueteras, etc.

b. **Servidores.** Los servidores se encuentran alojados físicamente dentro del Departamento de Informática dentro de una misma área conocida como granja de servidores. Entre los servidores más importantes tenemos en base de su función principal: de correo, Internet, base de datos, carpetas institucionales compartidas, de comunicaciones, servidor de aplicaciones, etc., este mantenimiento es proporcionado por los proveedores.

c. **Accesorios y periféricos.** Se refiere a escáneres de imagen, quemadores de cd/dvd externos, memorias flash, parlantes, etc.

d. **Equipo de respaldo y recuperación.** En la granja de servidores se cuenta con un equipo especializado en respaldos y recuperación mediante el cual se puede respaldar tanto la base de datos Oracle como información almacenada dentro de la red institucional.

e. **Equipo de Impresión.** Impresores láser, como de inyección de tinta y de matriz de puntos.

f. **Equipo de comunicación de red.** Consiste en los enrutadores, switch´s tanto de cobre como de fibra óptica así como el backbone de fibra óptica que enlaza los niveles del edificio terminando en la granja de servidores.

g. **Equipo de UPS.** Se cuenta con dos equipos de UPS los cuales proveen servicio a la totalidad de equipo informático del Instituto ubicado en oficinas centrales. El servicio es de tipo redundante, es decir, que un equipo es el principal y el otro actúa como secundario o de respaldo.

6.5.2 Mantenimiento externo (contratos)

6.5.2.1 Para los equipos de impresión de alto volumen, comunicación de red, servidores, equipos de respaldo, recuperación y UPS's, anualmente se realiza una o varias licitaciones públicas o por invitación a través de la DACI para

contratar los servicios de Mantenimiento tanto preventivo como correctivo a dichos equipos. La razón para ello es debido a la importancia radical que dichos equipos trabajen ininterrumpidamente 7/24 y 365 días del año.

6.5.2.2 Los términos generales que se incluyen en dichos procesos de licitación son los siguientes:

a. Satisfactorios tiempos de respuesta ante fallas
b. Que se incluyan partes de repuestos
c. Contratos anuales
d. Que se incluya mano de obra de personal humano
e. Mantenimientos tanto preventivos como correctivos
f. Visitas periódicas del personal

6.5.3 Mantenimiento interno

6.5.3.1 Para los equipos de computadoras personales, accesorios y periféricos será el personal de Soporte técnico del Departamento de Informática el responsable de realizar dos mantenimientos preventivos anuales (de forma semestral), el mantenimiento correctivo se realizará a solicitud del usuario. Aquellos equipos que se encuentren dentro del período de garantía, esta solamente aplica para hardware.

6.5.3.2 Como política general será el Departamento de Informática quién realizará dichos mantenimientos al equipo informático del Instituto.

7. Específicas para el uso de software de mensajería

7.1 El jefe de cada área organizativa del Instituto, será responsable del uso adecuado del software de mensajería, por parte del personal que se encuentre bajo su responsabilidad y velará porque dicha herramienta sea utilizada en beneficio de su trabajo.

7.2 Quedará al juicio del jefe de cada área organizativa del Instituto la suspensión del acceso a Internet.

7.3 Todo requerimiento de acceso a Internet deberá ser gestionado por el jefe de cada área organizativa del Instituto a través del formulario respectivo.

7.4 El Administrador de Red, deberá monitorear el ancho de banda de los servicios de Internet contratados para el mejor desempeño de este servicio.

8. Específicas para el uso de la red institucional

8.1 Los servicios disponibles son:

a. Correo electrónico
b. Acceso a red institucional
c. Acceso a los aplicativos Institucionales
d. Acceso a Internet
e. Acceso a los directorios de red Institucional

8.2 Las Gerencias y Jefaturas solicitarán por escrito al Departamento de Informática acceso para sus colaboradores a los servicios disponibles, con la respectiva justificación en el formulario para tal solicitud.

8.3 Los servicios son un privilegio, no un derecho, los mismos implican responsabilidad. Cualquier violación a las políticas establecidas puede resultar en la pérdida de los servicios y tomar acciones disciplinarias adicionales, las cuales podrán determinarse a nivel administrativo siguiendo los procedimientos existentes.

8.4 Cada usuario será responsable de las acciones efectuadas a través de los diferentes servicios que se le autoricen.

8.5 Los servicios ya otorgados y/o solicitados pueden ser negados al usuario que sea identificado como un riesgo de seguridad o tenga un historial problemático con otros accesos y/o sistemas computacionales a nivel Institucional.

8.6 El Departamento de Informática tiene la responsabilidad de controlar y recomendar suspender el servicio a cualquier usuario que viole las políticas o interfiera con los derechos de otros usuarios.

8.7 El Departamento de Informática tiene la responsabilidad de notificar a aquellas personas que se vean afectadas por las decisiones tomadas.

8.8 El estándar establecido para la creación de usuarios de red Institucional y para acceso a los aplicativos del IPSFA (Contabilidad, Compras, etc) es: primera letra del nombre más apellido, ejemplo: José Eduardo López Martínez sería jlopez.

8.9 De existir un usuario previo con el mismo acceso, se utilizará la primera letra del segundo nombre o el segundo apellido en lugar del primero, según sea el caso, ejemplos:

a. José Eduardo López Martínez podría ser elopez;
b. José Eduardo López Martínez podría ser jmartinez;
c. José Eduardo López Martínez podría ser emartinez; etc.

9. Específicas para niveles de seguridad y acceso en la red institucional.

9.1 El usuario puede cambiar su contraseña, de no cambiarla el servidor le avisa que debe hacerlo, sin intervención del administrador de red.

9.2 El acceso a la red es restringido, los usuarios solamente pueden hacer uso de las aplicaciones instaladas en el servidor y herramientas instaladas en su PC.

9.3 Los usuarios no están autorizados para instalar software en sus equipos asignados.

9.4 Para intercambiar información con otras Unidades tienen dos alternativas:

a. Una carpeta Institucional (común a todas las áreas)
b. Enviar la información adjunta en el correo electrónico interno el IPSFA como máximo debe contener 10MB.

9.5 Las políticas de seguridad de la red, son administradas desde el servidor controlador del dominio, el cual tiene diferentes tipos de usuarios que por medio de él acceden a la red, los cuales son:

a. **Administrador:** Este usuario tiene todos los derechos para la administración de los servidores y monitoreo de usuarios de red.
b. **Usuario de Operador Informático:** Tiene la capacidad de realizar algunas configuraciones a los equipos instalados en la red, respaldo de los servidores.
c. **Usuario de Red:** estos usuarios tienen derecho de acceder a la red pero no puede realizar cambios en los equipos, se han tomado medidas de seguridad las cuales se pueden nombrar las siguientes:

i. El usuario puede cambiar su contraseña, de no cambiarla el servidor le avisa que debe hacerlo, en un periodo basado en los estándares de un controlador de dominio sin intervención del administrador de red y de esta forma es personalizado.

ii. El acceso a la red es restringido, los usuarios solamente pueden hacer uso de las aplicaciones instaladas en el servidor y herramientas instaladas en su PC.

iii. El usuario no puede cambiar el entorno de su PC.

iv. No puede instalar programas sin previa autorización.

v. El usuario no puede tener acceso al panel de control de sus equipos.

vi. No puede ejecutar y cambiar la configuración de la red.

vii. No tiene acceso al registro del sistema.

viii. No puede editar desde la consola de Comandos.

ix. Todos los equipos (pc´s y laptop´s) deben tener instalado un antivirus corporativo, que es administrado desde un servidor.

9.6 Las medidas de seguridad que se han tomado, son para que el usuario no cambie el ambiente de su PC ocasionando fallas o que instale programas no autorizados y que no sean requeridos para el desarrollo de sus labores.

9.7 Dentro de la Red cada Unidad o Departamento tiene acceso a una carpeta compartida; solamente colaboradores del Departamento tiene acceso a ella; con el objetivo de intercambiarse información.

10. Específicas para la asignación de cuentas de correo electrónico

10.1 Proteger su cuenta de usuario asignada: guardar el secreto de su password, no prestar su clave de usuario bajo ninguna circunstancia.

10.2 Responsabilizarse de cualquier actividad que se realice con su password.

10.3 Hacer los respaldos correspondientes a su información particular en su disco duro y/o cualquier medio magnético, así como borrar periódicamente sus correos y archivos.

10.4 En cuanto a los password, el Departamento de Informática, dependiendo de alguna amenaza, podrá forzar a cambiar su password a todos los usuarios, usar programas para fijar password no reusables y encriptación de password, etc.

10.5 Los usuarios internos y externos estarán obligados a cumplir con las normas y políticas dadas por el Departamento de Informática.

11. Específicas para usuarios internos de correo electrónico

11.1 Todo empleado del IPSFA con un equipo asignado para su uso y que sea autorizado por su jefe inmediato superior tendrá acceso a una cuenta y correo

electrónico en el servidor designado para tales efectos en el Departamento de Informática mientras sea empleado del Instituto.

11.2 Es responsabilidad del usuario hacer buen uso de su cuenta de correo electrónico, entendiendo por buen uso:

a. El no enviar ni contestar cadenas de correo electrónico.
b. El uso de su cuenta de correo electrónico con fines de trabajo
c. La depuración de su bandeja de entrada de correos (INBOX) del servidor (no dejar correos por largos períodos).
d. El no hacer uso de la cuenta para fines comerciales.
e. El respetar las cuentas de correo electrónico de otros usuarios Internos y Externos.
f. El uso de un lenguaje apropiado en sus comunicaciones.

11.3 El estándar establecido para la creación de cuentas de correo electrónico es: nombre.apellido@ipsfa.com

11.4 Se asignará solamente una cuenta por usuario con su correo electrónico bajo el estándar establecido.

11.5 La creación de otras cuentas de correo electrónico se dará a consideración de la Unidad o Departamento solicitante.

11.6 La cuenta de correo es personal e intransferible no permitiéndose que segundas personas hagan uso de ella.

11.7 La vigencia de la cuenta de correo electrónico es durante la persona sea empleado del IPSFA.

11.8 El usuario será responsable de la información que sea enviada con su cuenta, por lo cual se asegurará de no mandar SPAMS de información o anexos que pudieran contener información nociva para otro usuario como virus o pornografía.

11.9 El usuario es responsable de respaldar sus archivos de correo manteniendo en el buzón de correo (INBOX) solamente documentos adjuntos más recientes, sus demás comunicados deberá mantenerlos en su equipo personal o en su defecto en la(s) carpeta(s) asignada(s) en el servidor para su área y/o Departamento.

11.10 Al responder comunicados generales o para un grupo específico de usuarios, el usuario deberá cuidar de no responder a TODOS los usuarios salvo cuando ésta sea la finalidad de la respuesta.

11.11 El Departamento de Informática se reserva el derecho de enviar al usuario la información que considere necesaria como un medio de comunicación Institucional.

11.12 La vigencia y espacio de las cuentas será definido por el Departamento de Informática de acuerdo a los recursos disponibles y con base en las necesidades del usuario.

11.13 El Departamento de Informática se reservará el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para la seguridad Institucional.

11.14 El Departamento de Informática realizará monitoreo del tamaño de los buzones y deshabilitara aquellos que considere que estén afectando la disponibilidad de espacio del servidor.

11.15 El usuario es responsable de respetar la ley de derechos de autor, no abusando de este medio para distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor.

11.16 El incumplimiento por parte del usuario del buen uso de su cuenta puede ocasionar la suspensión y posterior baja del sistema de su cuenta.

11.17 El usuario podrá generar sus listas de distribución de correo con un máximo de 20 direcciones de correo, siempre y cuando éstas no interfieran con el buen funcionamiento y la distribución del correo del servidor.

11.18 El Departamento de Informática no se compromete a entregar mensajes de correo a cuentas de uso gratuito como hotmail, yahoo, usa.net, excite, starmedia etc.

12. Específicas para usuarios externos de correo electrónico

12.1 Las cuentas y correos electrónicos para usuarios externos serán solicitados por la UCEFI (cuando se trate de los entes fiscalizadores del IPSFA) y/o a través de la Gerencia del IPSFA que desee un servicio de este tipo, especificando el objetivo del servicio solicitado y el período por el cual se requiere.

UNIDAD DE DESARROLLO ORGANIZACIONAL

12.2 Es responsabilidad de la UCEFI notificar de forma inmediata a el Departamento de Informática cuando el servicio solicitado para un usuario externo perteneciente a un ente fiscalizador ya no tenga validez.

12.3 El Departamento de Informática facilitará a los usuarios manejar el correo electrónico a través de sus cuentas, siendo éste un medio de comunicación formal a nivel Institucional, por lo que enviará los avisos y mensajes que considere necesarios a través de este medio.

12.4 Por seguridad (ya que en ellos puede disfrazarse un virus) no se pueden enviar, ni recibir archivos a través del correo electrónico institucional @ipsfa.com, aquellos que cumplan con los siguientes criterios y extensiones:

.ad.adb*.ade*.adp*.asp*.bas*.bat*.chm*.cmd*.com*.cpl*.crt*.dbx*.eml*.exe*.hlp*.hta*.htm*.html*.inf*.ins*.isp*.js*.jse*.lnk*.mde*.mdb*.mht*.mp3*.msc*.msi*.msp*.mst*.oft*.pcd*.pl*.pif*.php*.reg*.scr*.sct*.shb*.shs*.sht*.ttb*.txt*.uin*.rtf*.url*.vb*.vbe*.vbs*.vsd*.vss*.vst*.vsw*.wab*.ws*.wsc*.wsf*.wsh*.pif*.scr*.exe*.cmd*.bat*.zip*.emlbody.*data.*doc.*document.*file.*message.*readme.*test.*text.**.htt

folder.htt*.msg

document.*

msg.*

doc.*

talk.*

massage.*

creditcard.*

details.*

attachment.*

me.*

stuff.*

posting.*

textfile.*

concert.*

information.*

note.*

INSTITUTO DE PREVISION SOCIAL DE LA FUERZA ARMADA
UNIDAD DE DESARROLLO ORGANIZACIONAL

bill.*

swimmingpool.*

13. Específicas para la creación de acceso a internet

13.1 Las Jefaturas son responsables de solicitar al Departamento de Informática el acceso de aquellos subalternos que para fines de trabajo tendrán acceso a Internet.

13.2 La solicitud será hecha por escrito en el formulario correspondiente.

13.3 El uso de Internet es exclusivamente para las actividades Institucionales.

13.4 Las configuraciones de las estaciones de trabajo para acceder al servicio de Internet son responsabilidad exclusiva del personal del Departamento de Informática.

13.5 El uso de Internet es personal e intransferible, no se permite que segundas personas (personas externas al IPSFA) hagan uso del servicio.

13.6 Se harán excepciones para el uso de Internet cuando este sea requerido, justificado y autorizado para los integrantes de las delegaciones de los entes fiscalizadores con presencia en el Instituto.

13.7 A través de los equipos de monitoreo y análisis de tráfico instalados en el sitio central de la red, se detectarán a los usuarios que hagan mal uso de los servicios de Internet.

13.8 Las Gerencias y Jefaturas solicitarán, si así lo consideran conveniente, que se limite el acceso para determinados usuarios a sitios específicos de Internet.

13.9 El Departamento de Recursos Humanos deberá informar al Departamento de Informática inmediatamente cuando un empleado ha dejado de laborar en el IPSFA, con el objetivo de inhabilitar su acceso a Internet, correo electrónico, etc.

14. Específicas en internet

14.1 Todo archivo que se reciba por Internet es analizado automáticamente por el antivirus corporativo para asegurar que no contenga virus

14.2 Antes de abrir cualquier archivo recibido por Internet, el usuario debe asegurarse de que sea un archivo confiable.

14.3 El incumplimiento de la Normatividad Técnica en Tecnología de la Información, específicamente en el uso de Internet, será sancionado en los

términos que establece la Ley de Responsabilidades Administrativas de los servidores Públicos.

15. Específicas para el uso de equipo informático externo

15.1 Si se ingresa un equipo informático a las Instalaciones, que no sea propiedad del IPSFA, y se desea conectar a la red institucional, se deberá solicitar autorización al Jefe del Departamento de Informática; por un área o persona del IPSFA, que se haga responsable de tal situación.

16. Específicas para la administración de computadoras personales y laptops

16.1 El personal de soporte técnico del Departamento de Informática verificara que las computadoras personales y Laptops asignadas a los diferentes usuarios no tengan acceso a la administración de sus equipos.

16.2 El personal del Departamento de Informática verificará a nivel de todo el IPSFA el software instalado en los equipos informáticos refiérase a (computadoras personales y/o Laptops) que tienen asignados el personal del Instituto, con el fin de constatar que se esté cumpliendo las leyes o regulaciones tales como la Ley Reglamento de Fomento y Protección de la Propiedad Intelectual, en la instalación de software en los equipos informáticos.

16.3 El área de soporte del Departamento de Informática deberá configurar en todos los equipos informáticos del IPSFA refiérase a (computadoras personales y/o Laptops) un agente de acceso remoto que permita el apoyo remoto de la configuración y el software instalado en cada uno de los mencionados equipos a fin de garantizar que se esté cumpliendo las leyes o regulaciones tales como la Ley Reglamento de Fomento y Protección de la Propiedad Intelectual, en la instalación de software en los equipos informáticos.

17. Específicas para el uso de equipo y de recursos informáticos asignados

17.1 Para hacer uso del equipo y recurso informático asignado, el usuario debe ser empleado activo del IPSFA.

17.2 El uso de Internet debe ser únicamente para fines institucionales, definiéndose como institucionales a todas aquellas búsquedas de información que apoyen el trabajo del usuario.

17.3 El uso de equipo de digitalización de documentos (scanners) e impresoras es exclusivamente para actividades institucionales.

17.4 Para alargar la vida útil del equipo, se prohíbe ingerir alimentos y bebidas sobre el mismo, así como el fumar cerca del equipo informático.

17.5 Se recomienda a los usuarios almacenar los archivos de trabajo en las carpetas institucionales asignadas para cada área o unidades del IPSFA, para evitar cualquier pérdida de información valiosa.

17.6 El contenido de los discos duros de las estaciones de trabajo debe ser continuamente depurado para evitar la saturación de espacio. Será responsabilidad del usuario el respaldar la información.

17.7 El Departamento de Informática se reserva el derecho de revisión del contenido de lo almacenado dentro del equipo del usuario con el objetivo de velar por el correcto uso del recurso asignado.

17.8 Cualquier uso que cause efectos opuestos a la operación del Departamento de Informática o ponga en riesgo el uso o rendimiento de la plataforma informática Institucional, será analizado por la jefatura de la unidad para tomar medidas correctivas y preventivas a nivel técnico y/o administrativo según sea el caso.

17.9 El equipo y recursos asignados se entregarán en buenas condiciones. En caso de extravío o daño de equipo por parte del usuario, se informara a la administración del IPSFA para que se determinen responsabilidades y/o las acciones a seguir.

17.10 El personal del Departamento de Informática es el único autorizado de desconectar, mover, abrir el equipo y sus componentes.

17.11 Para eventos especiales que requieran el uso de recurso informático en específico y del cual no dispongan: El Departamento o Unidad interesada deberá solicitarlo por escrito o por correo electrónico, al Departamento de Informática, con un mínimo de dos días de anticipación.

17.12 Se consideran faltas, las siguientes infracciones:

a. Consumir alimentos, bebidas o fumar frente al equipo asignado.
b. Utilizar servicio de voz, sonido o imagen no autorizados.

c. Usar lenguaje soez en la comunicación de Internet y/o en correo electrónico.
d. Demorar la entrega de equipo en préstamo cuando sea solicitado por el Departamento de Informática, para labores de mantenimiento.
e. Conectar periféricos al equipo sin previa autorización por escrito a la jefatura de Informática.
f. Instalar juegos y jugar en las computadoras.
g. Utilizar Internet para fines no institucionales.

17.13 Se recomendarán las siguientes sanciones:

a. Amonestación por escrito con copia al expediente la primera vez.
b. Amonestación por escrito y suspensión del uso del servicio por un período de 3 meses en el caso de los incisos c, e, f y g.

17.14 Se consideran faltas graves, las siguientes infracciones:

a. Consultar y/o desplegar cualquier tipo de erotismo o de pornografía.
b. Mover máquinas, equipos, cables u otros elementos, sin supervisión y/o autorización del Departamento de Informática.
c. Utilizar el equipo asignado para piratería o acceso no autorizado (hacking) a servidores propios o ajenos.
d. Borrar el Software instalado por el Departamento de Informática.
e. Irrespetar de palabra o acción a los técnicos del Departamento de Informática.
f. Realizar acción voluntaria que cause daño a los equipos asignados.
g. Causar daños o perjuicios a terceras personas.
h. Otras, que afecten en forma grave el funcionamiento del equipo asignado o la red institucional.
i. Instalar software sin licencia, violando las leyes o regulaciones tales como la ley, reglamento de fomento y protección de la propiedad intelectual, en la instalación de software en el equipo asignado.

17.15 Se recomendarán las siguientes sanciones:

a. Las indicadas en los incisos b, d, e y f se sancionarán por primera vez con amonestación escrita y suspensión temporal del equipo y/o servicio

asignado; las reincidencias darán lugar a la suspensión definitiva del equipo y/o servicio asignado.

b. Las restantes faltas, serán sancionadas con la suspensión definitiva del equipo y/o servicio asignado.

c. Las amonestaciones por escrito serán comunicadas por el área de RRHH del IPSFA a petición de la jefatura del Departamento de Informática o de otra autoridad Institucional.

d. Las sanciones por faltas graves serán comunicadas por el área de RRHH.

e. El uso de software sin licencia, será responsabilidad directa del usuario el cual responderá ante los entes fiscalizadores.

f. Amonestación por parte de los entes fiscalizadores por falta de literal i).

18. Específicas para la adquisición de bienes informáticos

18.1 El Departamento de Informática efectuará el análisis y evaluación de la factibilidad de la compra de todos los bienes informáticos que se esté proponiendo adquirir en el IPSFA, emitiendo su recomendación técnica, con el objetivo de garantizar tanto compatibilidad técnica como la inversión a realizar.

18.2 En el caso de las adquisiciones de software la unidad solicitante deberá entregar al Departamento de Informática la(s) media(s) y licencia(s) originales para su instalación y posterior resguardo.

19. Específicas para el traslado o cambio de equipo informático

19.1 Todas las áreas del IPSFA deberán informar a el Departamento de Informática de todo traslado o cambios del personal con equipo informático asignado, con el objetivo de garantizar la seguridad de los sistemas, modificando y/o inhabilitando los diferentes accesos (correo electrónico, red institucional, a los aplicativos, etc.)

19.2 Todas las áreas del IPSFA deberán informar a el Departamento de Informática de todo traslado o cambios del equipo informático asignado a las áreas del IPSFA, a efectos de que sea el Departamento de Informática quién realice el traslado de dicho equipo garantizando su instalación, funcionamiento y actualización de su nueva ubicación tanto en los controles propios del Departamento de Informática como en los del área de activo fijo.

19.3 Todas las áreas del IPSFA deberán informar al Departamento de Informática, que si poseen equipo sin personal asignado en el área, este deberá ser entregado a el Departamento de Informática para su reubicación en otra área del Instituto donde se necesite.

20. Específicas para otorgar privilegios y derechos a usuarios de la Unidad de Auditoria Interna

20.1 Los privilegios de Administrador Local de las computadoras asignadas, serán otorgados únicamente al Coordinador de Auditoria en Informática y Auditor en Informática, dichos privilegios deberán estar detallados en un acta con la firma de los usuarios autorizados, en donde se responsabilicen de la administración de su contenido, evitando la instalación de programas de dudosa procedencia para evitar el ingreso de virus o Spyware e incumplir con las regulaciones establecidas en la Ley y Reglamento de Fomento y Protección de la Propiedad Intelectual.

20.2 Es responsabilidad del Administrador de la Base de Datos del Departamento de Informática, validar que el Coordinador de Auditoria en Informática y el Auditor en Informática no tengan privilegios de modificación al sistema informático NEO IPSFA.

20.3 El Administrador de la Base de Datos del Departamento de Informática, será el responsable de configurar el manejo de datos, así como el de asignar a los usuarios de Auditoria Interna autorizados, un nivel más bajo de prioridad que el de los usuarios operativos, para tratar de minimizar el impacto durante las horas de mayor actividad.

20.4 En los casos en que las consultas de datos, generen un volumen de información que pueda comprometer el rendimiento del servidor, la red o la base de datos; la Unidad de Auditoria Interna deberá informar previamente a el Departamento de Informática, para coordinar el monitoreo proactivo del servidor con el fin de mantener el funcionamiento normal de la red Institucional.

B. NORMAS

1. Administrativas

1.1 Todo requerimiento referente al soporte y mantenimiento del software y hardware será canalizado a través del Departamento de Informática, utilizando el formulario de Solicitud de Requerimiento y/o por medio de correo electrónico a helpdesk@ipsfa.com.

1.2 El Departamento de Informática tendrá la responsabilidad de emitir su opinión y/o recomendación técnica sobre la adquisición de software y equipo informático en IPSFA, áreas descentralizadas y unidades de negocio.

1.3 Para el cumplimiento de la anterior normativa, DACI deberá solicitar por escrito al Departamento de Informática la opinión técnica de la oferta de los proveedores y los requerimientos mínimos que deberá cumplir el hardware y el software, para poder iniciar el proceso de compra.

1.4 El Departamento de Informática será responsable de controlar el traslado, préstamos internos o cualquier otro tipo de movimiento del equipo informático del IPSFA y las Unidades descentralizadas, las cuales a su vez deberán informar a el Departamento de Informática dichos movimientos.

1.5 Todas las áreas del IPSFA y Unidades de Negocio, deberán dirigir a el Departamento de Informática cualquier consulta relacionada con el recurso informático.

1.6 Las diferentes Unidades y Departamentos del IPSFA son los responsables del manejo y proceso de su propia información. Las funciones del Departamento de Informática se limitan al soporte y mantenimiento de toda la instalación Informática (Hardware y Software).

1.7 Todo requerimiento de información realizada por los entes fiscalizadores deberá ser entregada por las áreas correspondientes, el Departamento de Informática será un apoyo para la generación de la información solicitada a petición de la UAIP y con visto bueno del área correspondiente.

1.8 Todo requerimiento de información realizado por Otras Instituciones, deberá ser canalizado por las áreas responsables, el Departamento de Informática será un apoyo para la generación de la información contando con el visto bueno del área correspondiente.

1.9 Todo requerimiento realizado a el Departamento de Informática por los Entes Fiscalizadores y la Unidad de Auditoría Interna deberá hacerse por escrito, con el fin de respaldar dicha solicitud.

1.10 Toda falla en el hardware y software del equipo informático, deberá reportarse inmediatamente al Departamento de Informática mediante el formulario de Solicitud de Requerimientos o correo electrónico dirigido a helpdesk@ipsfa.com.

1.11 Informática será la única Unidad autorizada para realizar y supervisar el mantenimiento preventivo y/o correctivo en las computadoras personales y los equipos informáticos en todas las áreas del IPSFA y sus Unidades de Negocio.

1.12 El Departamento de Informática será la única autorizada para supervisar y controlar el mantenimiento preventivo y correctivo de los impresores institucionales que cuentan con el servicio de mantenimiento.

1.13 El Departamento de Informática, deberá contar con una planificación para efectuar el mantenimiento de todos los equipos informáticos en todas las áreas del IPSFA y sus Unidades de Negocio.

1.14 La utilización de Internet, se canalizará a través de la Gerencia de cada área, la cual deberá ser justificada mediante memorándum, vía email o llamada telefónica.

1.15 Todas las funciones del Departamento de Informática, deberán ser efectuadas de acuerdo al Plan Operativo Anual de Trabajo. (POA).

1.16 A requerimiento de las áreas interesadas el Departamento de Informática prestará el apoyo necesario durante el proceso de inducción de personal, a fin de que éste sea capacitado debidamente en el uso del software y hardware específico del área a la cual está asignado.

1.17 La integridad y la seguridad lógica de los sistemas informáticos, serán garantizadas por el Departamento de Informática, así como la seguridad física.

1.18 Solamente el personal de Informática, estará autorizado para instalar y reinstalar el software de las computadoras personales y Laptops en las diferentes áreas del IPSFA y sus Unidades de Negocio.

1.19 El Jefe de informática podrá nombrar internamente del personal bajo su cargo, la figura de Administrador de Base de Datos Jr. (DBA Jr), para apoyar las funciones del Coordinador de Análisis y Programación relacionadas a la Base de Datos.

1.20 La persona nombrada internamente como DBA Jr., deberá cumplir realizar adicionalmente a sus funciones asignadas a su puesto de trabajo, las siguientes actividades:

a. Monitorear los respaldos de la base de datos y su envió al Sitio de Contingencia.
b. Monitorear el tráfico de la base de datos
c. Crear, modificar y eliminar objetos en la base de datos a demanda.
d. Coordinar con los Proveedores las asistencias técnicas necesarias para mantener en buen funcionamiento la Base de Datos.

2. Técnicas

2.1 El Departamento de Informática será responsable de la estandarización del software a utilizar a nivel Institucional.

2.2 El Departamento de Informática identificará, seleccionará, implementará y controlará el sistema operativo a ser utilizado en las computadoras personales del Instituto.

2.3 El Departamento de Informática contará con un plan para enfrentar contingencias de índole informático.

2.4 Será responsabilidad del Jefe del Departamento de Informática mantener actualizado en cuanto al aprendizaje de nuevas tecnologías que aparezcan en el mercado respecto a hardware y software, manteniendo para ello una política constante de capacitación y actualización de conocimientos.

2.5 El desarrollo de aplicaciones, deberá ser justificado en forma escrita por parte del área solicitante del IPSFA antes de iniciar el proceso.

2.6 El Departamento de Informática y los usuarios del sistema compartirán la responsabilidad en las fases de levantamiento de requerimientos, diseño e implementación de los sistemas de información.

2.7 Todo software aplicativo, estará debidamente documentado con su respectivo Manual de Usuario y será divulgado oportunamente a todas las áreas directamente involucradas.

2.8 La instalación del software estará sujeta a la factibilidad técnica del equipo en el cual estará instalado.

2.9 El software a instalar deberá contar con su respectiva licencia de uso.

2.10 El usuario deberá presentar la Solicitud y Análisis de Requerimientos (FORM-08-GG-INF-01). o correo electrónico de restauración de Información dirigido a hepldesk@ipsfa.com.

2.11 En general se realizan los respaldos de información en discos RDX.

2.12 Las cintas y discos RDX con respaldos semanales más recientes serán almacenadas en el sitio de contingencia fuera de las instalaciones del Instituto.

2.13 Se cuenta con la estructura alterna de respaldo para los siguientes puestos:

a. **Administrador de Base de Datos**, se contará con la figura interna de Administrador de Base de Datos Jr., que cuenta con conocimientos del Administrador de Base de datos en caso de ocurrir una contingencia será quien cubrirá las funciones del DBA.

b. **Administrador de Red**, contará con la figura interna de Administrador Red Jr., que cuenta con conocimientos de comunicación e infraestructura de redes en caso de ocurrir una contingencia será quien cubrirá las funciones del Administrador de Red.

c. **Coordinador de Análisis y Programación**, con base a la función de Administración del Neo-IPSFA, contará con la figura interna cubriendo la función de Administración del Neo-IPSFA alterna, que contará con los privilegios para realizar dichas funciones.

2.14 El acceso a la base de datos de producción del Sistema NEO-IPSFA estará bloqueado para realizar conexiones utilizando otros programas ajenos al Sistema NEO-IPSFA.

2.15 Los Analistas programadores del Departamento de Informática, tendrán restringido el acceso a la Base de datos de producción del Sistema NEO-IPSFA, desde otros programas utilizados para desarrollo de Sistemas Informáticos, administración o consultas de cualquier tipo (Ej: SQL Developer, TOAD, Developer Suite, etc).

2.16 Únicamente el Jefe del Departamento de Informática y el Administrador de Base de datos tendrán acceso completo a la base de datos de producción del Sistema NEO-IPSFA, para actividades relacionadas a la Administración de la misma.

3. Acceso a las instalaciones del Departamento de Informática

3.1 Las personas particulares que ingresen a las oficinas, salones o pasillos del Departamento de Informática, no deben portar bolsones, mochilas, maletines, cajas o depósitos de mediana o gran capacidad, sin previa autorización de la Jefatura de Informática.

3.2 Podrán ingresar y permanecer en el área del Departamento de Informática, empleados de otras unidades del IPSFA, proveedores, personas particulares o familiares que necesiten contactar al personal, siempre que el personal del Departamento de Informática a quien buscan, se encuentre presente y disponible, de lo contrario deberán esperar en la sala de recepción, en las salas de reunión o en otras áreas apropiadas.

3.3 El área de computadores y servidores principales dentro del Departamento de Informática, así como las áreas del UPS y la planta de Emergencia, tienen un nivel mayor restricción de acceso, y solo ingresarán a dichas áreas las personas autorizadas en virtud de sus funciones y actividades, o en casos especiales, con autorización de la jefatura del Departamento de Informática y deberán anotar la hora de ingreso y la hora de salida en el formulario Bitácora de Acceso a Granja de Servidores (FORM-08-GG-INF-03).establecido para dicho control.

4. Movimiento, préstamo y uso de equipo

4.1 Todo movimiento, préstamo y uso de equipo que requieran las distintas Unidades del IPSFA deberán ser autorizados por la Jefatura del Departamento de Informática siguiendo el procedimiento definido para tal fin.

UNIDAD DE DESARROLLO ORGANIZACIONAL

5. Referentes al Área de Análisis y Programación

5.1 Los analistas programadores no podrán atender requerimientos enviados por los usuarios de forma directa, por teléfono, o vía electrónica, salvo los casos de emergencia, para los cuales deberán enviar posteriormente la solicitud de requerimiento respectivo o por correo electrónico a la dirección helpdesk@ipsfa.com .

5.2 Es de carácter obligatorio que los analistas programadores registren el seguimiento y finalización de los requerimientos atendidos, además de comunicar a los usuarios en forma escrita la terminación de estos.

6. Para la reutilización de partes provenientes de equipo informático en desuso

6.1 Todo equipo informático que sea descargado, deberá ser trasladado al Área de Soporte Técnico del Departamento de Informática a través del formulario Solicitud de Traslado de Activo Fijo (FORM-09-GA-SGE-018), para realizarle una evaluación de las partes que pueden ser reutilizadas.

6.2 El desarme de los equipos informáticos en desuso será realizado exclusivamente por el Área de Soporte Técnico de la Unidad de Informática.

6.3 Toda remoción de piezas de equipos informáticos se realizara exclusivamente a aquellos equipos que se encuentren en desuso por motivos de: obsolescencia, desperfecto o falla.

6.4 El Área de Soporte Técnico de la Unidad de Informática será responsable de llevar un control las partes removidas de cada equipo, debiendo estas ser detalladas e incorporadas dentro de un inventario.

6.5 Al finalizar la remoción de partes de un equipo informático, el Área de Soporte Técnico del Departamento de Informática deberá realizar el trámite de Descargo del equipo informático y llenar el formulario Solicitud de Descargo de Activo Fijo (FORM-09-GA-SGE-017), debiendo anexar el detalle de las piezas extraídas al equipo.

7. Obsolescencia de equipos informáticos

7.1 Se considerará como equipo informático obsoleto:

a. Todo aquel que ya no pueda ser utilizado como herramienta de apoyo eficaz para atender los requerimientos de un Departamento (baja memoria ram, poca capacidad de disco duro y procesador de poca velocidad, etc.)

b. Todo aquel cuya reparación o mantenimiento requiera un costo igual o superior al 50% del valor de adquisición.

c. Aquel que ya no cumple con los requerimientos mínimos para instalarle software o actualizaciones.

d. Aquel que haya sobrepasado la vida útil (5 años) y ya no se pueda actualizar.

7.2 Está permitido extraer los componentes físicos de un equipo de cómputo que se considera obsoleto para incluirlos en otro equipo de cómputo a efecto de subsanar la obsolescencia del segundo y asegurar mayor tiempo de vida útil. (Ver procedimiento: Reutilización de partes provenientes de equipos informáticos en desuso).

7.3 El Jefe del Departamento de Informática y el Coordinador de Soporte Técnico serán los responsables de validar la obsolescencia de un equipo informático a través de un diagnostico u opinión técnica.

8. Funciones y responsabilidades del Administrador del sistema antivirus institucional

8.1 El Departamento de Informática por medio del Administrador de Red Jr. será la responsable de la administración total del software de seguridad (Antivirus) del IPSFA; pudiendo delegar en caso fortuito al Área de Soporte Técnico.

8.2 Será responsabilidad del Administrador de Red Jr., cumplir con la tarea asignada y controlar que el equipo informático del IPSFA tenga instalada y se mantenga actualizada a diario, la firma de virus de la Solución Antivirus Institucional.

8.3 El "Encargado de administrar el Sistema de Protección Antivirus Institucional", inspeccionara todo aquel equipo informático nuevo o equipo informático externo que solicite ingreso a la red Institucional; antes de ser entregado al usuario final, el cual deberá tener instalada la Solución Antivirus.

8.4 Periódicamente el "Encargado de administrar el Sistema de Protección Antivirus Institucional", efectuara un rastreo en el equipo informático del IPSFA, por medio de la consola administrativa de la Solución Antivirus, realizando las siguientes acciones:

a) Verificar que se encuentre aplicada la Actualización automática de las firmas antivirus proporcionada por el fabricante de la Solución Antivirus, en el

Servidor destinado como Servidor de Solución Antivirus.

b) Monitorear Actualización automática de las firmas antivirus proporcionadas por el fabricante de la Solución Antivirus, en los equipos conectados a la red institucional.

c) Realizar Actualización manual de las firmas antivirus en los equipos no conectados a la red institucional.

8.5 El "Encargado de administrar el Sistema de Protección Antivirus Institucional", deberá llevar un registro periódico de la actualización de todos los equipos desktop y laptops institucionales, que se encuentren dentro y fuera de la red institucional.

8.6 Para los casos de detección de ataques dirigidos a través de virus o malware, el "Encargado de administrar el Sistema de Protección Antivirus Institucional", deberá realizar inmediatamente las siguientes actividades:

a) Realizar el análisis del nivel de riesgo por medio del monitoreo de reportes y correos electrónicos generados por la consola administrativa.

b) Detectar y Aislar de la red equipo y/o medio detectado como foco de infección.

c) Realizar la toma de muestras de ataque y enviarlas para su análisis al fabricante de la solución antivirus.

d) Notificar al Jefe del Departamento de Informática.

e) Poner en marcha la metodología establecida para virus no controlados.

8.7 El "Encargado de administrar el Sistema de Protección Antivirus Institucional", será el responsable del mantenimiento e implementación tanto del servidor, como de la consola administrativa de Solución Antivirus Institucional, efectuando las siguientes acciones:

a) Realizar el estudio correspondiente para el cambio de versión de servidor y consola administrativa, tomando en cuenta los requerimientos y exigencias institucionales.

b) En cuanto a la implementación de normas, perfiles y nuevas políticas deberá realizarlas e implementarlas hasta obtener la autorización del Jefe del Departamento de Informática.

c) Deberá de contar con plan alternativo o de contingencia así como de respaldo.

de los perfiles y software en caso de siniestros.

9. Para la instalación de servidor de solución antivirus institucional

9.1 Se deberá contar con un servidor local de sistema de protección antivirus.

9.2 La instalación, licencia y uso de la consola administrativa está considerada y viene incluida en la versión Bussines del sistema de protección antivirus adquirido.

9.3 El Servidor de Antivirus se encuentra alojado en un equipo Virtual bajo sistema operativo Windows o Linux.

9.4 Del sistema de protección:

a) Se cuenta con ESET ENDPOINT Security Bussines Edition.

b) Se cuenta con ESET FILE SECURITY Bussines Edition.

c) Se cuenta con ESET MOBILE SECURITY Bussines Edition.

9.5 El Instituto contrata el sistema de protección con vigencia de enero a diciembre, por un total aproximado entre 300 y 380 licencias para usuarios finales.

10. Bases de datos utilizadas por la solución antivirus

10.1 El sistema de protección antivirus deberá permitir elegir el tipo de base de datos a utilizar, pudiendo escoger entre My SQL, MSSQL, Oracle.

10.2 La base de datos utilizada en el Instituto es: My SQL, MSSQL, Oracle.

11. Configuraciones en servidor y en consola administrativa de la solución antivirus

11.1 Implementación:

11.1.1 Seguridad Intrínseca.

a) Se cuenta con un sistema de seguridad múltiple (en referencia al uso, monitoreo, instalación e implementaciones que se quieran realizar en el Sistema de Protección Antivirus Institucional).

b) El acceso a la consola administrativa es vía web con usuario y contraseña, cuya licencia está asignada al "Encargado de administrar el Sistema de Protección Antivirus Institucional".

c) La implementación de ingreso de contraseña para acceder al servidor antivirus, a la consola administrativa, a los paquetes de instalación offline; así como también, para realizar cambios en la configuración del equipo informático, permite realizar una administración segura y de datos reales.

11.2 Configuración.

11.2.1 Para la instalación del sistema de protección antivirus institucional tanto en el servidor, como en la consola administrativa, se cuenta con una configuración estándar de comportamiento, establecida a criterio del fabricante.

11.2.2 Dicha configuración es 100% adaptable a las necesidades y requerimientos institucionales, siendo estas políticas en la consola antivirus la cual posee ambiente gráfico y agentes en los equipos clientes.

11.3 Configuraciones institucionales dentro del Sistema de Protección Antivirus Institucional

11.3.1 Por seguridad institucional, se maneja un estándar de configuración para todos los c1ientes finales. Y dicho perfil se ha modificado para cumplir con las exigencias de trabajo y requerimientos del Instituto:

a. Perfil Usuario Final:
   i. Permiso o bloqueo de dispositivos de almacenamiento.
   ii. Permiso o bloqueo de redes sociales, streaming, web.
   iii. Configuración para protección de equipos.
   iv. Permiso o bloqueo a red o redes sociales (mac, Windows, linux)
b. Perfil Servidores: Windows, Linux.
c. Configuración para protección de servidores.
d. Perfil BYOD: Configuración para protección de dispositivos móviles.

11.3.2 El cambio de perfil para un equipo informático, solo puede realizarlo el "Encargado de administrar el Sistema de Protección Antivirus Institucional", por medio de la autorización del Jefe del Departamento de Informática.

11.3.3 En caso de ocurrir fuga de información, introducción de virus y/o ataques por medio de los dispositivos de almacenamiento masivo, y el diagnóstico y/o reporte del servidor por medio de la consola administrativa, indica que se originó en el usuario al que se le realizó el cambio de perfil, la responsabilidad recaerá sobre el jefe inmediato de la unidad solicitante.

11.4 Actualizaciones de firmas de virus desktop y laptop.

11.4.1 El equipo informático realiza actualización de las firmas de virus de manera automática por medio de la red interna hacia un servidor web central, el cual es identificado como: (ip - adress:port): http://ipdelequipo:puerto , de acuerdo

a cada uno de los perfiles institucionales configurados. El servidor del sistema de protección realiza una conexión constante por medio de intemet, hacia los servidores propietarios de actualización del sistema de protección antivirus adquirido. Para realizar dicha conexión se utiliza usuario y contraseña proporcionados por el proveedor al momento de realizar el contrato de servicio. Dicha configuración, es aplicada de manera estándar tanto en el servidor como en la consola administrativa, y se realiza cada 60min. El servidor no realiza una conexión a intemet por cada usuario terminal que solicite actualizarse, sino que se crea una réplica (mirror), que contiene las actualizaciones correspondientes, siendo constantemente actualizada por el servidor, al mismo tiempo que se actualiza la base de firmas del servidor central institucional.

11.4.2 El equipo informático de escritorio, configurado de acuerdo a cada perfil, tiene establecida una "tarea programada" la cual indica que al iniciar el equipo, este envíe información de la firma de virus que posee hacia el servidor de antivirus institucional. Dicho servidor compara la firma de virus del equipo informático con la propia; si es inferior a la de la firma del servidor de antivirus, entonces envía la actualización correspondiente. Si el equipo informático no obtiene respuesta del servidor central de la solución antivirus institucional, otra "tarea programada" le indica que debe de esperar 20min. e intentarlo de nuevo.

11.4.3 Para las actualizaciones a los equipos informáticos es necesario que estén conectados en red, por lo que se solicita a las áreas que el equipo portátil sea conectado a la red interna por lo menos una vez a la semana.

11.5 Notificaciones

11.5.1 El sistema de protección antivirus Institucional, cuenta con un sistema de notificaciones:

a. Ventana emergente en pantalla para todos los usuarios de equipo informático.
b. Notificaciones en tiempo real de sucesos y alertas por medio de reporte en el monitoreo de la consola antivirus.

UNIDAD DE DESARROLLO ORGANIZACIONAL

11.5.2 Envío de un correo electrónico desde y hacia una cuenta previamente configurada. A nivel institucional se ha configurado la cuenta: alerta.virus@ipsfa.com, dicho correo envía una notificación en tiempo real especificando: nombre de amenaza detectada, hora de detección y nombre de equipo en el cual se ha detectado la amenaza. Misma que es administrada y monitoreada por el "Encargado de administrar el Sistema de Protección Antivirus Institucional".

11.5.3 Criterios de notificaciones:

a. Se toman en cuenta bajo previa configuración en el servidor, el tipo de alertas que se notificaran.
b. Las notificaciones de no actualización no son consideradas como de alto riesgo, sino como alerta leve al inicio. Ya que puede deberse a varios factores como:
   i. Saturación de tráfico de la red al momento de conectar con el equipo o con el servidor.
   ii. Que el equipo informático se encuentra apagado.
   iii. Saturación de actualizaciones en memoria caché del equipo informático.
   iv. Pérdida de conexión por aislamiento del equipo informático.
c. Si una notificación de no actualización no es causada por alguna de las anteriores se toma coma una alerta.

11.6 Alertas y Tratamientos

11.6.1 Las alertas reportadas por correo electrónico, que han sido detectadas por monitoreo mediante la consola antivirus, o por un usuario cuya alerta fue mostrada mediante pantalla emergente antivirus, son tratadas como únicas y específicas y se da el tratamiento adecuado según sea necesario:

11.6.1.1 Si el equipo informático de escritorio, no actualiza:

a. Rastrea en todo el equipo informático para detectar versiones antiguas de la firma de antivirus.
b. Contacta telefónicamente al usuario, y le comunica que instalara antivirus o actualización.
c. Realiza instalación remota de Antivirus.

d. Aplica actualización de la versión más reciente del Antivirus.

11.6.1.2 Si el equipo informático portátil no actualiza:

a. Verifica reporte de actualización de equipos fuera de red.

b. Contacta al usuario del equipo, y le solicita que conecte el equipo a la red para realizar la instalación remota del Antivirus, y/o coordina visita para realizar la instalación en el puesto de trabajo del usuario.

c. Realiza instalación de Antivirus.

d. Aplica actualización de la versión más reciente del Antivirus.

11.6.1.3 Si la alerta hace referencia a un ataque "día-0", el equipo o equipos se aíslan de la red institucional y se deberá contactar con el Soporte del antivirus institucional.

11.6.1.4 El sistema de protección antivirus a nivel institucional cuenta con una heurística avanzada la cual le permite detectar sospechas de ataques ya sea vía Web, o correo.

11.6.1.5 La actualización de firma de virus esta preestablecida cada 60 minutos en el servidor y cada 10 minutos en el equipo informático.

11.6.1.6 Alerta de contenido bloqueado "archivos en cuarentena". Si existe una alerta se verifica en la consola antivirus para saber su origen de la infección.

11.6.2 Si es por internet:

a. Se contacta te1efónicamente al usuario del equipo informático y se informa del proceso malicioso detectado.

b. Se genera un reporte y se informa a la coordinación y jefatura de informática.

c. Se aísla el equipo informático de la red.(de ser necesario)

d. Se procede a la desinfección del equipo, en dado caso la solución antivirus institucional no lo haga automáticamente.

e. Si existen daños o pérdida de información por causa del virus y/o amenaza, se intenta recuperar con la ayuda de utilitarios proporcionados por el fabricante del sistema de protección antivirus.

11.6.3 Si es por correo electrónico:

a. Se contacta telefónicamente a usuario de equipo informático y se informa del proceso malicioso detectado.

b. Se aísla el equipo informático de la red.(de ser necesario)

UNIDAD DE DESARROLLO ORGANIZACIONAL

c. Se realiza la toma de muestras y se envía al fabricante de la solución de sistema de protección antivirus para su análisis y pronta solución a la misma.

d. Se genera un reporte y se informa a la coordinación y jefatura de informática

e. Se solicita al Administrador de Redes, bloquear usuario específico en firewall para evitar el reenvío masivo o más ingreso de email infectado.

f. Se procede a la desinfección del equipo, en dado caso la solución antivirus institucional no lo haga automáticamente.

g. Si existen daños o pérdida de información por causa del virus y/o amenaza, se intenta recuperar con la ayuda de utilitarios proporcionados por el fabricante del sistema de protección antivirus.

11.6.4 Si es por medios de almacenamiento masivo:

a. Se contacta telefónicamente al usuario del equipo informático y se informa del proceso malicioso detectado.

b. Se realiza la toma de muestras y se envía al fabricante de la solución de sistema de protección antivirus para su análisis y pronta solución a la misma.

c. Se genera un reporte y se informa a la coordinación y jefatura de informática.

d. Se aísla equipo terminal de la red.(de ser necesario)

e. Se procede a la desinfección del equipo, en dado caso la solución antivirus institucional no lo haga automáticamente.

f. Si existen daños o perdida de información por causa del virus y/o amenaza, se intenta recuperar con la ayuda de utilitarios proporcionados por el fabricante del sistema de protección antivirus.

11.6.5 Si el virus no puede ser eliminado, contacta al proveedor para que determine cuál será la solución para eliminar la amenaza, el soporte por parte del fabricante es por el período contratado y está disponible durante el período contratado, siendo por vía telefónica y asistencia, ya sea en línea, remota o presencial, de ser requerido.

12. Específicas para la asignación y administración de direcciones y conexiones IP públicas.

12.1 El Administrador de la red del IPSFA será el encargado de asignar, controlar y configurar las direcciones IP públicas y privadas del IPSFA.

12.2 Las direcciones IP públicas del IPSFA sólo podrán ser utilizadas dentro de las instalaciones del Instituto y Unidades descentralizadas cuando éstas sean requeridas.

12.3 La asignación de direcciones IP públicas será para:

a. Correo
b. Correo Alterno
c. Firewall
d. Servidor Web
e. Servidor Web Alterno
f. Requerimientos de diferentes áreas del IPSFA para consultas en servidores externos de instituciones del Gobierno.
g. Servicios de Internet que se implementen y que utilicen IP's públicas.

13. Específicas para el Administrador de la red inalámbrica.

13.1 Son funciones del Administrador de la red del IPSFA:

a. Evaluar y analizar las necesidades de instalación de redes inalámbricas en las oficinas del IPSFA y sus Unidades descentralizadas.
b. Recomendar la incorporación de nuevas tecnologías que vayan orientadas a mejorar el rendimiento, capacidad, disponibilidad, seguridad y confiabilidad de la red inalámbrica.
c. Mantener un registro actualizado de todas las redes inalámbricas instaladas en el IPSFA y sus unidades descentralizadas.
d. Monitorear constantemente los equipos instalados para la red inalámbrica, a fin de prevenir o detectar accesos no autorizados.
e. Asignar y modificar las contraseñas de acceso a las redes inalámbricas.

13.2 La instalación de redes inalámbricas se realizará de acuerdo a los siguientes casos o necesidades:

a. Para conexiones de equipos propiedad del IPSFA, cuando no sea posible o viable económicamente el cableado estructurado tradicional.

b. Para brindar servicios de Internet y correo electrónico a empresas visitantes y Entes fiscalizadores.

c. Para brindar servicios de Internet y correo electrónico a miembros del Consejo Directivo del IPSFA.

d. Para brindar el servicio de acceso a la red institucional, NEO-IPSFA y servicios de internet a usuarios IPSFA autorizados.

14. Específicas para la seguridad de la red inalámbrica.

14.1 El acceso a las redes inalámbricas del IPSFA será limitado a los usuarios autorizados por el Departamento de Informática.

14.2 Los "SSID" o puntos de acceso de la red inalámbrica, serán configurados con las restricciones requeridas para su uso, por el Administrador de Red con el Visto Bueno del Jefe del Departamento de Informática.

14.3 El acceso a las redes inalámbricas del IPSFA, con equipos informáticos que no sean propiedad del IPSFA, deberá ser autorizado por el Jefe del Departamento de Informática.

14.4 Los usuarios con acceso a la red inalámbrica, no deberán revelar a otros usuarios las contraseñas de acceso a la red.

15. Específicas para el cambio de contraseña de usuario NEO-IPSFA.

15.1 El Administrador de la base de datos, será el responsable de programar periódicamente la función para realizar el cambio de contraseñas de usuarios del Sistema NEO-IPSFA.

15.2 El usuario NEO-IPSFA que desee cambiar su contraseña eventualmente podrá realizarlo en cualquier momento siguiendo los pasos descritos en la metodología para el cambio de contraseña de Usuario NEO-IPSFA.

16. Específicas de seguridad lógica para el uso de cuentas.

16.1 Todas las contraseñas de cuentas de red institucional tendrán como tiempo de vencimiento cuarenta y dos días, a excepción de las cuentas de servicios o genéricas.

16.2 Toda contraseña de cuenta de red institucional deberán tener como mínimo ocho caracteres en su contraseña.

16.3 Cuentas de servicio o genéricas.

16.3.1 El Administrador de red, será responsable de la creación, modificación, eliminación, administración y/o custodia de las cuentas de servicio o genéricas del Instituto.

16.3.2 Para crear una cuenta, solo puede realizarlo el administrador de red, ingresando al servidor controlador de dominio y al directorio activo.

16.3.3 El cambio, modificar o eliminación de una cuenta de servicio o genérica, solo puede realizarlo el administrador de red, por medio del servidor controlador de dominio, abre el directorio activo, busca la cuenta y cambia, modifica o elimina según sea el caso.

16.3.4 El administrador de red, administra las cuentas por medio de caducidad y ésta tendrá vencimiento según su finalidad de creación, determinando el tiempo de expiración o la longitud de la contraseña.

16.3.5 Será responsabilidad del administrador de red, mantener actualizado el uso de cuentas de servicios o genéricas, manteniendo para ello una constante supervisión.

17. Específicas para el resguardo de los archivos de respaldo elaborados en medios magnéticos.

17.1 Realizados los respaldos de los distintos servidores del Instituto en medios magnéticos, será responsabilidad del Coordinador de Soporte Técnico etiquetarlos y resguardarlos en el lugar dispuesto para tal finalidad.

17.2 El Coordinador de Soporte Técnico, será el responsable del control administrativo de los medios magnéticos resguardados con su respectiva identificación, así como de gestionar un reporte periódico detallando los medios magnéticos resguardados, e informar periódicamente al Jefe del Departamento de Informática.

18. Específicas para solicitar modificaciones o mejoras al sistema informático Radón.

18.1 Toda solicitud de modificación o mejora al sistema informático Radón, deberá realizarse por medio de Memorándum y deberá solicitar el visto bueno del Gerente General.

18.2 Toda solicitud de modificación o mejora al sistema informático Radón, debe ser remitida al Departamento de Informática, siempre que este firmada y sellada por el Gerente General.

18.3 Para iniciar cualquier modificación o mejora al sistema informático Radón, será necesario que el Departamento de Informática en conjunto con las Áreas involucradas, realicen un análisis a lo solicitado diagnosticando posibles problemas, requisitos, u otros; y este deberá comunicar al solicitante la decisión tomada en base a la justificación o razonamiento planteado por la Comisión formada para tal fin.

III. DESCRIPCIÓN DE PUESTOS

A. JEFE DEL DEPARTAMENTO DE INFORMÁTICA

1. IDENTIFICACIÓN

Nombre o Título del Puesto: **Jefe del Departamento de Informática.**
Unidad de Dependencia: **Departamento de Informática.**
Puesto del Superior Inmediato: **Gerente Administrativo.**
Unidad de Dependencia: **Gerencia Administrativa.**
Puestos que supervisa: • **Coordinador de Análisis y Programación.** • **Administrador de la Base de Datos.** • **Administrador de la Red.** • **Coordinador de Soporte Técnico.**

2. PROPÓSITO DEL PUESTO DE TRABAJO

Brindar una plataforma informática óptima y operacional, a los usuarios de todas las áreas del IPSFA y sus Unidades de Negocio, viabilizando sus procesos Institucionales en lo relacionado a la tecnología de la información.

3. UNIDADES Y ELEMENTOS DE COMPETENCIA

3.1 Planificar, coordinar, supervisar y dirigir todas las actividades de la Unidad.

3.1.1 Examinar los requerimientos de mecanización de la información, para evaluar su factibilidad

3.1.2 Establecer los sistemas informáticos a desarrollar y/o dar mantenimiento por el personal bajo su responsabilidad.

3.1.3 Mantener constante comunicación y participación con el personal de su Unidad.

3.1.4 Revisar periódicamente la programación de actividades.

3.1.5 Administrar todas las actividades relacionadas con el Sitio de Contingencia.

3.1.6 Proponer nuevas aplicaciones que sean factibles de implementar y desarrollar en las diferentes unidades del Instituto.

3.1.7 Planificar, dirigir e implementar los diferentes proyectos informáticos a nivel Institucional.

3.1.8 Recomendar la implementación de nuevas tecnologías en beneficio del desarrollo de la Institución.

3.1.9 Planificar, coordinar, supervisar y dirigir las actividades del Departamento de Informática, de las áreas de Soporte Técnico, Administrativa, Administración de Redes, Administración de Base de Datos y Análisis/Programación.

3.1.10 Implementar mecanismos de control para facilitar las labores de Auditoria de Informática.

3.1.11 Elaborar Plan de Capacitación para el personal del Departamento de Informática.

3.1.12 Informar a la Gerencia General de las actividades que realice la Unidad.

3.2 Elaborar el Plan de Trabajo de la Unidad, estableciendo metas a corto, mediano y largo plazo.

3.2.1 Coordinar la elaboración del Plan Estratégico Informático y el Plan de Contingencia y presentarlo a aprobación a la Gerencia General.

3.2.2 Hacer reuniones de trabajo para establecer responsabilidades y dar lineamientos para la formulación del plan operativo y el presupuesto anual.

3.2.3 Revisar y aprobar los planes operativos y el presupuesto del Departamento de Informática

3.2.4 Remitir a la Unidad de Desarrollo Organizacional y Departamento de Presupuesto los planes operativos y el presupuesto autorizado por la Gerencia General.

3.2.5 Dar seguimiento en la ejecución de los Planes Operativos y el presupuesto asignado a el Departamento de Informática.

3.2.6 Presentar propuestas de mejora a los procesos relacionados con las operaciones que se realizan, canalizándolas por medio de la Unidad de Desarrollo Organizacional.

3.3 Velar por el cumplimiento de políticas, normas y procedimientos que le competen al área.

3.3.1 Gestionar con la Unidad de Desarrollo Organizacional la actualización de políticas, normas y procedimientos relacionados con la plataforma informática institucional.

3.3.2 Divulgar las políticas, normas y procedimientos del Departamento de Informática.

3.3.3 Atender lineamientos de trabajo girados por la Gerencia General

3.4 Brindar atención a los Entes Fiscalizadores.

3.4.1 Implementar mecanismos de control sobre las recomendaciones de Entes Fiscalizadores.

INSTITUTO DE PREVISION SOCIAL DE LA FUERZA ARMADA
UNIDAD DE DESARROLLO ORGANIZACIONAL

3.4.2 Proporcionar equipo informático, accesos a Internet, correo electrónico, aplicativos institucionales, etc. a los funcionarios de los diferentes entes fiscalizadores, cuando sean requeridos.

3.4.3 Preparar informes a los diferentes entes fiscalizadores de acuerdo a sus requerimientos de información

3.5 Proponer actualización de hardware y software a nivel institucional.

3.5.1 Desarrollar estudios para proponer la adquisición de nuevos equipos, paquetes de aplicación o versiones más avanzadas de software y actualización de hardware, en base a las necesidades y el plan estratégico institucional.

3.5.2 Efectuar las evaluaciones técnicas y recomendaciones para la factibilidad de adquisición del equipo informático y Software requerido por las diferentes áreas a nivel Institucional, considerando la compatibilidad con la plataforma informática y salvaguardando los intereses institucionales.

3.6 Realizar otras funciones y tareas afines al puesto asignadas por su jefe inmediato.

4. PERFIL DEL PUESTO

4.1 Educación formal

Profesional graduado en Licenciatura en Ciencias de la Computación o Ingeniería en Sistemas.

4.2 Competencias genéricas del puesto

- Planificación y organización del trabajo
- Liderazgo.
- Toma de decisiones.
- Negociación.
- Trabajo en equipo.
- Orientación al cliente.
- Conocimientos y habilidades de Ofimática.

4.3 Competencias específicas o técnicas del puesto

- Sistemas Operativos (Windows y Linux).
- Arquitectura de Computadores.

- Conocimiento sobre normativas legales de Gobierno Electrónico en el contexto de la Modernización del Estado.
- Documentos electrónicos, firma electrónica simple y avanzada.
- Actualización sobre Tecnología de la información.
- Sistemas de seguridad en informática.
- Normativa legal vigente.
- Gestión y administración de Sistemas de redes
- Protocolos de red.
- Gestión y administración de Bases de datos.
- Sistemas de comunicaciones
- Sistemas Web; PHP; Seguridad en Internet
- Inglés avanzado.

4.4 Experiencia laboral requerida

- Cinco años en puestos similares.

5. RESPONSABILIDADES QUE INCLUYE EL PUESTO

5.1 Manejo de personal

- Personal asignado bajo su cargo.

5.2 Equipo de trabajo

- Equipo de trabajo asignado al puesto.

5.3 Fondos y Valores

- Control de las licencias de software adquiridas por el IPSFA

5.4 Responsabilidad en manejo de información.

- Información confidencial de la Unidad y de los sistemas del Instituto.

6. CONDICIONES DE TRABAJO

- Ambiente normal de oficina.

7. RIESGOS DEL CARGO

TIPO DE RIESGO	MOTIVO	CONSECUENCIA
Ocupacionales	Largas jornadas de trabajo.	Stress, Dolores musculares, cansancio físico, problemas gástricos, problemas de la visión, etc.
Operacionales	Daños imprevistos en el	Errores y Fallas en el Sistema

	Hardware y Software Institucional	informático de la institución.
Administrativos	Incumplimiento de las funciones relacionadas a su cargo.	Sanciones administrativas y legales.

8. RELACIONES DE TRABAJO, REQUERIDAS DEL PUESTO

8.1 Relaciones internas

PUESTOS	UNIDADES	CON EL PROPÓSITO DE
Gerente General	Gerencia General	Recibir lineamientos y rendir informes.
Jefe de Unidad	Unidad de Desarrollo Organizacional.	Coordinar la actualización de políticas y normas de Informática.
Gerentes y Jefes de Departamento, Unidad y Coordinadores.	Todas las Unidades del Instituto y Unidades de Negocio.	Asesoría relacionada con el Software y Hardware y el diseño y actualización de sistemas informáticos.

8.2 Relaciones externas

INSTITUCIÓN	CON EL PROPÓSITO DE
Entes Fiscalizadores.	Auditoria a los sistemas Informáticos y coordinar entrega de información.
Proveedores	Coordinación para la atención técnica.

9. ESTÁNDARES DE DESEMPEÑO DEL PUESTO DE TRABAJO

- Asegurar el funcionamiento de las tecnologías, sistemas y equipos informáticos del instituto en forma confiable y continua.
- Elaborar el Plan de desarrollo de Informática a nivel Institucional de acuerdo a prioridades.
- Identificar requerimientos y gestionar la actualización de políticas, normas y procedimientos relacionados con la plataforma informática institucional.
- Número de solicitudes de documentos y/o información de entes fiscalizadores que requieren ser atendidas.
- Recomendar la adquisición de nuevas tecnologías y/o desarrollo de proyectos informáticos de acuerdo a prioridades institucionales.

10. INDICADORES DE DESEMPEÑO

- Cumplimiento de los objetivos y metas establecidas en el PEI y POA.
- Plan Operativo Anual y Presupuesto del Departamento de Informáticas elaborados.
- Manuales, instructivos, planes, metodologías y otros documentos del Departamento de Informática actualizados en forma oportuna.
- Número de solicitudes atendidas de documentos y/o información solicitada por los entes fiscalizadores.
- Adquisición de nuevas tecnologías y/o aseguramiento del desarrollo de nuevos proyectos informáticos de acuerdo a prioridades y políticas institucionales.

B. COORDINADOR DE ANÁLISIS Y PROGRAMACIÓN

1. IDENTIFICACIÓN

Nombre o Título del Puesto: **Coordinador de Análisis y Programación.**
Unidad de Dependencia: **Departamento de Informática.**
Puesto del Superior Inmediato: **Jefe del Departamento de Informática.**
Unidad de Dependencia: **Departamento de Informática.**
Puestos que supervisa: • **Analista Programador.**

2. PROPÓSITO DEL PUESTO DE TRABAJO

Coordinar todas las actividades asociadas al análisis y programación de los sistemas informáticos de la Institución, reportar a la jefatura de Informática el progreso de los proyectos.

3. UNIDADES Y ELEMENTOS DE COMPETENCIA

3.1 Coordinar todas las actividades relacionadas con el análisis y programación de los sistemas del Instituto.

3.1.1. Planificar y organizar los requerimientos del mantenimiento a los aplicativos existentes, así como también a los nuevos proyectos de las áreas.

3.1.2. Recibir y evaluar los requerimientos de programación informática.

3.1.3. Coordinar proyectos y requerimientos informáticos del área de Análisis y

3.1.4. Programación sobre la base de las necesidades de los usuarios y los recursos disponibles.

3.1.5. Establecer estándares para técnicas de programación y documentación.

3.1.6. Supervisar la utilización de estándares en el desarrollo de software.

3.1.7. Supervisar la integración, prueba de programas y puesta en marcha de los Sistemas informáticos.

3.1.8. Mantenerse actualizado en lo relacionado a la plataforma de desarrollo de sistemas Institucionales

3.2 Verificar los Planes de Trabajo detallados para el diseño y programación de aplicaciones, en conjunto con los Analistas Programadores.

3.2.1. Elaborar POA para el Área de Análisis y Programación.

3.2.2. Seguimiento y ejecución de POA y Presupuesto asignado a el Departamento de Informática.

3.2.3. Participar en la elaboración de documentos institucionales relacionados a el Departamento de Informática.

3.2.4. Atención a Entes Fiscalizadores.

3.2.5. Coordinar y remitir informes a entes fiscalizadores del área de Análisis y Programación.

3.2.6. Realizar Informe de Actividades Relevantes mensualmente.

3.2.7. Elaborar POA para el Área de Administración de Bases de Datos.

3.3 Realizar otras funciones y tareas afines al puesto asignadas por su jefe inmediato.

4. PERFIL DEL PUESTO

4.1 Educación formal

Profesional Graduado en el área de Licenciatura en Ciencias de la Computación, Ingeniería en Sistema o áreas afines.

Experiencia comprobada con estudios de especialización en la herramienta de desarrollo y base de datos.

4.2 Competencias genéricas del puesto

- Integridad.
- Liderazgo.
- Trabajo en equipo.
- Responsabilidad.
- Planificación y organización del trabajo.
- Orden y Calidad.
- Atención y Servicio al Cliente.
- Discreción.
- Conocimiento y Habilidades de Ofimática.

4.3 Competencias específicas o técnicas del puesto

- Conocimiento de paquetes de computación en ambiente Windows: hojas electrónicas, procesadores de texto y utilitarios.

- Amplio conocimiento de la Plataforma de desarrollo de Proyectos de Sistemas
- Institucionales.
- Dominio de Lenguajes de Programación 4gl
- Conocimientos Básicos de Linux.
- Conocimiento de Base de Datos relacionadas.
- Redacción de informes técnicos
- Dominio del Inglés Técnico
- Conocimiento en redes
- Conocimiento en la ley IPSFA

4.4 Experiencia laboral requerida

- Tres años de experiencia en programación, de preferencia como coordinador de Proyectos de Sistemas y o como Administrador de Base de Datos (DBA).

5. RESPONSABILIDADES QUE INCLUYE EL PUESTO

5.1 Manejo de personal

- Ninguno.

5.2 Equipo de trabajo

- Equipo asignado bajo su responsabilidad.

5.3 Fondos y Valores

- Ninguno.

5.4 Responsabilidad en manejo de información.

- Acceso absoluto y completo de información relacionada con todos los sistemas informáticos de la institución.

5.5 Alto Grado de autonomía

Alto Grado de autonomía en las decisiones relacionadas con el desarrollo de sistemas

5.6 Responsabilidad

Responsabilidad sobre procesos de trabajo a nivel institucional, las consecuencias de error pueden perjudicar a toda la institución

6. CONDICIONES DE TRABAJO

- Condiciones ambientales de óptima temperatura, sin ruidos.

7. RIESGOS DEL CARGO

TIPO DE RIESGO	MOTIVO	CONSECUENCIA
Ocupacional	Enfermedad ocupacional	• Estrés • Artritis • Gastritis • Problemas visuales. • Lesión del Túnel Carpiano. • Problemas de vías respiratorias.
Administrativo	Incumplimiento de funciones específicas del puesto.	• Sanciones Administrativas y legales.

8. RELACIONES DE TRABAJO, REQUERIDAS DEL PUESTO

8.1 Relaciones internas

PUESTOS	UNIDADES	CON EL PROPÓSITO DE
Jefe de Departamento de Informática.	Informática	Establecer plan de trabajo.
Analistas Programadores	Informática	Apoyo de requerimientos.
Coordinador y Técnicos de Soporte	Informática	Apoyo de requerimientos.
Jefes y Coordinadores	Todas las unidades organizacionales del IPSFA.	Atención de requerimientos.

8.2 Relaciones externas

INSTITUCIÓN	CON EL PROPÓSITO DE
Entes Fiscalizadores	Auditorias Informáticas
Proveedores	Coordinar y supervisar las relaciones con la empresa contratada por el mantenimiento Oracle.
Bancos	Coordinar el envío y recepción de información.

9. ESTÁNDARES DE DESEMPEÑO DEL PUESTO DE TRABAJO

- Mantener en óptimas condiciones el funcionamiento de la base de datos y servidores de aplicativos del instituto.
- Elaborar el plan de trabajo relacionado a la base de datos, al análisis y programación de los sistemas del instituto.

UNIDAD DE DESARROLLO ORGANIZACIONAL

10. INDICADORES DE DESEMPEÑO

- Tiempo de funcionamiento activo del servidor de base de datos y servidor de aplicativos del instituto.
- Plan de trabajo de base de datos, análisis y programación de los sistemas del instituto elaborado.

C. ANALISTA PROGRAMADOR

1. IDENTIFICACIÓN

Nombre o Título del Puesto: **Analista Programador.**
Unidad de Dependencia: **Departamento de Informática.**
Puesto del Superior Inmediato: **Coordinador de Análisis y Programación.**
Unidad de Dependencia: **Departamento de Informática.**
Puestos que supervisa: • **Ninguno.**

2. PROPÓSITO DEL PUESTO DE TRABAJO

Desarrollar y mantener los sistemas de información en óptimas condiciones para brindar a las diferentes unidades del IPSFA, el soporte para el cumplimiento de los objetivos institucionales.

3. UNIDADES Y ELEMENTOS DE COMPETENCIA

3.1 Realizar el desarrollo de nuevas aplicaciones requeridas por las diferentes áreas del IPSFA, con base al ciclo de vida de los sistemas.

3.1.1 Realizar investigaciones y entrevistas a los usuarios para el establecimiento de los requerimientos.

3.1.2 Elaborar Plan de Trabajo detallado para el diseño y programación de aplicaciones nuevas, en conjunto con la coordinación del área.

3.1.3 Elaborar programas en base a los requerimientos solicitados.

3.1.4 Coordinar las pruebas con los usuarios de las aplicaciones en desarrollo.

3.1.5 Elaborar el manual del usuario y documentación técnica del aplicativo desarrollado.

3.1.6 Preparar y desarrollar capacitaciones a usuarios de los Sistemas.

3.1.7 Coordinar la puesta en producción de las aplicaciones desarrolladas.

3.2 Realizar el mantenimiento adecuado a las aplicaciones, de acuerdo a las necesidades del usuario.

3.2.1. Realizar el análisis de requerimiento.

3.2.2. Planear las modificaciones relacionadas con el requerimiento.

3.2.3. Desarrollar las modificaciones requeridas.

3.2.4. Realizar las pruebas de las modificaciones a los aplicativos.

3.2.5. Realizar la inducción y capacitación a los usuarios.

3.2.6. Actualizar la documentación técnica y manual de usuario.

3.2.7. Efectuar la puesta en producción.

3.2.8. Mantener actualizada la información de requerimientos.

3.2.9. 3.3.1 Realizar el registro, seguimiento y cierre de los requerimientos asignados.

3.3 Brindar soporte técnico a los usuarios en la utilización de los aplicativos.

3.4.1 Atender consultas telefónicas, asistencias en el lugar, correo electrónico, etc.

3.4 Realizar otras funciones y tareas afines al puesto asignadas por su jefe inmediato.

4 PERFIL DEL PUESTO

4.1 Educación formal

Profesional graduado en el área de Licenciatura en Ciencias de la Computación, Ingeniería en Sistemas o experiencia equivalente con 4º año de estudios como mínimo.

4.2 Competencias genéricas del puesto

- Iniciativa y creatividad
- Capacidad de análisis y síntesis.
- Objetividad
- Orientación al cliente
- Habilidad para comunicarse verbal y escrita
- Trabajo en equipo.
- Conocimiento y habilidades de ofimática

4.3 Competencias específicas o técnicas del puesto

- Amplio conocimiento de la Plataforma de desarrollo de Proyectos de Sistemas Institucionales.
- Dominio de lenguaje de programación.
- Conocimiento de Base de Datos relacionadas.
- Redacción de informes técnicos
- Dominio del Inglés Técnico

4.4 Experiencia laboral requerida

- Dos años como mínimo en puestos similares.

5 RESPONSABILIDADES QUE INCLUYE EL PUESTO

5.1 Manejo de personal

- Ninguno

5.2 Equipo de trabajo

- Equipo de cómputo como herramientas de trabajo.

5.3 Fondos y Valores

- Ninguno

5.4 Responsabilidad en manejo de información.

- Manejo de información confidencial relacionado a todos los sistemas informáticos de la institución.

6 CONDICIONES DE TRABAJO

- Condiciones de temperatura óptima y sin interferencias de ruidos.

7 RIESGOS DEL CARGO

TIPO DE RIESGO	MOTIVO	CONSECUENCIA
Ocupacional	Enfermedad ocupacional	• Estrés • Artritis • Gastritis • Problemas visuales. • Lesión del Túnel Carpiano. • Problemas de vías respiratorias.
Administrativo	Incumplimiento de Políticas y Normas informáticas.	• Sanciones penales y legales.

8 RELACIONES DE TRABAJO, REQUERIDAS DEL PUESTO

8.1 Relaciones internas

PUESTOS	UNIDADES	CON EL PROPÓSITO DE
Jefe de Departamento de Informática	Departamento de Informática	Supervisión y control de actividades.
Jefes y/o Coordinadores de áreas	Áreas organizacionales del IPSFA; relacionadas con el área de desarrollo asignada	Coordinación de requerimientos en aplicativos.

Usuarios finales	Áreas organizacionales del IPSFA; relacionadas con el área de desarrollo asignada	Atención a requerimientos y soporte en el uso de los aplicativos.

8.2 Relaciones externas

INSTITUCIÓN	CON EL PROPÓSITO DE
Entes Fiscalizadores	Auditorias Informáticas

9 ESTÁNDARES DE DESEMPEÑO DEL PUESTO DE TRABAJO

- Desarrollo de nuevas aplicaciones requeridas por las diferentes Áreas del instituto.
- Desarrollo y mantenimiento de aplicativos.
- Número de requerimientos, asistencias y/o consultas en lo relacionado a brindar soporte técnico de los aplicativos informáticos.

10 INDICADORES DE DESEMPEÑO

- Número de requerimientos atendidos eficiente y oportunamente.
- Mantenimiento de aplicativos eficiente y oportunamente.
- Atención oportuna de requerimientos, asistencia y/o consultas de las diferentes Áreas del instituto en forma oportuna y confiable.

D. ADMINISTRADOR DE LA RED

1. IDENTIFICACIÓN

Nombre o Título del Puesto: **Administrador de la Red.**
Unidad de Dependencia: **Departamento de Informática.**
Puesto del Superior Inmediato: **Jefe del Departamento de Informática.**
Unidad de Dependencia: **Departamento de Informática.**
Puestos que supervisa: • **Administrador de la Red Jr.**

2. PROPÓSITO DEL PUESTO DE TRABAJO

Planificar, organizar, controlar y monitorear la Red Institucional; proponer políticas de seguridad para los usuarios, brindar derechos de acceso a los diferentes aplicativos en la red, administración de la red, servidores y equipos de comunicación con el propósito de asegurar la buena conectividad de los equipos de comunicación, servidores y las diferentes estaciones de trabajo del IPSFA.

3. UNIDADES Y ELEMENTOS DE COMPETENCIA

3.1 Administración de servidores.

3.1.1 Proporcionar configuración y seguridad de los servidores.

3.1.2 Monitorear los servidores.

3.1.3 Implementar políticas.

3.1.4 Crear usuarios de red y correo electrónico.

3.1.5 Implementar normas de seguridad para la granja de servidores y toda la información contenida en estos.

3.1.6 Crear acceso a Internet.

3.1.7 Ejecutar el mantenimiento preventivo y correctivo a los servidores.

3.2 Administración de Red de datos institucional.

3.2.1 Monitoreo de la conectividad y comunicación entre redes, servidores y clientes internos y externos.

3.2.2 Monitoreo y afinamiento de la red para asegurar aceptables niveles de desempeño de la red.

3.2.3 Ejecutar los mantenimientos preventivos y correctivos a los equipos de comunicación.

3.2.4 Ejecutar el mantenimiento preventivo y correctivo a la red institucional.

3.2.5 Mantener en óptimas condiciones la configuración y seguridad de la red.

3.2.6 Mantener la arquitectura de la red institucional según estándares.

3.2.7 Administrar y controlar las direcciones IP públicas y privadas de la red institucional.

3.2.8 Analizar junto con el Jefe del Departamento de Informática las solicitudes de servicios de red requeridas por las diferentes áreas del IPSFA.

3.2.9 Atender todas las dificultades y soluciones relacionadas con el direccionamiento de la red, la conectividad general de las máquinas PC y la configuración de dispositivos de red (cableados e inalámbricos), así como IP´s, mascara de red, gateway, DNS, etc.

3.2.10 Llevar un control de las solicitudes de servicios de red atendidas y soluciones realizadas

3.2.11 Controlar los servicios disponibles de la red para todos los usuarios IPSFA.

3.3 Colaborar en la elaboración del POA del Departamento de Informática, en las actividades que le corresponden al Administrador de Red.

3.3.1 Realizar Informe de Actividades relevantes mensualmente.

3.4 Realizar otras funciones y tareas afines al puesto asignadas por su jefe inmediato.

4. PERFIL DEL PUESTO

4.1 Educación formal

Profesional en el área de Licenciatura en Ciencias de la Computación, Ingeniería en Sistemas, o experiencia equivalente comprobada.

4.2 Competencias genéricas del puesto

- Integridad.
- Liderazgo.
- Trabajo en equipo.
- Responsabilidad.
- Planificación y organización del trabajo.
- Orden y Calidad.

- Atención y Servicio al Cliente.
- Discreción.
- Conocimiento y Habilidades de Ofimática.

4.3 Competencias específicas o técnicas del puesto

- Dominio de configuración y administración de equipos de comunicación, servidores, switches, routers, firewall y herramientas para el mantenimiento de equipos informáticos.
- Dominio de Sistemas Operativos, Windows, Linux y Unix
- Diseño y configuración de redes.
- Administración de redes y servidores.
- Dominio de protocolos de comunicación.
- Dominio de la tecnología de Fibra Óptica y Par Trenzado

4.4 Experiencia laboral requerida

- Dos años como mínimo en puestos similares.

5. RESPONSABILIDADES QUE INCLUYE EL PUESTO

5.1 Manejo de personal

- Personal bajo su cargo.

5.2 Equipo de trabajo

- Equipo asignado bajo su responsabilidad.

5.3 Fondos y Valores

- Ninguno.

5.4 Responsabilidad en manejo de información.

- Manejo de información confidencial relacionado a todos los sistemas informáticos de la institución.

6. CONDICIONES DE TRABAJO

- Condiciones ambientales de óptima temperatura, sin ruidos.

7. RIESGOS DEL CARGO

TIPO DE RIESGO	MOTIVO	CONSECUENCIA
Ocupacional	Enfermedad ocupacional	• Estrés • Artritis • Gastritis • Problemas visuales. • Lesión del Túnel Carpiano. • Problemas de vías respiratorias.
Administrativo	Incumplimiento de Políticas y Normas informáticas.	• Sanciones penales y legales.

8. RELACIONES DE TRABAJO, REQUERIDAS DEL PUESTO

8.1 Relaciones internas

PUESTOS	UNIDADES	CON EL PROPÓSITO DE
Jefe de Departamento de Informática	Informática	Establecer plan de trabajo y proyectos. Informes POA del área.
Analistas Programadores	Informática	Solicitud y apoyo de requerimientos.
Soporte Técnico	Informática	Solicitud y apoyo de requerimientos.
Administrador de Base de Datos	Informática	Solicitud y apoyo de requerimientos.
Jefes y Coordinadores	Todas las unidades organizacionales del IPSFA.	Atención de requerimientos.

8.2 Relaciones externas

INSTITUCIÓN	CON EL PROPÓSITO DE
Proveedores	Coordinar y supervisar las relaciones con la empresa contratada como sitio de contingencia. Proveedores de Internet y VPN.
Entes Fiscalizadores	Auditorias Informáticas

9. ESTÁNDARES DE DESEMPEÑO DEL PUESTO DE TRABAJO

- Número de monitoreo realizado a los servidores del instituto.
- Mantener en óptimas condiciones de seguridad, conectividad y funcionamiento la red de datos institucional.
- Elaborar el plan de trabajo relacionado a las actividades relacionadas a la administración de los servidores y red de datos institucional.

10. INDICADORES DE DESEMPEÑO

- Asegurar el funcionamiento de los servidores del instituto en forma confiable y continua.
- Asegurar el funcionamiento de la red de datos institucional en forma confiable y continua.
- Plan de trabajo de las actividades relacionadas a la administración de los servidores red de datos del instituto elaborado.

E. ADMINISTRADOR DE LA RED JR.

1. IDENTIFICACIÓN

Nombre o Título del Puesto: **Administrador de la Red Jr.**
Unidad de Dependencia: **Departamento de Informática.**
Puesto del superior inmediato: **Administrador de la Red.**
Unidad de Dependencia: **Departamento de Informática.**
Puestos que supervisa: • **Ninguno.**

2. PROPÓSITO DEL PUESTO DE TRABAJO

Desarrollar eficientemente las tareas de apoyo enfocadas al control y monitoreo de la Red Institucional, así como la administración de las políticas de seguridad para los equipos informáticos del IPSFA a través del Antivirus. Atender las solicitudes de mejora del Sitio Web y realizar el mantenimiento requerido para el buen funcionamiento de este.

3. UNIDADES Y ELEMENTOS DE COMPETENCIA

3.1 Administración de servidores.

3.1.1 Monitorear los servidores.

3.1.2 Crear usuarios de red y correo electrónico.

3.1.3 Crear acceso a Internet.

3.1.4 Apoyar en las labores de mantenimiento preventivo y correctivo a los servidores.

3.2 Administración de Red de datos institucional.

3.2.1 Monitoreo de la conectividad y comunicación entre redes, servidores y clientes internos y externos.

3.2.2 Apoyar en las labores de mantenimiento preventivo y correctivo de los equipos de comunicación.

3.2.3 Apoyar en las labores de mantenimiento preventivo y correctivo a la red institucional.

3.2.4 Monitorear la configuración y seguridad de la red.

3.2.5 Monitorear la red institucional según estándares.

3.2.6 Monitorear las direcciones IP públicas y privadas de la red institucional.

3.2.7 Apoyar en la atención de todas las dificultades relacionadas con el direccionamiento de la red, la conectividad general de las máquinas PC y la configuración de dispositivos de red (cableados e inalámbricos), así como IP´s, mascara de red, gateway, DNS, etc.

3.2.8 Colaborar en el control de las solicitudes de servicios de red atendidas y soluciones realizadas

3.2.9 Monitorear los servicios disponibles de la red para todos los usuarios IPSFA.

3.3 Administración del Antivirus

3.3.1. Instalar y configurar la consola para la administración del software Antivirus.

3.3.2. Instalar y configurar el servidor web y aplicaciones web.

3.3.3. Implementar y controlar las políticas de seguridad en la consola antivirus, servidor antivirus y servidor web.

3.3.4. Reportar y capacitar al personal IPSFA sobre amenazas latentes relacionadas con el servidor web y demás aplicativos.

3.4 Colaborar en la elaboración del POA del Departamento de Informática, en las actividades que le corresponden al Administrador de Red.

3.4.1 Realizar Informe de Actividades relevantes mensualmente.

3.4 Realizar otras funciones y tareas afines al puesto asignadas por su jefe inmediato

4. PERFIL DEL PUESTO

4.1 Educación formal

Estudiante Universitario a nivel de cuarto Año de las carreras de Licenciatura en Ciencias de la Computación, Ingeniería en Sistemas.

4.2 Competencias genéricas del puesto

- Integridad.
- Liderazgo.
- Trabajo en equipo.
- Responsabilidad.
- Planificación y organización del trabajo.
- Orden y Calidad.
- Atención y Servicio al Cliente.

UNIDAD DE DESARROLLO ORGANIZACIONAL

- Discreción.
- Conocimiento y Habilidades de Ofimática.

4.3 Competencias específicas o técnicas del puesto

- Dominio de configuración y administración de equipos de comunicación, servidores, switches, routers, firewall y herramientas para el mantenimiento de equipos informáticos.
- Dominio de Sistemas Operativos, Windows, Linux y Unix
- Diseño y configuración de redes.
- Administración de redes y servidores.
- Dominio de protocolos de comunicación.
- Dominio de la tecnología de Fibra Óptica y Par Trenzado

4.4 Experiencia laboral requerida

- Dos años como mínimo en puestos similares.

5. RESPONSABILIDADES QUE INCLUYE EL PUESTO

5.1 Manejo de personal

- Ninguno.

5.2 Equipo de trabajo

- Equipo asignado bajo su responsabilidad.

5.3 Fondos y Valores

- Ninguno.

5.4 Responsabilidad en manejo de información.

- Manejo de información confidencial relacionado a todos los sistemas informáticos de la institución.

6. CONDICIONES DE TRABAJO

- Condiciones ambientales de óptima temperatura, sin ruidos.

7. RIESGOS DEL CARGO

TIPO DE RIESGO	MOTIVO	CONSECUENCIA
Ocupacional	Enfermedad ocupacional	• Estrés • Artritis • Gastritis • Problemas visuales. • Lesión del Túnel Carpiano. • Problemas de vías respiratorias.
Administrativo	Incumplimiento de Políticas y Normas informáticas.	• Sanciones penales y legales.

8. RELACIONES DE TRABAJO, REQUERIDAS DEL PUESTO

8.1 Relaciones internas

PUESTOS	UNIDADES	CON EL PROPÓSITO DE
Jefe de Departamento de Informática	Informática	Establecer plan de trabajo y proyectos. Informes POA del área.
Analistas Programadores	Informática	Solicitud y apoyo de requerimientos.
Soporte Técnico	Informática	Solicitud y apoyo de requerimientos.
Administrador de Base de Datos	Informática	Solicitud y apoyo de requerimientos.
Jefes y Coordinadores	Todas las unidades organizacionales del IPSFA.	Atención de requerimientos.

8.2 Relaciones externas

INSTITUCIÓN	CON EL PROPÓSITO DE
Entes Fiscalizadores	Auditorias Informáticas

9. ESTÁNDARES DE DESEMPEÑO DEL PUESTO DE TRABAJO

- Número de monitoreo realizado a los servidores del instituto.
- Mantener en óptimas condiciones de seguridad, conectividad y funcionamiento la red de datos institucional.
- Actualizar el Antivirus a nivel institucional.
- Elaborar el plan de trabajo relacionado a las actividades de administración de los servidores y red de datos institucional.

10. INDICADORES DE DESEMPEÑO

- Asegurar el funcionamiento de los servidores del instituto en forma confiable y continua.
- Asegurar el funcionamiento de la red de datos institucional en forma confiable y continua.
- Red y sitio web institucional protegidos con antivirus actualizado.
- Plan de trabajo de las actividades relacionadas a la administración de los servidores red de datos del instituto elaborado.

F. COORDINADOR DE SOPORTE TÉCNICO

1. IDENTIFICACIÓN

Nombre o Título del Puesto: **Coordinador de Soporte Técnico.**
Unidad de Dependencia: **Departamento de Informática.**
Puesto del superior inmediato: **Jefe del Departamento de Informática.**
Unidad de Dependencia: **Departamento de Informática.**
Puestos que supervisa: • **Técnico de Soporte.**

2. PROPÓSITO DEL PUESTO DE TRABAJO

Coordinar la atención a usuarios en el uso de hardware y software, los mantenimientos preventivos y correctivos de los equipos de cómputo del IPSFA, áreas descentralizadas y unidades de negocio, así como llevar control de los equipos informáticos.

3. UNIDADES Y ELEMENTOS DE COMPETENCIA

3.1 Coordinar todas las actividades encaminadas a que el hardware y software se encuentren en perfecto funcionamiento.

3.1.1 Supervisar el plan de trabajo para el mantenimiento preventivo/correctivo a los equipos informáticos que realizan otras empresas.

3.1.2 Establecer y ejecutar el plan de trabajo del mantenimiento preventivo desarrollado por el personal de Soporte Técnico.

3.2 Mantener el control sobre el hardware y software propiedad del Instituto.

3.2.1 Administrar el Sistema de control de Periféricos (Aplicación de control de equipos informáticos institucionales).

3.2.2 Realizar el inventario de Hardware en forma semestral de todo el equipo informático asignado a el Departamento de Informática

3.2.3 Resguardar y controlar el software en los equipos donde se encuentran instalados.

3.2.4 Administrar el software operativo y utilitario del Instituto.

3.3 Controlar y mantener actualizado el resguardo de información

3.3.1 Dar mantenimiento al control de Backus.

3.3.2 Resguardar y restaurar la información

3.3.2 Resguardar los tapes en el lugar asignado para esta actividad.

3.3.3 Administrar el proceso de envío y recepción de respaldos al sitio de contingencia

3.4 Elaborar POA para el Área de Soporte Técnico.

3.4.1 Realizar Informe de Actividades Relevantes mensualmente.

3.5 Control del Antivirus Institucional.

3.6.1 Mantener actualizado el servidor de antivirus y todos los equipos del IPSFA.

3.6 Realizar otras funciones y tareas afines al puesto asignadas por su jefe inmediato.

4. PERFIL DEL PUESTO

4.1 Educación formal

Profesional graduado en el área de Licenciatura en Ciencias de la Computación, Ingeniería en Sistemas o experiencia equivalente comprobada.

4.2 Competencias genéricas del puesto

- Integridad.
- Liderazgo.
- Trabajo en equipo.
- Responsabilidad.
- Planificación y organización del trabajo.
- Orden y Calidad.
- Atención y Servicio al Cliente.
- Discreción.
- Conocimiento y Habilidades de Ofimática.

4.3 Competencias específicas o técnicas del puesto

- Conocimiento de paquetes de computación en ambiente Windows 2000, XP Pro y Linux, hojas electrónicas, procesadores de texto y utilitarios para plataformas de equipos tanto personales como para servidores.
- Conocimientos de sistema operativo Windows y Linux.
- Conocimientos de Hardware.

4.4 Experiencia laboral requerida

- Dos años como mínimo en puestos similares.

5. RESPONSABILIDADES QUE INCLUYE EL PUESTO

5.1 Manejo de personal

- Personal asignado bajo su responsabilidad

5.2 Equipo de trabajo

- Equipo asignado bajo su responsabilidad.

5.3 Fondos y Valores

- Control de las licencias de software adquiridas por el IPSFA

5.4 Responsabilidad en manejo de información.

- Manejo de información confidencial relacionado a todos los sistemas informáticos de la institución.

6. CONDICIONES DE TRABAJO

- Condiciones ambientales de óptima temperatura.

7. RIESGOS DEL CARGO

TIPO DE RIESGO	MOTIVO	CONSECUENCIA
Ocupacional	Enfermedad ocupacional	• Estrés • Artritis • Gastritis • Problemas visuales. • Lesión del Túnel Carpiano. • Problemas de vías respiratorias.
Administrativo	Incumplimiento de funciones específicas del puesto.	• Sanciones Administrativas y legales.

UNIDAD DE DESARROLLO ORGANIZACIONAL

8. RELACIONES DE TRABAJO, REQUERIDAS DEL PUESTO

8.1 Relaciones internas

PUESTOS	UNIDADES	CON EL PROPÓSITO DE
Jefe de Departamento de Informática	Departamento de Informática	Coordinación en la elaboración de planes de trabajo correspondientes al área.
Jefes y/o Coordinadores de áreas	Áreas organizacionales del IPSFA; relacionadas con el área de desarrollo asignada.	Coordinación en la atención a requerimientos.
Usuarios finales	Áreas organizacionales del IPSFA; relacionadas con el área de desarrollo asignada.	Coordinación del personal asignado para el soporte técnico a usuarios.

8.2 Relaciones externas

INSTITUCIÓN	CON EL PROPÓSITO DE
Empresas contratadas para el mantenimiento preventivo y correctivo de equipo de impresión.	Coordinar el mantenimiento de equipo informático.
Proveedores de servicio	Coordinar él envió y traslado de respaldos al sitio de contingencia.

9. ESTÁNDARES DE DESEMPEÑO DEL PUESTO DE TRABAJO

- Cumplimiento del plan de mantenimiento preventivo de equipo de cómputo.
- Cumplimiento del plan de inventario semestral.
- Resguardo de información de forma eficaz y eficiente.
- Elaborar el plan de trabajo relacionado a las actividades de soporte técnico.
- Actualizar el Antivirus a nivel institucional.

10. INDICADORES DE DESEMPEÑO

- Cantidad de equipos de cómputo con mantenimiento completado a satisfacción.
- Inventarios de hardware y software actualizado.
- Información institucional resguardada en forma oportuna en el lugar asignado para tal finalidad.
- Plan de trabajo de las actividades relacionadas a soporte técnico.
- Red y sitio web institucional protegidos con antivirus actualizado.

G. TÉCNICO DE SOPORTE

1. IDENTIFICACIÓN

Nombre o Título del Puesto: **Técnico de Soporte.**
Unidad de Dependencia: **Departamento de Informática.**
Puesto del superior inmediato: **Coordinador de Soporte Técnico.**
Unidad de Dependencia: **Departamento de Informática.**
Puestos que supervisa: • **Ninguno.**

2. PROPÓSITO DEL PUESTO DE TRABAJO

Operar y velar por el perfecto funcionamiento y configuración del equipo informático con la finalidad de satisfacer las necesidades de los usuarios.

3. UNIDADES Y ELEMENTOS DE COMPETENCIA

3.1 Realizar y resguardar los respaldos de información para garantizar la restauración de información confiable en caso de contingencias presentadas en la operación de la red y aplicativos.

3.1.1 Controlar y resguardar los respaldos que se tienen en el Sitio de contingencia.

3.2 Implementar el plan de mantenimiento preventivo de equipo informático a nivel Institucional.

3.2.1 Efectuar mantenimiento preventivo y correctivo a las computadoras personales e impresores a nivel Institucional.

3.2.2 Dar seguimiento a las fallas de hardware y software que pudieran presentarse en los equipos informáticos del Instituto.

3.2.3 Mantener estadísticas de los problemas que se presentan con el equipo de cómputo.

3.2.4 Recibir, instalar y trasladar equipo de cómputo a las diferentes unidades organizativas del IPSFA.

3.2.5 Recibir y entregar equipo informático a las áreas asignadas.

3.2.6 Configuración de los equipos informático a ser entregados.

3.2.7 Instalar software y hardware para computadoras personales a las distintas Unidades.

3.3 Brindar soporte técnico a los usuarios en la operación de hardware y software.

3.3.1 Asistir técnicamente a los usuarios tanto en software como en hardware de computadoras personales.

3.4 Realizar otras funciones y tareas afines al puesto asignadas por su jefe inmediato.

4. PERFIL DEL PUESTO

4.1 Educación formal

- Técnico Operador de Computadoras o estudiante a nivel de tercer año de las carreras de Licenciatura en Ciencias de la computación, Ingeniería en sistemas o carreras afines.
- Estudios técnicos o certificaciones en redes Linux, mantenimiento de computadoras o computación administrativa.

4.2 Competencias genéricas del puesto

- Orden y Calidad
- Responsabilidad
- Iniciativa
- Orientación al Cliente
- Integridad.
- Discreción
- Conocimientos y habilidades de ofimática

4.3 Competencias específicas o técnicas del puesto

- Conocimiento de paquetes de computación en ambiente Windows 2000, XP Pro y Linux: hojas electrónicas, procesadores de texto y utilitarios para plataformas de equipos tanto personales como para servidores.
- Conocimiento para configurar y administrar controladores de dominio y equipos locales, cuentas de usuarios y de grupo, asignar contraseñas y permisos.
- Conocimientos sólidos de sistema operativo Windows y Linux.
- Protocolos de comunicación que se utilizan en los equipos de PCs.
- Habilidad para las matemáticas y la lógica.
- Conocimiento para realizar reparaciones, configuraciones y mantenimiento de diferentes tipos de equipos informáticos.

4.4 Experiencia laboral requerida

- Un año como mínimo en puestos similares.

5. RESPONSABILIDADES QUE INCLUYE EL PUESTO

5.1 Manejo de personal

- Ninguno

5.2 Equipo de trabajo

- Equipo asignado al puesto

5.3 Fondos y Valores

- Ninguno

5.4 Responsabilidad en manejo de información.

- Ninguna.

6. CONDICIONES DE TRABAJO

- Condiciones normales de oficina en el momento de dar mantenimiento de software.
- Atención en las diferentes instalaciones del IPSFA.

7. RIESGOS DEL CARGO

TIPO DE RIESGO	MOTIVO	CONSECUENCIA
Ocupacional	Enfermedades ocupacionales. Enfermedades de vías respiratorias	• Estrés • Artritis • Gastritis • Problemas visuales. • Lesión del Túnel Carpiano • Problemas de vías respiratorias. • Dolores musculares • Lesiones del cuello y espalda.
Administrativo	Incumplimiento de funciones específicas del puesto.	• Sanciones Administrativas y legales.

8. RELACIONES DE TRABAJO, REQUERIDAS DEL PUESTO

8.1 Relaciones internas

PUESTOS	UNIDADES	CON EL PROPÓSITO DE
Jefe de Departamento de Informática	Departamento de Informática	Coordinación en la elaboración de planes de trabajo correspondientes al área.
Jefes y/o Coordinadores de áreas	Áreas organizacionales del IPSFA; relacionadas con el área de desarrollo asignada.	Coordinación en la atención a requerimientos.
Usuarios finales	Áreas organizacionales del IPSFA; relacionadas con el área de desarrollo asignada.	Coordinación del personal asignado para el soporte técnico a usuarios.

8.2 Relaciones externas

INSTITUCIÓN	CON EL PROPÓSITO DE
Proveedores de servicio	Coordinar la compra de hardware para las Pc´s del Instituto.

9. ESTÁNDARES DE DESEMPEÑO DEL PUESTO DE TRABAJO

- Resguardo de información de forma eficaz y eficiente.
- Cumplimiento del plan de mantenimiento preventivo de equipo informático.
- Número de requerimientos, asistencias y/o consultas en lo relacionado a brindar soporte técnico en la operación de hardware y software.

10. INDICADORES DE DESEMPEÑO

- Información institucional resguardada en forma oportuna en el lugar asignado para tal finalidad.
- Número de equipos informáticos con mantenimiento preventivo realizado.
- Atención oportuna de requerimientos, asistencia y/o consultas de las diferentes Áreas del instituto en forma oportuna y confiable.

H. ADMINISTRADOR DE BASE DE DATOS

1. IDENTIFICACIÓN

Nombre o Título del Puesto: **Administrador de Base de Datos.**
Unidad de Dependencia: **Departamento de Informática.**
Puesto del Superior Inmediato: **Jefe del Departamento de Informática.**
Unidad: **Departamento de Informática.**
Puestos que supervisa: • **Ninguno.**

2. PROPÓSITO DEL PUESTO DE TRABAJO

Mantener la integridad y la disponibilidad de la Base de Datos Institucional para todos los aplicativos, así como de las diferentes instancias de desarrollo que existan.

3. UNIDADES Y ELEMENTOS DE COMPETENCIA

3.1 Definir, establecer, ejecutar esquemas (Organización física de la base de datos), políticas de seguridad y generación de DMP (archivos de Base de Datos) de la base de datos.

3.1.1 Definir la estructura de almacenamiento y del método de acceso.

3.1.2 Modificar el esquema y la organización física de la Base de Datos.

3.1.3 Establecer y ejecutar políticas de seguridad de la base datos.

3.1.4 Establecer las restricciones de seguridad sobre la base de datos.

3.1.5 Generación de DMP (Archivos de Base de Datos).

3.1.6 Optimizar la programación, desarrollo de sistemas.

3.1.7 Emplear herramientas de optimización sobre query´s con instrucciones PLSQL.

3.2 Mantener la base de datos optimizada y realizar el mantenimiento preventivo a los objetos de la base de datos.

3.2.1 Especificar las restricciones de integridad referencial a los Analistas Programadores en coordinación con el Coordinador de Análisis y Programación.

3.2.2 Coordinar con proveedor las asistencias técnicas a la base de datos de ser estas necesarias.

3.2.3 Realizar el mantenimiento a los Objetos de la Base de Datos.

3.2.4 Crear, modificar y eliminar objetos en la Base de Datos a demanda.

3.2.5 Proporcionar mantenimiento de usuarios, roles, grupos y perfiles.

3.2.6 Transferencia de Información al Sitio de contingencia

3.2.7 Copia de archivos DMP hacia servidores ubicados en el sitio de contingencia.

3.3 Elaborar POA para el Área de Administración de Bases de Datos.

3.5.1 Realizar Informe de Actividades Relevantes mensualmente.

3.4 Realizar otras funciones y tareas afines al puesto asignadas por su jefe inmediato.

4. PERFIL DEL PUESTO

4.1 Educación formal

Profesional graduado en Licenciatura de Ciencias de Computación o Ingeniería de sistemas con experiencia comprobada.

4.2 Competencias genéricas del puesto

- Integridad.
- Liderazgo.
- Trabajo en equipo.
- Responsabilidad.
- Planificación y organización del trabajo.
- Orden y Calidad.
- Atención y Servicio al Cliente.
- Discreción.
- Conocimiento y Habilidades de Ofimática.

4.3 Competencias específicas o técnicas del puesto

- Dominio de Bases de Datos relacionales
- Dominio de Lenguajes de Programación 4gl
- Dominio de idioma Ingles
- Conocimiento de redes
- Conocimiento de Sistemas Operativos Windows, Linux

4.4 Experiencia laboral requerida

- Dos años como mínimo en puestos similares.

5. RESPONSABILIDADES QUE INCLUYE EL PUESTO

5.1 Manejo de personal

UNIDAD DE DESARROLLO ORGANIZACIONAL

- Ninguno.

5.2 Equipo de trabajo

- Equipo asignado bajo su responsabilidad.

5.3 Fondos y Valores

- Ninguno.

5.4 Responsabilidad en manejo de información.

- Manejo de información confidencial relacionado a todos los sistemas informáticos de la institución.

6. CONDICIONES DE TRABAJO

- Condiciones ambientales de óptima temperatura, sin ruidos.

7. RIESGOS DEL CARGO

TIPO DE RIESGO	MOTIVO	CONSECUENCIA
Ocupacional	Enfermedad ocupacional	• Estrés • Artritis • Gastritis • Problemas visuales. • Lesión del Túnel Carpiano. • Problemas de vías respiratorias.
Administrativo	Incumplimiento de funciones específicas del puesto.	• Sanciones Administrativas y legales.

8. RELACIONES DE TRABAJO, REQUERIDAS DEL PUESTO

8.1 Relaciones internas

PUESTOS	UNIDADES	CON EL PROPÓSITO DE
Jefe de Departamento de Informática.	Informática	Establecer plan de trabajo.
Coordinador y Analistas Programadores	Informática	Apoyo de requerimientos.
Coordinador y Técnicos de Soporte	Informática	Apoyo de requerimientos.
Jefes y Coordinadores	Todas las unidades organizacionales del IPSFA.	Atención de requerimientos.

8.2 Relaciones externas

INSTITUCIÓN	CON EL PROPÓSITO DE
Entes Fiscalizadores	Auditorias informáticas
Proveedor	Asistencia Técnica.

9. ESTÁNDARES DE DESEMPEÑO DEL PUESTO DE TRABAJO

- Mantener en óptimas condiciones el funcionamiento de la base de datos.
- Cumplimiento del plan de mantenimiento preventivo de servidores de base de datos y aplicaciones.
- Elaborar el plan de trabajo relacionado a las actividades de base de datos.

10. INDICADORES DE DESEMPEÑO

- Aseguramiento del funcionamiento óptimo del servidor de base de datos y aplicaciones.
- Número de mantenimientos (tunning) mensuales servidores de base de datos y aplicaciones.
- Plan de trabajo de las actividades relacionadas a base de datos.

IV. DESCRIPCIÓN DE PROCEDIMIENTOS Y METODOLOGÍAS.

NOMBRE DEL PROCEDIMIENTO:

A. GESTIÓN DE REQUERIMIENTOS PARA APLICATIVOS DE LOS SISTEMAS NEO IPSFA Y RADON.

OBJETIVO DEL PROCEDIMIENTO:

Definir los lineamientos específicos y necesarios para la gestión de requerimiento para aplicativos de los sistemas NEO IPSFA y Radón.

PARTICIPANTES:

- Jefe del Departamento de Informática.
- Coordinador de Análisis y Programación.
- Analista Programador.
- Coordinador de Soporte Técnico.
- Jefe de la Unidad Solicitante.
- Gerente General.

DOCUMENTOS Y FORMULARIOS UTILIZADOS:

- Solicitud y análisis de requerimientos para aplicativos de los Sistemas Neo IPSFA y Radón. (FORM-17-GG-INF-08).

FRECUENCIA DE USO:

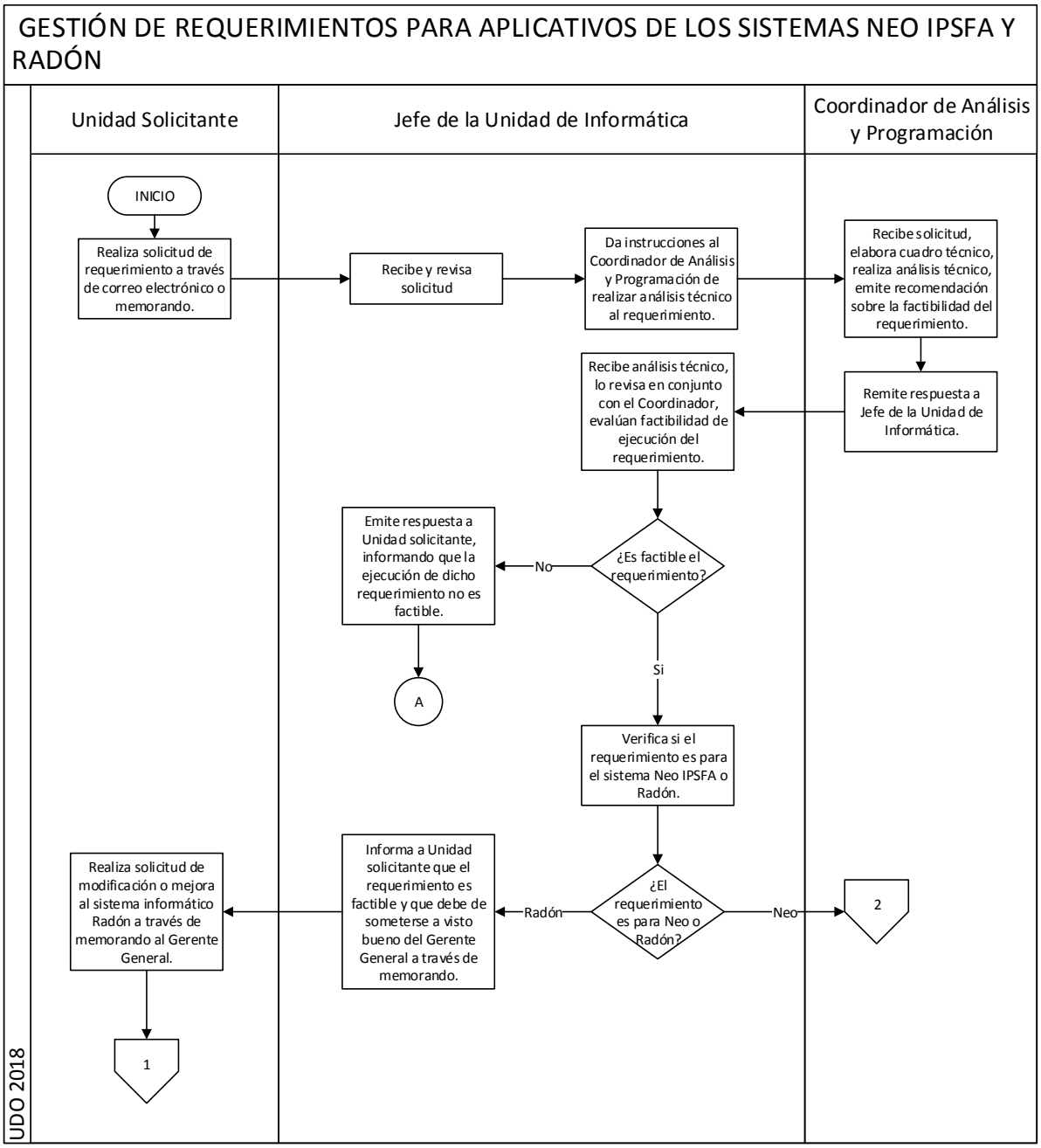
- Eventual.

A. GESTIÓN DE REQUERIMIENTOS PARA APLICATIVOS DE LOS SISTEMAS NEO IPSFA Y RADÓN.

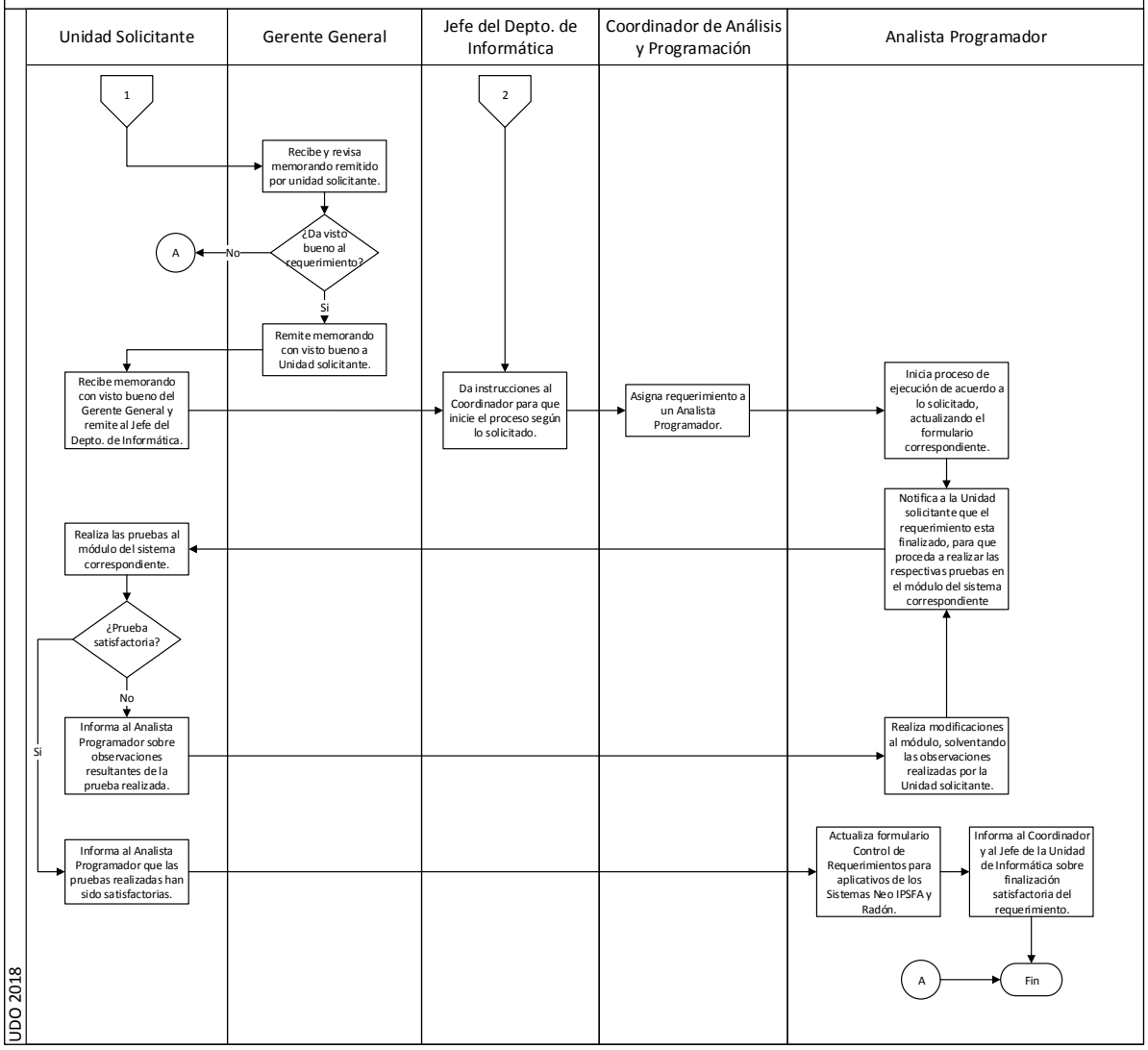
No.	RESPONSABLE	DESCRIPCIÓN
1		**Inicio del Procedimiento.**
2	**Unidad Solicitante**	Realiza solicitud a través de correo electrónico o memorando al Jefe del Departamento de Informática, especificando el requerimiento.
3	**Jefe del Departamento de Informática**	Recibe y revisa solicitud. Da instrucciones al Coordinador de Análisis y Programación de realizar análisis técnico al requerimiento.
4	**Coordinador de Análisis y Programación**	Recibe la solicitud, elabora cuadro técnico, realiza análisis técnico, emite recomendación sobre la factibilidad del requerimiento y lo remite a Jefe del Departamento de Informática.
5	**Jefe del Departamento de Informática / Coordinador de Análisis y Programación**	Recibe análisis técnico, lo revisa en conjunto con el Coordinador, evalúan factibilidad de ejecución del requerimiento, pudiendo suceder: a) Requerimiento sea factible: ir a paso 7. b) Requerimiento no sea factible: ir a paso 6.
6	**Jefe del Departamento de Informática**	Emite respuesta a Unidad solicitante, informando que la ejecución de dicho requerimiento no es factible. Ir a paso 21.
7		Verifica si el requerimiento es para el sistema Neo IPSFA o Radón: a) Requerimiento a sistema Radón: ir a paso 8. b) Requerimiento a sistema Neo-IPSFA: ir a paso 12.
8		Emite respuesta a Unidad solicitante, informando que dicho requerimiento es factible de realizarse y que debe someterse a visto bueno del Gerente General

		a través de memorando.
9	**Unidad Solicitante**	Realiza solicitud de modificación o mejora al sistema informático Radón a través de memorando al Gerente General.
10	**Gerente General**	Recibe y revisa memorando remitido por unidad solicitante, pudiendo suceder: a) De visto bueno a la solicitud: Remite memorando con visto bueno a Unidad solicitante. Ir a paso 11. b) Deniegue la solicitud: ir a paso 21.
11	**Unidad Solicitante**	Recibe memorando con visto bueno del Gerente General y remite al Jefe del Departamento de Informática.
12	**Jefe del Departamento de Informática**	Da instrucciones al Coordinador para que inicie el proceso según lo solicitado.
13	**Coordinador de Análisis y Programación**	Asigna requerimiento a un Analista Programador.
14	**Analista Programador**	Inicia proceso de ejecución de acuerdo a lo solicitado, actualizando el formulario Control de Requerimientos para aplicativos de los Sistemas Neo IPSFA y Radón (FORM-17-GG-INF-08), en el que se especifica los detalles del requerimiento, su fecha de inicio y de finalización.
15		Al tener finalizado el requerimiento, notifica a la Unidad solicitante para que proceda a realizar las respectivas pruebas en el módulo del sistema correspondiente y le indica que deberá de informar sobre resultados de la prueba a través de correo electrónico.

16	**Unidad Solicitante**	Realiza las pruebas al módulo del sistema correspondiente, pudiendo suceder: a) El requerimiento haya sido realizado satisfactoriamente: ir a paso 19. b) Se realicen observaciones: ir a paso 17.
17		Informa al Analista Programador asignado, a través de correo electrónico, sobre observaciones resultantes de la prueba realizada.
18	**Analista Programador**	Realiza modificaciones al módulo, solventando las observaciones realizadas por la Unidad solicitante. Ir a paso 15.
19	**Unidad Solicitante**	Notifica al Analista Programador asignado, a través de correo electrónico, que las pruebas realizadas han sido satisfactorias de acuerdo al requerimiento realizado.
20	**Analista Programador**	Actualiza formulario Control de Requerimientos para aplicativos de los Sistemas Neo IPSFA y Radón (FORM-17-GG-INF-08) e informa al Coordinador de Análisis y Programación y al Jefe de la Unidad de Informática sobre finalización satisfactoria del requerimiento.
21		**Fin del Procedimiento.**



GESTIÓN DE REQUERIMIENTOS PARA APLICATIVOS DE LOS SISTEMAS NEO IPSFA Y RADÓN



NOMBRE DEL PROCEDIMIENTO:

B. RECIBO, RESGUARDO Y ENTREGA DE EQUIPO INFORMÁTICO NUEVO.

OBJETIVO DEL PROCEDIMIENTO:

Definir las acciones para recibir, resguardar y entregar el equipo informático nuevo.

PARTICIPANTES:

- Coordinador de Soporte Técnico.
- Técnico de Soporte.
- Unidad Solicitante.

DOCUMENTOS Y FORMULARIOS UTILIZADOS:

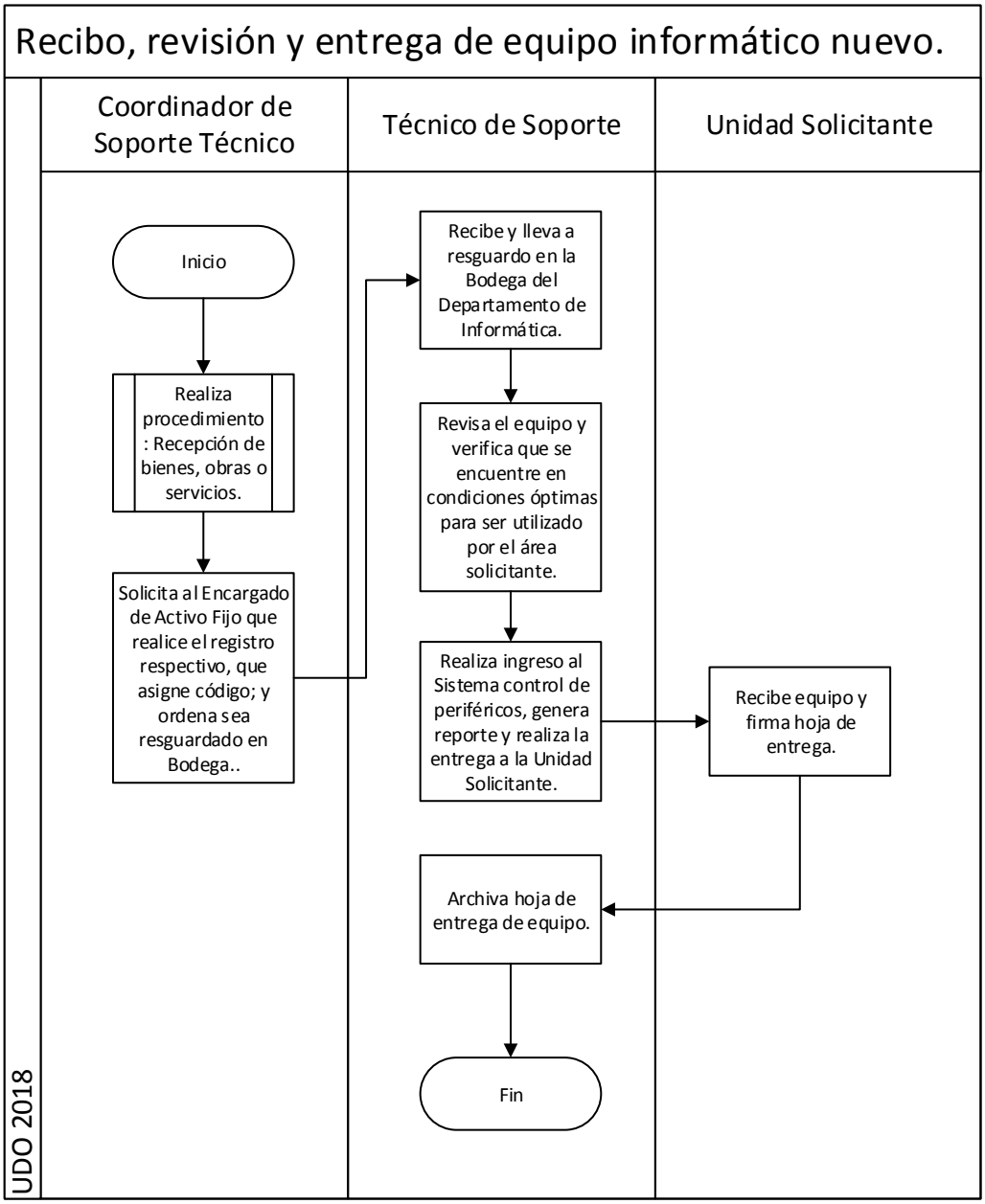
- Entrega e Instalación de Equipo Informático (Anexo 1).

FRECUENCIA DE USO:

- Eventual.

B. RECIBO, REVISIÓN Y ENTREGA DE EQUIPO INFORMATICÓ NUEVO.

No.	RESPONSABLE	DESCRIPCIÓN
1		**Inicio del Procedimiento.**
2	**Coordinador de Soporte Técnico**	Realiza procedimiento: Recepción de bienes, obras o servicios, descrito en el Manual de Organización y Funcionamiento del Área de Activo Fijo.
3		Solicita al Encargado de Activo Fijo realice el registro respectivo en la base de datos de activo fijo y que ponga el código respectivo.
4		Ordena al Técnico de Soporte que lleve el equipo informático a resguardo.
5	**Técnico de Soporte**	Recibe y lleva a resguardo en la Bodega de el Departamento de Informática.
6		Revisa el equipo y verifica que se encuentre en condiciones óptimas para ser utilizado por el área solicitante.
7		Realiza el ingreso al Sistema control de periféricos detalladamente y genera el reporte en sistema "Entrega e Instalación de Equipo Informático." (Anexo 1)
8	**Unidad Solicitante**	Recibe el reporte de "Entrega e Instalación de Equipo Informático" y firma de recibido.
9	**Técnico de Soporte**	Archiva Hoja de entrega de Equipo.
10		**Fin del Procedimiento.**



NOMBRE DEL PROCEDIMIENTO:

C. TRASLADO DE EQUIPO INFORMÁTICO.

OBJETIVO DEL PROCEDIMIENTO:

Definir los lineamientos para controlar y supervisar el traslado de equipo informático.

PARTICIPANTES:

- Usuario Solicitante.
- Coordinador de Soporte Técnico.
- Técnico de Soporte.
- Encargado de Activo Fijo.

DOCUMENTOS Y FORMULARIOS UTILIZADOS:

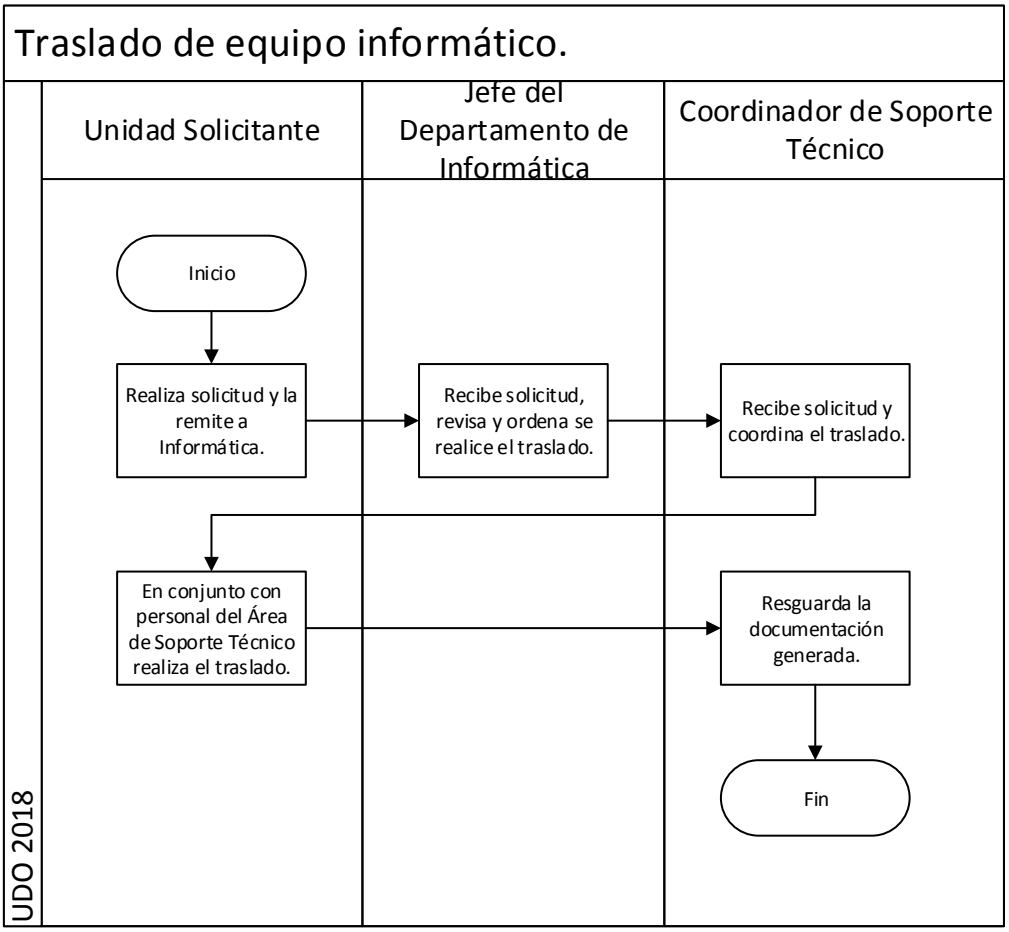
- Solicitud de Traslado de Activo Fijo FORM-09-GA-SGE-018

FRECUENCIA DE USO:

- Eventual.

C. TRASLADO DE EQUIPO INFORMÁTICO

No.	RESPONSABLE	DESCRIPCIÓN
1		**Inicio del Procedimiento.**
2	**Unidad Solicitante**	Llena formulario Solicitud de Traslado de Activo Fijo (FORM-09-GA-SGE-018).
3		Gestiona firmas correspondientes y autorización del Jefe del Departamento de Informática para el traslado del equipo informático.
4	**Jefe del Departamento de Informática**	Recibe Solicitud de Traslado de Activo, revisa, autoriza el traslado y lo remite al Coordinador de Soporte Técnico.
5	**Coordinador de Soporte Técnico**	Recibe solicitud de traslado autorizada y coordina con la Unidad Solicitante dicho traslado.
6	**Unidad Solicitante**	En conjunto con el Área de Soporte Técnico realiza: Procedimiento Asignación o Traslado de Activo Fijo, descrito en el Manual de Organización y Funcionamiento del Área de Activo Fijo.
7	**Coordinador de Soporte Técnico**	Resguarda la documentación generada.
8		**Fin del Procedimiento.**


Traslado de equipo informático.
Unidad Solicitante
Jefe del Departamento de Informática
Coordinador de Soporte Técnico
Inicio
Realiza solicitud y la remite a Informática.
Recibe solicitud, revisa y ordena se realice el traslado.
Recibe solicitud y coordina el traslado.
En conjunto con personal del Área de Soporte Técnico realiza el traslado.
Resguarda la documentación generada.
Fin
UDO 2018

NOMBRE DEL PROCEDIMIENTO:

D. SALIDAS DE EQUIPO INFORMÁTICO.

OBJETIVO DEL PROCEDIMIENTO:

Definir los lineamientos para controlar el equipo informático que sale de las instalaciones del IPSFA para ser reparado por una Empresa externa o para ser utilizado en otras instalaciones.

PARTICIPANTES:

- Usuario Solicitante.
- Encargado de Activo Fijo.
- Coordinador de Soporte Técnico.
- Técnico de Soporte.

DOCUMENTOS Y FORMULARIOS UTILIZADOS:

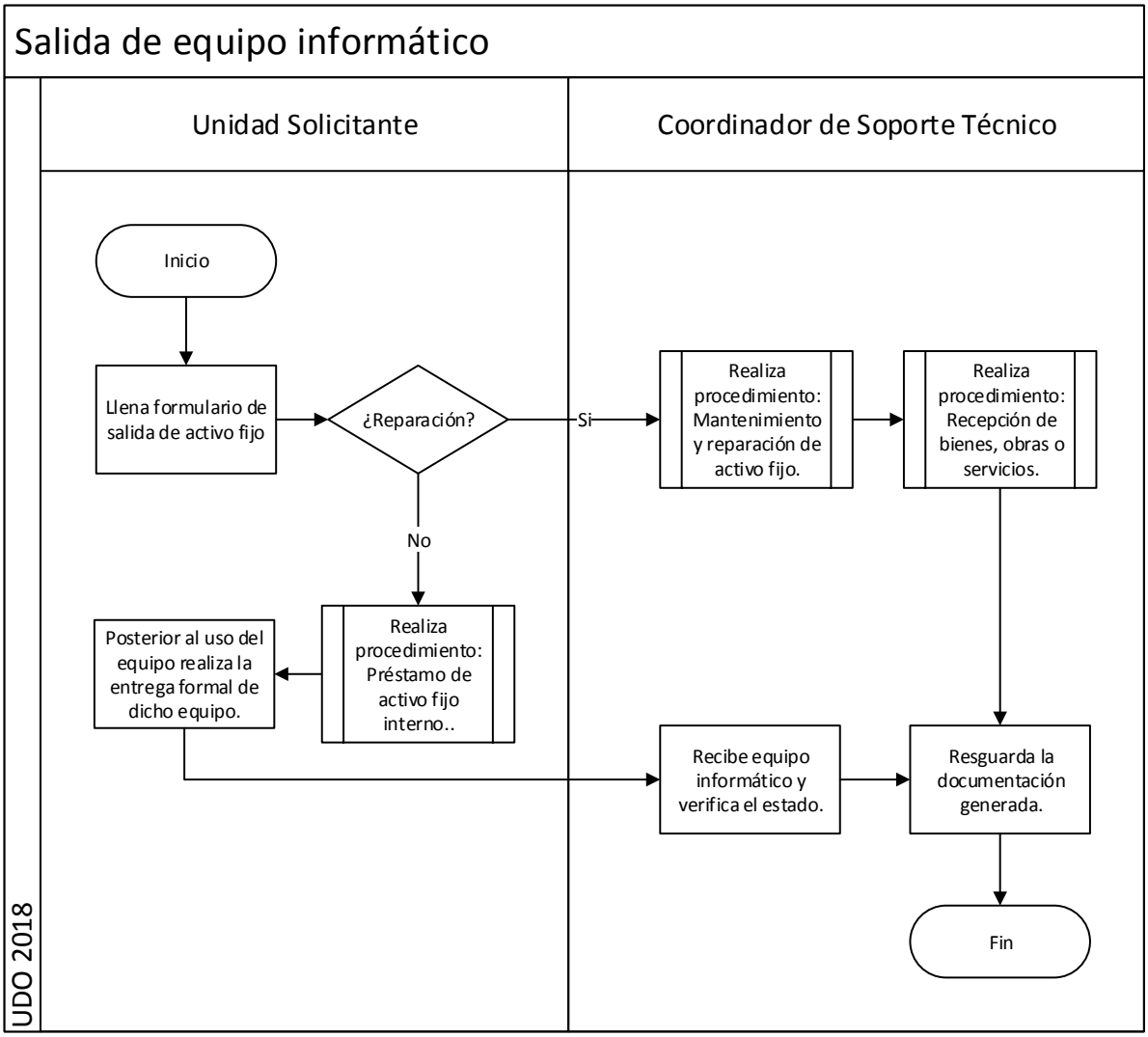
- Solicitud de Salida de Activo Fijo FORM-09-GA-SGE-016

FRECUENCIA DE USO:

- Eventual.

D. SALIDAS DE EQUIPO INFORMÁTICO

No.	RESPONSABLE	DESCRIPCIÓN
1		**Inicio del Procedimiento.**
2	**Unidad Solicitante**	Llena formulario de Salida de Activo Fijo (FORM-09-GA-SGE-016), gestiona las autorizaciones correspondientes y remite el original al Encargado de Activo Fijo y una copia al Coordinador de Soporte Técnico.
3		¿Reparación? Si, ir a paso: 4; No, ir a paso: 6.
4	**Coordinador de Soporte Técnico**	En conjunto con la Unidad Solicitante realiza procedimiento: Mantenimiento y Reparación de Activo Fijo, descrito en el Manual de Organización y Funcionamiento del Área de Activo Fijo.
5		En conjunto con la Unidad Solicitante realiza procedimiento: Recepción de bienes, obras o servicios, descrito en el Manual de Organización y Funcionamiento del Área de Activo Fijo. Ir a paso: 9.
6	**Unidad Solicitante**	Realiza procedimiento: Préstamo de Activo Fijo Interna, descrito en el Manual de Organización y Funcionamiento del Área de Activo Fijo.
7		Entrega Equipo Informático.
8	**Coordinador de Soporte Técnico**	Recibe equipo informático y verifica estado.
9		Resguarda la documentación generada.
10		**Fin del Procedimiento.**



NOMBRE DEL PROCEDIMIENTO:

E. DESCARGO DE EQUIPO INFORMÁTICO.

OBJETIVO DEL PROCEDIMIENTO:

Controlar equipo informático que será descargado de los Activos Fijos del IPSFA.

PARTICIPANTES:

- Departamento de Informática y
- Activo Fijo.

DOCUMENTOS Y FORMULARIOS UTILIZADOS:

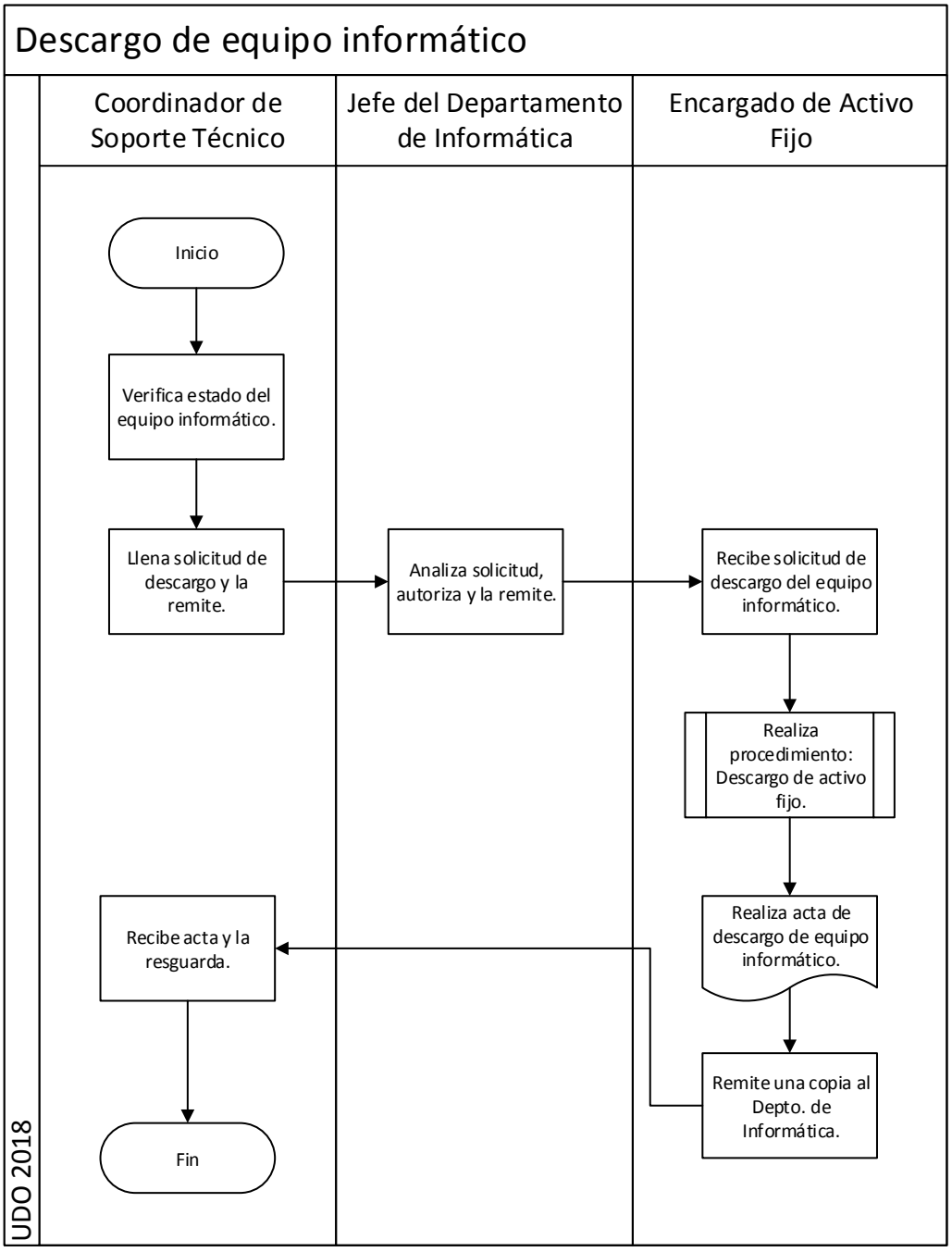
- Solicitud de Descargo de Activo Fijo FORM-09-GA-SGE-017

FRECUENCIA DE USO:

- Eventual.

E. DESCARGO DE EQUIPO INFORMÁTICO

No.	RESPONSABLE	DESCRIPCIÓN
1		**Inicio del Procedimiento.**
2	**Coordinador de Soporte Técnico**	Verifica el equipo informático y evalúa si se encuentra dañado o si se considera obsoleto y se procede a elaborar descargo. Llena Solicitud de Descargo de Activo Fijo (FORM-09-GA-SGE-017) y la envía para autorización del Jefe del Departamento de Informática.
3	**Jefe del Departamento de Informática**	Analiza solicitud y firma de autorizado, luego la traslada al Área de Activo Fijo.
4	**Encargado de Activo Fijo**	Recibe solicitud de descargo de equipo informático con las autorizaciones.
5		Realiza procedimiento: Descargo de Activo Fijo, descrito en el Manual de Organización y Funcionamiento del Área de Activo Fijo.
6		Realiza acta de descargo de equipo informático que deberá ser firmada por el Encargado de Activo Fijo, Gerente Administrativo, Departamento de Informática y Gerente General. Envía copia del acta de descargo con las firmas respectivas a el Departamento de Informática para su resguardo.
7	**Coordinador de Soporte Técnico**	Resguarda Acta de Descargo.
8		**Fin del Procedimiento.**


Descargo de equipo informático
Coordinador de Soporte Técnico
Jefe del Departamento de Informática
Encargado de Activo Fijo
Inicio
Verifica estado del equipo informático.
Llena solicitud de descargo y la remite.
Analiza solicitud, autoriza y la remite.
Recibe solicitud de descargo del equipo informático.
Realiza procedimiento: Descargo de activo fijo.
Realiza acta de descargo de equipo informático.
Remite una copia al Depto. de Informática.
Recibe acta y la resguarda.
Fin
UDO 2018

NOMBRE DEL PROCEDIMIENTO:

F. CREACIÓN DE USUARIO DE RED.

OBJETIVO DEL PROCEDIMIENTO:

Detallar las actividades para la creación de usuarios de red de las diferentes áreas y unidades descentralizadas del IPSFA.

PARTICIPANTES:

- Informática.
- Unidad Solicitante.

DOCUMENTOS Y FORMULARIOS UTILIZADOS:

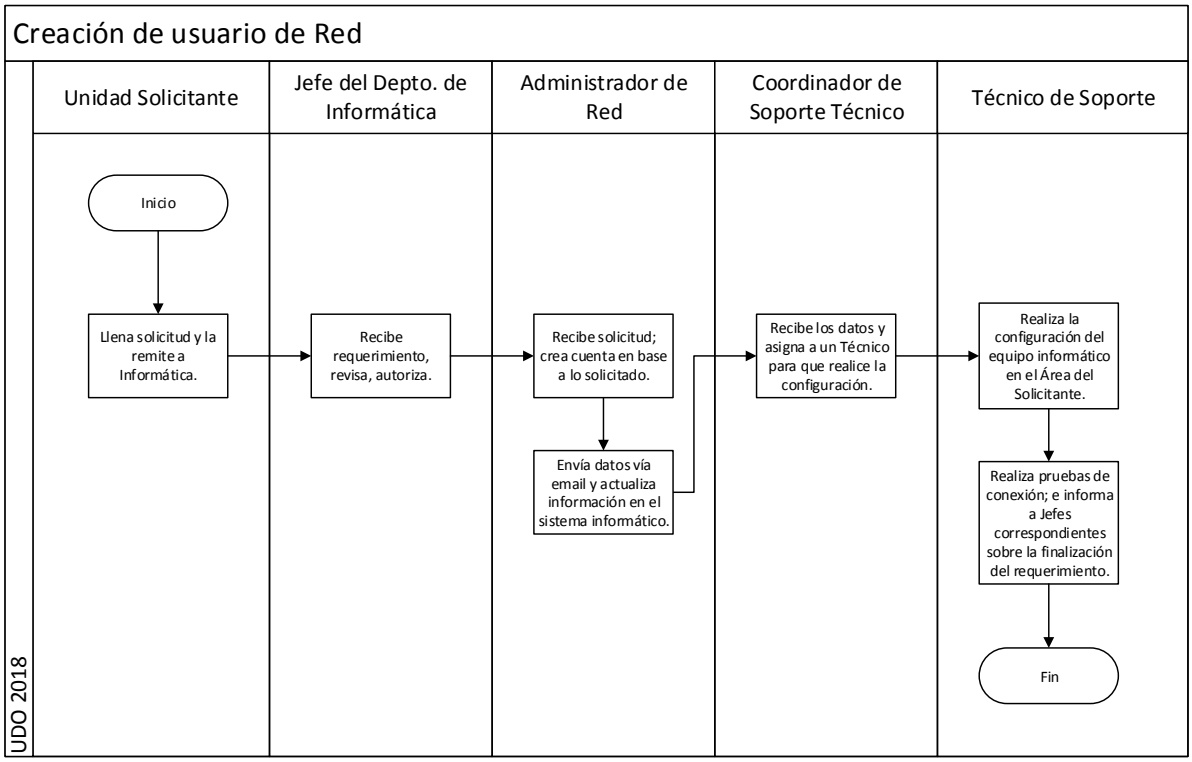
- Formulario N° 1 Solicitud de Acceso a Internet y Software de Mensajería.

FRECUENCIA DE USO:

- Eventual

F. CREACIÓN DE USUARIO DE RED

No.	RESPONSABLE	DESCRIPCIÓN
0.		**Inicio del Procedimiento.**
1.	**Unidad Solicitante**	Llena solicitud de acceso a Internet y software de mensajería y remite a el Departamento de Informática.
2.	**Jefe del Departamento de Informática**	Recibe el requerimiento, revisa y autoriza la creación de la cuenta. Posteriormente remite solicitud autorizada al Administrador de red.
3.	**Administrador de Red**	Revisa la solicitud e identifica el área o Departamento. Ingresa a servidor de dominio para la creación de la cuenta en base al perfil solicitado. Crea la cuenta en base a inicial de primer Nombre seguido del Apellido. Asigna contraseña a la cuenta creada. Una vez creada la cuenta envía los datos a través de correo electrónico al Coordinador Área de Soporte de Informática. Actualiza información en el sistema informático.
4.	**Coordinador de Soporte Técnico**	Recibe los datos y asigna al Técnico de Soporte para que realice la configuración del perfil en el equipo.
5.	**Técnico de Soporte**	Se desplaza al Área o Departamento correspondiente para configurar el equipo del Usuario definido en la solicitud.
6.		Realiza prueba de conexión en la red de Servidores Institucionales. Notifica vía correo electrónico al Jefe del Departamento de Informática, Coordinador de Soporte y Administrador de Red sobre la finalización del requerimiento.
7.		**Fin del Procedimiento**.



NOMBRE DEL PROCEDIMIENTO:

G. CREACIÓN DE CUENTA DE CORREO ELECTRÓNICO INSTITUCIONAL

OBJETIVO DEL PROCEDIMIENTO:

Detallar las actividades para la creación de cuenta de correo electrónico para las diferentes áreas y unidades descentralizadas del IPSFA.

PARTICIPANTES:

- Informática.
- Unidad Solicitante.

DOCUMENTOS Y FORMULARIOS UTILIZADOS:

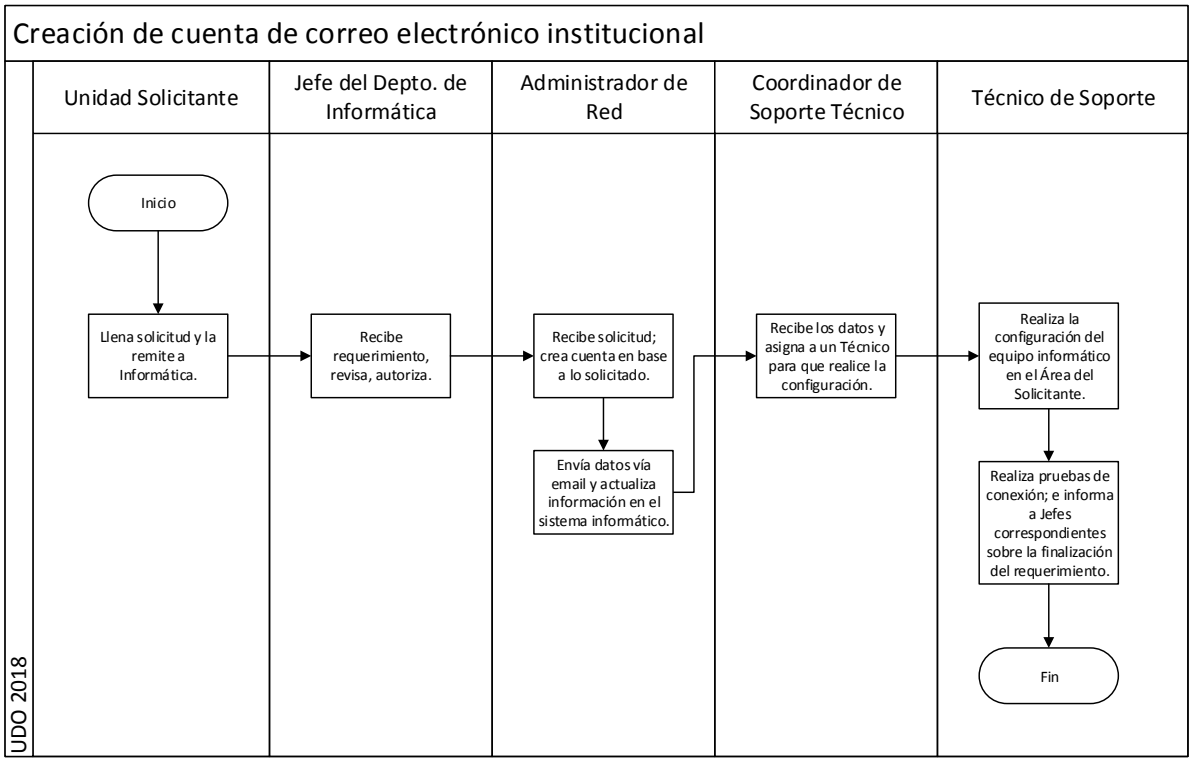
- Formulario N° 1 Solicitud de Acceso a Internet y Software de Mensajería.

FRECUENCIA DE USO:

- Eventual

G. CREACIÓN DE CUENTA DE CORREO ELECTRÓNICO INSTITUCIONAL

No.	RESPONSABLE	DESCRIPCIÓN
0.		**Inicio del Procedimiento.**
1.	**Unidad Solicitante**	Llena solicitud de acceso a Internet y software de mensajería y remite a el Departamento de Informática.
2.	**Jefe del Departamento de Informática**	Recibe el requerimiento, revisa y autoriza la creación de la cuenta de correo. Posteriormente remite solicitud a Administrador de red.
3.	**Administrador de Red**	Revisa la solicitud, ingresa a servidor de correo para la creación de la cuenta. Crea la cuenta de correo en base al primer nombre, seguido del primer apellido separado por un punto, luego el nombre del dominio @ipsfa.com.; Asigna contraseña a la cuenta creada; Una vez creada envía datos a través de correo electrónico al Área de Soporte de Informática.
4.	**Coordinador de Soporte Técnico**	Recibe los datos y asigna al Técnico de Soporte para que realice la configuración del Equipo.
5.	**Técnico de Soporte**	Se desplaza al Área o Departamento correspondiente para configurar en el equipo la cuenta de correo electrónico
6.		Realiza pruebas de envío y recepción de correo en la nueva cuenta. Notifica vía correo electrónico al Jefe del Departamento de Informática, Coordinador de Soporte y Administrador de Red sobre la finalización del requerimiento.
7.		**Fin del Procedimiento**.



NOMBRE DEL PROCEDIMIENTO:

H. REUTILIZACIÓN DE PARTES PROVENIENTES DE EQUIPOS INFORMÁTICOS EN DESUSO.

OBJETIVO DEL PROCEDIMIENTO:

Identificar las actividades a seguir para la reutilización de partes provenientes de equipos informáticos en desuso a nivel institucional.

PARTICIPANTES:

- Departamentos y Unidades de negocio del IPSFA.
- Área de Soporte Técnico del Departamento de Informática.
- Área de Activo Fijo del Departamento de Servicios Generales.

DOCUMENTOS Y FORMULARIOS UTILIZADOS:

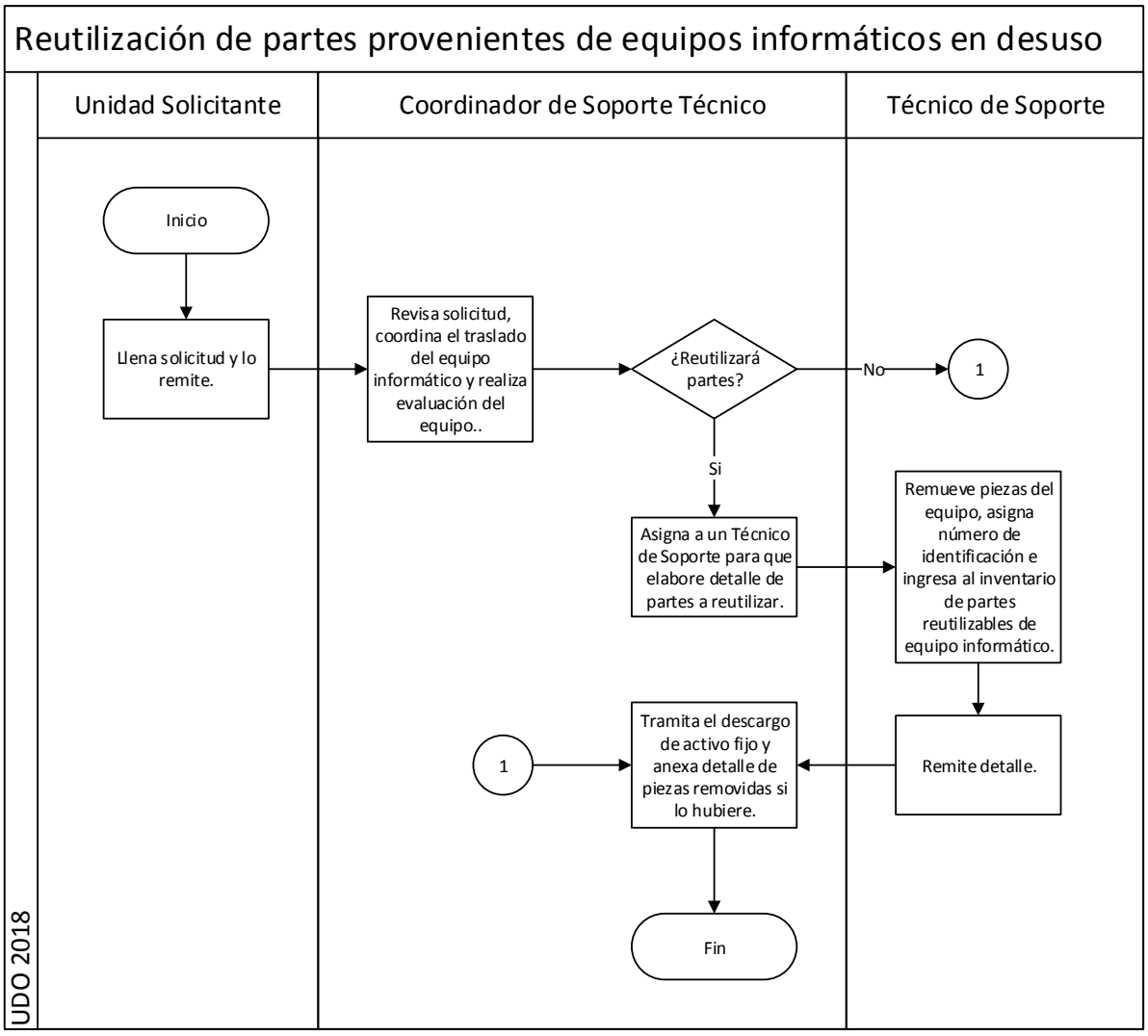
- Solicitud de Descargo de Activo Fijo. (FORM-09-GA-SGE-017)
- Solicitud de Traslado de Activo Fijo. (FORM-09-GA-SGE-018)

FRECUENCIA DE USO:

- Eventual.

H. REUTILIZACIÓN DE PARTES PROVENIENTES DE EQUIPOS INFORMÁTICOS.

No.	RESPONSABLE	DESCRIPCIÓN
1.		**Inicio del Procedimiento.**
2.	**Unidad Solicitante**	Remite al Departamento de Informática el formulario de traslado de activo fijo FORM-09-GA-SGE-018, del equipo informático con sus respectivas firmas.
3.	**Coordinador de Soporte Técnico**	Revisa formulario y coordina el traslado del equipo informático.
4.		Realiza evaluación del equipo pudiendo suceder: a) Que no se reutilizarán partes (paso N° 8). b) Se utilizarán partes (paso N°5).
5.		Asigna a un Técnico de Soporte para que elabore detalle de las partes a reutilizar.
6.	**Técnico de Soporte**	Remueve piezas del equipo, asigna número de identificación e ingresa al inventario de partes reutilizables de equipo informático.
7.		Remite detalle al Coordinador de Soporte Técnico.
8.	**Coordinador de Soporte Técnico**	Tramita el descargo de activo fijo FORM-09-GA-SGE-017, y anexa detalle de las piezas removidas al equipo si lo hubiere.
9.		**Fin del Procedimiento.**


Reutilización de partes provenientes de equipos informáticos en desuso
Unidad Solicitante
Coordinador de Soporte Técnico
Técnico de Soporte
Inicio
Llena solicitud y lo remite.
Revisa solicitud, coordina el traslado del equipo informático y realiza evaluación del equipo..
¿Reutilizará partes?
No
1
Si
Asigna a un Técnico de Soporte para que elabore detalle de partes a reutilizar.
Remueve piezas del equipo, asigna número de identificación e ingresa al inventario de partes reutilizables de equipo informático.
Remite detalle.
1
Tramita el descargo de activo fijo y anexa detalle de piezas removidas si lo hubiere.
Fin
UDO 2018

NOMBRE DEL PROCEDIMIENTO:

I. SOLICITUD DE ACCESO A REDES INALÁMBRICAS

OBJETIVO DEL PROCEDIMIENTO:

Conocer los pasos para solicitar y autorizar el acceso a las redes inalámbricas del IPSFA y de sus Unidades descentralizadas.

PARTICIPANTES:

1. Jefe de la Unidad Solicitante.
2. Jefe del Departamento de Informática.
3. Administrador de Red

DOCUMENTOS Y FORMULARIOS UTILIZADOS:

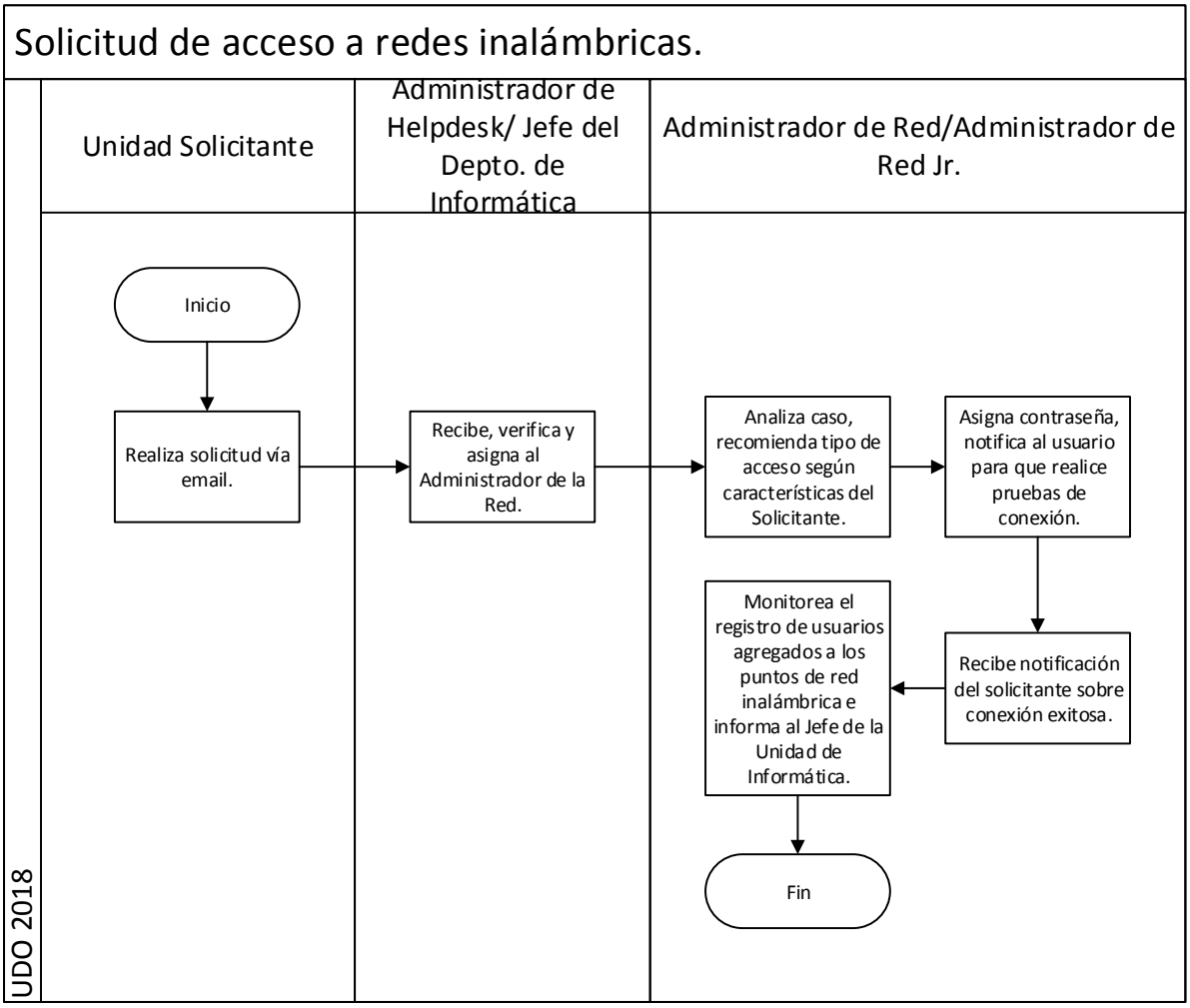
Solicitud de acceso a redes inalámbricas (email)

FRECUENCIA DE USO:

Eventual

I. SOLICITUD DE ACCESO A REDES INALÁMBRICAS

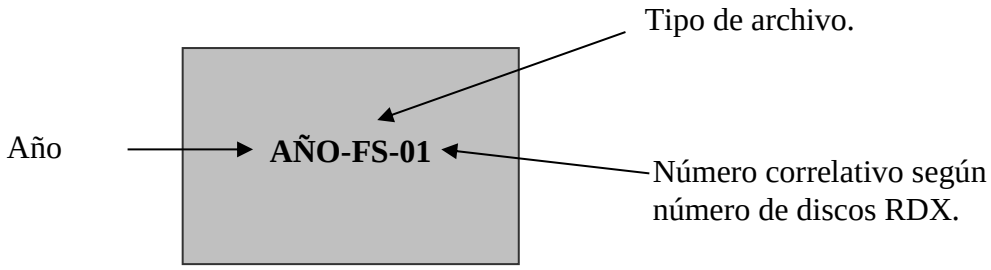
No.	RESPONSABLE	ACTIVIDAD
1.		**Inicio del Procedimiento.**
2.	**Unidad Solicitante.**	Solicita requerimiento de acceso a la red inalámbrica a través de correo electrónico a helpdesk@ipsfa.com o jefe.informatica@ipsfa.com
3.	**Administrador de Helpdesk/ Jefe del Departamento de Informática**	Remite correo electrónico al Administrador de Red.
4.	**Administrador de Red/ Administrador de Red Jr.**	Analiza caso, recomienda acceso a través del SSID apropiado de acuerdo a las características de la Unidad solicitante.
5.		Asigna contraseña, notifica al usuario para que realice las pruebas de conexión.
6.		Recibe notificación del solicitante sobre conexión exitosa.
7.		Monitorea el registro de usuarios agregados a los puntos de red inalámbrica e informa al Jefe de Informática.
8.		**Fin del Procedimiento.**


Solicitud de acceso a redes inalámbricas.
Unidad Solicitante
Administrador de Helpdesk/ Jefe del Depto. de Informática
Administrador de Red/Administrador de Red Jr.
UDO 2018
Inicio
Realiza solicitud vía email.
Recibe, verifica y asigna al Administrador de la Red.
Analiza caso, recomienda tipo de acceso según características del Solicitante.
Asigna contraseña, notifica al usuario para que realice pruebas de conexión.
Recibe notificación del solicitante sobre conexión exitosa.
Monitorea el registro de usuarios agregados a los puntos de red inalámbrica e informa al Jefe de la Unidad de Informática.
Fin

NOMBRE DE LA METODOLOGÍA:

J. REALIZACIÓN DE RESPALDOS SISTEMÁTICOS.

Todo respaldo deberá ser enviñetado de acuerdo con el período de la semana de trabajo y especificando el mes y año a que corresponden.



1. Servidores File Server:

- Tiene instalado sistema operativo Windows Server 2008 Estándar R2
- Tiene la última actualización de sistema operativo, disponible por el fabricante del software.

Técnico de Soporte Informático:

- Realiza respaldo del archivo de configuración de cuentas de dominio y derechos de usuarios.
- Realiza el respaldo de la información que contiene el equipo, por medio del software de respaldo del sistema operativo.
- El respaldo se realiza de lunes a viernes; Se realiza de forma completa o total cada quince días (dos veces en el mes); siendo de forma incremental los demás días del mes.
- Estos son resguardados en discos internos del servidor de respaldo y al siguiente día enviados al sitio de contingencia vía red de datos o físicamente.

2. Servidor de Aplicaciones ORACLE:

Este servidor tiene instalado:

- Sistema operativo ORACLE V.M
- Último software disponible recomendado por el fabricante de la base de datos ORACLE.
- ORACLE OAS, ORACLE WEB LOGIC cuenta con el último nivel actualización recomendado por el fabricante del sistema.

Técnico de Soporte Informático:

- Realiza el respaldo de la información de los aplicativos, mediante software de respaldo del sistema operativo.
- El respaldo se realiza todos los días de forma total.
- Estos son resguardados en discos internos del servidor de respaldo y al siguiente día enviados al sitio de contingencia vía red de datos o físicamente.

3. Servidor de Correo:

- Tiene instalado sistema operativo LINUX SUSE 7.2.

Administrador de la Red:

- Realiza respaldo de las cuentas cuando hayan modificaciones de archivo de configuración.

4. Dos Servidores de PROXY:

- Tiene instalado sistema operativo LINUX SUSE 9.0
- Tiene instalado sistema operativo LINUX SUSE 7.2

Administrador de RED:

- Realiza respaldo de los archivos de configuración de acceso a los usuarios para el acceso a Internet, cuando se realiza cambio en la configuración como adicionar un nuevo usuario.

5. Servidores WEB:

- Tiene instalado sistema operativo Windows 2000 Advanced server

Técnico de Soporte Informático:

- Se respaldan archivos de configuración.
- El respaldo se realiza de lunes a viernes, es incremental de lunes a jueves y completo el viernes.

- Los archivos ROOT y MYSQL (IPSFA03) se resguardan en el tape del servidor APPL de igual manera los archivos del sitio IPSFA04. Mientras que el ADMON es resguardado en un tape individual.
- Estos son resguardados en Disco RDX y enviados al sitio de contingencia.

6. Servidor de Producción Base de Datos:

- Tiene instalado sistema operativo Red Hat 5.2.
- Contiene la última actualización del sistema operativo recomendado por el fabricante.
- Tiene instalado una base de datos ORACLE.
- Tiene configurado la interconexión a la unidad de almacenamiento Hitachi, para el manejo de base de datos en producción.

Administrador de RED y Administrador de Base de Datos (DBA):

- Se realizan respaldos de los archivos de base de datos y se copian a discos.
- Los archivos son resguardados durante dos meses en disco, al mismo tiempo se realiza copia en cinta, y se envía al sitio de contingencia.

7. Servidor Standby:

- Tiene instalado sistema operativo Windows 2003 Enterprise.
- Contiene la última actualización del sistema operativo recomendado por el fabricante.
- Tiene instalado una base de datos ORACLE.

Administrador de RED y Administrador de Base de Datos (DBA)

- Tiene el funcionamiento de respaldar base datos de producción en sitio de contingencia.

NOMBRE DE LA METODOLOGÍA:

K. ELABORACIÓN DE RESPALDOS DIARIOS.

NORMAS APLICABLES.

Los procesos de respaldos son ejecutados automáticamente a partir de las 22:00 horas y no interfieren con el trabajo de usuarios o procesos que se encuentren laborando a esa hora.

Inicio de la Metodología.

Administrador de Base de Datos:

1. Los respaldos diarios se hacen utilizando un utilitario de Oracle llamado Export y se ejecutan programados automáticamente mediante la utilería del Sistema Operativo.

2. El Administrador de Base de Datos desarrolla un script el cual es ejecutado por utilería Cron, en donde se detallan las instancias a respaldar y verifica que se haya realizado el respaldo correctamente en el servidor de producción.

3. Revisa al día siguiente la consistencia de archivos de respaldo y el Administrador de Red se encarga del almacenamiento en medios magnéticos en forma correcta.

4. El área de Soporte Técnico realiza el resguardo de los archivos de respaldo en el sitio de contingencia.

Fin de Metodología.

NOMBRE DE LA METODOLOGÍA:

L. ELABORACIÓN DE RESPALDOS A SOLICITUD DE LAS UNIDADES DEL IPSFA.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar la elaboración de respaldos a solicitud de las Unidades del IPSFA.

Inicio de la Metodología.

Usuario

1. El usuario solicita al Departamento de Informática por medio de correo electrónico dirigido al Jefe de dicha Unidad y al Administrador de Red, los alcances del respaldo necesitado.

Área de Soporte Técnico

2. El Coordinador de Soporte Técnico evalúa la metodología más eficiente para efectuar el respaldo, además de corroborar que dicho proceso no afecte a los demás usuarios y procesos del sistema.
3. Procede a realizar el respaldo solicitado tanto en disco como en medio magnético.
4. Informa por medio de correo electrónico al usuario solicitante del respaldo, una vez haya finalizado el proceso.
5. Etiqueta e identifica el Tape-Backup y procede a su almacenamiento en el Área de Soporte Técnico.
6. Posteriormente se realiza el traslado para su resguardo en el Sitio de Contingencia.

Fin de la Metodología.

NOMBRE DE LA METODOLOGÍA:

M. ELABORACIÓN DE RESPALDOS PARA ESQUEMA O INSTANCIA DE BASE DE DATOS.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar la elaboración de respaldos para esquema o instancia de base de datos.

Inicio de la Metodología.

Usuario

1. El usuario solicita al Departamento de Informática por medio de correo electrónico dirigido helpdesk@ipsfa.com con copia al Jefe de dicho Departamento y al Administrador de Base de Datos, los alcances del respaldo necesitado.

Administrador de Base de Datos

2. El Administrador de Base de Datos evalúa la metodología más eficiente para efectuar el respaldo, además de corroborar que dicho proceso no afecte a los demás usuarios y procesos del sistema.
3. Procede a realizar el respaldo solicitado tanto en disco y/o medio magnético.
4. Informa por medio de correo electrónico al usuario solicitante del respaldo, una vez haya finalizado el proceso.
5. Etiqueta e Identifica el Tape-Backup y procede a su almacenamiento en el Área de Informática en el caso que así fuere solicitado.

Fin de la Metodología.

NOMBRE DE LA METODOLOGÍA:

N. RESTAURACIÓN DE INFORMACIÓN.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar la restauración de información.

Inicio de la Metodología.

Usuario

1. El usuario solicita al Departamento de Informática por medio de correo electrónico dirigido al Jefe de dicha Unidad y al Administrador de Red la restauración de la información.

Área de Soporte Técnico

2. Coordinador de Soporte Técnico verifica el requerimiento con el Analista Programador asignado a la aplicación que se desea restaurar para efectuarla en forma óptima, oportuna y eficiente.
3. Procede a la búsqueda de la información respaldan tanto en disco como en medios magnéticos.
4. Ejecuta actividades para la restauración de la información solicitada y verifica.
5. Informa al usuario solicitante una vez la información se encuentre restaurada.

Fin de Metodología.

NOMBRE DE LA METODOLOGÍA:

O. ACTUALIZACIÓN DE OBJETOS FUENTES Y COMPILADOS.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar la actualización de objetos fuentes y compilados.

NORMAS APLICABLES

1. Los analistas Programadores serán los responsables de llevar un control de versiones de los objetos fuentes y compilados modificadas en la siguiente ubicación //sv_admón./FUENTES_ORACLE/nombre_del_analista.
2. El control de versiones de fuentes y compilados modificados deben de atender los siguientes estándares:
   Creación de carpeta con el nombre del objeto.
   Incluir dentro de la misma las sub-carpetas que correspondan a la fecha de actualización
3. El acceso a la carpeta de fuentes del sistema Neo IPSFA; se definirá de acuerdo al módulo que cada Analista Programador tenga asignado y con derechos sólo de lectura.
4. La actualización de las fuentes modificadas a la carpeta de fuentes del sistema (//ipsfa04/src) será responsabilidad del Administrador del sistema informático que se le asignó la tarea de administración de las fuentes del sistema sin restricciones.
5. Será responsabilidad de cada Analista Programador, el mantener un respaldo actualizado de los archivos fuentes y compilados de una aplicación a través de las solicitudes necesarias para su actualización.

Inicio de la Metodología.

Analista Programador

1. Realiza el respaldo de la fuente del objeto a modificar, a fin de llevar un control de versiones; tomándola de la carpeta //Ipsfa04/src y ubicados en la carpeta para el control de versiones //sv_admón./FUENTES_ORACLE/nombre.del.analista/
   Ej: Forma a resguardar SIS55M39
   //sv_admon/FUENTES_ORACLE/nombre_del_analista/formas/SIS55M39/00fecha de primera versión tomada de los archivos fuente.
   1era carpeta SIS55M39

UNIDAD DE DESARROLLO ORGANIZACIONAL

2da carpeta 00_25112009 (fuente tomada por primera vez).

3era carpeta 01_18122009 (fuente con la primera modificación).

Etc...

2. Posterior al haber realizado las modificaciones de acuerdo a los requerimientos solicitados por las diferentes áreas, deberá realizar las siguientes actividades:

   a) Digitar la siguiente información en la porción del código modificado (dentro de la forma, reporte, etc):

      --Fecha de modificación: DD/MM/AAAA

      --Nombre del Analista programador: Juan Pérez

      --Breve Explicación: Se agregó variable por xxxxxx.....

   b) Actualiza las modificaciones realizadas en la forma PT00FM23-registro de bitácora modificaciones de objeto.

   c) Registra la solicitud de requerimiento para la actualización de fuentes y compilados a través del correo electrónico helpdesk@ipsfa.com , detallando el nombre del módulo, sub-modulo, nombre del fuente, tipo de objeto y numero de bitácora registrado en la forma PT00FM23-registro de bitácora modificaciones de objeto.

3. Coloca en la carpeta //ipsfa04/fuentes_del_sistema_modificados_IPSFA, en la subcarpeta para ser tomados para la actualización a las carpetas fuentes y compilados del sistema informático.

Administrador de NEO-IPSFA

4. Recibe la solicitud del requerimiento, verifica que el objeto a modificar contenga la descripción y responsable del cambio, que se realice la actualización en la forma PT00FM23 y actualiza la fuente solicitada en la carpeta de fuentes del sistema (//ipsfa04/src), realiza la actualización de los archivos fuentes en carpetas del sistema informática de acuerdo al aplicativo a actualizar.
5. Coloca en producción la versión compilada del objeto en la carpeta //Ipsfa04/neo/run y la fuente del objeto en la carpeta correspondiente al módulo, sub-módulo y objeto a que corresponda: //Ipsfa04/ src /nombre_del_aplicativo_a_actualizar.
6. Registra el seguimiento y finalización del requerimiento confirmando la atención y lo envía por correo electrónico.

Fin de la Metodología

NOMBRE DE LA METODOLOGÍA:

P. ACTUALIZACIÓN DE LIBRERÍAS.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar la actualización de librerías.

NORMAS APLICABLES

1. Los analistas Programadores serán los responsables de llevar un control de versiones de las librerías modificadas en la siguiente ubicación: //sv_admón./FUENTES_ORACLE/nombre_del_analista.
2. El control de versiones de fuentes debe de atender los siguientes estándares: creación de carpeta con el nombre de la librería, incluir dentro de la misma las subcarpetas que correspondan a la fecha de modificación.
3. El acceso a de las librerías del sistema informático; se definirá de acuerdo al módulo que cada Analista Programador tenga asignado y con derechos sólo de lectura.
4. La actualización de las de las librerías modificadas a la carpeta de librerías del sistema (//ipsfa04/src) será responsabilidad del Administrador del sistema informático que se le asignó la tarea de administración de las fuentes del sistema sin restricciones.
5. Será responsabilidad de cada Analista Programador, el mantener un respaldo actualizado de las librerías correspondientes al módulo de su responsabilidad a través de las solicitudes necesarias para su actualización.

Inicio de la Metodología.

Analista Programador

1. Realiza la solicitud de actualización del fuente de la librería a modificar; a través del registro de requerimientos a la dirección de correo electrónico helpdesk@ipsfa.com enviado por correo electrónico.
2. Actualiza las modificaciones realizadas en la forma PT00FM23-registro de bitácora modificaciones de objeto.
3. Coloca la fuente de la librería modificada en la siguiente dirección: Ej: //Ipsfa04//neo/fuentes_del_sistema_modificados_ IPSFA/Librerías.

UNIDAD DE DESARROLLO ORGANIZACIONAL

Administrador del sistema informático

4. Recibe la solicitud del requerimiento y toma la fuente de la librería solicitada; la cual se colocada en la carpeta: //Ipsfa04//neo/fuentes_del_sistema_modificados_ IPSFA/Librerías.
5. Coloca en producción la versión compilada del objeto en la carpeta: //Ipsfa04/lib, si la actualización procede pasamos al punto 8, si no continuamos.
6. Coloca en producción la versión compilada del objeto en la carpeta que fuera permitida; lo cual dependerá de si ésta se encuentra en uso o no: //Ipsfa04/run2 o //Ipsfa04/run3
7. Realiza las coordinaciones con el Administrador de la red para la actualización de la librería de la carpeta temporal (//Ipsfa04/run2 o //Ipsfa04/run3) a la definitiva //Ipsfa04/lib ; a través de requerimiento remitido por correo electrónico
8. Registra el seguimiento y finalización del requerimiento confirmando la atención y lo envía por correo electrónico desde el helpdesk@ipsfa.com

Fin de la Metodología.

NOMBRE DE LA METODOLOGÍA:

Q. NUEVOS OBJETOS EN NEO IPSFA PROGRAMACIÓN A PARTIR DE LA FORMA ESTÁNDAR

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar nuevos objetos en Neo IPSFA-Programación a partir de la forma estándar.

NORMAS APLICABLES:

El analista Programador deberá tomar como base el documento Estándares de Programación para Aplicativos NEO-IPSFA (*Anexo No. 10*), que contiene la estructura general de opciones y herramientas de una forma en Developer, Triggers Base, Alertas, Mensajes para Información al Usuario, Librería por Default, Manejo de Bloques, Canvas o Lienzo, Áreas de Trabajo, Parámetros Generales de la Aplicación, Property Classes, Atributos o Propiedades para los Elementos en las Canvas, Windows, Espacio donde se Muestra un Canvas, Estructura General de Opciones o Herramientas de un Reporte en Developer, Parámetro Default en la Aplicación Base de Reportes, Campos formula asociados al despliegue del encabezado y pie de página del reporte, Programas asociados al reporte base, Layout para la presentación de los parámetros y datos del reporte.

Inicio de la Metodología

Analista Programador

1. Se basará para desarrollar los formularios en el archivo Formbase que contiene los estándares para crear nuevos formularios. El formulario que corresponde al base se encuentra en la siguiente ubicación //ipsfa04/neo/base
2. Se basará para desarrollar los reportes en el archivo Rmachote que contiene los estándares para crear nuevos reportes. El reporte que corresponde al base se encuentra en la siguiente ubicación //ipsfa04/neo/base

3. Si el aplicativo es nuevo deberá solicitar la nomenclatura al Administrador del NEO-IPSFA para mantener los estándares establecidos. Dicha nomenclatura es manejada en el NEO-IPSFA por el tipo PT0001.
4. Si el objeto corresponde a aplicativos ya existentes deberá mantenerse la nomenclatura ya existente; y atender los correlativos de formas, reportes y librerías en producción en el NEO-IPSFA. El analista programador puede determinar el valor consecutivo con la consulta a la carpeta de objetos compilados //ipsfa04/neo/run o ipsfa04/neo/lib; dependiendo del tipo de objeto a crear.
5. Elabora formulario o reportes según requerimiento, basándose en los formatos bases mencionados anteriormente, dichos archivos se encuentran bajo la estructura de directorios del sistema en la carpeta denominada base.
6. La nomenclatura de los objetos del aplicativo deben seguir el siguiente estándar:
   - Identificación del aplicativo: indicativo de tres caracteres que corresponde al identificador colocado al módulo.
   - Identificador de tipo de objeto: M: Forma de mantenimiento, C. Forma de consulta, P: forma de proceso, R: Reporte y L: librería.
   - Correlativo: valor consecutivo por tipo de objeto.
   - Ejemplo: SIF50P26.
7. El analista programador será el responsable de mantener actualizada la documentación relacionada con el nuevo aplicativo u objeto desarrollado y la ayuda en línea para cada objeto.
8. Se pone a producción en el Sistema atendiendo el procedimiento para la Actualización de Objetos del NEO-IPSFA. Posterior a las etapas del ciclo de vida de los sistemas.

Administrador de NEO-IPSFA

9. Recibe la solicitud del requerimiento, verifica que el objeto a adicionar contenga toda la documentación correspondiente al tipo de objeto en la forma PT00FM04-Mantenimiento de Objetos y actualiza la fuente solicitada en la carpeta de fuentes del sistema (//ipsfa04/src), realiza la puesta en producción del (los) archivos fuentes en carpetas de NEO-IPSFA de acuerdo al aplicativo.
10. Verifica la creación de la ayuda en línea para el objeto nuevo creado (solamente para las Formas - Herramientas para el manejo documental). (*Anexo No. 11*).

UNIDAD DE DESARROLLO ORGANIZACIONAL

11. Coloca en producción la versión compilada del objeto en la carpeta //Ipsfa04/neo/run y la fuente del objeto en la carpeta correspondiente al módulo, submódulo y objeto a que corresponda: //Ipsfa04/ src /nombre_del_aplicativo_a_actualizar.
12. Registra el seguimiento del requerimiento confirmando la atención al Analista Programador y lo envía por correo electrónico desde el helpdesk@ipsfa.com.

Fin de la Metodología

NOMBRE DE LA METODOLOGÍA:

R. CHECK LIST DE EQUIPOS DE RED DE DATOS Y SERVIDORES

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar el check list de equipos de red de datos y servidores.

NORMAS APLICABLES

El informe que genera la presente metodología se enviará quincenalmente a la Jefatura del Departamento de Informática FORM-08-GG-INF-04

Inicio de la Metodología.

Administrador de Red

1. Monitoreo de switch: los sw son los equipos de comunicación instalados en los diferentes niveles de IPSFA, los cuales permite que se tengan accesos a red de datos, la verificación se realiza mediante Software (Host Monitor), que está constantemente realizando chequeo de las conexiones.
2. Chequeo de enlace VPN: los enlaces VPN son las conexiones o enlaces dedicados que tienen las unidades de negocio del IPSFA la cual por medio de ellos ingresan a los Aplicativos, Mail, Carpetas compartidas, Internet, la verificación se realiza mediante Software (Host Monitor), que está constantemente chequeando las conexiones.
3. Chequeo de servidores institucionales: equipos en los cuales se encuentran instalados las Bases de Datos, Aplicativos, Correo Dominio IPSFA, Internet, Carpetas compartidas Institucionales, se verifica Logs o Alarmas, Espacio en Disco, Procesos, Memoria, enlaces de red, Cuentas de Usuarios, Bases de Datos, Mail Queue, Antivirus Corp.
4. Chequeo de aire acondicionado de granja de servidores: se revisa que tenga la temperatura adecuada, para el buen funcionamiento de los equipos instalados.

   En caso que en el transcurso de los 15 días ocurriese algún inconveniente se estaría enviando el informe correspondiente al Jefe del Departamento de Informática en el mismo formulario.

Fin de la Metodología.

INSTITUTO DE PREVISION SOCIAL DE LA FUERZA ARMADA
UNIDAD DE DESARROLLO ORGANIZACIONAL

NOMBRE DE LA METODOLOGÍA:

S. TUNING A LA BASE DE DATOS

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar tuning a la base de datos.

NORMAS APLICABLES

El informe que genera la presente metodología se enviará mensualmente a la Jefatura del Departamento de Informática.

Inicio de la metodología.

Administrador de la Base de Datos

1. Buscar las tasas de crecimiento dañinas o peligrosas: revisar los cambios en el crecimiento de los segmentos cuando son comparados con reportes anteriores para identificar segmentos con rangos de crecimiento dañino o peligroso.
2. Review Tuning Opportunities: revisar Puntos comunes de Tuning de Oracle Tales como cache hit ratio, latch contention, y otros puntos que tienen que ver con la administración de memoria.

   Comparar con reportes anteriores (historial) para identificar las tendencias (trends) dañinas que determinan el impacto que causaron los ajustes de los tunings recientes.
3. Búsqueda de I/O Contention: revisar la Actividad de database file. Comparar la última salida para identificar las tendencias que podrían conducir a una posible contención. Es necesario correr el script disk_read.sql
4. Revisión de Fragmentación: investigar fragmentación, es necesario correr el script check_frag.sql.

   Los resultados obtenidos pueden ser: 1 ‘No Frag’, Bubble Frag’, considerando que:

   No Frag y Bubble Frag no son dañinos para la base de datos, siempre y cuando en tamaño sean iguales.
5. Hacer proyecciones de Funcionamiento de los recursos en el Futuro: comparar reportes de CPU, memoria, red y utilización de disco de ambos Oracle y el Sistema Operativo

para identificar tendencias que podrían llevar a la contención a alguno de los recursos en futuro cercano.

6. Comparar las tendencias del funcionamiento de acuerdo al porcentaje de disponibilidad para poder ver cuando el sistema se saldrá de límites.
7. Realizar Tuning y Mantenimientos: hacer los ajustes necesarios para evitar la contención de los recursos del sistema. Esto puede incluir programar Down-Time o solicitar recursos adicionales.

Fin de la Metodología.

NOMBRE DE LA METODOLOGÍA:

T. ENVÍO DE DMP AL SITIO DE CONTINGENCIA

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar el envío de DMP al Sitio de Contingencia.

NORMAS APLICABLES

Se enviarán los DMP al sitio de contingencia diariamente por medio de FTP (File Transfer Protocol) u otro canal de comunicación, al inicio del día siguiente al que se han generado los respaldos.

Inicio de la metodología.

Administrador de la Base de Datos

1. Se conecta al servidor de base de datos de producción ubicando el archivo generado por el sistema de forma automática durante la noche, luego se conecta al sitio de contingencia por medio de FTP u otro canal de comunicación, busca la carpeta donde se transferirá el archivo e inicia transferencia.
2. Una vez terminada la transferencia verifica que el archivo ha sido enviado correctamente.
3. Cierra conexión con el sitio de contingencia.

Fin de la metodología.

NOMBRE DE LA METODOLOGÍA:

U. MONITOREO DEL ANCHO DE BANDA DE INTERNET.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar el monitoreo del ancho de banda de internet.

Inicio de la Metodología

Administrador de Red

1. Accede al sitio Web determinado por el proveedor del servicio.
2. Genera diagnóstico del estado de ancho de banda.
3. Elabora informe – Test de velocidad (*Anexo No. 2*).
4. Resguarda Test para presentarlo como evidencia del POA sobre monitoreo de los enlaces.

Fin de la Metodología

NOMBRE DE LA METODOLOGÍA:

V. PROGRAMACIÓN A PARTIR DE LA FORMA ESTÁNDAR

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar la programación a partir de la forma estándar.

NORMAS APLICABLES:

El analista Programador deberá tomar como base el documento Estándares de Programación para Aplicativos NEO-IPSFA (*Anexo No. 3*), que contiene la estructura general de opciones y herramientas de una forma en Developer, Triggers Base, Alertas, Mensajes para Información al Usuario, Librería por Default, Manejo de Bloques, Canvas o Lienzo, Áreas de Trabajo, Parámetros Generales de la Aplicación, Property Classes, Atributos o Propiedades para los Elementos en las Canvas, Windows, Espacio donde se Muestra un Canvas, Estructura General de Opciones o Herramientas de un Reporte en Developer, Parámetro de Default en la Aplicación Base de Reportes, Campos formula asociados al despliegue del encabezado u pie de página del reporte, Programas asociados al reporte base, Layout para la presentación para los parámetros y datos del reporte.

Inicio de la Metodología

Analista Programador

1. Se basará para desarrollar los formularios en el archivo Formbase que contiene los estándares crear nuevos formularios.
2. Se basará para desarrollar los reportes en el archivo Rmachote que contiene los estándares para crear nuevos reportes.
3. Si el aplicativo es nuevo deberá solicitar la nomecaltura al Administrador del NEO-IPSFA para mantener los estándares establecidos.
4. Elabora formulario o reportes según requerimiento, basándose en los formatos bases mencionados anteriormente, dichos archivos se encuentran bajo la estructura de directorios del sistema en la carpeta denominada base.
5. Se pone a producción en el Sistema. Posterior a las etapas del ciclo de vida de los sistemas.

Fin de la Metodología.

UNIDAD DE DESARROLLO ORGANIZACIONAL

NOMBRE DE LA METODOLOGÍA:

W. OPTIMIZACIÓN DE LA BASE DE DATOS.

OBJETIVO DE LA METODOLOGÍA:

Verificar el buen funcionamiento de las diversas bases de datos del IPSFA.

1. PROCEDIMIENTOS DIARIOS:

1.1 Verificar que todas las instancias estén arriba:

a) Asegurarse que la base de datos esté disponible. Conectándose en cada una de las instancias que se administran y correr los reportes diarios o scripts de Prueba.

b) Implementación Opcional: usando Oracle Enterprise Manager's.

1.2 Buscar alguna alerta nueva en los registros de LOG:

a) Conectarse a cada una de las instancias administradas.

b) Usando 'telnet' o programas parecidos.

c) Para cada una de las instancias administradas, ir al the background dump destination, usualmente $ORACLE_BASE/<SID>/bdump. Ej.:oracle/admin./IPSFADES/bdump, es necesario asegurarse de hacer esto para cada una de las bases SID administradas.

d) En el prompt, use el comando de Unix 'tail' o también el comando 'less' para ver el alert_<SID>.log, o también otra forma es examinar la entrada más reciente en el archivo.

1.3 Verificar si el DBSNMP está corriendo:

a) Conectarse en cada una de las maquinas o servidores que se administran para revisar el proceso 'dbsnmp'.

b) Para Unix: en la línea de comando, digitar ps –ef | grep dbsnmp. Debería de haber dos procesos corriendo de dbsnmp. Si no, restart DBSNMP. (en algunos casos esta opción puede estas deshabilitada por políticas internas ; si este es el caso, obviar este paso de la lista o cambiar el ítem por "verificar si el DBSNMP no está corriendo".)

c) Para Solaris: ps –e | grep dbsnmp

1.4 Verificar si el respaldo de la base de datos fue finalizado satisfactoriamente.

1.5 Verificar si el respaldo fue grabado a tape satisfactoriamente.

1.6 Verificar si existen suficientes recursos para un funcionamiento aceptable:

a) Verificar el espacio libre de cada tablespaces.

b) Para cada una de las instancias, es necesario verificar si existe suficiente espacio libre para el crecimiento diario previsto. En fecha <date>, el espacio mínimo para <se repite por cada >: [< tablespace > es < cantidad >]. Cuando los datos entrantes son estables, y crecimiento promedio diario puede ser calculado, entonces el espacio libre mínimo debe ser por lo menos <tiempo para: solicitar, adquirir o instalar más discos> para el crecimiento diario.

i. Conectarse en cada una de las instancias, correr el script free.sql para revisar el espacio libre en mb de cada tablespaces. Compare el espacio mínimo libre en MB para cada tablespace. Identifique cada condición low-space y corríjalo.

Free.sql

```
--
-- free.sql
--
--  To verify free space in tablespaces
--  Minimum amount of free space
--  document your thresholds:
--  <tablespace_name> = <amount> m
--

SELECT  tablespace_name, sum ( blocks ) as free_blk , trunc ( sum ( bytes ) / (1024*1024) ) as free_m
, max ( bytes ) / (1024) as big_chunk_k, count (*) as num_chunks
FROM dba_free_space
GROUP BY tablespace_name
```

ii. Conectarse en cada una de las instancias, correr el script space.sql para revisar el porcentaje libre en cada tablespaces.

Space.sql

```
--
-- space.sql
--
-- To check free, pct_free, and allocated space within a tablespace
--
-- 11/24/98
```

```
SELECT tablespace_name, largest_free_chunk
    , nr_free_chunks, sum_alloc_blocks, sum_free_blocks
    , to_char(100*sum_free_blocks/sum_alloc_blocks, '09.99') || '%'
      AS pct_free
FROM ( SELECT tablespace_name
          , sum(blocks) AS sum_alloc_blocks
       FROM dba_data_files
       GROUP BY tablespace_name
     )
   , ( SELECT tablespace_name AS fs_ts_name
          , max(blocks) AS largest_free_chunk
          , count(blocks) AS nr_free_chunks
          , sum(blocks) AS sum_free_blocks
            FROM dba_free_space
            GROUP BY tablespace_name )
WHERE tablespace_name = fs_ts_name
```

c) Compare el espacio mínimo libre en porcentaje para cada tablespace. Identifique cada condición low-space y corríjalo.

d) Verificar rollback segment.

El estatus debe estar ONLINE, no OFFLINE o FULL, excepto en algunos casos se puede tener rollback segment especial para batch jobs largos de quien su estado normal es OFFLINE.

i. Opcional: cada base de datos puede tener una lista de nombres rollback segment y sus estados previstos.

ii. Para el estatus actual de cada ONLINE o FULL rollback segment (por ID no por nombre), hacer query en V$ROLLSTAT.

iii. Para los parámetros de almacenamiento y nombres de TODOS LOS rollback segment, hacer query en DBA_ROLLBACK_SEGS. El campo ESTADO de esa vista es menos exacto que V$ROLLSTAT, sin embargo, como carece de los estados PENDING OFFLINE y FULL, muestra estos como OFFLINE y ONLINE respectivamente.

e) Identificar malas proyecciones de crecimiento.

Buscar los segmentos en la base de datos que se están saliendo (running out) de los recursos (ej. extents) o están creciendo en una tarifa excesiva. Los parámetros de almacenamientos para estos segmentos pueden necesitar ser ajustados. Por Ejemplo, si algún objeto alcanza 200 como

numero de Extetns Actuales y es un objeto que se supone que será grande, es necesario mejorarlo o actualizar los max_extents a unlimited.

i. Para recopilar la información diaria del sizing, correr el script analyze5pct.sql. Ahora bien si se está recopilando la información volumétrica de forma nocturna se puede saltar este paso.

analyze5pct.sql

```
--
-- analyze5pct.sql
--
-- To analyze tables and indexes quickly, using a 5% sample size
-- (do not use this script if you are performing the overnight
-- collection of volumetric data)
--
-- 11/30/98

BEGIN
  dbms_utility.analyze_schema ( '&OWNER', 'ESTIMATE', NULL,
5 ) ;
END ;
/
```

ii. Para revisar los current extents, correr el script nr_extents.sql

nr_extents.sql

```
--
-- nr_extents.sql
--
-- To find out any object reaching <threshold>
-- extents, and manually upgrade it to allow unlimited
-- max_extents (thus only objects we *expect* to be big
-- are allowed to become big)
--
-- 11/30/98

SELECT e.owner, e.segment_type , e.segment_name , count(*) as
nr_extents , s.max_extents
, to_char ( sum ( e.bytes ) / ( 1024 * 1024 ) , '999,999.90') as MB
FROM dba_extents e , dba_segments s
WHERE e.segment_name = s.segment_name
  AND e.owner = s.owner              -- 2001.10.19 Evgueni B. fix
GROUP BY e.owner, e.segment_type , e.segment_name ,
s.max_extents
HAVING count(*) > &THRESHOLD
   OR ( ( s.max_extents - count(*) ) < &&THRESHOLD )
ORDER BY count(*) desc
```

iii. Consultar: current table sizing information

iv. Consultar: current index sizing information

f) Consultar: growth trends

g) Identificar space-bound objects.

Space-bound objects' next_extents es el más grande extend que los tablespaces pueden ofrecer. Space-bound objects puede dañar la operación de la base de datos. Si conseguimos tal objeto, primero es necesario investigar la situación. Entonces podremos usar el ALTER TABLESPACE <tablespace> COALESCE. o agregar otro datafile.

i. Corra el script spacebound.sql. si todo está bien, Cero rows retornaran del Query.

spacebound.sql

```
--
-- spacebound.sql
--
-- To identify space-bound objects.  If all is well, no rows are returned.
-- If any space-bound objects are found, look at value of NEXT extent
-- size to figure out what happened.
-- Then use coalesce (alter tablespace <foo> coalesce;).
-- Lastly, add another datafile to the tablespace if needed.
--
-- 11/30/98

SELECT a.table_name, a.next_extent, a.tablespace_name
FROM all_tables a,
   ( SELECT tablespace_name, max(bytes) as big_chunk
     FROM dba_free_space
     GROUP BY tablespace_name ) f
WHERE f.tablespace_name = a.tablespace_name
 AND a.next_extent > f.big_chunk
```

h) Procesos para revisar la contención para CPU, memoria, red o recursos de disco.

i. Para dicha revision es necesario ver Task Manager (Windows), Histograma

2. PROCEDIMIENTOS NOCTURNOS

2.1 La mayoría de las bases de datos de producción (y muchas de las bases de datos del desarrollo y de prueba) pueden beneficiarse ejecutando procesos nocturnos para el monitoreo de la base de datos.

a) Recopilar datos Volumétricos

Este ejemplo recopila table row counts. Puede fácilmente ampliarse a otro tipo de objetos como indexes, y otro tipo como average row sizes.

b) Analizar Schemas y Collect Data.

La idea aquí es utlizar los comandos more time consuming and more accurate ANALYZE COMPUTE y guardar los resultados, which show up in the data dictionary, to a more permanent store.

i. Si ya se ha creado la tabla de volumetrics con mk_volfact.sql

mk_volfact.sql

```
--
-- mk_volfact.sql (only run this once to set it up; do not run it nightly!)
--
-- -- Table UTL_VOL_FACTS

CREATE TABLE utl_vol_facts
 (
  table_name              VARCHAR2(30),
  num_rows                NUMBER,
  meas_dt                DATE
 )
TABLESPACE platab
 STORAGE   (
     INITIAL     128k
     NEXT       128k
     PCTINCREASE 0
     MINEXTENTS  1
     MAXEXTENTS  unlimited
   )
/

-- Public Synonym

CREATE PUBLIC SYNONYM utl_vol_facts FOR &OWNER..utl_vol_facts
/
```

```
-- Grants for UTL_VOL_FACTS

GRANT SELECT ON utl_vol_facts TO public
/
```

ii. Para obtener de manera nocturna la sizing information, es necesario correr el script analyze_comp.sql.

analyze_comp.sql

```
--
-- analyze_comp.sql
--
BEGIN
  sys.dbms_utility.analyze_schema ( '&OWNER','COMPUTE');
END ;
/
```

iii. Para recopilar las estadísticas resultantes es necesario correr el script pop_vol.sql

pop_vol.sql

```
-- pop_vol.sql
insert into utl_vol_facts
select table_name
    , NVL ( num_rows, 0) as num_rows
    , trunc ( last_analyzed ) as meas_dt
from all_tables          -- or just user_tables
where owner in ('&OWNER') -- or a comma-separated list of owners
/
commit
/
```

iv. Examinar la data, probablemente semanal o mensual. Se puede utilizar MS Excel y una conexión ODBC para examinar y graficar el crecimiento de datos.

3. PROCEDIMIENTOS SEMANALES

3.1 Buscar Objetos que este rompiendo las reglas (break rules):

Por cada object-creation policy (naming convention, storage parameters, etc.) tener un chequeo automatizado para verificar que se está siguiendo la política.

a) Cada objeto en un tablespace dado, debe tener el exactamente el mismo tamaño por NEXT_EXTENT, el cual debe hacer match con el tablespace default para NEXT_EXTENT. Por ejemplo En fecha 12/14/98, por defecto NEXT_EXTENT para DATAHI es 1 gig (1048576 kilobytes), DATALO es mb 500 (524288 kilobytes), y los ÍNDICES son mb 256 (262144 kilobytes).

i. Par revisar el settings de NEXT_EXTENT, correr el script nextext.sql.

nextext.sql

```
--
-- nextext.sql
--
-- To find tables that don't match the tablespace default for NEXT extent.
-- The implicit rule here is that every table in a given tablespace should
-- use the exact same value for NEXT, which should also be the tablespace's
-- default value for NEXT.
--
-- This tells us what the setting for NEXT is for these objects today.
--
-- 11/30/98

SELECT segment_name, segment_type, ds.next_extent as Actual_Next
, dt.tablespace_name, dt.next_extent as Default_Next
FROM dba_tablespaces dt, dba_segments ds
WHERE dt.tablespace_name = ds.tablespace_name
  AND dt.next_extent !=ds.next_extent
AND ds.owner = UPPER ( '&OWNER' )
ORDER BY tablespace_name, segment_type, segment_name
```

ii. Para revidar los extents existentes, es necesario correr el Script existext.sql

existext.sql

```
--
-- existext.sql
--
```

```
-- To check existing extents
--
-- This tells us how many of each object's extents differ in size from
-- the tablespace's default size. If this report shows a lot of different
-- sized extents, your free space is likely to become fragmented.  If so,
-- this tablespace is a candidate for reorganizing.
--
-- 12/15/98

SELECT segment_name, segment_type
, count(*) as nr_exts
, sum ( DECODE ( dx.bytes,dt.next_extent,0,1) ) as nr_illsized_exts
, dt.tablespace_name, dt.next_extent as dflt_ext_size
FROM dba_tablespaces dt, dba_extents dx
WHERE dt.tablespace_name = dx.tablespace_name
AND dx.owner = '&OWNER'
GROUP BY segment_name, segment_type, dt.tablespace_name,
dt.next_extent
```

b) Todas las tablas deben de tener unique primary keys.

i. Para revisar missing PK, Correr el Script no_pk.sql.

No_pk.sql

```
--
-- no_pk.sql
--
-- To find tables without PK constraint
--
-- 11/2/98

SELECT table_name
FROM all_tables
WHERE owner = '&OWNER'
MINUS
SELECT table_name
FROM all_constraints
WHERE owner = '&&OWNER'
AND constraint_type = 'P'
```

ii. Para revisar disabled PK, Correr el Script disPK.sql.

disPK.sql

```
--
-- disPK.sql
--
-- To find out which primary keys are disabled
--
```

```
-- 11/30/98

SELECT owner, constraint_name, table_name, status
FROM all_constraints
WHERE owner = '&OWNER' AND status = 'DISABLED' AND
constraint_type = 'P'
```

c) Todas las primary key indexes debe ser unique. Correr el Script nonuPK.sql para revisarlo.

nonuPK.sql

```
--
--  nonuPK.sql
--
-- To find tables with nonunique PK indexes.  Requires that PK
names
-- follow a naming convention.  An alternative query follows that
-- does not have this requirement, but runs more slowly.
--
-- 11/2/98


SELECT index_name, table_name, uniqueness
FROM all_indexes
WHERE index_name like '&PKNAME%'
  AND owner = '&OWNER' AND uniqueness = 'NONUNIQUE'

SELECT c.constraint_name, i.tablespace_name, i.uniqueness
FROM all_constraints c , all_indexes i
WHERE c.owner = UPPER ( '&OWNER' ) AND i.uniqueness =
'NONUNIQUE'
AND c.constraint_type = 'P' AND i.index_name = c.constraint_name
```

d) Todos los índices deben estar en el tablespace asignadoa a los INDEXES. Para asignar los indices a ese tablespace se puede ejecutar el siguientes script mkrebuild_idx.sql.

mkrebuild_idx.sql

```
--  mkrebuild_idx.sql
--
-- Rebuild indexes to have correct storage parameters
--
-- 11/2/98

SELECT 'alter index ' || index_name || ' rebuild '
    , 'tablespace INDEXES storage '
```

```
    || ' ( initial 256 K next 256 K pctincrease 0 ) ; '
FROM all_indexes
WHERE ( tablespace_name != 'INDEXES'
      OR next_extent != ( 256 * 1024 )
    )
  AND owner = '&OWNER'
/
```

e) Los esquemas deben ser identicos entre instancias, especificamente la de Producción y Desarrollo.

i. Para revisar la consistencia entre los tipos de datos, correr el script datatype.sql.

datatype.sql

```
--
-- datatype.sql
--
-- To check datatype consistency between two environments
--
-- 11/30/98

SELECT
  table_name,
  column_name,
  data_type,
  data_length,
  data_precision,
  data_scale,
  nullable
FROM all_tab_columns -- first environment
WHERE owner = '&OWNER'
MINUS
SELECT
  table_name,
  column_name,
  data_type,
  data_length,
  data_precision,
  data_scale,
  nullable
FROM all_tab_columns@&my_db_link  -- second environment
WHERE owner = '&OWNER2'
order by table_name, column_name
```

ii. Para revisar otro object consistency, correr el script obj_coord.sql.

obj_coord.sql

```
--
-- obj_coord.sql
--
-- To find out any difference in objects between two instances
--
-- 12/08/98

SELECT object_name, object_type
FROM user_objects
MINUS
SELECT object_name, object_type
FROM user_objects@&my_db_link
```

iii. Mejor aún se puede utilizar Quest Software's Schema Manager.

3.2 Búsqueda de violaciones en la política de seguridad. (Security policy violations)

3.3 Buscar en SQL*Net logs por errores, issues:

a. Client side logs

b. Server side logs

3.4 Archivar todos los Alert Logs en un historial

3.5 Visitar homepages, para búsqueda de actualizaciones, código y técnicas mas recientes.

i. Oracle Corporation

c. http://www.oracle.com

d. http://technet.oracle.com

e. http://www.oracle.com/support

f. http://www.oramag.com

b) Quest Software

g. http://www.quests.com

c) Sun Microsystems

h. http://www.sun.com

4. PROCEDIMIENTOS MENSUALES

4.1 Buscar las tasas de crecimiento dañinas o peligrosas:

a) Revisar los cambios en el crecimiento de los segmentos cuando son comparados con reportes anteriores (historial) para identificar segmentos con rangos de crecimiento dañino o peligroso.

4.2 Review Tuning Opportunities:

a) Revisión de Puntos comunes de Tuning de Oracle Tales como cache hit ratio, latch contention, y otros puntos que tienen que con la administración de memoria. Comparar con reportes anteriores (historial) para identificar las tendencias (trends) dañinas determinan el impacto que causaron los ajustes de los tunings recientes.

4.3 Búsqueda de I/O Contention:

a) Revisar la Actividad de database file. Comparar la última salida para identificar las tendencias que podrían conducir a una posible contención.

4.4 Revisión de Fragmentación:

a) Investigar fragmentación (ej. row chaining, etc.).

4.5 Hacer proyecciones de Funcionamiento de los recursos en el Futuro:

a) Comparar reportes de CPU, memoria, red y utilización de disco de ambos Oracle y el SO para identificar tendencias que podrían llevar a contención a alguno de los recursos en futuro cercano.

b) Comparar las tendencias del funcionamiento de acuerdo al porcentaje de disponibilidad para poder ver cuando el sistema se saldrá de límites.

4.6 Realizar Tuning y Mantenimientos:

a) Hacer los ajustes necesarios para evitar la contención de los recursos de sistema. Esto puede incluir programar Down-Time o solicitar recursos adicionales.

NOMBRE DE LA METODOLOGÍA:

X. CONTROL DE ACCESOS DESDE LA ADMINISTRACIÓN DEL NEO-IPSFA.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar el control de accesos desde la administración del Neo IPSFA.

NORMAS APLICABLES:

1. Todo acceso será canalizado a través de los responsables de los aplicativos, estos gestionarán por medio de correo electrónico o en el formulario de requerimientos dichos accesos ante el Departamento de Informática.
2. El Administrador del Neo-IPSFA, será el responsables de proporcionar los accesos a los roles del Neo-IPSFA que sean detallado en el requerimiento.

Inicio de la Metodología

Unidad Solicitante

1. Hará una solicitud vía correo electrónico al responsable del módulo de los accesos que requiere para un usuario en específico.

Responsable del (los) aplicativos

2. Enviará a el Departamento de Informática, el requerimiento detallando los datos siguientes: usuario, roles que serán asociados (Formas, Reportes, etc.), vía correo electrónico o utilizando el formulario de requerimientos.

Administrador Neo-IPSFA

3. Verificar los roles que le corresponden de acuerdo al detalle de lo requerido
4. Adicionar los roles al usuario especificado.
5. Comunicar vía correo electrónico que los roles han sido asignados.

Fin de la Metodología.

INSTITUTO DE PREVISION SOCIAL DE LA FUERZA ARMADA
UNIDAD DE DESARROLLO ORGANIZACIONAL

NOMBRE DE LA METODOLOGÍA:

Y. CREACIÓN DE USUARIOS EN BASE DE DATOS Y ADMINISTRACIÓN NEO-IPSFA.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar la creación de usuarios en base de datos y administración Neo IPSFA.

NORMAS APLICABLES:

1. Todo acceso será canalizado a través de los responsables de los aplicativos, estos gestionarán por medio de correo electrónico dirigido a helpdesk@ipsfa.com o en el formulario de requerimientos dichos accesos ante el Departamento de Informática.
2. El Administrador de la Base de Datos (DBA), será el responsables de crear el usuario en la Base de Datos.
3. El Administrador del NEO-IPSFA, será el responsables de crear el usuario en la administración del NEO-IPSFA.

Inicio de la Metodología

Unidad Solicitante

1. Solicitará la creación y/o modificación de usuario para los aplicativos, desde formulario de requerimientos creación y/o modificación de usuarios y/o correo electrónico a helpdesk@ipsfa.com.
2. En caso de que se requiera la desactivación de un usuario para los aplicativos deberá llenar el Formulario de Desactivación de Usuarios y/o modificación de usuarios vía correo electrónico a helpdesk@ipsfa.com.

Administrador de Base de Datos o Administrador Neo-IPSFA

3. Procederá a crear, modificar y/o desactivar, el usuario de acuerdo a lo requerido.
4. El administrador que atendió el requerimiento, notificará vía correo electrónico al usuario que su solicitud ha sido atendida y remitirá clave creada cuando sea el caso.

Fin de la Metodología.

UNIDAD DE DESARROLLO ORGANIZACIONAL

NOMBRE DE LA METODOLOGÍA:

Z. MODIFICACIÓN, CREACIÓN Y ELIMINACIÓN DE OBJETOS EN BASE DE DATOS

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar en caso de modificación, creación y eliminación de objetos en base de datos.

Inicio de la Metodología

Analista Programador

1. Solicita por medio de un correo electrónico a la dirección helpdesk@ipsfa.com la creación, modificación o eliminación del objeto de base de datos.

Administrador de NEO-IPSFA

2. Verifica que se realice la documentación respectiva del cambio de estructuras, vistas, etc
3. Asigna el requerimiento al Administrador de Base de Datos.

Administrador de Base de Datos

4. Verifica el nombre del objeto y sintaxis del scrip de creación, modificación o eliminación del objeto.
5. Se conecta a la base de datos con el usuario propietario (donde se creara el objeto).
6. ejecuta el scrip que contiene la creación modificación o eliminación del objeto.
7. En el caso de que el requerimiento sea de creación se otorgan privilegios y sinónimos sobre el objeto.
8. Notifica por medio de correo electrónico, al Analista programador que se realizó el requerimiento solicitado.

Fin de la Metodología

NOMBRE DE LA METODOLOGÍA:

AA. REUNIONES DE TRABAJO CON USUARIOS

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar las reuniones de trabajo con los usuarios.

NORMAS APLICABLES

Para los casos en que se desarrolle nuevos aplicativos y modificaciones a procesos principales, el Analista Programador deberá elaborar una minuta de reunión, al finalizar cada sesión de trabajo con los usuarios, donde especificará los participantes, los puntos tratados y acordados, remitiendo copia al Coordinador de Análisis y Programación.

Inicio de la Metodología

Analista Programador

1. Solicitará al Coordinador él envió de la convocatoria al área responsable del aplicativo, detallando motivo de la reunión.(Creación de nuevos aplicativos, nuevos procesos, desarrollo de proyectos).
2. Deberá llenar la minuta de reunión, con puntos tratados, acordados, detallando los participantes. (Anexo No. 12).
3. Entregará minuta de reunión firmada por los integrantes en la reunión al Coordinador de Análisis y Programación.

Coordinador de Análisis y Programación

4. Hará la convocatoria a los usuarios por medio de correo electrónico, solicitando confirmación a la misma.
5. Resguardará la minuta de reunión en la siguiente dirección: Documentación NEO-IPSFA\MinutasdeReunion\aplicativo.

Fin de la Metodología.

NOMBRE DE LA METODOLOGÍA:

BB. CONTROL MENSUAL DEL MONITOREO Y RENDIMIENTO DE LA BASE DE DATOS.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para realizar el control mensual del monitoreo y rendimiento de la base de datos.

NORMAS APLICABLES

Mensualmente el Administrador de la base de datos generará un reporte del rendimiento de la base de datos, el cual enviará a la Jefatura del Departamento de Informática.

Inicio de la metodología.

Administrador de la Base de Datos

1. **Busca las tasas de crecimiento dañinas o peligrosas.**
   Revisa los cambios en el crecimiento de los segmentos comparados con reportes anteriores, para identificar segmentos con rangos de crecimiento dañino o peligroso.
2. **Revisa Objetos dentro de la Base de Datos**
   a) Revisar los objetos inválidos dentro de la base de datos como: triggers desactivados o vistas invalidas y le ejecución del programa utlrp.sql para mantener en mejor estado la base de datos.
   b) Revisa el log de la base de datos.
3. **Revisar el Hardware de mantenimiento de almacenamiento (+ASM)**
   a) Revisar el estado del Hardware de mantenimiento de almacenamiento (+ASM) que se encuentre activo.
   b) Revisar el log de alertas del mismo.
4. **Revisar el servidor de base de datos.**
   a) Revisar el espacio de los datafiles del servidor de la base de datos, para que la base se ejecute sin ningún problema.

UNIDAD DE DESARROLLO ORGANIZACIONAL

b) Revisar el Backup de la base de datos diariamente que sea efectuado en el servidor.

5. **Revisa la conexión del Sitio de Contingencia**

a) Revisa que se encuentre activa.la conexión entre el sitio de contingencia y el IPSFA.

b) envía diariamente el DMP'S de respaldo más actualizado al sitio de contingencia.

6. **Revisa el Servidor de Aplicaciones**

a) Revisa los componentes que estén activos.

b) Revisa el espacio del servidor.

7. **Actualización de bases de datos de prueba**

a) Actualiza la instancia de prueba de manera total cada día lunes o cuando se requerido por el área de análisis y programación.

Fin de la Metodología.

NOMBRE DE LA METODOLOGÍA:

CC. CAMBIO DE CONTRASEÑA DE USUARIO NEO-IPSFA.

OBJETIVO DE LA METODOLOGÍA:

Conocer los pasos para que los usuarios del NEO-IPSFA puedan realizar el cambio de contraseña en el momento que consideren conveniente.

CONSIDERACIONES PARA EL CAMBIO DE CONTRASEÑA:

- Contraseñas con 8 dígitos como mínimo
- Se recomienda usar números y letras para mayor seguridad
- No se permite reutilizar contraseñas.

Inicio de la Metodología

Usuario NEO-IPSFA

1. Ingresa a la pantalla de inicio del Sistema NEO-IPSFA
2. Ingresa con su usuario y contraseña.
3. Selecciona el botón cambiar contraseña.
4. Despliega pantalla que le pide ingresar la contraseña actual, la nueva contraseña y la confirmación de esta.
5. Llena los cambios requeridos y presiona el botón cambiar.
6. Sistema despliega mensaje en pantalla “contraseña cambiada”.
7. Presiona botón aceptar
8. Sistema despliega mensaje “la contraseña ha sido cambiada con éxito”

Fin de la Metodología.

NOMBRE DE LA METODOLOGÍA:

DD. ASIGNACIÓN DE PRIVILEGIOS EN ACCESOS DE INTERNET.

OBJETIVO DE LA METODOLOGÍA:

Conocer los pasos para realizar la asignación de privilegios en accesos de internet.

Inicio de la Metodología

Jefe de la Unidad Solicitante

1 Solicita al Jefe del Departamento de Informática vía email, llamada telefónica o por medio de memorándum la asignación de privilegios en accesos de internet.

Jefe del Departamento de Informática

2 Verifica requerimiento; y en caso de otorgar el visto bueno a lo solicitado, ordena al Administrador de Red/Administrador de Red Jr., que asigne privilegios en accesos de internet según lo autorizado.

Administrador de Red/ Administrador de Red Jr.

3 Asigna privilegios en accesos de internet según lo autorizado.

4 Notifica al solicitante recomendando que realice el cierre de la sesión de trabajo del equipo informático asignado y que vuelva a ingresar, con la finalidad de activar los cambios realizados para que los pueda utilizar.

5 Informa al Jefe del Departamento de Informática los detalles del caso.

6 Fin de la Metodología

NOMBRE DE LA METODOLOGÍA:

EE. ASIGNACIÓN DE ACCESOS INFORMÁTICOS A EMPLEADOS IPSFA.

OBJETIVO DE LA METODOLOGÍA:

Conocer los pasos para realizar la asignación de accesos informáticos a empleados IPSFA.

Inicio de la Metodología

Jefe de la Unidad Solicitante

1 Solicita al Jefe del Departamento de Informática vía email, llamada telefónica o por medio de memorándum la asignación de accesos informáticos/recursos informáticos.

Jefe del Departamento de Informática

2 Verifica requerimiento; y en caso de otorgar el visto bueno a lo solicitado, designa a un Coordinador del Departamento de Informática según lo solicitado, para que habilite el acceso informático según lo autorizado.

Coordinador designado del Departamento de Informática

3 Habilita acceso informático según lo autorizado.

4 En caso de habilitar acceso a red, notifica al solicitante recomendando que realice el cierre de la sesión de trabajo del equipo informático asignado y que vuelva a ingresar, lo anterior con la finalidad de activar los cambios realizados y que los pueda realizar.

5 En caso que se haya habilitado otro acceso solo notificará al solicitante y realizará pruebas de acceso.

6 Informa al Jefe del Departamento de Informática los detalles del caso.

Fin de la Metodología

UNIDAD DE DESARROLLO ORGANIZACIONAL

NOMBRE DE LA METODOLOGÍA:

FF. SUSPENSIÓN DE ACCESOS INFORMÁTICOS EN CASO DE DESPIDO O RENUNCIA DE EMPLEADOS IPSFA.

OBJETIVO DE LA METODOLOGÍA:

Conocer los pasos para realizar la suspensión de accesos a recursos compartidos en caso de despido o renuncia de empleados IPSFA.

Inicio de la Metodología

Jefe del Departamento de Recursos Humanos

1 Notifica al Jefe del Departamento de Informática, vía email el personal que se encuentra despedido o que ha renunciado del IPSFA.

Jefe del Departamento de Informática

2 Toma medidas de precaución para manejar de forma confidencial, las actividades a realizar.

3 Informa de la situación al Coordinador de Análisis y Programación, y al Administrador de Red.

4 Si el personal que está en calidad de despedido/renuncia aún realiza trabajos en el IPSFA, ordena que se realice un respaldo de la data de los usuarios correspondientes; y comunica al Jefe del Departamento de Recursos Humanos que está listo el backup y le solicita el visto bueno para suspender los accesos informáticos.

5 Ordena se realice la suspensión de los accesos informáticos de los usuarios correspondientes.

Coordinador de Análisis y Programación

6 Realiza el bloqueo de todos los sistemas administrativos y aplicativos del IPSFA a los usuarios correspondientes; e informa al Jefe del Departamento de Informática.

Coordinador de Análisis y Programación

7 Realiza el bloqueo de cuentas de correo, usuario de red, acceso a internet, etc. a los usuarios correspondientes; e informa al Jefe del Departamento de Informática.

Fin de la Metodología

UNIDAD DE DESARROLLO ORGANIZACIONAL

NOMBRE DE LA METODOLOGÍA:

GG. PUESTA EN CUARENTENA DE EQUIPOS INFECTADOS CON VIRUS O MALWARE.

OBJETIVO DE LA METODOLOGÍA:

Conocer los pasos a realizar para poner en cuarentena equipos infectados con virus o malware.

Inicio de la Metodología

Administrador de Red/ Administrador de Red Jr.

1 Identifica la amenaza y la vía de ataque, a través del aviso del antivirus (vía correo electrónico), o al momento de monitorear el servidor del antivirus.

2 Identifica los equipos infectados.

3 Pone en cuarentena los equipos infectados, debiendo realizar como mínimo las siguientes tareas:

a. Aislar de la red institucional los equipos infectados, y
b. Notificar al usuario del porque se está aislando el equipo infectado de la red.

4 Realiza un escaneo profundo con el antivirus institucional al equipo infectado, analizando la amenaza para eliminarla; en caso de no poder eliminar la amenaza, contacta a la empresa de soporte técnico del antivirus para que eliminen la amenaza.

5 Una vez eliminada la amenaza, realiza limpieza del equipo informático y pruebas de funcionamiento hasta asegurar el funcionamiento óptimo de dicho equipo.

6 Conecta nuevamente el equipo, y notifica al/los usuario(s) que se ha(n) conectado nuevamente el/los equipo(s); y realiza recomendaciones de uso para evitar futuras infecciones.

7 Una vez resuelto el ataque, debe revisar el incidente y de ser necesario modificar los procedimientos internos para evitar la reiteración del tipo de ataque en el futuro.

8 Informa al Jefe del Departamento de Informática los detalles del incidente.

Fin de la Metodología

NOMBRE DE LA METODOLOGÍA:

HH. INCLUIR EN RED WIFI A EQUIPOS PERSONALES DE EMPLEADOS IPSFA Y VISITAS OFICIALES.

OBJETIVO DE LA METODOLOGÍA:

Conocer los pasos a realizar para incluir en red wifi equipos personales de empleados IPSFA y visitas oficiales.

Inicio de la Metodología

Administrador de Red/ Administrador de Red Jr.

Equipos personales.

Red wifi contralada vía MAC Address

1 En caso de equipos personales, el dueño del dispositivo (Laptops, tablets, smarphones, etc.) lo solicita al Jefe del Departamento de Informática a través de email, llamada telefónica o de manera personal.

2 Al tener el visto bueno del Jefe del Departamento de Informática, se prepara el dispositivo para poder instalar solución antivirus institucional; esto implica desinstalar cualquier otra solución antivirus que está instalada en dicho dispositivo.

3 En el caso de Smartphone y Tablet instala un cliente antivirus eset mobile security; y en el caso de laptops instala cliente endpoint.

4 Actualiza y escanea dispositivo con licencia institucional en busca de malware o virus para eliminarlos y poder contactar de manera segura el equipo a la red wifi institucional.

5 Si el equipo se encuentra limpio de amenazas informáticas, busca la dirección MAC Address para ingresar en sistema wifi y poder autorizar la conexión de dichos dispositivo.

6 Ingresa contraseña de la red wifi y comprueba la navegación del dispositivo.

7 Informa al usuario que se encuentra listo el dispositivo.

Visitas Oficiales.

8 En caso de visitas de corto tiempo, se les provee contraseña de la red wifi con SSID "CONSEJO" que puede ser usada únicamente en la sala de Consejo Directivo.

9 En caso de visita oficial de tiempo mayor a dos días, se conecta el dispositivo a red wifi con SSID “invitados”: el encargado de la visita oficial, solicita acceso a internet a través de la UAIP de manera oficial.

10 La UAIP traslada la solicitud al Jefe del Departamento de Informática para su visto bueno.

11 Al tener el visto bueno del Jefe del Departamento de Informática, registra equipo en bitácora “Control Antivirus para equipos de instituciones Externas”.

12 Prepara dispositivo para poder instalar la solución antivirus institucional; esto implica desinstalar cualquier otra solución antivirus que está instalada en dicho dispositivo y un usuario con permisos de administrador; además registra si el equipo contiene spyware, software de hacking, ni software de monitoreo hacia la red interna; en caso de detectar este tipo de software es notificado al usuario para su desinstalación.

13 En el caso de Smartphone y Tablet instala un cliente antivirus eset mobile security; y en el caso de laptops instala cliente endpoint.

14 Actualiza y escanea dispositivo con licencia institucional en busca de malware o virus para eliminarlos y poder contactar de manera segura el equipo a la red wifi o cableada institucional. Al terminar el escaneo determina que el equipo se encuentre limpio de amenazas informáticas.

15 En caso de conectar a red wifi, busca la dirección MAC Address para ingresar en sistema wifi y poder autorizar la conexión de dichos dispositivo.

16 En caso de conectarse con cable red, se le ingresa una dirección IP de la red LAN con restricciones en el perímetro.

17 Informa al usuario que se encuentra listo el dispositivo

Fin de la Metodología

NOMBRE DE LA METODOLOGÍA:

II. RESGUARDO DE DISCOS REMOVIBLES RDX EN EL SITIO DE CONTINGENCIA.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a realizar para realizar el resguardo de discos removibles RDX en el sitio de contingencia.

Inicio de la Metodología

Administrador de Red/ Administrador de Red Jr.

1 Cuando el disco removible RDX esté completamente lleno, realiza la entrega al Coordinador de Soporte Técnico para que actualice la bitácora e identifique el disco.

Coordinador de Soporte Técnico.

2 Recibe disco removible RDX, copia reporte, actualiza bitácora e identifica el disco.

3 En conjunto con el Administrador de Red/ Administrador de Red Jr., realiza el traslado de los discos removibles RDX, de las oficinas centrales de la Torre IPSFA al Sitio de Contingencia.

4 Realiza el resguardo de los disco removibles RDX en el Sitio de Contingencia; y se trasladan nuevamente a las instalaciones de la oficina central de la Torre IPSFA.

5 Resguarda la documentación generada.

Fin de la Metodología.

NOMBRE DE LA METODOLOGÍA:

JJ. ASESORÍA TÉCNICA PARA ADQUISICIÓN DE NUEVOS SOFTWARES.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para brindar asesoría técnica a unidades solicitantes para la posible adquisición de nuevos softwares.

Inicio de la Metodología

Unidad Solicitante

1. Realiza solicitud de opinión técnica sobre nuevo software, a través de correo electrónico o memorando al Jefe de la Unidad de Informática, especificando cual es el nuevo software que desea adquirir.

Jefe de la Unidad de Informática

2. Recibe y revisa solicitud. Da instrucciones al Coordinador de Soporte Técnico de realizar análisis técnico respectivo.

Coordinador de Soporte Técnico

3. Recibe la solicitud, elabora cuadro técnico, realiza análisis técnico, emite recomendación sobre la factibilidad de la adquisición del nuevo software y lo remite a Jefe de la Unidad de Informática.

Jefe de la Unidad de Informática

4. Recibe análisis técnico, lo revisa en conjunto con el Coordinador, evalúan factibilidad de adquisición del nuevo software.
5. Informa a la Unidad Solicitante sobre factibilidad o no factibilidad de la adquisición del nuevo software, pudiendo también tener como resultado una recomendación de otro software o versión para la finalidad de la Unidad Solicitante.

Unidad Solicitante

6. En caso de resultar factible la adquisición del nuevo software o aceptar recomendación de otro software o versión, inicia proceso de compra a través del DACI.

Fin de la Metodología.

UNIDAD DE DESARROLLO ORGANIZACIONAL

NOMBRE DE LA METODOLOGÍA:

KK. INSTALACIÓN DE NUEVOS SOFTWARES.

OBJETIVO DE LA METODOLOGÍA:

Definir los pasos a seguir para la instalación de nuevos softwares adquiridos por el Instituto.

Inicio de la Metodología

Unidad Solicitante

1. Realiza requerimiento de instalación de nuevo software adquirido al Jefe de la Unidad de Informática, especificando en que computadora o computadoras se requiere la instalación.

Jefe de la Unidad de Informática

2. Solicita a la Unidad Solicitante el medio magnético u óptico donde se encuentra el software adquirido, manuales, licencias u otros documentos relacionados.

Unidad Solicitante

3. Remite al Jefe de la Unidad de Informática medio magnético u óptico donde se encuentra el software adquirido, manuales, licencias u otros documentos relacionados.

Jefe de la Unidad de Informática

4. Recibe y entrega nuevo software con sus respectivos complementos al Coordinador de Soporte Técnico para que inicie con la instalación en la computadora o las computadoras requeridas.

Coordinador de Soporte Técnico

5. Recibe todo el paquete del software (manuales, licencias, medio magnéticos, otros) y procede a realizar la instalación en la computadora o las computadoras indicadas por la Unidad Solicitante.
6. Procede a realizar el resguardo en la Unidad de Informática de los manuales, licencias, medio magnéticos y otros, correspondientes del nuevo software.

Fin de la Metodología.

V. GLOSARIO

1 **USUARIO:** Se considera usuario de la red del Instituto de Previsión Social de la Fuerza Armada, IPSFA; a cualquier persona que desde una computadora conectada a la misma, genere tráfico dentro de esta. Se pueden considerar dos clases de usuarios: internos y externos.

2 **USUARIO INTERNO:** Es el personal empleado del Instituto y sus Unidades de negocio.

3 **USUARIO EXTERNO:** Se considera cualquier entidad o persona ajena a la Institución (por ejemplo personal de entes fiscalizadores realizando una Auditoría).

4 **CUENTAS Y CORREOS ELECTRÓNICOS:** Es una herramienta que brinda el IPSFA para que el personal pueda:

- Mantener contacto entre sus diferentes Unidades y Departamentos.
- Mantener comunicación con proveedores y/o contactos ajenos al IPSFA.
- Entre muchos otros beneficios.

VI. MISCELÁNEOS

A. DISPOSICIONES FINALES

1. El presente Manual entrará en vigencia a partir de la fecha de su aprobación, dejando sin efecto cualquier anterior a éste.

2. Toda modificación a su contenido, deberá ser canalizada a través de la Unidad de Desarrollo Organizacional.

3. Todo cambio realizado fuera de los procesos normales de trabajo establecidos, será responsabilidad exclusiva del jefe del departamento o gerente de área respectivo al aprobar dicho cambio; el cual deberá quedar debidamente documentado.