Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

ÍNDICE

Calle 23 e/ N y O, Vedado
dni@infomed.sld.cu
Telf.: 8329897

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

CAPITULO I Generalidades

Generalidades.

El presente Manual tiene por objeto establecer las políticas y procederes generales para la organización y funcionamiento de la actividad informática en el Sector de la Salud en todo el territorio Nacional.

Misión.

Contribuir al desarrollo sostenible y fortalecimiento del Sistema de Salud cubano a través del uso intensivo de las Tecnologías de la Información y las Comunicaciones y sus aplicaciones en los procesos de la red de sistemas y servicios de salud que garanticen el acceso, vinculación única y continuada en la atención del paciente y la comunidad, la formación y preparación de su capital humano, el desarrollo de redes de apoyo e investigación que favorezcan las prestaciones en todos los niveles de atención y coadyuve a garantizar la salud de la población.

Visión.

El Sistema Nacional de Salud dispone de una Intranet de la salud, ciberinfraestructura corporativa con un alto grado de informatización, seguridad, estándares e interoperabilidad conformada por sus sistemas, servicios e instituciones que garantiza el flujo e intercambio informativo para la atención directa, agilización de trámites, ayuda al diagnóstico, evaluación y control de los procesos del paciente, la comunidad y la dirección de los servicios.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Objetivos de Trabajo.

CRITERIOS DE MEDIDA	CRITERIOS DE EVALUACIÓN	GRADO DE EVALUACIÓN
1,25, Garantizado el desarrollo del proceso de informatización. (L-123- 108 -271 - 272) Evaluación: B: todos B R: evaluados de R o B M: 3 M	Porciento de clínicas internacionales con acceso a internet.	B: mayor o igual a 90 R: 70 a 89 M: inferior a 70
	Porciento de salas de atención médica internacional con acceso a internet	B: mayor o igual a 69 R: 60 a 68 M: inferior a 59
	Porciento de farmacias internacionales con acceso a internet de banda ancha.	B: mayor o igual a 90 R: 70 a 89 M: inferior a 70

CRITERIOS DE MEDIDA	CRITERIOS DE EVALUACIÓN	GRADO DE EVALUACIÓN
1.26. Lograda la conectividad a internet Y ADSL de los profesionales y unidades de salud. (L-123) Evaluación: B: todos B y 1 R R: 3 R M: 1 M	Porciento de policlínicos con autorizo de acceso a internet	B: mayor o igual a 70 R: entre 60 y 79 M: inferior a 50
	Porciento de hospitales con autorizo de acceso a Internet	B: mayor o igual a 90 R: entre 70 y 89 M: inferior a 70
	Porciento de farmacias principales, especiales de áreas conectadas por ADSL	B: mayor o igual a 70 R: entre 60 y 69 M: inferior a 60
	Incrementado el número de cuentas de acceso telefónico a profesionales de la salud	B: mayor o igual a 10 mil R: entre 8 mil y 9 999 M: inferior a 8 mil
	Porciento de hospitales y policlínicos con proyectos de informatización	B: mayor o igual a 95 R: entre 85 y 95 M: inferior a 85

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

	Porciento de unidades de salud conectadas por banda ancha (mayor 256 KB).	B: mayor o igual a 90 R: entre 70 y 88 M: inferior a 70

CRITERIOS DE MEDIDA	CRITERIOS DE EVALUACIÓN	GRADO DE EVALUACIÓN
1.27. Implementada la sostenibilidad de las soluciones informáticas. ·(L-123, L-128) Evaluación: B: todos B y 1 R R: 3 R M: 1 M	Implementada la Historia Clínica Digital en los 12 institutos de investigación, salas de atención a pacientes extranjeros, clínicas internacionales y en 16 hospitales provinciales	B: igualo mayor a 90 R: entre 80 y 89 M: inferior a 79
	Implantar la solución Galen Clínicas para policlínicos en 24 unidades del país	B: igualo mayor a 90 R: entre 80 y 89 M: inferior a 79
	Implantar la solución Galen Clínicas en 16 clínicas estomatológicas del país, incluyendo las internacionales	B: igualo mayor a 90 R: entre 80 y 89 M: inferior a 79
	Implantar el registro de trabajadores de la salud	B: igualo mayor a 90 R: entre 80 y 89 M: inferior a 79

Definición de Términos empleados.

Informatización: Aplicación de sistemas y equipos informáticos al tratamiento de la información, como soporte en la toma de decisiones en los procesos administrativos y asistenciales.

TIC: Tecnología de la Información y las Comunicaciones.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Bitácora: Registro de incidencias informáticas y afectaciones en los servicios y procesos que ocurren en los centros a todos los niveles. Quedarán también registradas las causas que originaron estas incidencias y las posibles soluciones.

Valores Compartidos*.*

Lealtad a los Principios de la Revolución: Fidelidad y compromiso con la ideología y las conquistas alcanzadas por la Revolución, dentro de las cuales una de las más preciadas, resguardo y protección de la información que se genera.

Moral: Comportamiento conforme a los principios del socialismo, el internacionalismo, la conducta revolucionaria y profesional como fundamento de todas nuestras actividades.

Ética Socialista: Comportamiento conforme a la moral revolucionaria, reflejado en conductas sobre la base de valores humanos, patrios y profesionales como fundamento de todas las actividades del Sistema de Salud.

Responsabilidad: Obligación con el cumplimiento del deber, tanto en el orden individual como organizacional.

Profesionalidad: Poseer y aplicar las competencias y experiencias requeridas para garantizar la aplicación de las buenas prácticas informáticas y la calidad técnica y humana en los servicios.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Solidaridad: Sentimiento de ayuda mutua entre los seres humanos y los pueblos para dar apoyo al proceso Revolucionario

Valores Deseados.

Humanidad: Actitud de sensibilidad y comprensión del desempeño en el respeto absoluto a la condición humana, donde prevalezca el trato respetuoso y digno a compañeros de trabajo, al individuo, la familia y la comunidad.

Disciplina: Conducta acorde con las normas y principios del revolucionario y cumplimiento de las funciones inherentes a su puesto de trabajo con calidad.

Consagración: Dedicación, compromiso y entrega absoluta en su desempeño diario.

Abnegación: Actuar con altruismo, generosidad y desinterés en las funciones que realizan los individuos para el cumplimiento de los servicios de salud.

Desinterés y modestia: Desprendimiento personal, amor a la verdad, austeridad y sencillez en su actuación.

Honestidad y honradez: Rectitud en la conducta y en el actuar, en correspondencia con la moral revolucionaria, sustentada en el honor, la sinceridad, austeridad, modestia y el cumplimiento de la palabra empeñada en todos los momentos de actuación.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Sentido de la crítica y la autocrítica: Receptividad ante los señalamientos y recomendaciones, así como la valentía para señalar oportunamente a los compañeros sus deficiencias en el actuar y la capacidad de realizar profundos auto análisis de la conducta individual, que conduzca a la decisión de cambiar.

Iniciativa: Capacidad técnica y de gestión para abordar los problemas que puedan limitar la calidad del desempeño de los servicios de salud y generar variantes de posibles soluciones informáticas.

Creatividad: Capacidad técnica y de gestión para intervenir con un desempeño efectivo y eficiente de los servicios de salud a través de la búsqueda de lo nuevo y útil para cada circunstancia, innovando en aras de generar soluciones informáticas.

CAPÍTULO II De la organización

De los Niveles de Dirección

La actividad de Informática tiene los siguientes niveles de dirección:

a) Primer nivel: Director de Informática y Comunicaciones.

b) Segundo nivel: Especialistas de la Dirección de Informática y Comunicaciones.

c) Tercer nivel: Jefes de Informática y Comunicaciones Provinciales y Especialistas de unidades de Subordinación Nacional.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

d) Cuarto Nivel: Especialistas de Informática y Comunicaciones Municipales.

e) Quinto Nivel: Especialistas de Informática y Comunicaciones de unidades de salud.

De la política de cuadros

El Director de Informática y Comunicaciones, además de los Jefes de Informática Provinciales están en la obligación a seleccionar y preparar sus dos reservas de cuadro. En particular presta atención directa a la captación, caracterización, identificación de necesidades de aprendizaje y definición del plan de preparación individual de cada uno.

Se realiza reuniones periódicas con (el o los) Integrantes de la reserva para examinar su desarrollo y conocer sus Inquietudes y propuestas sobre los principales problemas que enfrenta el grupo y como darles solución.

CAPÍTULO III De la calidad en la prestación de los servicios informáticos

La calidad de un servicio informático se logra cuando el mismo es sobre la base de las óptimas prestaciones, teniendo en cuenta los recursos disponibles y logrando la adhesión y satisfacción del usuario y del prestador del servicio, con la atención recibida y brindada respectivamente.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Los principios, por los que se rigen la calidad en los servicios informáticos, son los siguientes:

a) La calidad del trabajo de los servicios informáticos es una responsabilidad de todos los niveles del Departamento, Grupo o área de Informática.

b) Para el perfeccionamiento continuo de la calidad de los servicios informáticos se requiere como cimiento un colectivo de trabajadores motivado, comprometido, con sólidos valores humanos, morales y éticos en correspondencia con la ideología de la Revolución Cubana y la Ética Informática.

c) La realización del perfeccionamiento continúo a todos los niveles de dirección del Departamento, Grupo o área de Informática de Informática.

d) Estará dado por, el desempeño de los recursos humanos, los aseguramientos y la conducción por parte de la DIC encaminado a:
   - Calidad del colaborador significa:
     - Competencia.
     - Preparación continua.
     - Compromiso con los objetivos de trabajo.
     - Contribuir a un excelente clima laboral.
     - Demostrar compromiso con la satisfacción del cliente.
     - Practicar el trabajo en equipo.

   - Emplear tecnologías de avanzada significa:
     - Usar y dominar herramientas modernas de las Tecnologías de la Información.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

- Desarrollar procesos eficaces, eficientes, efectivos y adaptables.

- Que innova permanentemente significa:
  - Mejora continua.
  - Se acometen con arrojo las transformaciones necesarias.
  - Grupo emprendedor.
  - Grupo que experimenta.

CAPITULO IV De las reuniones

Las reuniones se programan y se realizan para analizar, chequear o informar a los miembros a todos los niveles de la actividad de Informática los aspectos que se consideran necesarios para alcanzar calidad en el trabajo y elevar los niveles educacionales, políticos, científico – técnicos y administrativos; y garantizar la participación activa en la toma de decisiones y dar cumplimiento a los objetivos de trabajo.

Las reuniones se clasifican en Ordinarias y Extraordinarias. Como ordinarias estarán las reuniones de coordinación y puntualización de las tareas semanales y la video-conferencia con los Jefes y/o especialistas provinciales mensualmente. Las reuniones extraordinarias son de índole educacional, técnico o administrativas, no son programadas, se realizan según las necesidades existentes.

Estructura de las reuniones.

En las reuniones convocadas, no se dejarán de chequear los temas siguientes:

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

a) Chequeo de acuerdos.

b) Estado de la Informatización.

c) Estado del equipamiento informático y radiocomunicaciones.

d) Estado de la implementación del Galen Clínica y otras aplicaciones con alcance nacional.

e) Estado de la conectividad, implementación del servicio de Internet en las instituciones.

f) Estado de la implementación del sistema de control de Flota GPS.

CAPÍTULO V De la planificación y el control económico.

Es responsabilidad del Director de Informática y Comunicaciones, además de cada Jefe Provincial, Municipal y hasta nivel de Unidad, controlar la planificación y plan económico al nivel correspondiente:

a) Levantamiento estricto de las necesidades a todos los niveles para tener una planificación adecuada de los recursos necesarios.

b) Control de la ejecución del Presupuesto aprobado por partidas perteneciente al área.

c) Control del destino final de los recursos adquiridos.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

CAPÍTULO VI De los documentos del Área de Informática.

Documentación de las unidades de salud*:*

a) Plan para el desarrollo y uso de las TIC, incluyendo el Plan de Informatización.

b) Bitácora del centro.

c) Manual de Instalaciones de los Servidores de la institución.

d) Control de los medios informáticos hasta nivel de componentes, así como su ubicación.

e) Descripción de la red del centro, con el Plan de Redireccionamiento IP.

f) Configuración, contraseña, dirección IP y MAC de todos los elementos que conforman la red: AP, servidores, etc.

g) Listado de usuarios con acceso a los diferentes servicios que se prestan en la institución.

h) Análisis mensual del comportamiento de los servicios de navegación.

Actividad de Informática de los Centros Asistenciales.

a) Medios Tecnológicos.
   - Levantamiento del 100% del equipamiento con que contamos, conciliado con los departamentos económicos.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

- Actualización de las descripciones correcta de los medios.
- Control de equipamiento por proyectos según corresponda.

b) Control periódico de software de diagnóstico para el registro de las características técnicas de nuestros equipos.

c) Control del proceso de implementación del Galen Clínica.

CAPÍTULO VII. Procedimientos.

Documentación Necesaria.

Para el control y monitoreo de los procesos del Área de Informática se relacionan los documentos que permiten el desarrollo de las actividades mencionadas a lo largo del documento:

Parte de Conectividad y servicios de internet de las instituciones de salud	Direcciones Provinciales (mensual)
Parte del equipamiento informático y de radiocomunicaciones.	Direcciones Provinciales (semanal)
Certificación de Destino Final de productos recibidos	Direcciones Provinciales (por asignación)
Parte del estado de la implementación de sistema de control de flota GPS.	Direcciones Provinciales (semanal)
Demanda de Conectividad	Direcciones Provinciales (anual) Dirección de Informática (anual)

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Medidas y Procedimientos

Toda institución que haga uso para el desempeño de su actividad de las tecnologías de la información está en la obligación de diseñar, implantar y mantener la adecuación a la institución de los procedimientos que a continuación se reflejan.

Procedimiento No.1: Otorgar (retirar) el acceso de los usuarios a los servicios y tecnologías de información.

Solamente tiene autorización de utilizar las tecnologías y sus servicios, todo aquel personal aprobado previamente por la dirección del centro.

a) El Jefe del Área presentará al Grupo de Informática, la propuesta para otorgar o retirar el acceso a las TIC por un usuario, en el caso de que se apruebe el acceso se informará mediante una breve descripción las medidas de protección física y lógicas que debe cumplir.

b) El usuario firmará compromiso del reglamento de empleo de las TIC, el documento original lo guardará el Grupo de Informática.

c) Cada usuario que haga uso de los servicios de la red tendrá una cuenta de acceso compuesta por un identificador (loggin) y una contraseña (password).

d) En caso de autorización de acceso, el Administrador de la red asignará un identificador personal y único para el acceso a los sistemas y servicios el cual estará asociada al nombre del usuario y definirá en el servidor los atributos en correspondencia con la autorización otorgada.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

e) Se le asigna al usuario una contraseña inicial para ser utilizada en su primera conexión, obligándolo a cambiarla una vez que se conecte.

f) En el caso de retirar el acceso presentará breve informe refiriendo los motivos de la propuesta y si es definitiva o temporal.

g) En caso de autorización de retiro de acceso el Grupo de Informática cancelará la cuenta y permisos de acceso.

h) Se realizará control trimestral de este procedimiento, por parte de los encargados de chequear esta acción.

Este procedimiento se cumple también para los sistemas implementados en la institución, donde el Grupo de Informática tendrá el control de los usuarios con su nivel de acceso del sistema en cuestión.

Procedimiento No. 2: Autorización y control de la entrada/salida de las TIC.

a) El Jefe de Área donde se encuentra la TIC a trasladar, a parte de la solicitud a la administración, presentará solicitud de autorización al Grupo de Informática para el movimiento del activo.

b) Se habilitará un registro que tendrá que llenarse cada vez que se realice un movimiento de las TIC hacia o desde fuera del centro. Se encargarán de llenar el registro en conjunto (el área que posee el activo y el Grupo de Informática).

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

c) Se consignará en el registro la fecha del movimiento, datos del equipo objeto del movimiento, de qué lugar se extrae o proviene y a qué lugar se lleva y motivo por el que se realiza el movimiento (ejemplo: evento, exposición, reparación, etc).

d) En el caso de las Laptops el movimiento será autorizado por el Jefe de Departamento a donde pertenece, el que responderá ante cualquier incidente derivado de este movimiento.

e) El Grupo de Informática realizará y controlará mensualmente, las TIC y sus componentes (número de serie de c/u, estado físico, cambios realizados), para esto utilizará un Sistema de Control de Componentes.

f) Informará a la Jefe del área y al Director del Centro, cualquier cambio tanto en el hardware como en el software de cualquier equipo de la entidad.

g) En caso de entrada de alguna tecnología el Grupo de Informática se encargará de realizarle un chequeo del hardware como el software que contenga el equipo, y en caso de ser PC, chequear que no posea virus. Una vez instalada se insertará en el Sistema de Control de Equipamiento Informático, construyendo la ficha técnica.

Procedimiento No. 3: Gestión de Incidentes de Seguridad Informática.

a) Los usuarios están en la obligación de informar cualquier incidente o violación que se produzca a su Jefe inmediato superior y al Grupo de Informática.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

b) El Grupo de Informática informará del incidente a las instancias superiores, valorando las pérdidas y consecuencias, se anotará en el Registro de Incidencias.

c) De conjunto se realizará informe detallado que como mínimo incluirá:
   - En qué consistió el incidente o violación.
   - Fecha y hora de comienzo del incidente y su detección.
   - Implicaciones y daños para la entidad y para terceros.
   - Acciones iniciales tomadas.
   - Evaluación preliminar.

d) En caso de incidente se delimitarán responsabilidades, y cuando lo requiera se tomarán las medidas disciplinarias correspondientes.

e) Se creará una comisión de investigación en caso de incidente y la cual tomará acciones dirigidas a eliminar las causas que los propiciaron.

f) Se consideran Incidentes de Seguridad Informática:
   - Acciones no Autorizadas contra la red o las TIC.
   - Cambios de las características del Hardware.
   - Cambios de las características del Software o BD.
   - Denegación o Interrupción de servicios de la red.
   - Desfiguración de sitio Web.
   - Detección de Hoax (noticias falsas sobre virus u otra cuestión para su reenvío), en este caso hay que parar el envío del Hoax e informar de inmediato).

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

- Intercepción de las telecomunicaciones.
- Pornografía.
- Programas malignos o nuevos virus detectados.
- Pruebas o escaneos ilegales a la red.
- Robo de información.
- Detección de información de contenido negativo.
- Comercialización ilegal de cuentas de conexión u otros servicios informáticos.
- Robos de cuentas.
- Fraude.
- Robo de Hardware.
- Suplantación de identidad.
- Vulnerabilidades conocidas.
- Información Dudosa.

Procedimiento No. 4: Cadenas de mensajes.

En caso de ser detectados este tipo de mensajes, se procederá de acuerdo a las acciones que a continuación se describen, con el fin de evitar sobrecargas de las conexiones de la red con la posible saturación de los canales y memoria, con la consiguiente disminución de las prestaciones y hasta su posible salida de servicio.

a) Si lo detecta un usuario deberá informar de inmediato al Grupo de Informática.

b) El Grupo de Informática, revisará el encabezamiento del mensaje para determinar su origen.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

c) El Grupo de Informática incluirá la dirección de procedencia del mensaje en una lista de filtraje, para que posteriores mensajes procedentes del mismo remitente sean eliminados automáticamente por el sistema.

d) De ser posible, contactará con el usuario de la máquina de donde se originó el mensaje y se le pondrá al corriente de lo sucedido.

e) Se realizarán las acciones de acuerdo al Procedimiento No.3

Procedimiento No. 5: Mantenimientos de los equipos, soportes y datos.

El mantenimiento a los equipos se realizará de acuerdo al cronograma planificado.

a) El mantenimiento será realizado siempre en presencia y bajo la supervisión de personal responsable y que en caso del traslado del equipo fuera de la entidad la información clasificada o limitada será borrada físicamente o protegida su divulgación, además que el medio tendrá el movimiento de "Medio Básico" y cumplimiento del Procedimiento No. 2.

b) Se mantendrá actualizado el registro correspondiente por el técnico perteneciente a la institución.

c) En caso de los mantenimientos a soportes y datos se realizará de igual manera.

Procedimiento No. 6: Control de medios informáticos.

a) El Grupo de Informática, realizará y controlará mensualmente, la identificación de los medios informáticos, sus componentes (número de

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

serie, estado físico, cambios realizados), para esto utilizará un Sistema de Control de Componentes.

b) Informará al Jefe del Área y a la Dirección del centro, cualquier cambio tanto en el hardware como en el software de cualquier equipo del Departamento.

c) El Grupo de Informática archivará este informe y se responsabilizará porque se mantenga actualizado.

Procedimiento No. 7: Permisos de acceso a los sistemas.

a) El acceso a los diferentes sistemas, será aprobado por el Jefe de Área y la Dirección del Centro, en función al trabajo que desempeña el especialista.

b) El documento aprobado estará bajo la custodia del Grupo de Informática.

Procedimiento No. 8: Gestionar las claves de acceso.

a) El acceso a los diferentes sistemas y servicios de la red, estará basado en el uso de claves de accesos, las cuales estarán en correspondencias con las políticas establecidas en este manual.

b) El Grupo de Informática configura cada servicio de acuerdo con las políticas de contraseñas establecida y teniendo en cuanta la información que se protege.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

c) El usuario tendrá acceso a los sistemas y servicios que tendrá aprobado, en lo cual el Administrador de Sistema le creerá una cuenta que tendrá para su acceso una clave de acuerdo al tipo de servicio o sistema que utilizará.

d) El usuario deberá cambiar dicha clave cada vez que sea requerido por el sistema o en caso de algún incidente que implique el uso de su cuenta de acceso.

e) El usuario será el único responsable de su clave de acceso sea de uso personal y privado

Procedimiento No. 9: Proceso de salvas.

La periodicidad de las salvas será función del ritmo de modificación de los archivos, principalmente lo defino el área dueño de la información. Para el calendario de salvado se establecerán 3 niveles:

1. Copias del sistema operativo y utilidades.
   - Con periodicidad baja, se tendrán las salvas —o discos originales— debido a los cambios de versiones. Los sistemas operativos se encuentran en discos compactos o en memorias USB.

2. Programas y aplicaciones.
   - Con una periodicidad mayor, se salvarán cada vez que exista un cambio en los mismos. Los programas y aplicaciones se encuentran en discos compactos o en memorias USB.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

3. Los datos
   - Se harán las salvas diarias, mensual o con otra periodicidad, según la aplicación y el tipo de la información que se requiera —bases de datos, archivos de datos, etc. al finalizar la sesión de trabajo del periodo que corresponda.
   - Es responsabilidad del Jefe del área de establecer la periodicidad para la ejecución de la salva de la información vital de su área. Al mismo tiempo de mantener actualizado el registro de salva que existen en cada departamento.

En el caso de sistemas, programas de aplicación y documentos, tendrán que ser sometidos antes de la salva definitiva al proceso de identificación y/o descontaminación con los antivirus instalados. La política de las salvas la determina el Jefe del área correspondiente, siendo el técnico que ejecuta el trabajo el encargado de realizarla y guardar los soportes en el lugar destinado para ello dentro del departamento.

A los soportes magnéticos que contengan las salvas se les pondrá en un lugar bien visible una etiqueta que identifique la fecha y el nombre de la salva. Los soportes magnéticos que contengan las salvas estarán protegidos físicamente contra escritura, también en una localización física que reúna las condiciones de protección ante cualquier eventualidad.

Procedimiento No. 10: Salva y análisis de registros o trazas de auditoria.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

a) Los registros de trazas son analizados por el Administrador de Red y el Especialista de seguridad informática.

b) Se realizará y entregará informe mensual, del chequeo de esta actividad, a la Dirección del Centro.

c) Para la salva de estos registros, el Grupo de Informática, contará con los medios necesarios, y su periodicidad de resguardo es un tiempo no menor de un año.

Procedimiento No. 11: Autorización y control del acceso a las tecnologías de información por personal externo a la entidad.

a) Todo personal que arribe al centro quedara registrado en el Registro de Visitantes del centro, donde uno de los datos recogidos es el lugar hacia donde irá.

b) El Jefe del área será el responsable del acceso y uso de las tecnologías que esta persona haga en su radio de dirección.

c) Si el personal ajeno, pero autorizado debidamente por la Dirección del Centro, hace uso de alguna tecnología informática, se registrará en el registro de usuario sus datos personales, hora y trabajo realizado.

Procedimiento No. 12: Controlar acciones para cubrir brechas de seguridad en la red y corrección de errores del sistema.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

a) El Grupo de Informática será el encargado de chequear continuamente el estado y actualización de los sistemas y servicios informáticos, he informar de existir alguna anomalía a la Dirección del Centro.

b) Periódicamente se comprobarán y chequearán por el especialista de Seguridad Informática el cumplimiento de los procedimientos y controles establecidos en el sistema informático del centro.

c) Cualquier anomalía detectada se le comunicará a la Dirección del Centro y este a su vez activará el Plan de Contingencia.

Procedimiento No. 13: Selección y certificación de candidatos para cumplir Misión Internacionalista como Informático.

a) Los candidatos deben plasmar la disposición de cumplir misión internacionalista.

b) Se requiere que haya estado ocupando una plaza o cumpliendo los objetivos de trabajo de informática en la institución un tiempo mayor de 2 años, excepcionalmente 1 año si posee evaluación sobresaliente en sus resultados.

c) A cada candidato se le practicará un examen de demostración de conocimientos, habilidades y capacidades que lo habilitan para cumplir las diferentes tareas y funciones requeridas en las misiones, siendo el responsable de esta acción el coordinador provincial.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

d) Es requisito para cumplir misión como informático poseer un documento certificativo o aval firmado por el coordinador provincial de informática, además de cumplir con los demás requerimientos para los colaboradores.

e) Cada provincia podrá organizar cursos de adiestramiento, habilitación y capacitación en los requerimientos para el trabajo en Informática en las diferentes misiones.

Conocimientos que debe poseer un candidato a cumplir misión internacionalista como informático:

- Conocimiento de manejo de Bases de Datos SQL y la administración de los servidores SQL para la replicación de Datos.
- Instalación y configuración de Sistemas Operativos para administrar su función, habilidades y recursos.
- Configurar la red inalámbrica (AP y WIFI) así como sus servicios.
- Conocimiento en equipamiento, Redes y Servidores para prestar servicios de conectividad.
- Tener conocimiento de Hardware, poseer capacidad de manipularlo.
- Conocimientos sobre seguridad informática y políticas antivirus

Durante el cumplimiento de la misión conocerán en el caso que se requiera, además:

1. Configuración de la TV satélite y saber reubicar la señal en la institución donde esté instalado.
2. Habilidades básicas en el uso y funcionalidades del Versat.
3. Instalación, manipulación y uso del Galen Lab. (Misión en Venezuela).

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Procedimiento No. 14: Distribución de computadoras.

a) La Dirección de Informática enviará la propuesta de distribución aprobada para cada destino del Plan a los vicedirectores Generales y Jefes de Informática de las provincias.

b) El Jefe de Informática de cada Provincia evaluará las condiciones de los locales donde se instalarán las computadoras asociadas al Plan.

c) Cada unidad coordinará localmente las necesidades para garantizar la solución de los problemas de infraestructura para la instalación de las computadoras.

d) El Jefe de Informática Provincial y el Vicedirector General certificarán el destino final de las computadoras.

Procedimiento No. 15: Solicitud del Servicio de Internet a las instituciones de salud (INFOMED o ETECSA).

a) La Institución debe de enviar a través de la oficina de control para la información clasificada (OCIC) la documentación correspondiente para la solicitud de autorización de uso de internet institucional.

b) La Dirección de Informática y Comunicaciones efectuará la revisión de la documentación de la solicitud. Dará paso a la elaboración y envío de la carta de solicitud de aprobación del Viceministro(a) al Ministro para la autorización de internet a la institución en un plazo no mayor de 30 días.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

c) La Dirección de Informática y Comunicaciones enviará la carta aprobada por el Ministro, a través de la oficina de control para la información clasificada (OCIC), a la Institución para darle paso a la ejecución del autorizo.

d) La Institución registrará copia de la carta de aprobación del Ministro a INFOMED para ejecutar la autorización. En caso de ser a través de ETECSA se aclarará en la solicitud de este detalle para el autorizo de la contratación del servicio por ETECSA.

El servicio de Internet a Pacientes extranjero se dispondrá del servicio Nauta por ETECSA, no se autoriza brindar este servicio por el Internet de la Institución.

Procedimiento No. 16: Creación de usuario para consulta o gestión de información en el Registro Informatizado de Salud a nivel Nacional.

El siguiente procedimiento es para los usuarios del Nivel Nacional, debe de ser adaptado e implementado a las necesidades del resto de los niveles del Sistema Nacional de Salud.

a) El Director Nacional de cada módulo desarrollado para su actividad, es el responsable de la introducción y validación de la calidad de la información del mismo.

b) El Director de Informática y Comunicaciones es el responsable de garantizar el funcionamiento de cada módulo y atender las solicitudes de modificación o cambio en los sistemas.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

c) El Director Nacional responsable de cada módulo es quien autoriza mediante modelo de solicitud para usuario de los componentes informáticos del Sistema Nacional de Salud, a los funcionarios y cuadros con capacidad de visualización de la información bajo su responsabilidad. Ejemplo Registro de Unidades (Director de Planificación, Registro de Personal de la Salud, Director de Trabajo).

d) La Dirección de Informática y Comunicaciones con el modelo de solicitud de usuario procede a la creación de la cuenta de acceso.

e) La Dirección de Informática y Comunicaciones se responsabiliza en la auditoría, control y supervisión de la información y del historial de navegación de cada usuario.

Procedimiento No. 17: Trasferencia tecnológica de las aplicaciones.

Las transferencias de tecnología previstas, va a constituir el traspaso de los conocimientos necesarios para la utilización y puesta en marcha de las aplicaciones desarrolladas por una empresa hacia otra, con el fin de asegurar continuidad, mejores prácticas y niveles de efectividad.

La transferencia, de manera general, abarcará el conjunto de las siguientes acciones:

a) Transmisión de conocimientos técnicos especializados bajo la forma de capacitaciones.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

b) Transmisión de conocimientos tecnológicos para instalar y utilizar las aplicaciones.

c) Materiales destinados a la formación del personal. Entrega de manuales detallados e instrucciones específicas.

De esta manera se establecen las siguientes pautas para trasferir las aplicaciones:

a) El traspaso de las aplicaciones tiene que desarrollarse en un ambiente con conexión real a INFOMED y a la plataforma centralizada SiSalud.

b) Los especialistas de la empresa que inicia la entrega, presentarán las aplicaciones y capacitarán detalladamente a los especialistas de la empresa receptora, en todo el funcionamiento y puesta en marcha de dichas aplicaciones.

c) Los especialistas de la empresa que inicia la entrega, entregarán a la empresa receptora los manuales de usuarios de las aplicaciones a transferir.

d) El soporte de primer y segundo nivel lo asumirán los especialistas de la empresa receptora.

e) El soporte de tercer nivel se re seccionará por los especialistas de la empresa receptora que tramitarán después a los especialistas de la empresa que inició la entrega mediante un REPORTE.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Procedimiento No. 18: Distribución y recogida de equipamiento informático en la Empresa de SERVISAP.

a) El equipamiento informático se distribuye a las instituciones a partir de una pauta de distribución de la Dirección de Informática y Comunicaciones.

b) La Dirección de Informática y Comunicaciones entregará las distribuciones del equipamiento informático a la dirección de la Empresa SERVISAP, al Director de unidades de Subordinación Nacional y/o al Vicedirector Provincial que atiende el área de informática, además del Grupo de Informática de la provincial o instituciones implicadas.

c) Las unidades de salud recogerán el equipamiento asignado en las EPAS en el caso de las Provincia y las unidades de Subordinación Nacional directo en SERVISAP (en la Tropical). Cumpliendo los términos del contrato.

d) Cualquier problema que ocurra con el equipamiento cargado debe ser conciliado con la empresa donde se recogió.

e) Una vez que se realice la recepción del equipamiento y se instale en su destino, el Grupo de Informática Provincial debe de emitir a la Dirección de Informática y Comunicaciones el certifico de Destino Final del o los equipamientos recibidos.

Procedimiento No. 19: Uso de la telefonía celular.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

a) Los teléfonos se deben utilizar exclusivamente para desempeñar funciones laborales del Sistema Nacional de Salud. El Ministerio de Salud se reserva el derecho de revisar la utilización del dispositivo telefónico ante cualquier sospecha de un uso inapropiado del mismo.

b) La asignación del servicio así se realiza con la autorización del Consejo de Dirección y el Ministro de Salud.

c) El Incremento de tiempo asignado y de la cantidad de mensajes deben solicitarse por escrito con una debida argumentación y solo podrá ser autorizado algún tipo de incremento por el Ministro de Salud.

d) El uso del servicio puede ser auditado por personas y entidades debidamente facultadas y autorizadas a ejecutar este tipo de acción.

e) Cuando se está en presencia de otras personas, pero de manera no formal para evitar molestar, se debe conectar el dispositivo en modo de vibración o al menos bajar el volumen del tono.

f) Zonas libres de móviles, en reuniones del primer nivel o donde se traten temas estratégicos con las máxima Dirección del Organismo debemos preocuparnos y asegurar la no presencia del móvil, a no ser que se autorice a mantenerlo, en este último caso se deberá dejar en silencio.

g) No se está autorizado a alterar, modificar o instalar nuevas aplicaciones o el sistema operativo en el dispositivo móvil si no se está autorizado por el Jefe Inmediato Superior y realizado esto por el Grupo de Informática del Ministerio de Salud. Quedando demostrado que lo instalado o modificado

se requiere para trabajar y no afecta el funcionamiento del equipo, así como que lo mismo no incurre en ninguna violación legal de derechos de autor o propiedad.

h) Queda prohibido ceder o prestar el teléfono celular asignado, sus accesorios o el derecho de uso a terceras personas, formal o informalmente, ya sea temporal o permanentemente, para fines y acciones diferentes a los intereses del Ministerio de Salud.

i) Responsabilidad de custodia o conservación: el beneficiario del servicio de telefonía celular será responsable de su custodia, conservación, uso correcto y racional.

   - En caso de que se presente una actividad delictiva con respecto al extravío, robo o daño del teléfono celular o de sus accesorios, deberá solicitar de inmediato la suspensión del servicio al proveedor, presentar la respectiva denuncia policial ante la autoridad competente e informar a la Administración del MINSAP Nivel Central por escrito, dentro de las 48 horas. hábiles posteriores a los hechos.

   - Ante algún desperfecto del equipo o problemas con el servicio se debe notificar inmediatamente a la Administración Interna.

j) De la devolución del equipo: en caso de cese de funciones y/o jubilación el beneficiario deberá en el término de cinco días hábiles al momento de su notificación hacer entrega al superior inmediato del equipo de telefonía celular asignado, en el mismo estado de conservación en el que le fue

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

entregado, excepto por el deterioro razonable del uso que se le ha dado, debiendo suscribirse el acta de entrega pertinente.

Procedimiento No. 20: Contaminación por virus informáticos.

Como política el antivirus a utilizar en el sistema de salud en todo el territorio Nacional, es el Segurmática en su versión superior como antivirus de procedencia nacional. En aquellas computadoras que sus recursos le permitan poner 2 antivirus se usará otro de procedencia extranjera autorizado (dígase antivirus libres “FREE” excepto Nod32).

En caso de falsa Alerta sobre virus mediante el correo:

a) No reenviar el mensaje de alerta recibido, como generalmente se sugiere en el texto del mensaje y, si la persona que nos envió el mensaje es usuario de nuestra red, indicarle que se abstenga de reenviarlo al resto de los usuarios.

b) El Grupo e Informática investigará la autenticidad del mensaje, para lo cual accederá a los sitios conocidos que distribuyen información actualizada sobre virus, a fin de corroborar la verdadera existencia del virus acerca del cual se genera la supuesta alerta.

c) Si se logra verificar que se trata de una falsa alarma, lo notificará a la persona que envió la alerta a fin de evitar que se siga difundiendo. Si la alerta es real, se procederá a la información de forma organizada y clara a todos los usuarios de la red.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

En caso de contaminación por virus en las PC:

a) Se procederá al cese de la operación de las PC implicadas y a su desconexión de las redes cuando corresponda.

b) El usuario de la TI procederá (si está capacitado) a desinfectar su equipo, si no puede, recurrirá al Grupo de Informática para que este proceda.

c) Verificará que en la máquina contaminada se esté ejecutando una versión actualizada del programa antivirus instalado.

d) De no cumplirse, se procederá a la actualización del programa antivirus y se llevará a cabo la descontaminación.

e) En el caso de la aparición de un virus desconocido, proceder al aislamiento del fichero contaminado si es posible. Enviar muestra a Segurmática para que sea actualizado en la base de datos del sistema, y así potenciaremos la calidad del producto de procedencia nacional.

El Grupo de Informática:

a) Procederá a descontaminar los medios contaminados.

b) De no ser exitosa la descontaminación, y se detecte afectación en el medio este interrumpirá su funcionamiento y formatear el medio con el fin de volverlo a poner en funcionamiento.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

c) De ser exitosa la descontaminación, lo informa y pone en operación el medio.

d) Revisa los soportes y el resto de las tecnologías.

e) Investiga causas de aparición.

f) Anotar en el Registro de Incidencias.

g) Se realizará las acciones de acuerdo al Procedimiento No. 3.

Procedimiento No. 21: Activación del Servicio de Telefonía Internacional.

Tiene como objetivo facilitar la comunicación internacional de los pacientes y acompañantes extranjeros. Este servició solo podrán optar las instituciones aprobadas del Sistema Nacional de Salud con servicios a pacientes y acompañantes extranjeros.

Responsabilidades:

Cargo	**Responsabilidad**
Director de la Institución.	Firmar suplemento del contrato con ETECSA para la habilitación del servicio 166 para llamadas Internacionales por tarjetas propias.
Director de la Institución.	Garantizar el cumplimiento en su institución de lo establecido por Control Interno referente al tratamiento contable y de efectivo respecto a las tarjetas propias en CUC.
Director de la Sucursal de Servicios Médicos de la provincia.	Garantizar el cumplimiento en su institución de lo establecido por Control Interno referente al tratamiento contable y de efectivo respecto a las tarjetas propias en CUC.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Insumos:

La institución previamente, solicitará la habilitación del servicio 166 de llamadas Internacionales con ETECSA a los números fijos o en los troncos de pizarras (en caso de tener extensiones) ubicados en las habitaciones. También firmará un contrato con la Sucursal de Servicios Médicos de la Provincia para la adquisición de las tarjetas propias.

Desarrollo del Procedimiento:

Unidad administrativa / Cargo	**Actividad**
Dirección de la Institución.	1. Definirá los números Fijos y/o los números de extensiones de pizarras para la habilitación del servicio 166 para llamada internacional por servicios de tarjetas propias. 2. Ubicará estas estaciones telefónicas en las habitaciones o salas donde radica el paciente extranjero. 3. Firmará contrato con la Sucursal de Servicios Médicos de la Provincia para la adquisición de las tarjetas propias en CUC para llamadas Internacionales. 4. Garantizará el cumplimiento del procedimiento de Control Interno en cuanto a la contabilidad y efectivo de la adquisición y venta de las tarjetas propias en CUC.
Sucursal de Servicios Médicos de la Provincia	1. Demandará a ETECSA la cantidad de tarjetas propias en CUC necesarias para garantizar el aseguramiento de los servicios en las instituciones aprobadas en su Provincia.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

	2. Ejecutará el del procedimiento de Control Interno en cuanto a la contabilidad y efectivo de la adquisición y venta de las tarjetas propias en CUC.
Administración de la Institución	1. Solicitará en la oficina comercial de ETECSA la habilitación del servicio 166 de llamadas Internacionales por servicio de tarjetas propias. 2. Garantizará la venta de las tarjetas a los pacientes Extranjeros. 3. Ejecutará el del procedimiento de Control Interno en cuanto a la contabilidad y efectivo de la adquisición y venta de las tarjetas propias en CUC.

Políticas del Servicio:

a) El servicio 166 de llamada Internacional habilitado en la institución tiene que ser a través de servicios de tarjetas propias.

b) Los números fijos y/o los números de extensiones de pizarras escogidos para la habilitación del servicio 166 de llamada Internacional por servicios de tarjetas propias, estarán ubicados en las habitaciones o salas donde radica el paciente extranjero.

c) La administración de la institución garantizará la venta de las tarjetas propias en CUC a los pacientes extranjeros para llamadas Internacionales.

Procedimiento No. 22: Habilitación del Servicio de Televisión Internacional por Tele-cable.

Tiene como objetivo facilitar la visibilidad de la televisión Internacional por Tele-cable a los pacientes y acompañantes extranjeros. Este servició solo podrán optar las instituciones aprobadas del Sistema Nacional de Salud con servicios a pacientes y acompañantes extranjeros.

Responsabilidades:

Cargo	Responsabilidad
Presidente de Servicios Médicos Cubano	1. Proponer al Ministro de Salud la actualización de la lista de instituciones con la aprobación del servicio de Televisión Internacional por Tele-cable. 2. Enviar a la Empresa de Tele-cable Nacional carta de autorizo con listado de las Instituciones por provincia con la aprobación de contratar el servicio de Televisión Internacional por Tele-cable.
Director de la Institución.	1. Solicitar a la Empresa de Tele-cable la contratación del Servicio de Televisión Internacional.

Insumos:

La institución previamente, solicitará la contratación del Servicio de Televisión Internacional a la Empresa de Tele-cable para las habitaciones y/o salas donde radican los pacientes y acompañantes extranjeros.

Desarrollo del Procedimiento.

Unidad administrativa / Cargo	Actividad
Presidente de Servicios Médicos Cubano.	1. Comunica, a los directores de las

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

	Sucursales de Servicios Médicos Cubana en las provincias, de las instituciones aprobadas a contratar el servicio de Televisión Internacional por Tele-cable.
Director de la Sucursal de Servicios Médicos de la Provincia	1. Notificará la Dirección Administrativa de las instituciones aprobadas a contratar el Servicio de Televisión Internacional por Tele-cable.
Dirección de la Institución	1. Solicitará en la oficina comercial de la Empresa de Tele-cable en la provincia, la contratación del Servicio de Televisión Internacional. 2. Garantizará la activación del Servicio de Televisión Internacional por Tele-cable, solo en las habitaciones y/o salas donde radica los pacientes y acompañantes extranjeros.

Políticas del Servicio:

a) El Servicio de Televisión Internacional solo estará instalado en las habitaciones y/o salas donde radican los pacientes y acompañantes extranjeros.

Procedimiento No. 23: Procedimiento para instalación de navegación nacional y correo electrónico por APN de INFOMED.

Paso: 1: habilitar la APN de Infomed en el móvil:

a) En dependencia de la actualización del sistema operativo del móvil ir a:
b) Ajustes
c) Redes móviles
d) APN ó Puntos de Acceso.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

En este punto se debe con figurar la APN de Infomed.

a) Crear nueva APN
b) Nombre: infomed
c) APN: Infomed
d) Nombre de usuario: infomed
e) Contraseña: infomed
f) Se le indica guardar
g) Se activa la APN Infomed.

Paso 2: Habilitación de datos en el móvil.

Se va al menú que se despliega desde la vertical hacia abajo, se busca la opción de activar datos, se activa.

Paso 3: Configurar correo electrónico

Se inicia la aplicación de correo que se va a utilizar.

Se crea una nueva cuenta:

Se siguen los pasos para la creación:

a) Nombre de usuario, completo con @infomed.sld.cu
b) Contraseña
c) Servidor entrante: pop3.sld.cu
d) Servidor saliente: smtp.sld.cu
e) Puerto 25
f) Tipo de seguridad: ninguna
g) Se deshabilita el acceso obligatorio.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Paso 4: Habilitar el servicio de navegación en las redes cubanas.

a) Instalar la versión para móvil de mozilla Firefox.
b) Instalar en el móvil mozilla.
c) Abrir mozilla
d) Colocar en el buscador: about:config
e) Colocar en el buscador: Type, sustituir el valor de 5 por 1 en network.proxy.type
f) Colocar en el buscador: ssl
g) Colocar en network.proxy.ssl: proxy.sld.cu
h) Colocar en network.proxy.ssl_port: 3128
i) Colocar en el buscador: http
j) Colocar en network.proxy.http: proxy.sld.cu
k) Colocar en network.proxy.http_port: 3128
l) Colocar el url: www.cubadebate.cu
m) Comprobar que funciona la navegación.

Medidas de Protección Física.

Medidas requeridas y de obligatorio cumplimiento para cada tipo de área que pueda existir en las instituciones de salud:

Áreas Limitadas:

a) Se ubicarán en locales cuyas puertas y ventanas estén provistas de cierres seguros.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

b) A los locales que tengan ventanas que se comuniquen con el exterior de la instalación, se le aplicarán medidas que garanticen su seguridad y que eviten la visibilidad hacia el interior del mismo.

c) Se prohíbe el acceso de personal no autorizado por la dirección de la entidad.

Áreas Restringidas:

Además del cumplimiento de lo establecido en el área limitada, serán establecidas las siguientes:

a) Tienen que permanecer cerradas, incluso cuando existan personas laborando en ellas, y el acceso a las mismas debe ser controlado mediante los documentos de registros que para ello se establezcan.

b) El personal que acceda a estas áreas deberá cumplir requisitos especiales de idoneidad.

c) Los medios informáticos no podrán estar conectados de manera física o lógica a medios que se encuentren fuera del alcance de estas áreas ni a redes públicas de transmisión de datos.

d) Se aplicarán sistemas de detección y alarma que permitan una respuesta, efectiva ante accesos no autorizados cuando no se encuentre el personal que labora en las mismas.

e) Se implementarán mecanismos y procedimientos de supervisión de la actividad que se realiza en estas áreas.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

f) Se prohíbe la introducción de soportes ópticos y magnéticos personales, excepto los que hayan sido autorizados de forma expresa por la dirección de la entidad.

g) Se prohíbe la introducción de cámaras fotográficas, de grabación de imágenes o cualquier tipo de almacenamiento digital ajeno a la misma.

Áreas Estratégicas:

Además del cumplimiento de lo establecido en el área Limitada y área Restringida, serán establecidas las siguientes:

a) Todo el personal que labora en ellas o que por razones de servicio sea autorizado a permanecer en las mismas, deberá contar con una identificación personal visible que distinga el área.

b) Se implementarán medios especiales de supervisión de la actividad que en ellas se realiza.

c) El acceso a estas áreas por personas ajenas a la misma solo se realizará de manera excepcional, restringida y bajo supervisión, mediante un permiso especial en cada caso emitido por la dirección de la entidad.

Podrá tener acceso a todos los locales el personal de mantenimiento y el de limpieza, en gestiones propias de su trabajo, y siempre en presencia de un miembro del área accedida.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Todas las computadoras, con independencia de su función y del área en que se encuentren estarán protegidas y selladas de manera que no pueda ser abiertas sin autorización y en caso de serlo poder detectar esta acción.

El mantenimiento y reparación del equipamiento informático se realizará exclusivamente por el personal designado, el técnico de la institución acompañará y comprobará el buen funcionamiento y calidad de los trabajos realizados.

Los bienes informáticos del centro serán para uso exclusivo del mismo.

Medidas en las áreas.

a) El área de trabajo debe estar limpia, libre de agua, polvo, papeles o sustancias que puedan causar accidentes o incendios.
b) Prohibido fumar en el área.
c) Prohibido ingerir alimentos en el área.
d) Señalizar el tipo de voltaje de cada tomacorriente.
e) Garantizar la climatización y ventilación de los equipos, y velar por el cumplimiento del mantenimiento periódico de los mismos (sólo el personal especializado para ello).
f) Cumplir con las normas de protección, en caso de traslado de los equipos fuera de sus locales.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

g) Las líneas de alimentación eléctrica para los equipos de computación, no deben alimentar equipos de fuerza o altos consumos a la misma red.

h) Al ocurrir tormentas eléctricas, se desconectarán todos los equipos, salvo una imperiosa necesidad.

i) Los servidores y equipos fundamentales, deben estar conectados a fuentes de energía, y éstas deben poseer limitadores de voltaje.

j) Al concluir la jornada laboral los equipos deberán quedar apagados y desconectados.

k) Los equipos sólo serán operados por el personal autorizado.

l) Todos los usuarios cumplirán de forma estricta lo establecido en la Resolución 85/2007 para el ahorro de energía en los sistemas informáticos.

Cada usuario mantendrá bajo su custodia los soportes magnético-ópticos de interés particular para su trabajo y es responsable de garantizar las copias de seguridad que se requieran.

Sistema de Control de Acceso

a) El acceso a estos locales está limitado.

b) En la puerta deberá reflejarse el nombre de los funcionarios autorizados a entrar en los locales.

c) Está prohibido atender visitas en el local de los Servidores.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

d) Para permitir el acceso al personal no autorizado, sólo estará facultado el Director o los Responsables de Área.

e) Los equipos solo podrán moverse de su local por reparación o porque se considere su traslado a otro local habilitado al respecto. Para ello existe un reglamento interno correspondiente al traslado de medios.

Medidas a las tecnologías de Información.

a) La tecnología de la información destinada al procesamiento de ésta debe ponerse de forma que evite la visibilidad de dicha información a distancia, minimizando la posibilidad de captación de las emisiones electromagnéticas y garanticen un mejor cuidado y conservación de las mismas.

b) Cada una de las PC que lo cumplirá los tres niveles de acceso.

c) Si personal ajeno, pero autorizado debidamente hace uso de alguna tecnología informática, se registrará en el Libro de Incidencias sus datos personales, hora y trabajo realizado.

d) Para la aceptación de un nuevo usuario de la red y de correo, tendrá que solicitarse por su Jefe de área, quien gestionará el servicio de acceso a los mismas.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

e) Todo personal vinculado con este medio informático (estación de trabajo), responde por el mismo y por la protección de la información que se le confíe para el desarrollo de su trabajo.

f) La reparación y mantenimiento de los mismos se realiza sólo por el personal autorizado, siempre en presencia de una persona del departamento o administrador de la red y/o informático.

g) Los equipos sólo podrán moverse de su local para su reparación, o porque se considere su traslado a otro local que se decidiera habilitar al respecto. Para ello existe un reglamento interno del Centro para el traslado de medios básicos que deberá ser cumplido de manera estricta.

Medidas a los soportes de información

Los equipos que contengan información clasificada y/o sensible no están autorizados a salir de la entidad si no se ha borrado antes los datos con un proceso seguro. Estos a su vez están bajo la custodia de los que la usan, y las salvas de información estarán en CD o dispositivos externos autorizados.

Identificación

Los soportes autorizados a utilizar dentro de la entidad se identificarán de forma claramente visible, etiquetando estos con dicha clasificación incluyendo de forma escrita su función y utilidad, y solo estos serán los autorizados a utilizarse. En el caso de dispositivos de salva periódica se adiciona la fecha y contenido de la salva, de acuerdo a la política establecida en el área.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Conservación

a) El traslado de los soportes se hará respetando las normas de conservación de los mismos, para garantizar la integridad de la información.

b) Aplicar la protección contra escritura, tanto por software o hardware, de los datos que no requieran actualización periódica.

c) Mantener los discos originales de instalación, protegidos físicamente contra escritura.

d) Mantener actualizado el registro de soportes magnéticos.

e) Los soportes y tecnologías se conservan en el área en cuestión agrupados en cajas, de acuerdo a su función, las cuales a su vez son guardados en gavetas destinadas para este fin. Las condiciones de conservación resultan favorables, desde el punto de vista de temperatura, humedad e higiene.

Destrucción

Los soportes que sufran deterioros irrecuperables se procederán a su destrucción en presencia del Especialista de Seguridad informática y Grupo de Informática.

En caso de traslado por mantenimientos o reparación se limpiará el equipo de toda información de importancia.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Medidas Técnica o Lógica.

Identificación de usuarios.

Las cuentas de usuarios están diseñadas para permitir la navegación de estos por la red y el acceso a los servicios. Para la creación de una cuenta a un usuario determinado es preciso que esté presente una planilla, donde se especifica sus datos personales y los servicios que se le brindará, esta planilla debe estar debidamente respaldada por la firma y el cuño de sus superiores.

La identificación para el acceso a los sistemas y servicios estará asociada al nombre del usuario y configurada por el Grupo de Informática previa autorización. A cada usuario se le asigna un identificador personal y único. El Grupo de Informática conservará planillas recibidas. De igual forma se procede en caso de cancelación de identificadores de usuarios una vez que concluya la necesidad de su uso. Se puede cancelar una cuenta cuando el centro del usuario expida una carta donde se solicita la cancelación de los servicios para dicho usuario.

Autenticación de usuarios.

Existen contraseñas en el SETUP de cada computadora, así como en el protector de pantalla de cada usuario y en las aplicaciones que así lo requieren. En las aplicaciones quedan establecidos los permisos para los usuarios autorizados. Cada usuario de la red posee una contraseña que consta de 8 dígitos o más, combinados con caracteres especiales y alfanuméricos, para acceder a su cuenta.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Las claves de los servidores, servicios y aplicaciones importantes son cambiadas cada un período mínimo de 3 meses para garantizar la fortaleza de éstas.

La identificación y autenticación de los usuarios a nivel de Sistema Operativo se realiza mediante nombre de usuario y contraseña de uso estrictamente personal, de forma que ningún usuario, a diferencia de los administradores de la red, pueda abrir una sesión ajena a la suya o acceder a otro servicio. De detectar la violación de alguna contraseña esta es cambiada en el momento y tomadas las medidas correspondientes en cada caso.

Causas que motivan el cambio de contraseña antes del plazo establecido.

a) Olvido por parte del usuario de la contraseña o simplemente porque desea cambiarla.

b) Detección ya sea por el usuario o por el Responsable de SI que la clave de éste está siendo utilizada por otra persona.

c) Cambios de departamento o local que lleven a que el usuario entre a otro grupo en dependencia de su localización actual.

Control de acceso a los activos y recursos.

Con relación al personal con acceso al sistema informático, no todos los usuarios de la red tienen los mismos derechos de acceder a la información e incluso de modificarla; sólo el Grupo de Informática tiene acceso pleno a todos los servicios.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Cada usuario tiene definido, según su categoría y sus necesidades, un sistema de derechos que le permiten trabajar con mayor o menor acceso, con los recursos de la red.

Los privilegios son otorgados de acuerdo con el trabajo que realiza el usuario en particular y de la necesidad de tener acceso a cierta información de la Red.

Todos los servicios que se prestan están sometidos a un proceso de chequeo de traza semanal, lo que asegura el pleno conocimiento de los sucesos que ocurren con relación a programas y dispositivos auxiliares en el servidor.

Los privilegios de acceso a cierta información de la Red son suspendidos de acuerdo al tiempo que el usuario determine, en el caso de que se detecte que el usuario no está haciendo uso de la información o uso indebido de la misma se le son denegados los privilegios de acceso y se toman las medidas correspondientes en cada caso.

En caso de que exista en el servidor una carpeta para uso compartido llamada “Común”, la cual pueda estar diseñada para el intercambio solo de documentos durante el día, se limpia como una tarea automática programada en el servidor a las 12:01 am.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Integridad de los ficheros y datos.

El acceso a los ficheros de datos está en dependencia del tipo de usuario y de la función que realiza los cuales pueden ser permisos de solo lectura, de solo escritura o acceso total.

Todo software antes de su explotación, se someterá a una cuarentena técnica, para no poner en riesgo la integridad de la información, en el caso que se requiera. Esta acción será chequeada por el administrador de la red y/o informático junto al especialista de seguridad informática.

Los Password de Administración de la red, con introducción de caracteres especiales de al menos 8 dígitos, deben estar en un sobre sellado en la Dirección y sólo abrirlo en caso extremo de ausencia del mismo. Al abrirlo, el Director o su sustituto deben firmar un acta donde se justifiquen las causas.

Los Sistemas Operativos están preparados para brindar a cada usuario el control sobre sus archivos. La administración de la red revisa diariamente el estado de los ficheros básicos del sistema, así como los datos sensibles inherentes a este. Se encuentran instaladas las herramientas para el control y notificación de cambios significativos que puedan afectar el correcto funcionamiento del sistema y sus servicios.

En las estaciones de trabajo y en los servidores se actualiza semanalmente el antivirus aprobado para su uso, y se chequea con frecuencia donde es de uso obligatorio. Esta labor de instalación y actualización es responsabilidad del Grupo de Informática.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

Dicho antivirus protege no sólo los ficheros de datos sino también los correos electrónicos. Todos los soportes externos que se inserten en las estaciones de trabajo serán chequeados inicialmente.

De seguridad de Operaciones.

Sistemas de salva de respaldo.

a) Todos los ficheros de sistema de las estaciones de trabajo, así como los software de aplicación de los mismos deben estar debidamente salvados y protegidos contra escritura y borrado. La salva forma parte de la política de salva de todos los sistemas y datos del área.

b) La política de las salvas la determina el Jefe del área correspondiente, siendo el técnico que ejecuta el trabajo el encargado de realizarla y guardar los soportes en el lugar destinado para ello dentro del departamento.

c) Se realizan inspecciones en las diferentes áreas donde se encuentran los ordenadores para supervisar el cumplimiento de las medidas impuestas.

Pruebas de inspección

El Grupo de Informática realizará sin previo aviso toda prueba de inspección que estime pertinente para garantizar el cumplimiento del Plan de Seguridad Informática aprobado en la Institución. Donde quedara registrada dicha visita en los registros establecidos.

Calle 23 e/ N y O, Vedado

dni@infomed.sld.cu
Telf.: 8329897

El especialista de Seguridad Informática, ante posibles violaciones, informará de inmediato a su máxima dirección. Auxiliados por los sistemas operativos instalados y las herramientas de Administración de Red, todas las trazas de auditorías realizadas serán archivadas para llevar un historial de todo lo acontecido en el trabajo de control de la seguridad de la Red.

En caso de detectarse por parte del Grupo de Informática o cualquier individuo que se está haciendo uso indebido por parte de un usuario de estos servicios, estos inmediatamente son retirados y se crea una comisión encargada de realizar las investigaciones ante la detección de violaciones.

Anexo 1. Guía de Control Ministerial.

Indicador	Aspectos a controlar	Normativa Reguladora	Acciones de control
1. Cumplimiento de lo establecido en los lineamientos de seguridad de las tecnologías de la información.	1. Se analizan los temas relativos a la Seguridad Informática en los Consejos de Dirección de las Entidades.	Acuerdo 6058/2007 CECM	Comprobar que en las actas de los consejos de dirección a todos los niveles correspondientes si se tiene un punto sobre de seguridad informática donde el responsable de la actividad informática rinda cuentas: - Principales vulnerabilidades de la red, posibles soluciones. - Necesidades de inversión tecnológica. - Plan de Informatización de la entidad.
2. Cumplimiento de lo establecido en el reglamento de seguridad de las tecnologías de la información	1. Los bienes informáticos están identificados, controlados y bajo la custodia de una persona.	Resolución 127/2007	Comprobar si existe inventario actualizado de los medios hasta nivel de componentes y si están bajo la custodia de una persona.
	2. El uso de las TIC y sus servicios por parte del personal está aprobado por la Dirección de la entidad y la asignación de cuentas para el empleo de estos servicios es aprobada y documentada.		Comprobar existencia de un procedimiento efectivo que garantice la aprobación del empleo de las TIC y sus servicios y la asignación/cancelación de cuentas de acceso. Verificar evidencia de las cuentas asignadas.

Indicador	Aspectos a controlar	Normativa Reguladora	Acciones de control
	3. Están implementados adecuadamente los controles y procedimientos para la protección contra códigos malignos.		Comprobar actualización y efectividad de los productos antivirus empleados.
	4. Se cuenta con un sistema fiable de respaldo de la información que garantice la continuidad del proceso después de un incidente o afectación.		Comprobar existencia de copias de la información que lo requiera.

Indicador	Aspectos a controlar	Normativa Reguladora	Acciones de control
3. Cumplimiento de lo establecido para la certificación de los sistemas contables financieros sobre las tecnologías de la información	1. Los sistemas contables financieros soportados en las tecnologías de la información cuentan con el registro establecido.	Resolución 12/2005	- Comprobar que la versión del Sistema Contable Financiero (SCF) utilizado se encuentre certificado y vigente. - Sentarse en la PC para comprobar el entorno de despliegue del SCF. o Parches de seguridad o Antivirus actualizado o Cantidad de usuarios con permisos administrativos - Pedir la plantilla real del departamento de Economía a la Dirección de Recursos Humanos, y comprobar que el registro de usuarios en el SCF está actualizado. - Pedir registro de usuarios que trabajan con el SCF y sus respectivos niveles de acceso.
4. Cumplimiento de las medidas establecidas para el ahorro energético en los sistemas informáticos	1. Está activado el Modo de bajo consumo o de espera.	Resolución 85/2007	Se recomienda entre cinco y diez minutos para el monitor y para el disco duro y entre 15 y 30 minutos para la opción inactividad del PC.
	2. Está habilitado el modo de hibernación.		Se recomienda seleccionar como lapso de tiempo para pasar al modo de hibernación un tiempo no menor de dos horas y no mayor de 6 horas.

Indicador	Aspectos a controlar	Normativa Reguladora	Acciones de control
5. Cumplimiento de lo establecido para el registros de software	1. Se encuentra en el Sistema de Registro de Producto de Software cada producto que compra o que vende.	Resolución 33/2008	- Pedir el Plan de Seguridad Informática para comprobar que las aplicaciones fundamentales se encuentren declaradas en él. - Comprobar que se encuentren registrados los software producidos por empresas desarrolladoras y que hayan sido adquiridos de forma comercial. - Revisar en las estaciones de trabajo que las versiones de los software empleados coincidan con lo declarado en el Plan de Seguridad Informática. - En caso de ser productor de software, verificar: o Copia de autorización comercialización emitida por el Mincom. o Certificaciones de registro de cada uno de los software comercializados, así como de sus liberaciones y versiones. o Que la fecha inscrita en los certificados de registro no haya superado los 2 años. - Revisar los expedientes de facturación de venta de productos de software, para comprobar que no se haya vendido algo que no se encuentre registrado.

Indicador	Aspectos a controlar	Normativa Reguladora	Acciones de control
6. Cumplimiento de lo establecido en el reglamento para el ordenamiento de los recursos de numeración IP.	1. Los titulares de las Redes Privadas de Datos deben elaboran un Plan de Direccionamiento sobre la base de los recursos de numeración IP.	Resolución 71/2015	Comprobar que el Plan de direccionamiento se encuentre elaborado a los diferentes niveles. - Revisar que el plan de direccionamiento se corresponda con lo real implementado en la Red Privada de Datos desde las PC hasta los nodos.
	2. Los titulares de las redes privadas de datos mantienen constancia actualizada y auditable de los planes de direccionamiento.		Comprobar que el Plan de direccionamiento a los diferentes niveles este firmado y acuñado por quien corresponda.
	3. El Plan de Direccionamiento elaborado se aprueba por el responsable de la actividad de informática del titular de la red privada de datos.		Comprobar que el plan de direccionamiento a los diferentes niveles este firmado y acuñado por quien corresponda.
	4. Existe un procedimiento y términos asociados a la asignación de las direcciones IP.		Comprobar que exista un procedimiento relacionado con la asignación de las direcciones IP

Indicador	Aspectos a controlar	Normativa Reguladora	Acciones de control
	5. El procedimiento está aprobado por el responsable de la actividad informática.		Comprobar que el procedimiento este firmado por el responsable de la actividad informática.
	6. El titular de la red privada de datos como parte de la administración de la red, vela por la actualización permanente del Plan de cada red, subred o nodo.		Revisar si los responsables se planifican en su plan de trabajo acciones de control para comprobar el estado de la implementación de la resolución.
	7. Los titulares de las redes privadas de datos deben entregar copia de la base de datos de los planes de direccionamiento, con la asignación a sus usuarios de las direcciones IP reales, a la Dirección General de Informática.		Comprobar que exista correspondencia entre el Plan de direccionamiento del organismo con el recibido en el Mincom.

7 Cumplimiento de lo regulado en el Reglamento de Redes Privadas de Datos.	1. Que la Red cuente con la Licencia Actualizada (o una copia de la misma)	Resolución 128/2011 Artículo 12	1. Chequear que la entidad, en caso de ser titular, posea la licencia para operar la red privada de datos y se encuentre actualizada. 2. Chequear que la entidad, en caso de ser una subred, posea la copia de la licencia emitida al titular de la red y que se encuentre actualizada.
	2. Que las redes mantengan las características técnico-organizativas registradas en su inscripción o que los cambios se hayan informado.	Resolución 128/2011 Artículo 16	Verificar que los datos técnico-organizativos de la red coincidan con los registrados en SICNET
	3. Que en el caso de tener implementado el servicio de VPN o el servicio de VoIP, cuente en uno u otro caso. con la autorización respectiva	Resolución 128/2011 Artículo 7	1. Verificar la existencia de la Licencia que autoriza el empleo de la Voz por IP 2. Verificar la existencia del Autorizo para el empleo de Redes Privadas Virtuales, VPN
8. Cumplimiento de lo regulado en el Reglamento para el empleo de	1. Que la Red cuente con el Permiso actualizado para empleo de los equipos (o una copia del mismo)	Resolución 127/2011. Art. 2, Inc. 2,3	Chequear que la entidad posea el Permiso para emplear medios inalámbricos en la banda de 2,4 Ghz dentro de la red privada de datos.

sistemas de acceso inalámbrico de alta velocidad en la banda de frecuencias de 2,4 GHz	2. Que todo equipo en explotación tenga registrada la identificación (siglas) MAC del mismo y muestre la SSID identificativa de su red.	Resolución 127/2011. Art. 2, Inc. 2,6 al 2,9	Verificar que tanto la dirección MAC como la identificación SSID estén registradas.
9. Cumplimiento de lo regulado en el empleo de la banda de frecuencias de 5 725 a 5 850 MHz. para la implementación de redes de área local por radio inalámbricas (RLAN) como parte de las redes privadas de datos.	1. Que los enlaces establecidos posean la autorización de operación dentro de la red privada de datos.	Resolución 156/2011. Resuelvo Cuarto	Chequear que la entidad posea el Permiso para emplear medios inalámbricos en la banda de 5,7 Ghz dentro de la red privada de datos.
	2. Que todo equipo en explotación muestre la SSID identificativa de su red y tenga registrada la identificación (siglas) MAC del mismo.	Resolución 156/2011. Resuelvo Decimoséptimo y Decimoctavo	Verificar que tanto la dirección MAC como la identificación SSID estén registradas.
10. Cumplimiento de lo establecido para los sistemas de radiocomunica	1. Que exista el documento que autoriza el sistema de frecuencia del servicio móvil marítimo en la banda de VHF.	Resolución 2010002	Chequear que el usuario posea la resolución de referencia.

ciones (Estaciones repetidoras, equipos fijos, móviles y portátiles)	2. Que se empleen correctamente los parámetros técnicos establecidos en sistema 4170 del servicio móvil marítimo en la banda de VHF.	Resolución 2010002	Verificar que: 1. la potencia máxima de transmisión no exceda los 25 watts; 2. el sistema trabaje en régimen de explotación simplex; y 3. opere en modo de emisión F3E
	3. Que las frecuencias y distintivos de llamadas utilizadas correspondan con las autorizadas en el sistema 4170	Resolución 2010002	1. Chequear que las frecuencias utilizadas correspondan con las autorizadas para el sistema 2. Comprobar que se emplee correctamente el distintivo de llamada
	4. Que existan las licencias de operación para todas las estaciones radioeléctricas de cada uno de los sistemas y resoluciones antes mencionadas	Resolución 2010002	Verificar que el usuario posea las licencias de operación de cada una de las estaciones radioeléctricas.
	5. Que las licencias de operación para las estaciones radioeléctricas estén actualizadas	Resolución 2010002	Verificar que las licencias de operación de cada una de las estaciones radioeléctricas estén actualizadas en correspondencia con lo existente.

11. Cumplimiento de lo establecido para los sistemas de radiocomunicaciones (Estaciones repetidoras, equipos fijos, móviles y portátiles)	1. Que exista el documento que autoriza el sistema de frecuencia del servicio fijo en la banda de onda corta (HF).	Resolución 990084	Chequear que el usuario posea la resolución de referencia.
	2. Que se empleen correctamente los parámetros técnicos establecidos en sistema 4158 del fijo en la banda de onda corta (HF).	Resolución 990084	1. la potencia máxima de transmisión no exceda los 100 watts; 2. el sistema trabaje en régimen de explotación simplex; y 3. opere en modo de emisión J3E
	3. Que las frecuencias y distintivos de llamadas utilizadas correspondan con las autorizadas en el sistema 4158	Resolución 990084	1. Chequear que las frecuencias utilizadas correspondan con las autorizadas para el sistema 2. Comprobar que se emplee correctamente el distintivo de llamada
	12. Que existan las licencias de operación para todas las estaciones radioeléctricas de cada uno de los sistemas y resoluciones antes mencionadas	Resolución 990084	Verificar que el usuario posea las licencias de operación de cada una de las estaciones radioeléctricas.

	13. Que las licencias de operación para las estaciones radioeléctricas estén actualizadas	Resolución 990084	Verificar que las licencias de operación de cada una de las estaciones radioeléctricas estén actualizadas en correspondencia con lo existente.
12. Cumplimiento de lo establecido para los sistemas de radiocomunicaciones (Estaciones repetidoras, equipos fijos, móviles y portátiles)	1. Que exista el documento que autoriza el sistema de frecuencia del servicio móvil terrestre en la banda de VHF	Resolución 990083	Chequear que el usuario posea la resolución de referencia.
	2. Que se empleen correctamente los parámetros técnicos establecidos en sistema 4021 del servicio móvil terrestre en la banda de VHF	Resolución 990083	4. la potencia máxima de transmisión no exceda los 100 watts; 5. el sistema trabaje en régimen de explotación simplex; y 6. opere en modo de emisión J3E
	3. Que las frecuencias y distintivos de llamadas utilizadas correspondan con las autorizadas en el sistema 4021	Resolución 990083	3. Chequear que las frecuencias utilizadas correspondan con las autorizadas para el sistema 4. Comprobar que se emplee correctamente el distintivo de llamada

	4. Que existan las licencias de operación para todas las estaciones radioeléctricas de cada uno de los sistemas y resoluciones antes mencionadas	Resolución 990083	Verificar que el usuario posea las licencias de operación de cada una de las estaciones radioeléctricas.
	5. Que las licencias de operación para las estaciones radioeléctricas estén actualizadas	Resolución 990083	Verificar que las licencias de operación de cada una de las estaciones radioeléctricas estén actualizadas en correspondencia con lo existente.