República de Cuba

PLAN DE SEGURIDAD INFORMATICA

UNIVERSIDAD DE CIENCIAS PEDAGÓGICAS "ENRIQUE JOSÉ VARONA"

TITULO: PLAN DE SEGURIDAD INFORMATICA

REV. 00	ELABORADO	REVISADO	APROBADO
NOMBRE	Lic. Jorge Abraham Díaz Sosa	Dr C. Georgina Díaz Fernández	Dr C. Alfredo Díaz Fuentes
CARGO	J. Seguridad Informática	Vicerrectora	Rector
FIRMA			
FECHA	20 septiembre 2008		

REV.	ELABORADO	REVISADO	APROBADO
NOMBRE	Dr. C. Alejandro Miguel Rodríguez Cuervo	Dr. C. Georgina Díaz Fernández	Dr. C. Deysi Fraga Cedré
CARGO	Esp. Seguridad Informática	Vicerrectora	Rectora
FIRMA			
FECHA	Enero 2013	Enero 2013	Enero 2013

PAGINAS REVISADAS:

REV.	ELABORADO	REVISADO	APROBADO
NOMBRE	Issel Puig González	Dr. C. Miguel Alejandro Rodríguez Cuervo	Dr. C. Deysi Fraga Cedré
CARGO	Esp. Seguridad Informática	Director Informatización	Rectora
FIRMA			
FECHA	Octubre 2017	Octubre 2017	Octubre 2017

PAGINAS REVISADAS:

REV.	ELABORADO	REVISADO	APROBADO
NOMBRE			
CARGO			
FIRMA			
FECHA			

PAGINAS REVISADAS:

INDICE

PRESENTACIÓN DEL DOCUMENTO

El Plan de Seguridad Informática constituye una exigencia de la Resolución No. 127 de 2007 del Ministerio de la Informática y las Comunicaciones (MIC) que pone en vigor el Reglamento de Seguridad para las Tecnologías de la Información y garantiza un respaldo legal que responde a las condiciones y necesidades del proceso de informatización del país.

Las medidas de contingencia están contenidas dentro del Plan de Seguridad Informática. En las mismas se reflejan las medidas que deben tomarse con el fin de garantizar la continuidad de los procesos informáticos ante cualquier desastre o eventualidad que puedan provocar su interrupción en cada área y las acciones necesarias para contrarrestarlas o enfrentarlas en el menor plazo posible.

Dada la necesidad de garantizar la Seguridad y Protección de los recursos informáticos de la Universidad y la información que se procesa, intercambia reproduce y conserva mediante el uso de las tecnologías informáticas y de comunicaciones hace imprescindible poner en vigor un Plan de Seguridad Informática, que regule la disciplina informática en todos los estudiantes y trabajadores de todas las áreas de la Universidad, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

La seguridad informática en la Universidad conjugara un conjunto de medidas de (administrativas, organizativas, físicas, técnicas, legales y educativas) con un enfoque integral y un tratamiento en sistema, dirigidas a prevenir, detectar y responder a las acciones que pongan en riesgo la integridad, confidencialidad y disponibilidad, de la información que se procesa, intercambie, reproduzca o conserve a través de las tecnologías informáticas, así como el correcto uso del Correo Electrónico e Internet.

Las medidas de protección física y sobre el secreto estatal que se recogen en este Plan están en correspondencia con lo establecido en el Decreto Ley No. Decreto ley 199 sobre la seguridad y protección de la información oficial.

El presente plan está en conformidad con el Acuerdo No. 6058 del Comité Ejecutivo del Consejo de Ministros, de fecha 9 de julio del 2007, aprobó los Lineamientos para el Perfeccionamiento de la Seguridad de las Tecnologías de la Información en el país y la Resolución Ministerial 127/2007 del Ministerio de Informática y las Comunicaciones, de fecha 24 de Julio de 2007, aprobó el Reglamento de Seguridad para las Tecnologías de la Información que rigen la seguridad de las tecnologías de la información.

1. ALCANCE

Son objeto de análisis para la confección de este Plan de Seguridad así como el estricto cumplimiento de todo lo contenido dentro de él, todos los bienes informáticos y de comunicación que se encuentran en las áreas del edificio de la Universidad Pedagógica “Enrique José Varona” y las que están ubicadas en otros locales fuera del Edificio central como: Facultad de Lenguas Extranjeras, Facultad de Ciencias Naturales y Exactas, Facultad de Ciencias Técnicas, Facultad de Humanidades, Facultad de Ciencias de la Educación, Dirección de Economía y Servicios, Museo de la Alfabetización y la residencia de profesores Villa Varona, la Biblioteca Orestes Gutiérrez y la escuela especial “Dora Alonso” subordinadas al MINED, con las cuales se posee un convenio de colaboración (anexo). Todas estas instalaciones están ubicadas dentro de la Ciudad Escolar Libertad (CEL) como lo muestra el mapa del **ANEXO 1**. Este plan abarcará todas las tecnologías informáticas instaladas en cada área de la institución.

Por su importancia se destacan las estaciones de trabajo que se emplean en las Direcciones de Cuadros, Preparación para la Defensa, el Nodo de Comunicaciones, así como las estaciones de trabajo que emplean el sistema económico contable de la Universidad y el SIGENU.

Igualmente se tiene en cuenta la protección del servidor controlador de dominio primario de la red que está en el local del

Nodo de comunicación y las conexiones que garantizan el funcionamiento correcto de la red local, así como los servidores de correos y proxy.
Se concibe, por último, la protección del resto de la información que se procesa en la Universidad.

2. CARACTERIZACIÓN DEL SISTEMA INFORMÁTICO

- **Objeto social y datos generales que identifican a la Universidad.**

La Universidad de Ciencias Pedagógicas "Enrique José Varona" (UCPEJV) es un centro perteneciente al Ministerio de Educación Superior (MES), encargada de la formación de profesores para las diferentes educaciones de la capital, posee además convenios de colaboración con otros países y provincias del país para la formación de Doctores y Máster en Ciencias Pedagógicas, desarrolla cursos de postgrado, maestrías y diplomados a los docentes, independientemente de que su radio de acción principalmente es la capital de país, tiene alcance nacional por los elementos aportados anteriormente.
La Universidad cuenta con una plantilla de 675 docentes y 347 no docentes y un potencial de 198 Doctores en Ciencias y 353 Máster en Ciencias.
La Universidad cuenta con una Red Wifi con puntos de acceso en las áreas correspondientes al edificio central, Facultad de Ciencias de la Educación, el Museo de la Alfabetización, Facultad de Lenguas Extranjeras, Vice Rectoría, Facultad de Ciencia Naturales y Exactas, Facultad de Ciencias Técnicas y Facultad de Humanidades con un enlace punto a punto desde la Villa Varona, dependencias autorizadas para recibir estos servicios, su alcance es limitado, para un radio de alrededor de 50 metros.
Los servicios autorizados para la navegación con la red Wifi están explicados en el **Manual de Procedimientos de la Universidad referidos a la seguridad informática**,

Los servicios que reciben los usuarios de las tecnologías informáticas y las redes en la Universidad son los establecidos en las Instrucción #1 del MES: Tablas con el resumen de los usuarios que reciben servicios telemáticos que se ofrecen en la red de la Universidad.

Total de usuarios de la Red	
Personal/cuentas	**Cantidad**
Estudiantes	2888
Docentes	798
No docentes	114
Cuentas institucionales para organismos y eventos	3
Total	**3803**

Estas cifras son variables en dependencia de las altas y bajas que se producen.

Los servicios telemáticos que brinda la red son: Correo nacional e internacional y Navegación nacional e internacional.

En cuanto a servicios de navegación tenemos el portal Varona, asociados a este se prestan los servicios de blog, mensajería instantánea, foro, centro de recursos multimedia, Varona virtual, mediateca, Web docente y ftp, además de los servicios por autenticación como correo e Internet.

La universidad cuenta con dos portales, uno interno y otro externo según establece la Resolución Rectoral 14/2016

La red interna de la Universidad, está caracterizada en 3 escenarios para el uso de las tecnologías informáticas que son los siguientes:

1. PC por cada usuario (accede un solo usuario)

2. PC utilizada por varios usuarios (departamentos, otras oficinas, etc.).
3. Laboratorios

Además, las PC se agrupan a partir de:

- La información que se procesa.
- Cargo del o responsabilidad que desempeña el usuario que la trabaja.

A partir de lo anterior las estaciones de trabajo de la Universidad están agrupadas en las siguientes clases:

Clase A:

1. PC de Directivos de primer Nivel (Rectora y Asesores).
2. PC de Vicerrectores, Decanos, Jefe del órgano de cuadros, preparación para la defensa, directores de contabilidad, ATM, secretaria general, secretarias de las facultades y asesoría jurídica.
3. PC que procesan información clasificada y limitada en las áreas.
4. PC que trabajan con datos que tributan a la información clasificada y limitada
5. PC de comunicación en tiempo de guerra.

Clase B:

1. PC de los Vicedecanos, directores y jefes de Dpto. de la universidad.
2. PC que contienen información vital que tributan para la toma de decisiones.
3. PC con información de economía.
4. PC con información de Proyectos con Instituciones Internacionales o con investigaciones sociales de gran impacto en la sociedad.

Clase C:

1. PC con información de planes de estudio.
2. PC con información de producciones de recursos para la educación (Software Educativos, Sistemas).
3. PC con información de proyectos de inversiones.
4. PC con información de distribución de recursos.
5. PC con información de facturación.
6. PC con evaluaciones de los docentes, técnicos y cuadros de dirección.

Clase D:

1. PC que trabajan o procesan información relacionada con la gestión contable y financiera.

Clase E:

1. PC para la gestión de comunicaciones de las redes.

Clase F:

1. PC con otras informaciones.
2. Laboratorios docentes (estudiantes y profesores)

En el manual de procedimientos explican los distintos tipos de clases que se establecen en la universidad.

- **Características del procesamiento de la información Limitada, Secreta y Confidencial, a través de las tecnologías de información.**
  En la Institución por lo general no se procesa información clasificada ni secreta en máquinas conectadas a la Red. Las máquinas que contienen información sensible o limitada como las que trabajan en las oficinas de secretaria general, secretarias de las facultades, Rectoría, cuadros, asesoría jurídica y preparación para la defensa, el tipo de información de las mencionadas anteriormente están identificadas en las PC que las contienen y son manipuladas por sus respectivos jefes, así como las salvas de la información. La información que contienen los servidores es confidencial ya que cualquier problema en ella produciría la salida de funcionamiento del servicio o del sistema, obstaculizando los servicios de mensajería nacional e interna, es decir dentro y fuera de la Institución.
  La información que se procesa en la Dirección de Economía y Servicios, a través de los sistemas contables, las PC están conectadas en una Intranet independiente a las del resto de la universidad, el Dpto. de economía tiene un servidor con los softwares que utilizan para la gestión económica, control de medios básicos y nóminas, solo es manipulada por las personas autorizadas en esa área.
- **Diagrama de flujo de información que ilustre la relación interna y externa, así como los medios que utilizan para procesar la misma y topología de las redes de transmisión de datos con que cuentan.**

El diagrama de flujo de información se muestra en el **ANEXO 1a**. Como se puede apreciar en el mismo existe un centro de informática, que es el encargado de recepcionar toda la información que llega a la Universidad, existiendo un intercambio por correo electrónico entre el centro de informática por la Red Local y también a través del correo con las diferentes áreas del Ministerio de Educación Superior que están conectadas.

La Dirección de Economía envía hacia el Ministerio de Educación Superior los balances financieros impresos y un fichero en Excel que resume datos predefinidos mensualmente. Internamente procesan caja y banco, nominas, medios básicos y medios de rotación y envían comprobantes hacia la Contabilidad General, pero todos están en aplicaciones ubicadas en el servidor ubicado en la Dirección de Contabilidad, aunque se ejecutan en las estaciones de trabajo.
El área de planificación y estadísticas envía información oficial al MES relacionada con las altas, bajas y traslados.
La información que se procesa por las diferentes áreas de la universidad se transmite por la red interna y externa a través de correo electrónico hacia las diferentes direcciones y departamentos del de la universidad, del MES y otras instituciones.
Las salvas se hacen diariamente en carpetas individuales en cada equipo de las compañeras que trabajan directamente cada sistema y es responsabilidad de cada jefe del área y del personal designado para realizarlo.

3. RESULTADOS DEL ANÁLISIS DE RIESGOS.

Teniendo en cuenta el **análisis de riesgo previo** a la elaboración del plan de seguridad, los activos informáticos de la Universidad son:

TABLA 1

No.	Descripción	Tipo	Ubicación
1	Componentes de red y comunicaciones (switches, modem- routers, cableado y puntos de acceso)	HW	Local del Nodo y todas las áreas que cubre la red.
2	Servidores (Proxy, Correo, DNS, FTP, Hosting, DHCP)	HW-SW	Local del Nodo
3	Sistema de nóminas y sistema de medios básicos del Dpto de contabilidad.	SW-DT	Economía
4	Aplicaciones del Portal y servicios asociados.	SW-HW-DT	Local del Nodo.
5	Información Limitada o sensible de la oficina de la oficina de PPD, secretaria general y secretaria de cada facultad, Rectoría, Cuadros y otros directivos.	SE-DT	Local de la Jefa de Cuadros, Jefe de PPD, Rectora, Decanos, secretaria general y de las facultades.
6	Estaciones con acceso a Internet	SW-DT	Toda el área de la Universidad
7	Restantes estaciones de trabajo	SW-DT	Toda la Universidad
8	Salva en soporte magnético de los datos e información.	DT	Toda la Universidad
9	SIGENU	HW-SW-DT	Local del Nodo.

Leyenda: HW - Hardware SW- Software DT – Datos

La determinación de la importancia la realizamos de forma numérica asignando valores entre 0 y 10. De esta forma, los bienes informáticos pueden tener una importancia baja, media, alta o muy alta según los siguientes valores:

- Importancia baja de 0 a 3,5
- Importancia media de 3,6 a 6.0
- Importancia alta de 6,1 a 7,9
- Importancia muy alta de 8,0 a 10

Con importancia **muy alta** y de carácter vital se distinguen los componentes de red y comunicaciones (switches, modem-routers, cableado y puntos de acceso), Servidores (Proxy, Correo, DNS, FTP, Hosting, DHCP), aplicaciones del Portal y servicios asociados, SIGENU, sistema de nóminas y sistema de medios básicos del Dpto de contabilidad, ya que ellas constituyen un punto crítico para el funcionamiento de la Universidad. Por este motivo, estas estaciones de trabajo y las aplicaciones asociadas se consideran de **misión crítica**.

De importancia **alta**, se cataloga la información limitada en las oficinas de cuadros y preparación para la defensa, las salvas en soporte magnético de los datos e información de la Universidad de las Vicerrectorías, secretaria general y de las facultades, ya que la pérdida o extravío de las mismas ocasionaría la pérdida del patrimonio histórico del centro y el control de los recursos.

De importancia media en este momento se califican las estaciones de trabajo con acceso a Internet y el resto de las estaciones, pues todavía la Universidad, su personal no cuenta con la suficiente experiencia en el empleo de estas tecnologías, además que el servicio será ofrecido según la Instrucción #1 del MES y la Resolución Rectoral #20 de 2017

No.	AMENAZAS	BIENES INFORMATICOS								
		1	2	3	4	5	6	7	8	9
1	Acceso no autorizado	-	X	X	X	X	X	X	X	X
2	Modificación o divulgación de información no autorizada	-	X	X	X	X	X	X	X	X
3	Contaminación por programas malignos			X	X	X	X	X	X	X
4	Fuga de información	-	X	X	X	X	X	X	X	X
5	Fallo de software	X	X	X	X	X	X		X	X
6	Fallo de hardware	-	X	X	X	X	X			
7	Fallo de energía eléctrica	X	X	X	X	X	X	X	X	X
8	Error de operación	X	X	X	X	X	X		X	X
9	Robo o hurto parcial o total de TI	X	X	X	X	X	X	X	X	X
10	Deterioro físico y obsolescencia técnica	X	X	X	X	X	X	X	X	X
11	Falla de comunicación		X	X	X		X	X		
12	Modificación de los controles de seguridad		X	X	X	X			X	X
13	Tormentas eléctricas severas	X	X	X	X	X	X	X	X	X

ESTIMACION DE RIESGO SOBRE LOS ACTIVOS Y RECURSOS

DOMINIO	RIESGOS													RIESGO	IMP	PESO
	1	2	3	4	5	6	7	8	9	10	11	12	13			
Componentes de red y comunicaciones (switches, modem- routers, cableado y puntos de acceso)			0,2	0,3	0,8	0,8	0,9	0,3	0,2	0,8	0,2	0,3	0,8	**0,35**	**9**	**3,12**
Servidores (Proxy, Correo, DNS, FTP, Hosting, DHCP)	**0,3**	0,3	0,2	0,3	0,8	0,8	0,9	0,3	0,2	0,8	0,2	0,3	0,8	**0,39**	**8,67**	**3,40**
Sistema de nóminas y sistema de medios básicos del Dpto de contabilidad.	0,8	0,8	0,7	0,6	0,5	0,4	0,8	0,5	0,7	0,4	0,3	0,8	0,7	**0,50**	**8,5**	**4,22**
Aplicaciones del Portal y servicios asociados.	**0,2**	**0,5**	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	**0,26**	**8,5**	**2,22**

Información Limitada, de la oficina de la oficina de PPD, Cuadros y otros directivos.	**0,3**	**0,8**	0,8	0,6	0,6	0,4	0,7	0,3	0,3	0,3	0,3	0,3	0,3	**0,42**	6,5	**2,70**
Estaciones con acceso a Internet	**0,3**	0,2	0,3	0,3	**0,3**	0,2	0,3	0,3	**0,3**	0,2	0,3	0,3	0,3	**0,23**	4,83	**1,11**
Restantes estaciones de trabajo	**0,2**	0,2	**0,6**	0,2	**0,2**	0,2	**0,2**	0,2	**0,2**	0,2	**0,2**	0,2	0,2	**0,20**	5,67	**1,13**
Salva en soporte magnético de los datos e información.	0.3	0,5	0,5	0.3	0,5	0,5	0.3	0,5	0,5	0.3	0,5	0,5	0,4	**0,27**	6	**1,62**
SIGENU	**0,2**	**0,5**	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	0,3	**0,26**	8,5	**2,22**
TOTALES															**66,17**	**21,75**

Se considera que:

- Riesgo bajo de 0 a 0,35
- Riesgo medio de 0,36 a 0,59
- Riesgo alto de 0,60 a 0,79
- Riesgo muy alto de 0,80 a 1,0

En la actualidad, el riesgo de contaminación con programas malignos en la entidad en general es bajo, debido a que se utiliza el Segurmática Antivirus Corporativo 1.72 y como antivirus internacionales el Nod 32 V4, 5, 6, 7, 8 o el Kaspersky, en las estaciones de trabajo, en el servidor de correo se utiliza el SSPAMASSASSIN como ANTISPAM y el CLAMAV.
Para la valoración de errores en la operación de los Sistemas instalados se tuvo en cuenta que las personas que operan los sistemas principales tienen la experiencia profesional para no cometer errores serios. Además, el Administrador de la Red que opera los servidores tiene los conocimientos suficientes como para que el trabajo fluya sin errores.

El equipamiento con que cuenta la entidad en general es bastante obsoleto y se encuentra en un estado técnico aceptable.
La política de salvas implementada prevé que las informaciones importantes para la institución almacenadas en una PC, si esta máquina falla, se tenga una versión lo más actualizada posible de la información que contenía su disco duro guardad en DVD.
Las fallas de software podrían presentarse, pero en las aplicaciones consideramos que es más baja la probabilidad de que esto suceda. Donde puede ser que existan fallos es en el software base por el empleo de sistemas operativos con desactualizaciones en los parches de seguridad. Debe implementarse una política de actualizaciones de los sistemas operativos y otras aplicaciones utilizadas en la entidad de manera de poder minimizar el riesgo de los fallos posibles en sistemas y aplicaciones tales como el Internet Explorer, sistema que soporta el portal varona. Por este motivo, el riesgo se considera medio.
Las fallas por tormentas eléctricas severas se consideran con riesgo alto, ya que la red de la Universidad no cuenta con tierra física, las UPS están en mal estado y se deben tomar las medidas para desconectar los equipos de la red eléctrica ante la presencia de tormentas eléctricas severas.

La probabilidad de fallas de las comunicaciones se considera en general, baja. En la actualidad, disponen de una línea fibra óptica a través de un modem de 20 MBits.
El personal que labora con las tecnologías informáticas es confiable, además se ha concientizado sobre la necesidad de la seguridad informática y más de 500 trabajadores recibieron el curso de seguridad informática. Asimismo, en la entidad no se procesa información clasificada a través de las mismas. Teniendo en cuenta todo lo anterior consideramos que la divulgación de información no autorizada es poco probable.

El personal autorizado para el acceso al internet se concibe con medidas de seguridad mínimas como la de identificación y autenticación del usuario para el acceso a internet, entre otras, lo que hace que el uso no autorizado de esos servicios sea difícil.

La amenaza de afectaciones debido a fallos de fluido eléctrico tiene alta probabilidad de materializarse, pues no se cuenta en los servidores y otros dispositivos con el respaldo eléctrico necesario para la continuidad del trabajo de los servicios en la red. Las UPS de los servidores son insuficientes para garantizar que estos continúen brindando servicio en caso de interrupciones del fluido eléctrico mayores de 15 o 20 minutos.

No hemos considerado en este Análisis de Riesgos desde el punto de vista informático como una amenaza real la posibilidad de que la información o el equipamiento se destruya por causa de un incendio, ya que al no existir un sistema de alarma contra incendios pudiera resultar alta la probabilidad de que esto ocurra si se presentara un siniestro en horario no laboral y tendría una incidencia muy grande en el resultado cuantitativo del análisis. Pero teniendo en cuenta las características de la edificación y de la construcción, y su locación geográfica, no cercana a lugares propensos a la propagación de incendios, en realidad las probabilidades de ocurrencia de un siniestro son bajas.

El peso total del riesgo entonces es Bajo (21,75/ 66,17= 0,33)

,

El presente plan durante su desarrollo tendrá en cuenta el análisis realizado y se incluirán medidas para solucionar los problemas detectados. En caso que no se puedan acometer algunos de los trabajos antes de finalizar la elaboración del plan, se propondrá que formen parte del programa de seguridad.

4. POLÍTICAS DE SEGURIDAD INFORMÁTICA

- **Prioridades en cuanto a las características de la información para garantizar su confidencialidad, integridad y disponibilidad.**
    1. Los bienes informáticos a proteger son el hardware, o sea, las tecnologías informáticas y de comunicaciones, el software y los datos.
    2. La información es un bien, un recurso y como tal debe protegerse. Los datos son los más expuestos a todo tipo de riesgos puesto que son accedidos por más personas y sometidos a las mismas amenazas no intencionadas que los demás.
    3. Las características a priorizar de la información son en orden de importancia: la confidencialidad (impedir la divulgación no autorizada), la integridad (impedir la modificación no autorizada) y la disponibilidad (impedir la retención no autorizada). En el caso concreto del acceso a Internet prima la disponibilidad del servicio.
- **Adquisición, uso, mantenimiento y traslado de tecnologías de información de la entidad.**
    1. Es responsabilidad de cada trabajador el uso racional del equipamiento informático con que cuenta para el desarrollo de su trabajo.
    2. Tanto la introducción de nuevas tecnologías informáticas, como software serán avalados por la Dirección Administrativa y por el personal del nodo y el especialista de seguridad informática de la Universidad.
    3. El traslado fuera del centro de cualquier equipo informático debe ser autorizado por el jefe administrativo del área, siguiendo los lineamientos establecidos por el sistema de medios básicos de la entidad.
- **Flujo de información interna y externa**
    1. El flujo de información interno se realizará fundamentalmente a través de la red local, correo electrónico y servicio de FTP.
    2. El externo se realizará principalmente a través del correo electrónico, servicio ftp o de soportes magnéticos como memorias flash, CD, DVD y discos duros externos.
- **Determinación de responsabilidades en cuanto a la propiedad y administración de la información.**
    1. El personal que trabaje con las tecnologías informáticas y de comunicaciones responderá por la protección de la información que se le confíe.
    2. Cualquier violación que se detecte en materia de seguridad informática en cada área de la institución, se comunicará de inmediato al jefe administrativo del área, a los especialistas o activista de seguridad informática de la misma, quien tomará las medidas correspondientes.

3. En materia de seguridad informática cada trabajador, queda subordinado al jefe administrativo de su área el cual será asesorado por el especialista o activista de seguridad informática correspondiente a su área.
4. Cada trabajador responderá porque cualquier nuevo soporte que vaya a ser introducido en el sistema sea chequeado antes de ser utilizado.

- **Intereses de seguridad ante nuevos proyectos de desarrollo.**

1. Todos los nuevos desarrollos serán orientados a las nuevas herramientas de programación orientados a objetos por lo que se garantizará el modularidad.
2. La calidad del proyecto en todas sus etapas se garantiza de la siguiente forma:

- Etapa de análisis y diseño: el Jefe de cada proyecto lo presenta y se discute en un consejo técnico del área que avala su calidad y aprueba la continuación del proyecto.
- Etapa de Programación, puesta a punto: Se hacen revisiones cruzadas entre los integrantes del proyecto y se pilotean con datos reales.
- Implantación: se le instala al usuario en su máquina y se explota como fase de prueba.

3. Para la adquisición de nuevo software, siempre que existan distintas ofertas, se tendrá en cuenta además de las necesidades por las que se requiere hacer la compra, las opciones que en materia de seguridad éstos posean.

- **Gestión para la implantación de nuevas versiones de sistemas y aplicaciones.**

1. La instalación de Sistemas Operativos, software base, utilitarios, software de propósito general y software educativos, será aprobado por el especialista o activista de Seguridad Informática de la institución y autorizado por la Dirección de informatización a partir de la evaluación de los administradores de la Red de la Universidad y otro personal designado cuyos nombres se indican en el **ANEXO 3.**
2. Se habilitará para cada microcomputadora un registro de software autorizado y el control de los componentes internos de cada computadora. (**Manual de procedimientos**) (**Registro 9)**
3. Es tarea del Dpto. de administrador de la Red y del especialista de Seguridad Informática, la validación de todo software que se adquiera.

- **Preparación y realización de auditorías.**

1. Se realizarán auditorías tanto internas como externas, para conocer la marcha del Plan de Seguridad Informática y la preparación de los trabajadores en este sentido.
2. Las auditorías internas se efectuarán dos veces al año y se creará una comisión para la misma, la cual estará compuesta por al menos cuatro compañeros.
3. Las auditorías externas se realizarán por el MES y otras instituciones nacionales como la Contraloría General y la OSRI, según las fechas en las tengan programadas.

- **Control de acceso a los activos informáticos.**

1. La política de control de acceso que se aplicará es de mínimo privilegio, cerrada y no discrecional. Es decir, cada persona tendrá acceso a la información imprescindible para el desarrollo de su trabajo, y todo lo que no está explícitamente permitido queda prohibido. La decisión sobre quiénes tendrán acceso a determinado fichero y quiénes no corresponden a los niveles superiores y no a su creador.
2. Los usuarios de la red están obligados a registrarse para el uso de los servicios de la universidad y no tienen privilegios de administración si no es el administrador de equipo.
3. Las PC con usos compartidos tendrán la configuración de una sesión de administrador y otras para usuarios estudiantes, profesores o visitantes, la contraseña de administración la tendrá el jefe del área o el especialista o activista de seguridad informática del área.
4. Las áreas con tecnologías informáticas contarán con un registro de incidencias, control de acceso y uso de las tecnologías y el control de los componentes internos de las PC, además de estar selladas con el sello del taller de servicios técnicos de CINESOFT, según se establece en el manual de procedimientos.

5. Ningún personal está autorizado a abrir las PC para realizar reparaciones, solo está autorizado para estos servicios el personal del taller de servicios técnicos de CINESOFT y se reflejará en el registro de incidencias las reparaciones realizadas al equipo y los cambios de piezas realizadas.
6. Las PC que fueron repotenciadas por COPEXTEL tienen 1 año de garantía y es el personal de esa entidad el único autorizado para su reparación en ese periodo, contando con un sello de garantía y otro de CINESOFT.

- **Conexión a redes de alcance global y la utilización de sus servicios.**

1. Utilización de los servicios de internet sólo podrá efectuarse en las microcomputadoras autorizadas y los usuarios que estén autorizados a estos servicios según Instrucción # 1 del MES y la RR # 20
2. Se conectarán a Internet las estaciones de trabajo autorizadas, contando con la seguridad que brinda el Modem-Router y la red en una zona segura detrás del Proxy.
3. Se utilizarán los servicios FTP, WWW, correo electrónico y mensajería instantánea (chat en línea) para los cuales se establecen reglas de Filtrado y autentificación en el Proxy.
4. Aún cuando es posible la creación de cuentas de correo en un sitio de correo libre como Yahoo, Hotmail u otros, los usuarios se abstendrán de hacerlo y utilizarán el correo institucional, pues en la entidad ya existe una política definida para el uso del correo electrónico.
5. Los usuarios autorizados deberán firmar un acta de compromiso del uso de las tecnologías informáticas y las normas éticas que deben cumplir para su utilización **(ANEXO 4 y 5)**
6. El servicio de correo electrónico sólo podrá ser utilizado por el personal autorizado de las distintas áreas de la Universidad.

- **Entrada, salida y utilización de soportes magneto-ópticos en la entidad.**

1.- Es responsabilidad de cada trabajador de la entidad que todo soporte magneto-óptico que salga de la misma no viole los requisitos en lo que a materia de Seguridad Informática se refiere.

2.- Se utilizarán los soportes más adecuados (de acuerdo al volumen de información) para la realización de salvas que se conservarán bajo la custodia de los jefes administrativos y una copia en un FTP privado en los servidores de la Universidad.

3.- Todos los soportes magneto-ópticos que entren en cualquier área de la Universidad para ser utilizados en alguno de los equipos de un área determinada serán revisados contra virus por el activista de seguridad informática del área o por los técnicos de laboratorios que da atención a esa área. Los trabajadores que introduzcan dichos soportes están en la obligación de informar sobre esto al Especialista de Seguridad Informática de su área.

- **Seguridad de las comunicaciones**

1. Todo el equipamiento que da soporte a la red se mantendrá en locales cerrados, climatizados y el personal que labore debe ser de alta confiabilidad.
2. Los estudiantes y trabajadores tendrán su cuenta de usuario con contraseña para acceder al correo electrónico y otros servicios de la red según establece la RR # 20 de 2017
3. Tendrá mensajería internacional sólo el personal autorizado por la dirección de la Universidad.
4. En caso de recibirse anexos a los mensajes se tendrá en cuenta la revisión antivirus y el proceso de cuarentena de ser necesario. Se prohíbe el intercambio de archivos ejecutables vía correo electrónico.
5. Los adjuntos de correo electrónico se enviarán compactados y con un tamaño no mayor de 1MB.
6. Para los usuarios que utilizan Outlook Express para el correo electrónico, envinarán sus correos en texto plano y tendrán desactivada la opción de vista previa.
7. Los usuarios que posean equipos portátiles personales con Wifi, tendrán este servicio solicitado por sus jefes a la Dirección de Informatización o podrán realizarlo personalmente al nodo, la cual habilitara el servicio siguiendo el procedimiento establecido para el mismo.
8. Los estudiantes extranjeros que se encuentran en la Universidad realizando pasantías, maestrías o doctorados, la Dirección de Relaciones Internacionales hará la solicitud por escrito a la Vicerrectoría de tecnología, la cual aprobará los servicios a los que tendrán acceso siguiendo el procedimiento establecido para el mismo.

- **Salva y conservación de la información**

1. Se realizarán salvas periódicas de la información que se procesa en la entidad con el objetivo de su conservación y posterior utilización en caso necesario, siendo responsabilidad de cada Jefe de Área el que sus subordinados salven y responsabilidad del administrador de la red conservar las salvas de las Bases de Datos.
2. Se realizará la salva de la información de forma periódica en CD-ROMS o HD Externos y en los servidores del nodo.
3. El especialista de Seguridad Informática y los activistas por áreas velarán por el cumplimiento del procedimiento para la salva y conservación de la información, obligatorio para todas las áreas.
4. Se guardarán soportes con copias de información fuera de la entidad, concretamente en Hospital Juan Manuel Márquez. Además, se conservan copias de aquellos elementos indispensables para continuar el procesamiento de las aplicaciones críticas en esta misma locación.
5. El nodo realizará salvas de las configuraciones de los servidos y los logs de navegación semanalmente, las mismas serán resguardadas y protegidas y serán guardadas por un año.
6. El personal que administra el portal Varona y otros sitios de la Universidad como las revistas electrónicas y sitios de las facultades y carreras y sus servicios hará las salvas correspondientes del mismo una vez al mes, además de actualizar los parches de seguridad de las aplicaciones que lo soportan.
7. Los procedimientos para las salvas de información se complementan en el **manual de procedimientos**.

- **Personal**

1. Cada trabajador que se incorpore nuevo a la Universidad y necesite la utilización de las tecnologías informáticas y de comunicaciones para su actividad profesional, se le instruirá sobre la importancia de la seguridad informática y las sanciones que podrían imponerse a los que no protejan la información en la institución.
2. El departamento de personal le entregará al trabajador el documento **COMPROMISO PARA EL EMPLEO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y SUS SERVICIOS POR LOS USUARIOS RED DE LA UCP ENRIQUE JOSÉ VARONA, (anexo 4)** el cual firmará y será ubicado en su expediente laboral.
3. Los activistas de seguridad informática de las áreas serán instruirán a los trabajadores sobre los aspectos básicos de la seguridad informática.
4. En caso de violación en materia de seguridad informática, se comunicará al especialista de seguridad informática, y se creará una comisión encargada de analizar la violación correspondiente.
5. Los trabajadores no operarán las tecnologías informáticas y de comunicaciones sin estar previamente adiestrados y autorizados por los Jefes Administrativos.
6. Los trabajadores conocerán las sanciones administrativas a imponer de no cumplir con lo que se regule en el Plan de Seguridad Informática.
7. En caso de ser necesaria la contratación de personal externo, es necesario que se autorice por parte del Jefe de Área, si va a hacer uso de las tecnologías informáticas y de comunicaciones.

- **Clasificación de la información**

1. La información limitada o confidencial que se procesa en la Universidad no se encuentra en ninguno de los equipos que están conectados en RED, y se mantienen todas las medidas de seguridad establecidas en la Ley de Secreto Estatal. Se especifica sus medidas y cuidados de dicha información y las máquinas se mantienen identificadas.
2. Además, se considera como información confidencial aquella que se encuentra en los servidores del Nodo, ya que la salida de funcionamiento de uno de ellos afectaría el trabajo de las áreas y la conexión de la institución con **Internet**.
3. El personal autorizado a procesar y manejar la información clasificada por áreas se relaciona en el **ANEXO 3.** El resto de la información que se procesa, intercambia y almacena en las tecnologías informáticas es ordinaria.
4. La máxima dirección de la Universidad, de conjunto con los Jefes de Áreas y la persona encargada de elaborar la información, serán los encargados de clasificarla, según el Decreto Ley 199/99 y la Lista Interna.
5. En caso de tener que transmitir en alguna ocasión información clasificada a través de la red de la misma se enviará encriptada, previa coordinación con el MININT.
6. En caso de comenzarse a procesar información clasificada, las aplicaciones destinadas para ello asignarán en la pantalla y en cada hoja de la salida por la impresora, la categoría de la clasificación de la información o un término de advertencia, según corresponda.

5. SISTEMA DE SEGURIDAD INFORMATICA

5.1.- Medios Humanos.

El máximo responsable de la Seguridad Informática en la Universidad es su rectora **Deysi Fraga Cedré.** Como tal, es la encargada de la aprobación de este plan de seguridad y la máxima responsable de su cumplimiento. Se ha definido una estructura funcional que atiende toda la actividad de seguridad informática de la Universidad, y que incluye un grupo central de seguridad informática y activistas de seguridad informática en cada una de las áreas, además de un especialista de seguridad informática que se subordina a la Dirección de Informatización. Este cargo lo ocupa el compañero **Issel Luis Puig González.** El **ANEXO 6**, se muestran los integrantes del grupo central de seguridad informática y lo activistas de seguridad informática por áreas.

- **Entre las atribuciones y funciones del especialista y el grupo central de seguridad informática se encuentran:**

a) Organizar y controlar la actividad de seguridad informática.
b) Evaluar el estado de cumplimiento y aplicación de la base legal vigente en la materia.
c) Supervisar el trabajo del personal que responde por la seguridad informática en las diferentes áreas de la Universidad y organizar su preparación.
d) Proponer medidas ante violaciones de la base legal establecida en la materia.

- **Otras atribuciones y funciones del especialista en seguridad informática, del grupo central y los activistas de seguridad informática de las áreas se encuentran:**

a) Controlar como se implanten y cumplen todas las Medidas para la Seguridad Informática que se establecen en el presente Plan de Seguridad Informática. En caso de incumplimientos de las mismas lo informará por escrito a los niveles superiores.
b) Elaborar los procedimientos indispensables para garantizar la seguridad de los sistemas informáticos.
c) Establecer el chequeo previo y posterior de todo soporte magnético que participe en eventos, ferias, exposiciones u otras actividades similares de carácter nacional e internacional, con el objetivo de evitar la posible propagación de algún virus informático y sus consecuencias.
d) Controlar de forma sistemática la integridad de todo software que se encuentra autorizado para su explotación.
e) Velar porque se apliquen los productos de protección actualizados y certificados.
f) Velar que los administradores de la red, técnicos de laboratorios y usuarios aplique los mecanismos de seguridad establecidos para cada área.
g) Definir las condiciones necesarias y someter todo nuevo software que llegue a la entidad al proceso de cuarentena que se detalla en el sistema de medidas.
h) Realizar las actividades previstas en la revisión de todos los soportes magnéticos que se introduzcan en su área de responsabilidad.
i) Comunicar a los jefes administrativos de las diferentes direcciones y departamentos cuando en ellos no se posean y/o apliquen las herramientas tecnológicas de protección actualizada y certificada de acuerdo a las medidas recogidas en el presente Plan de Seguridad Informática.
j) Registrar los virus que aparezcan en la entidad y tratar de determinar quiénes los introducen y cómo, sea de forma intencional o no.
k) Ante indicios de contaminación por un virus informático nuevo o desconocido, aislarlo o apagar el equipo y preservar la microcomputadora infestada y comunicarse de inmediato con el Jefe Inmediato Superior y la Empresa de Consultoría y Seguridad Informática (**SEGURMATICA)**, a través de los teléfonos **7878-1987, 7878-1462 ó 7878-2665** y a la **Dirección de Protección del MININT** (teléfonos **7857-7376 ó 7857-7377).**
l) Analizar periódicamente los registros de auditoría.
m) Apoyar y participar en cuanto al estudio y aplicación del sistema de seguridad de las tecnologías informáticas y de comunicaciones, y en la determinación de las causas y condiciones que propician un hecho de violación en el uso y conservación de estos equipos y la información que se procese, intercambie, reproduzca y conserve en estos equipos.
n) Planificar y coordinar las auditorías periódicas a la actividad de Seguridad Informática.

ñ) Proponer el plan para la capacitación del personal vinculado a la seguridad informática y al personal de la institución con el objetivo de contribuir al conocimiento y cumplimiento de las medidas establecidas en el presente Plan, así como con el resto de las normativas que sobre esta materia se emitan.

o) Ante la ocurrencia de un hecho de violación a la seguridad informática informará de inmediato a su jefe administrativo del área quien deberá informar a la Dirección del Ministerio y de la Universidad, se creará una comisión encargada de realizar las investigaciones con el fin de esclarecer lo ocurrido, precisar los responsables y comunicarlo al órgano correspondiente del Ministerio del Interior.

- **Los administradores de la Red tienen, en relación con la seguridad informática las siguientes obligaciones:**

a) Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red.
b) Realizar el análisis sistemático de los registros de auditoría que proporciona el sistema operativo de la red.
c) Garantizar que los servicios implementados sean utilizados para los fines que fueron creados.
d) Comunicar a la dirección de la entidad los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes.
e) Activar los mecanismos técnicos y organizativos de respuesta ante los distintos tipos de incidentes y acciones nocivas que se identifiquen, preservando toda la información requerida para su esclarecimiento.
f) Participar en la elaboración de los procedimientos de recuperación ante incidentes y en sus pruebas periódicas.
g) Informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento.
h) Participar en la confección y actualización del Plan de Seguridad Informática.

- **Además, deberán cumplimentar las siguientes:**

1. Administrar los recursos de la red y cumplir lo establecido para los medios básicos del Institución
2. Proteger la integridad, confidencialidad y disponibilidad del funcionamiento de la red y la información que circula por ella.
3. Elaborar y hacer conocer el Manual de procedimientos que regirá el trabajo y las transmisiones de la red, así como, velar porque se cumpla lo establecido y tomar las medidas técnicas necesarias con los infractores.
4. Realizar las salvas del sistema operativo, los logs de los servidores y las aplicaciones, así como, la de los datos con la periodicidad requerida por la frecuencia de actualización de los mismos y su preservación durante un año.
5. Establecer un mecanismo de coordinación y aviso con el resto de las redes nacionales, para cuando se considere necesario.
6. Copiar las actualizaciones de los antivirus, aplicaciones que soportan el portal y parches de seguridad de los sistemas operativos autorizados en la universidad en el servidor para que después se puedan actualizar en las estaciones de trabajo.
7. Mantener un chequeo permanente de las estaciones de trabajo en la red, monitoreando varias veces al día el estado de cada estación de trabajo.

- **Responsabilidades**.

- La actualización del Plan de Seguridad Informática, de acuerdo a nuevas características y eventos que surjan, después de su aprobación e implantación inicial está a cargo del grupo central de seguridad informática y del nodo.
- Corresponde en primera instancia al especialista de seguridad informática velar por el establecimiento de todas las medidas descritas en el Plan de Seguridad Informática.
- La autorización para la adquisición de nuevos software y tecnologías informáticas se realiza bajo la aprobación de la Rectora de la Universidad. Los administradores y los activistas de las áreas y facultades y el especialista de seguridad informática son los encargados de mantener actualizado el inventario de las tecnologías informáticas de la universidad.
- Los mantenimientos y/o reparaciones de las tecnologías informáticas son responsabilidad del técnico de la empresa CINESOFT ubicado en nuestra Universidad.
- El acceso a **INTERNET** es para docentes y alumnos y aquellos autorizados por la RR #20 de 2017 y deben cumplir con las regulaciones y medidas que se establecen en el presente plan.
- Cada vez que se reciba un nuevo software en la entidad, el activista de Seguridad Informática del área que lo recibe, deberá realizar las anotaciones correspondientes en el **Registro de software de nueva adquisición** (**Registro 1**). En caso de que el software sea descargado de internet, se debe incluir en este registro, el nombre del software y si

está apto para el uso después de pasar un proceso de cuarentena.

- Cada máquina tiene el **Registro de Software Autorizado** (**Registro 2**), siendo los técnicos de laboratorios y los activistas de Seguridad Informática de las áreas los encargados de que inicialmente quede en las microcomputadoras realmente el software autorizado (estampará su firma en el modelo), según definiciones previas del Jefe del Área. Posteriormente, para la inclusión de nuevo software o la actualización de los existentes, se seguirá el mismo mecanismo.
- Los usuarios tendrán acceso al uso de las tecnologías donde estas se encuentran según se defina en el punto de **Sistema de Control de acceso** de las medidas de Seguridad Física.
- Corresponde a cada uno de los trabajadores que hagan uso de las tecnologías informáticas y de comunicaciones el cumplimiento de las medidas que se plantean en este Plan de Seguridad.
- Por la importancia de Internet, particularizamos en la necesidad de utilizar sus servicios en función de la razón social de la universidad, los usuarios respetando las normas éticas (**ANEXO No. 4)** y todas las medidas que en relación con el tema establece este Plan.
- El especialista de Seguridad Informática de la Universidad conjuntamente con los activistas de Seguridad Informática de las áreas debe velar por el cumplimiento de todas las medidas descritas en este Plan para las tecnologías informáticas.
- El personal de nodo y los usuarios de las tecnologías informáticas en la universidad deberán utilizar los productos antivirus actualizados y certificados.
- Los activistas de seguridad informática de las áreas, el personal del nodo, el jefe de Cesofte son responsables de crear las condiciones necesarias y someter al proceso de cuarentena todo nuevo software que se prevea su generalización y realizar las actividades previstas en la revisión de los soportes magnéticos que se introduzcan en su área de responsabilidad.
- Los usuarios al realizar el intercambio de sistemas y programas de aplicaciones mediante las tecnologías de comunicaciones se realizarán de la siguiente manera: Previamente al envío de información, se utilizará un programa identificador/descontaminador de virus para revisar los ficheros ejecutables que van a ser transmitidos y posteriormente a la recepción de ficheros ejecutables se someterá a los mismos al proceso de cuarentena establecido.
- Cada trabajador que haga uso de las tecnologías informáticas y de comunicaciones corresponde el cumplimiento de las medidas que se plantean en este Plan de Seguridad.
- El especialista de Seguridad Informática de la universidad. velará por que las aplicaciones cumplan con las medidas de protección orientadas para las tecnologías informáticas e informará a las instancias competentes cuando se produzcan incumplimientos en este sentido.

5.2. - MEDIDAS Y PROCEDIMIENTOS DE SEGURIDAD INFORMÁTICA

5.2.1.- De protección física.

Se deben proteger dentro de este Plan de Seguridad las áreas con equipamiento informático, haciendo énfasis en:

√ NODO de Comunicaciones donde se encuentran los servidores fundamentales, ubicado en el Centro de Informática por la entrada del parqueo.

√ Locales donde se encuentran las microcomputadoras autorizadas a hacer uso por la red de los Servicios de Internet.

El local donde están instaladas las tecnologías informáticas tiene una construcción sólida, pues las oficinas son de mampostería. En el local del NODO, donde se encuentran los servidores, y otras tecnologías informáticas es de mampostería, con una sola puerta de entrada o, en su interior las divisiones son de mampostería, el local de los servidores está asegurado con una reja de acceso además de la puerta. No hay extintores en ninguna de las Áreas del NODO se cuenta con una alarma para la detección de intrusos.

El cableado de la red se encuentra protegido en las paredes con canaletas.

No todos los locales con tecnologías informáticas están climatizados. El local donde se encuentran los servidores tiene buena climatización.

No existe tierra física para las estaciones de trabajo en la red local y los servidores. En el edificio no hay pararrayos ni está aterrado. El anexo 10 muestra un esquema de la Red de la Universidad.

Se recomienda adquirir UPS para las PC que aún no tienen de igual manera realizar el aterramiento del edificio.

5.2.1.1. A las áreas con tecnologías instaladas.

El local del Nodo se considera **reservado** por el equipamiento que allí se encuentra, el software instalado y la información de los servidores, así como las máquinas con acceso a Internet, de igual manera se considera un lugar con estas características y por la información que procesa y almacena el local de contabilidad ubicado en la Dirección de Economía y servicios, ya que se tienen el control de las nóminas, inventarios, dietas y otros servicios.

A las tecnologías informáticas de cada área solo tiene acceso el personal asignado y otro personal del área que autorice el jefe administrativo y se anotará en el Registro Control de Acceso a las tecnologías **(Registro 2).**

En el Centro de Informática solamente tienen acceso a los servidores los Administradores de la Red, el Jefe del NODO y el especialista de Seguridad Informática de la Universidad. En caso que un trabajador de otra área necesite por motivos justificados el uso de una de las tecnologías para el desempeño de su labor, el jefe del área le solicita a la otra área su autorización para utilizarla.

Los laboratorios docentes ubicados en las diferentes facultades y el CDIP, podrá ser utilizado por el personal de la Universidad, registrado en registro de control de acceso de cada laboratorio **(Registro 2).**

En el caso de personal ajeno a la universidad, para utilizar alguna tecnología informática el Jefe de esa área es quien lo autoriza, además de estar siempre en compañía de una de las personas responsabilizadas con dichos equipos, ya sea el técnico de laboratorio, persona responsable del equipo o el propio jefe administrativo del área y se anotará en el Registro Control de Acceso a las tecnologías **(Registro 2).**

Todos los trabajadores de la universidad con servicios en la intranet deben firmar el **ACTA DE COMPROMISO** que constituye el **ANEXO 5** y el código de **Normas Éticas** generales para el uso y explotación de **Internet** y el correo que se relacionan en el **ANEXO 4.**

No se permitirá que personal ajeno a la entidad haga uso de los servicios de Internet.

El horario de conexión a Internet será las 24 horas y tendrá en cuenta que la persona designada esté entrenada en el uso de las mismas y conoce las medidas que establece este plan para garantizar la seguridad de la información que en ella se procesa.

Además, podrán hacer uso de las tecnologías informáticas de las diversas áreas autorizadamente y siempre en compañía de una de las personas responsabilizadas con dichos equipos:

- El especialista de Seguridad Informática de la universidad para verificar el cumplimiento de las medidas de seguridad informática.
- Activista de Seguridad Informática del área correspondiente.
- Miembros del equipo que realiza las auditorías, en cumplimiento de esta tarea.
- Administradores de la red y los técnicos del taller para mantenimiento y reparación del equipamiento.

La permanencia fuera del horario laboral sólo se permite con la autorización del Jefe o director del área correspondiente, quien envía una carta y dos copias, con el/los nombres de los cos. que se autorizan entregándose una al Oficial de Guardia y la otra al CVP.

La llave del NODO se encuentra bajo la custodia del director del mismo o de la persona que se designe en un sobre sellado en el puesto de mando de la universidad.

Fuera del horario laboral no está permitida la permanencia de ningún compañero en el nodo, salvo previa autorización del director emitiendo un documento escrito que lo acredite y autorice su estancia en el lugar.

Al culminar la jornada laboral siempre será activada la alarma contra intrusos ubicada en el nodo.

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

El encargado de abrir y cerrar cada local con tecnologías informáticas es la persona responsable del mismo.

Específicamente, en etapas de vacaciones los locales se cierran con llave y con un sello en cada una de las puertas.

5.2.1.2.- A las Tecnologías Información.

Se implementa el Registro de control de soportes (**Registro 3),** en las áreas y del Nodo de Comunicación donde se llevará la relación de los soportes de la Base de Software correspondiente a cada una, en correspondencia a los que se utilizan. Asimismo, el activista de Seguridad Informática de cada área llevará este registro para los soportes destinados a la salva de la información de su área. Cada soporte deberá tener en su etiqueta el área a que corresponde y el número de identificación correspondiente según dicho Registro. De igual manera las salvas que realicen las áreas en los servidores del nodo de plasmará de la misma manera los datos correspondientes en el registro y en el soporte se plantea ubicado en los servidores del nodo.

Todo soporte con información que entre o salga del local, se identificará en su etiqueta el contenido de la misma. A los soportes magnéticos que contengan las salvas se les pondrá en un lugar bien visible una etiqueta que identifique la unidad, la fecha y el nombre de la salva, el nivel de clasificación, la periodicidad y el ciclo de retención.

Conservación.

Los soportes que se consignan en los Registros de Control de Soportes magnéticos (**Registro 3**) se conservarán en las áreas correspondientes, en estantes o gavetas con llaves que reúnan las condiciones en cuanto a temperatura, humedad relativa y resistencia al fuego.

Las copias de las salvas (no menos de dos ejemplares) se tendrán en el local destinado para la conservación y custodia del material informático en el Centro de Informática, detallándose nombre de la salva, ciclo de retención No. De soporte y lugar de conservación, además se registrará en el registro de salvas (**Registro 4**). Los activistas de Seguridad Informática de cada área llevarán estos Registro y además serán los encargados de controlar el préstamo y chequeo mediante el Registro de entrega/recepción de soportes magnéticos (**Registro 3**).

Cada técnico o especialista mantendrá bajo su custodia los soportes de interés particular para su trabajo siempre observando las normas para la correcta conservación y manipulación de estos soportes.

- **Destrucción.**

Las personas responsabilizadas con el manejo de la información clasificada o sensible, una vez que dicha información cumpla con su finalidad, debe eliminar ésta mediante el borrado físico del soporte. Para el sistema operativo Windows XP se puede utilizar el software File OK (desarrollado por Segurmática). Esta información tendrá que hacerse en una máquina no conectada a la red y una vez concluido el trabajo.

Al concluir la vida útil de un soporte, se trata de borrar la información que contiene y se le da de baja del Registro de control de soportes magnéticos (**Registro 3**).

- **Traslado.**

Para el traslado de información proveniente de otra entidad o hacia otra entidad, se anotará en el Registro De Entrada/Recepción de Soportes Magnéticos (**Registro 3**).

Para el traslado de soportes se tendrá en cuenta que:

- El Jefe del Área es el único facultado para autorizar el traslado.
- En el campo Observaciones del **Registro 3** se dejará constancia del hecho, realizándose el chequeo establecido (en cuanto a información que contiene, libre de virus, etc.).

El activista de la Seguridad Informática del área deberá realizar el chequeo antivirus a los soportes y anotar el hecho en el Registro de Incidencias de la Seguridad Informática

La persona que realice el traslado se responsabiliza con su custodia y entrega en el lugar indicado.

Durante las inspecciones que realiza el especialista de Seguridad Informática, chequeará entre otros aspectos, el cumplimiento del acceso a las tecnologías informáticas por las personas autorizadas.

En cualquier caso, ante el incumplimiento de las medidas de seguridad previstas, la persona responsable del equipo está sujeta a una sanción que en dependencia de la gravedad de los hechos pudiera llegar hasta retirar el acceso a las

tecnologías de información

La entrada, salida y traslado de las tecnologías de información deberá ser autorizada por el jefe administrativo y se aplicarán los procedimientos contables establecidos. Este movimiento debe ser del conocimiento del especialista o los activistas de Seguridad Informática, quién debe dejar constancia de ello en el Registro de entrada, salida y movimiento de tecnologías de información (**Registro 4**). Se excluyen de esta regulación las laptops, que por sus características la persona responsable de las mismas (según consta en Acta de Responsabilidad Material firmada y archivada en la Dirección) pueden moverse con ellas en atención a las necesidades de trabajo.

- **Sobre el control y uso de las laptops y tablets que forman parte de los recursos informáticos de la universidad**
  Dada la existencia de laptops en la universidad, se establece el procedimiento con el objetivo de regular su uso, el cual se encuentra en el **manual de procedimientos**.
- El personal que se encarga del mantenimiento y la reparación de las tecnologías informáticas tendrá acceso a la microcomputadora que requiera sus servicios, siempre en compañía de una de las personas responsabilizadas con dicha máquina, debiendo llenar y mantener actualizado el Registro de mantenimientos a equipos (**Registro 5**), donde hará constar las tareas realizadas en los mismos.

5.2.1.3.- A los soportes de información.

Se mantienen identificados los soportes que corresponden a discos de software base (Sistema Operativo Windows XP SP, WIN 7, 8, 10·, Office, etc.) y las copias. Para ello existe el Registro de Control de Soportes (**Registro 3**). El jefe administrativo de cada área realizará los trámites correspondientes con la Vicerrectoría Económica para adquirir los CD o DVD necesarios para tener copias del software base y las salvas de la información. Los jefes administrativos de las áreas de común acuerdo con la Vicerrectora de Tecnología autorizarán la realización de las copias del software base por parte del nodo o de Cesofte.

Cada técnico o trabajador mantendrá bajo su custodia los soportes de interés particular para su trabajo. Los Jefes de cada Área serán los responsables del control de los soportes asignados a su área, a través del Registro de Control de Soportes establecido.

La Base de Software estará bajo el cuidado del administrador de la red en el Local de Informática. Las copias de las salvas de las Bases de Datos .de contabilidad las tendrá en jefe del área económica.

5.2.2.1. Protección de Entrada a las Tecnologías de Información.

Todas las estaciones de trabajo existentes en la universidad deberán estar configuradas según las siguientes clases

Clase A:

1. PC de Directivos de primer Nivel (Rectora y asesores).
2. PC de Vicerrectores, Decanos, Jefe del órgano de cuadros, preparación para la defensa, directores de contabilidad, ATM, secretaria general, secretarias de las facultades y asesoría jurídica.
3. PC que procesan información clasificada y limitada en las áreas.
4. PC que trabajan con datos que tributan a la información clasificada y limitada
5. PC de comunicación en tiempo de guerra.

Clase B:

1. PC de los Vicedecanos, directores y jefes de Dpto. de la universidad.
2. PC que contienen información vital que tributan para la toma de decisiones.
3. PC con información de economía.
4. PC con información de Proyectos con Instituciones Internacionales o con investigaciones sociales de gran impacto en la sociedad.

Clase C:

1. PC con información de planes de estudio.
2. PC con información de producciones de recursos para la educación (Software Educativos, Sistemas).
3. PC con información de proyectos de inversiones.
4. PC con información de distribución de recursos.

5. PC con información de facturación.
6. PC con evaluaciones de los docentes, técnicos y cuadros de dirección.

Clase D:

1. PC que trabajan o procesan información relacionada con la gestión contable y financiera.

Clase E:

1. PC para la gestión de comunicaciones de las redes.

Clase F:

1. PC con otras informaciones.
2. Laboratorios docentes (estudiantes y profesores)

En el **manual de procedimiento** se establece la configuración para cada tipo de clase.

5.3.2.2. Identificación y autentificación de usuarios.

Se establece identificación de usuarios en las PCs para tener acceso a los servicios de la red local, así como para establecer la conexión a los servicios de Internet.

Todas las estaciones poseerán contraseñas de acceso a los recursos disponibles en la red. Estas contraseñas de forma general deberán cumplir con los siguientes requisitos:

- Tendrán un período de vigencia con cotas mínimas de 7 días y máximas de 45 días de duración. No obstante, se permitirá cambiarlas fuera de estos términos de tiempo.
- Las contraseñas deben poseer un mínimo de 8 caracteres de longitud, siempre que el sistema lo permita.
- Los 8 caracteres deben ser caracteres alfanuméricos, de ellos al menos 1 debe ser caracteres especiales.
- Las contraseñas no deben ser palabras existentes en el diccionario ni deben guardar relación con la función de la PC y su operador.

La identificación y autenticación de usuarios se realizará mediante el nombre del usuario y su contraseña. Para el caso de los usuarios de la red interna la autenticación se realizará en un servidor Proxy corriendo sobre Linux en su distribución Debian utilizando las facilidades que para ello posee este sistema operativo. Dentro de estas facilidades se tendrá en cuenta la aplicación de una “Política de Cuentas” que incluirá:

- Tiempo de validez mínimo y máximo de una contraseña.
- Longitud mínima de una contraseña.
- Inhabilitación temporal de cuentas cuando el sistema registre 3 intentos fallidos de acceso.

Se tendrán en cuenta, además, en este servidor los siguientes detalles en el perfil de cada usuario:

- Se habilitará la opción “Cambiar contraseña en el próximo inicio de sesión”.
- No se habilitará “El usuario no puede cambiar la contraseña”.
- No se habilitará “La contraseña nunca expira”.

Para las cuentas de correo creadas en el servidor en el software POSPFIE que corre en la distribución Debian, se tendrán en cuenta los siguientes aspectos:

- Ninguna cuenta se creará sin contraseña.
- No tendrán acceso a un shell válido. El usersbin/nologin”. Cada usuario tendrá un grupo independiente. (CRHWOT)
- Cada usuario tiene un grupo independiente.
- El nombre de usuario y la contraseña solamente serán válidos para acceder a todos los servicios de la universidad.

Asimismo, las estaciones de trabajo de la red interna que trabajen sobre Windows XP o Linux solicitarán contraseñas locales de usuario para el acceso a sus recursos.

Solo el administrador que esté a cargo de dicho servicio tiene los privilegios suficientes para cambiar la contraseña de usuario.

Para el caso específico de los administradores de red la contraseña del supervisor deberá ser cambiada periódicamente, en un plazo no mayor de 45 días. Estas contraseñas tendrán como mínimo 8 caracteres de longitud. Estas serán encriptadas

en MD5.

La relación de todas las contraseñas, tanto de un tipo como de otro, permanecerá almacenada en sobre sellado bajo la custodia del Director del Centro Informática y Comunicaciones. Cada vez que una de estas contraseñas sea modificada el registro deberá actualizarse. Si por alguna razón es necesario romper el sello para tener acceso a las contraseñas, esta operación debe quedar registrada y debe realizarla únicamente el Especialista de Seguridad Informática o en su defecto el Director del Centro Informática y Comunicaciones de la universidad.

- **Control de acceso a los activos y recursos.**

Para el caso de las áreas, Dptos. y oficinas que una misma máquina es utilizada por más de un usuario, tendrá una sesión de administrador, que administrará el jefe del área, quien tendrá la responsabilidad y custodia del equipo y una sesión invitado para el acceso del resto del personal a los sistemas instalados de propósito general para realizar las tareas afines a su responsabilidad. En el caso de las áreas, Dptos. y oficinas que la cantidad de personas que acceden a una misma PC no exceden de 5 se habilitará la sesión de administración que será responsabilidad del jefe administrativo y cinco sesiones de trabajo habilitada para cada uno de los usuarios con un identificador diferente y un perfil diferente y con contraseñas seguras.

En el caso de los laboratorios tendrá dos sesiones, una sesión de administrador que administrará el técnico de laboratorio y la sesión estudiante o invitado de trabajo que será libre para el uso de los estudiantes y profesores, en el caso que tengan que utilizar los servicios habilitados en la red, tendrá que autentificarse reconociendo si está autorizado o no para este servicio.

Cada usuario laborará en las tecnologías informáticas que se le designe por su Jefe de Área. En caso que sea necesario compartir recursos de una estación de trabajo, se hará con carácter temporal y estableciendo la contraseña correspondiente. Una vez cumplido el objetivo se restablecerán las condiciones iníciales.

Los sistemas de aplicaciones cuentan con un personal fijo para su operación.

El uso de los servicios de Internet por parte de los usuarios queda registrado en los logs del servidor, y se limita a las PCs que tienen acceso a ese servicio.

Los especialistas y activistas de Seguridad Informática se encargarán de mantener actualizado el Libro de Incidencias, que se detalla en el **Registro 6**, donde se anotarán eventos de especial interés tales como aparición de virus informáticos, roturas, mantenimientos, etc.

Al hacer uso de los servicios y recursos de Internet se tendrá en cuenta lo siguiente:

- Todo el software que sean descargados por cualquier vía deberán ser sometidos a un proceso de cuarentena, siguiendo los pasos que se detallan en el punto “Protección contra programas dañinos”.
- No estará permitido el acceso a los sitios que ofertan cuentas de correo gratuitos tanto dentro como fuera del país.
- No estará permitido el acceso a sitios con información que lacera la imagen de la revolución cubana.
- No estará permitido el acceso a sitios con información que vaya en contra de las normas elementales de conducta social y moral.
- Se tendrá cuidado en habilitar el uso de “cookies” en los navegadores cuando se esté visitando sitios ubicados en la “Zona de Internet”.
- Para los documentos de Office, basta con habilitar como parte de las protecciones estándares la opción de “abrir sin macros”.
- Con el uso de los navegadores que se emplean en la universidad Internet Explorer y Mozilla Firefox, se activará la ficha de Seguridad en la zona media alta de seguridad para evitar entrar en sitios dudosos y no se recordaran contraseñas.

- **Contabilidad de las acciones que realizan los usuarios.**

Para el caso de los usuarios de la red se llevará el registro de eventos del servidor Proxy en el cual quedará registrado:

- Nombre del usuario
- Hora de conexión
- Sitio visitado.
- Tráfico total de entrada y de salida.
- Hora de desconexión.

Para los usuarios que se conectan de forma remota este servicio se dará cuando la universidad tenga las condiciones técnicas y de seguridad creadas para ofrecerlo:

Traza de Auditoría sobre Acciones que Amenazan la Seguridad.

En el Servidor Proxy se habilitarán en el Plan de Auditoría (Audit Policy) en los siguientes eventos:

- Administración de usuarios y grupos (User and group management). Describe cambios de alto nivel a la base de datos de cuentas de usuario, tales como Usuarios creados o cambios en la membresía de los grupos.
- Cambios en el Plan de Seguridad (Security Policy Change). Registra cambios de alto nivel en el Plan de Seguridad, tales como asignación de privilegios.
- Uso de los derechos de usuario (Use of User Rights). Intentos exitosos o no de uso de privilegios. Información sobre cuando algún privilegio especial es asignado.
- Sistema (System). Indica que algo está ocurriendo que afecta la seguridad de todo el sistema o el registro de auditoría.
- Seguimiento de procesos: Suministra información detallada sobre el seguimiento de un proceso.
- Inicio y cierre de sesión: Registra los intentos de inicio y cierre de sesión, tanto exitosa como fallida.
- Accesos a archivos y objetos: Accesos exitosos y fallidos a objetos protegidos

En los servidores con GNU Linux. Distribución Debian se habilitarán los registros de eventos a través del uso de las facilidades del “syslog daemon”. Los elementos que se tendrán en cuenta serán:

- Errores del sistema.
- Problemas con el kernel.
- Alertas de seguridad.
- Violaciones o errores en el servicio de correo.
- Mensajes emergentes.
- Errores con la ejecución de las tareas del “cron”.

El sistema posee, además, una herramienta denominada Squid que por defecto se ejecuta diariamente, semanalmente y mensualmente, generando reportes del sistema que incluyen:

- Anormalidades detectadas en la red.
- Conteo del tiempo total de conexión de los usuarios al sistema.
- Detalles de las modificaciones realizadas a la base de datos de usuarios.
- Detalles de las modificaciones realizadas al fichero de los grupos.
- Listado de ficheros con privilegios “user” con dueño “root”.
- Detección de cuentas sin contraseña o con una contraseña débil.
- Intentos fallidos de conexión al servidor por parte de los usuarios.
- Detalles de mensajes rechazados por el servidor.
- Estado de la carga promedio del sistema.

Durante el uso de Internet, se podrá auditar la actividad específica desarrollada por los usuarios haciendo uso de las posibilidades que en este sentido brindan las aplicaciones **SQUID NT, SARG, MYSARG.** Para el control y uso de del ancho de banda de la red se utilizará la aplicación **mrtg** y para el control de la gestión de corres se utilizará **lsoqlog.**

5.3.2.4.- Integridad de los ficheros y datos.

1. Utilizando las facilidades de GNU Linux Debian se restringirá los permisos a los ficheros y directorios del servidor que por su importancia para el sistema que así lo ameriten. Para ello los administradores de la red deben tomar las siguientes medidas:

- Establecer los permisos adecuados para cada objeto se utilizan los comandos. CHMOT para dar permisos y el CHWOE para cambiar el propietario, que varía los permisos de cada uno.
- Se mantendrá la información actualizada de la configuración, que permita el rápido restablecimiento de la misma y con

la menor afectación posible ante la ocurrencia de hechos que así lo requieran.

- Quien detecte indicios de difusión de mensajes contrarios al interés social, la moral y las buenas costumbres, o la integridad o seguridad del estado, debe comunicarlo de inmediato al especialista de Seguridad Informática de área, quien a su vez lo trasmitirá a su Jefe Inmediato Superior y este lo informará al Director del CICOM para conjuntamente con el Especialista de Seguridad Informática y Jefe de Protección Física, investigarán y tomarán las medidas correspondientes, posteriormente lo informarán a los órganos competentes del Ministerio del Interior.
- En el directorio raíz de la partición de sistema, algunos ficheros del sistema operativo deben ser protegidos por ser críticos para la seguridad de los mismos. (Shadow, Group, passwd, init, rd.bemz y linuxkernel286).

2. En cada estación de trabajo sólo se compartirán aquellos recursos necesarios e imprescindibles para el desarrollo del trabajo de otros. Es absolutamente necesario establecer para el control de acceso a los recursos compartidos o bien una contraseña o especificar los usuarios y grupos que podrán hacer uso de estos recursos.
3. En general se habilitará el uso de refrescadores de pantalla con contraseña, lo que evitará que la información sea vista en momentos de inactividad y la entrada de intrusos, así como la protección del monitor.
4. Se contará con productos antivirus en las diferentes computadoras y se mantendrán los mismos debidamente actualizados. Para ello, se utilizará la vía FTP de la universidad, se utiliza el Segurmática Antivirus Corporativo 7,2 como antivirus internacionales el Nod 32 V4, V5, V6, V7 y V8. Los activistas de seguridad informática de las áreas crearán para cada microcomputadora, el disco respaldo que permita la restauración del sistema al producirse cualquier incidente que la afecte.
5. El activista de Seguridad Informática velará porque se efectúe el chequeo de todos los soportes magnéticos de propiedad personal o de otra entidad que se introduzca en la universidad antes de su utilización.
6. Para el envío de “anexos” a través del correo electrónico es necesario que el remitente exprese al destinatario que le adjunta un fichero y además su nombre y longitud en bytes. La persona que recibe un “anexo” debe exigir que se cumpla con esta condición. La longitud no debe exceder de un 5 MB y este compactado.
7. Se habilitarán las protecciones estándares de Office, que hacen que al tratar de abrir documentos que contienen macros, se alerte al usuario, dándole la posibilidad de abrirlo sin las macros, que es lo recomendado.
8. Se mantendrán los sistemas y aplicaciones actualizadas con las versiones de Service Pack y parches de seguridad para Windows que publiquen sus productores.
9. No se adquirirán copias de software de procedencia desconocida.
10. En caso de detectar un virus desconocido el activista de Seguridad Informática procederá como se describe en el **manual de procedimientos.**
11. Se prohíbe terminantemente el intercambio de códigos de virus entre personas o grupo de personas.
12. Los Administradores de la Red así como los activistas de Seguridad Informática de las áreas realizarán la salva de patrones de las microcomputadoras y del software de la máquina en la que se vaya a someter a cuarentena algún software. Esto deberá realizarse inmediatamente antes del comienzo de las pruebas de la cuarentena.

Los CD y/o DVD con las salvas de patrones se guardarán protegidos en el lugar destinado para la guarda de soportes en el área, hasta que termine la cuarentena del software bajo prueba.
En el caso del software, los patrones son tamaño, fecha y hora de creación.

- **Corta fuego para conexión segura a Internet**

El IPTABLE es el cortafuego usado desde los servidores que corre sobre la distribución Debian de GNU Linux.

Protección Contra Programas Malignos.

- Se contará con los productos antivirus certificados en las diferentes áreas de la universidad y se mantendrán los mismos actualizados. El Especialista de Seguridad Informática cuando reciba una nueva versión de **Segurmática,** debe informar a los Especialistas de Seguridad Informática de cada área, de la disponibilidad **de** este producto para que sea instalado en cada una de las máquinas en su área.
- En el caso de **Internet** deben utilizarse adicionalmente los antivirus internacionales Karspesky o Nod 32.
- Los Administradores de la Red así como los Especialistas de Seguridad Informática de las áreas realizarán la salva de patrones de las microcomputadoras y del software de la máquina en la que se vaya a someter a cuarentena algún

software. Esto deberá realizarse inmediatamente antes del comienzo de las pruebas de la cuarentena.

- Las salvas de patrones se guardarán protegidos en el lugar destinado para la guarda de soportes en el área, hasta que termine la cuarentena del software bajo prueba.
- En el caso del software, los patrones son tamaño, fecha y hora de creación.
- Los activistas de Seguridad Informática de cada área velarán porque se efectúe el chequeo de todos los soportes magnéticos de propiedad personal o de otra entidad que se autoricen introducir en el UCPEJV, antes de su utilización.
- Los activistas de Seguridad Informática de cada área se encargarán de someter a un "proceso de cuarentena" al software, sistemas y programas de aplicaciones adquiridos a través de **Internet** o a través de terceros**,** según se detalla en el **Manual de Procedimientos,** que se anexa en su epígrafe **Protección contra programas dañinos.** Este proceso se realizará en una microcomputadora no comprometida con el sistema de información de la entidad de la que se deben conocer todos sus patrones.
- El intercambio de sistemas y programas de aplicaciones, así como documentos de Word se realizará de la siguiente manera: Previamente al envío de información, se utilizará un programa identificador/descontaminador de virus para revisar los ficheros y posteriormente a la recepción, de tratarse de software o aplicaciones, se someterán al proceso de cuarentena establecido. De pasar con éxito la cuarentena, si van a ser usados al menos en una de las microcomputadoras del Institución, se incluirán en el Registro de software autorizado.
- En caso de detectar un virus desconocido los Especialistas de Seguridad Informática de las áreas procederán a aislarlo como se describe en el Manual de Procedimientos **(Protección contra programas dañinos)**. Si posteriormente resulta imposible la descontaminación manual se contactará al personal de **Segurmática.** De hecho, debe reportarlo obligatoriamente a Segurmática (tel. **870-0619, 878-1987**) y a la Dirección de Protección del MININT (tel. **857-7376, 857-7377**).
- Se prohíbe terminantemente el intercambio de códigos de virus entre personas o grupo de personas.

➢ **Control de acceso.**

En los servidores se mantendrán actualizadas las cuentas de usuario, eliminando aquellos usuarios que causen baja de este servicio y dándoles cuentas nuevas a nuevos usuarios.

Es necesario establecer el control al acceso a los recursos compartidos o bien una contraseña o especificar los usuarios y grupos que podrán hacer uso de estos recursos.

El control de acceso se realizará mediante la definición de 3 Niveles de acceso elementales para los usuarios:

- Mensajería Nacional

Podrá enviar y recibir mensajería electrónica desde y hacia cualquier Dirección de correo en el territorio nacional con posibilidad para la navegación dentro de los sitios cubanos.

- Mensajería Internacional

Podrá enviar y recibir mensajería electrónica hacia y desde cualquier otra dirección de correo en el mundo, siempre y cuando esta dirección no esté filtrada, con posibilidad para la navegación dentro de los sitios cubanos.

- Acceso a Internet.

Podrá tener acceso a todos los sitios y recursos de Internet, siempre y cuando estos no estén filtrados, teniendo en cuenta lo estipulado en los documentos.

5.3.2.5 Auditoria y alarmas.

En el proxy también se habilitarán los mecanismos de auditoría que permitan controlar la actividad desarrollada por los usuarios autorizados a utilizar Internet.

Todos estos chequeos los realizará el administrador de la red designada y el especialista de Seguridad Informática semanalmente.

5.3.3 MEDIDAS DE SEGURIDAD DE OPERACIONES

Para la selección de los mecanismos de seguridad se han tenido en cuenta las plataformas que utiliza la universidad para su trabajo.

Basado en ello se analizaron las posibilidades de cada una de ellas en materia de seguridad.

Criterios para la Selección de Mecanismos de Seguridad

Para la selección de los mecanismos de seguridad se han tenido en cuenta la política de seguridad informática definida, así como las plataformas que utiliza el Ministerio de Educación.
Se realizó un proceso de análisis para determinar las posibilidades de cada una de ellas en materia de seguridad. Determinando realmente que los servidores de la universidad para los diferentes servicios se instalaran en GNU Linux Debian Lenny 5.0, Squeezy 6.0 y Wheezy 7.0.
Los servidores se encuentran virtualizados en su gran mayoría, no están virtualizados Proxy IPLAC, los Servidores de Correo de la UCPEJV y el de las Direcciones Municipales de Educación.
En el caso de las estaciones de trabajo (Windows XP SP3 y Windows 7 u 8) se ha contemplado el control de acceso físico a los locales que las contienen y el acceso lógico con la autenticación de aquellos usuarios que trabajan localmente en esas máquinas y la compartición de recursos en función de usuarios para aquellos autorizados a trabajar con esta información desde la red.
Asimismo para la conexión a Internet se implementó un servidor Proxy SQUID, que garantiza en uno de los casos el acceso a los servicios de Internet al grupo de usuarios autorizados de la universidad.

Autorización y denegación de servicios a los usuarios.

FTP, WWW y correo electrónico.

Los docentres y estudiantes tendrán acceso a estos servicios según se establece en la **RR-#20 y la instrucción 1 del MES de 2016**

Para el uso de estos servicios existe un Código de Ética que deben cumplir los usuarios autorizados.
Aunque es posible acceder a un sitio de correo libre durante el uso del servicio WWW, los usuarios se abstendrán de hacerlo respetando la política establecida en la entidad para el uso de ese servicio, salvo que estén autorizados para ello.
Si se detectaran violaciones, la dirección institucional tiene facultades para denegar al usuario implicado al uso de los servicios, lo que indicaría al administrador de la red, quien se encargaría de indicar las medidas técnicas para garantizarlo.

5.3.3.1. Sistemas de Salva de respaldo

Se establece con carácter obligatorio las salvas o copias de seguridad de la información con la periodicidad y ciclo de retención que se indican a continuación, según las necesidades particulares de actualización de la misma. Estas salvas estarán siempre debidamente actualizadas.

La información a salvar de importancia en los servidores sería:

- Sistema Operativo
- Registro de configuraciones del Sistema
- mylogs, syslog, acceslog (Ficheros asignados a cada cuenta de usuario que se ejecutan cada vez que el usuario se conecta al sistema).
- Programas y Aplicaciones contenidos en el servidor
- Información del sistema
- Información del trabajo (Bases de datos, ficheros, sitios, cursos a distancia, etc.)

Centro de Informática y comunicaciones

- Software base (Sistema Operativo de las estaciones de trabajo, Microsoft Office)
- Programas y Aplicaciones correspondientes a las áreas
- Información de trabajo (Bases de datos, ficheros, etc.)

Área de Trabajo

- Software base (Sistema Operativo de las estaciones de trabajo, Microsoft Office)
- Información de trabajo (Bases de datos, ficheros, etc.)

Responsables del Proceso de salva de la información

- Los jefes de áreas o Directores son los responsables de organizar la salva de la información del área respectiva, definiendo la información a salvar y al especialista encargado de esto.
- Los jefes administrativos y el especialista de Seguridad Informática de las áreas garantizarán que la salva de las áreas quede debidamente resguardada.
- En el caso de la información sensible la salva debe ser hecha solo por el personal autorizado para el procesamiento de este tipo de información.
- La salva de la información procedente de Internet será responsabilidad del personal autorizado a utilizar estos servicios.

- El personal responsabilizado de hacer las salvas hará las anotaciones correspondientes en el **Registro 7** Salva de la Información existente en cada área se reportarán en las Observaciones el éxito o falla de la salva.
- En caso de fallar el proceso de salva, ya sea por problemas de software o de hardware, el responsable de esta tarea debe comunicarlo directamente al Jefe de área quien determinará los pasos a seguir con vistas a restaurar lo más rápidamente posible el proceso de salva.

Periodicidad del proceso de salva.

Se establece con carácter obligatorio las salvas o copias de seguridad de la información en el soporte adecuado y con la periodicidad y ciclo de retención que se indican en el manual de procedimientos, según las necesidades particulares de actualización de la misma para lo cual se habilitará un **Registro 7 Salvas de la Información**. Estas salvas estarán siempre debidamente actualizadas, por el personal designado por cada área.

Se habilitará en el nodo este servicio para las diferentes áreas...

La periodicidad de las salvas será función del ritmo de modificación de los ficheros, de tal manera que, en caso de no disponer de estos, los ficheros salvados permitan reanudar los tratamientos sin pérdida de información.

Para el calendario de salvado se establecerán 4 niveles:

- Copias del Sistema Operativo y Utilidades; con periodicidad baja, se tendrán las salvas (imagen o discos originales) debido a los cambios de versiones.
- Programas y Aplicaciones; con una periodicidad mayor, se salvarán cada vez que exista un cambio en los mismos.
- Los Datos: se hará la salva discrecionalmente de la información correspondiente a los Sistemas al finalizar la sesión de trabajo, así como de los datos correspondientes al resto de las aplicaciones donde se incluyan las modificaciones y/o actualizaciones de la información correspondiente a ese día., Se realizan en CD, DVD, HDD externo, memorias flash que posean los jefes de área y usuarios.
- Salva diaria discrecional de la información de Internet que así lo amerite, al finalizar la sesión de trabajo, si algún usuario autorizado lo cree necesario.
- En el caso de sistemas y programas de aplicación obtenidos de Internet, tendrán que ser sometidos antes de la salva definitiva a un proceso de cuarentena detallado en el punto de Protección contra programas dañinos del Manual de Procedimientos.

Proceso de salvas

- El Administrador de la Red creará y mantendrá actualizado el Disco para Reparación de Emergencia de los Servidores lo que se logra ejecutando la utilidad SFDISK u otras herramientas para estos fines.
- Cuando se hagan cambios en el Sistema Operativo o se instale en el caso del servidor se deben tener en cuenta los cambios que esto puede provocar en el proceso de copia y restauración.
- Cuando se hagan cambios en la computadora como instalar un nuevo controlador o unidad de backup o cambios del BIOS de la Motherboard se deben tener en cuenta los cambios que esto puede provocar en la copia o restauración de la información.
- Al hacer cambios de software o hardware relacionado con la copia debe tenerse en cuenta quizás las viejas salvas no podrán ser usadas.

Almacenamiento y conservación de los soportes destinados al proceso de salva.

- En las áreas del centro de Informática del Nodo de Comunicaciones y Cesofte se tendrán la salva de la base de software (Sistemas Operativos, Aplicaciones, etc.) correspondiente a cada una.
- Los soportes donde se hagan las salvas diarias de los datos correspondientes a las estaciones de trabajo se guardarán en lugares destinados para estos fines en cada área.
- La información clasificada o sensible será almacenadas y guardadas en estantes a la información diaria y tendrán cierre con llave además de un sello.
- Los estantes destinados para el almacenamiento de las salvas tendrán cierres seguros, estarán ubicados en locales con la debida climatización y poseerán las condiciones adecuadas en cuanto a temperatura, humedad, resistencia al fuego etc.
- Los soportes magnéticos que contengan las salvas estarán protegidos físicamente contra escritura.

- El traslado de los soportes se realizará respetando las normas de conservación de los mismos (no exponerlos a altas temperaturas ni a campos magnéticos, no tocarlos por las partes descubiertas) con el objetivo de garantizar la integridad de la información que contienen.

Tiempo de conservación de las salvas

- El tiempo de permanencia de la información guardada será determinado por cada Jefe de área. las salvas de los logs de los servidores del nodo serán guardadas por un año.

5.2.3.2. Mantenimiento y reparación de las tecnologías de información.

El mantenimiento (que se efectúa trimestralmente) y la reparación del equipamiento informático serán realizados por los propios técnicos de la Empresa EMPROMAVE que pertenece al MINED en presencia y bajo la supervisión del especialista responsable. Se designará por el área de Servicios Técnicos el especialista encargado de esta actividad y se hará constar cada reparación o mantenimiento en el **Registro de Incidencias a la Seguridad Informática (Registro 6).**
En caso que sea necesario el traslado fuera del Institución, se hará el movimiento establecido para ello con la autorización del Jefe del área.

5.3.3.3. Control del uso, traslado y entrada de tecnologías de información.

Los soportes magnéticos que contienen información, sistemas y/o programas de aplicación de las tecnologías informáticas de cada área solo pueden introducirse y/o extraerse con la anuencia del Jefe de Área. **(Registro 4)** habilitado al respecto.

En cada soporte magnético se señalizará en forma clara y visible su No. De registro y su contenido fundamental.

Para utilizar soportes de propiedad personal o de otra entidad será necesario contar con la autorización de responsable que tiene asignado el equipo, debiendo ser revisados contra virus informáticos u otros programas dañinos.

Al solicitarse y entregarse los soportes magnéticos a los trabajadores se asentarán en el "Registro de Entrega/Recepción" **(Registro 3)**. Al ser devueltos los soportes magnéticos se revisarán contra virus informáticos y después se hará constar la devolución en el Registro.

El traslado de los soportes magnéticos se realizará respetando las normas de conservación de los mismos, con el objetivo de garantizar la integridad y confidencialidad de la información que contienen y cumplirán las medidas de protección establecidas.

Cualquier movimiento, traslado de las tecnologías informáticas fuera del local para una reparación o por cualquier eventualidad, debidamente autorizada se anotara en el **registro de Incidencias**. Aclarando en observaciones motivos y hacia donde va, así como todos los datos de la persona que traslade el equipo y quede bajo su custodia, por parte de contabilidad se hará el movimiento de tarjeta de medio básico.

5.2.3.4. Pruebas de Inspección.

El especialista de Seguridad Informática de la universidad conjuntamente como los de las áreas quedan responsabilizados con la aplicación de todas las medidas de seguridad informática establecidas, exigiendo a los Administradores de Red, técnicos encargados del mantenimiento y demás personal involucrado, que también lo haga.
A los 30 días de la entrada en vigor del Plan de Seguridad Informática y después de los chequeos previstos en el párrafo anterior, se realizará la primera auditoría interna para evaluar la situación que presenta la implantación del mismo. Posteriormente con una periodicidad no mayor de 6 meses deberán continuar realizándose estas auditorías internas.

Para asegurar de que funcionen correctamente instauran un sistema de pruebas, que realizan al unísono y encaminadas en dos direcciones, como se detalla en el Manual de Procedimientos, epígrafe **Inspecciones.**

Las inspecciones se realizarán en cada área de la universidad por parte de los Especialistas de Seguridad Informática. Cada vez que realizan una inspección anotarán los resultados en el respectivo **Registro de Inspecciones (Registro 8).**
Las inspecciones se realizarán a nivel de área y de toda la universidad.
Las inspecciones las realizará el especialista de Seguridad Informática de conjunto con el grupo de activistas de las diferentes áreas y estarán encaminadas en dos direcciones:

Primero:

Chequeará las tareas funcionales que debe efectuar cada cual de acuerdo a su responsabilidad.

- Intercambio con directivos, profesores, estudiantes y demás personas que utilizan las tecnologías informáticas para comprobar que dominan y cuáles son sus tareas en el sistema de seguridad informática.
- Igualmente hablará con los autorizados a navegar por INTERNET para conocer si saben qué deben hacer, cuáles son las sanciones a las que están sujetos, etc.
- Contactará a los usuarios del correo electrónico para verificar que cumplen con las medidas de protección contra programas dañinos, y aplican las medidas de seguridad y procedimientos definidos en este plan.

Previamente realizará un estudio del uso de los servicios por el personal del área visitada (correos, navegación) y realizará escaneo de red a las PC del área que será visitada.

Segundo:

- Realizará inspecciones independientes a cada una de las máquinas, efectuando pruebas en las que trate de violentar las medidas de seguridad.
- La frecuencia de las pruebas en ambas direcciones dependerá del dominio de cada implicado de sus responsabilidades, en el primer caso, y de la detección o no de huecos en la seguridad, en el segundo.
- El especialista de Seguridad Informática, cada vez que realiza una inspección anotará los resultados en el Registro **de Inspecciones (Registro 8).**
- Aquellos hechos que comprometan la seguridad informática serán anotados por el Responsable de Seguridad Informática en el Registro de incidencias.

5.2.3.5.- Auditoria

Se realizarán auditorias periódicas para controlar el cumplimiento de las medidas de seguridad informática en relación con las tecnologías informáticas objeto de este Plan de Seguridad, por una comisión integrada por las siguientes personas:

1. Especialista de Seguridad Informática
2. Activista de Seguridad Informática de áreas seleccionada
3. Uno de los Administradores de la Red
4. Jefe de Protección Física

Durante la realización de las auditorías el equipo designado hará uso de las trazas que se conservan por sistema operativo de las acciones desarrolladas por los usuarios (incluyendo su actividad en internet), además de los registros disponibles, los resultados de las inspecciones realizadas por el especialista de Seguridad Informática y cualquier otro material que considere necesario para poder desempeñar su tarea.
Las auditorías se realizarán de forma sorpresiva y se comprobará fundamentalmente lo siguiente:

a. Que esté implantado el sistema de nivel de acceso a los locales.
b. La organización y configuración de las PC de uso compartidos y en correspondencia con las clases definidas.
c. Que los equipos estén correctamente instalados según las normas correspondientes y que los locales cuenten con las condiciones requeridas tanto técnicas (climatización y/o ventilación, instalación eléctrica, líneas de comunicaciones, etc.) como de protección física (cierres seguros).
d. Que estén implantados los mecanismos de identificación y autenticación de usuarios y de control de acceso y que éstos cumplan los requisitos establecidos.
e. Que exista la relación de softwares autorizados, que se mantenga actualizado, y por tanto coincida realmente con el software existente en las microcomputadoras.
f. Que los equipos se utilicen en las funciones para las que fueron asignados.
g. Que el equipo esté protegido con productos antivirus y que éstos estén actualizados, que se cumplan las normas en cuanto a protección contra escritura en los disquetes que contienen sistemas, programas e información que no requiere

actualización periódica, así como que se cumpla con el proceso de cuarentena para el software nuevo y las demás regulaciones de protección contra virus informáticos.

h. Que se tenga la información necesaria para la restauración del sistema informático.
i. Que todos los soportes magnéticos estén debidamente registrados y que no estén utilizándose soportes ajenos a la entidad. Se comprobará también que todos estén debidamente identificados.
j. Que se realicen y posean debidamente registradas las salvas o copias de seguridad, según las periodicidades establecidas y en el soporte más adecuado, de la información necesaria para la buena marcha de los trabajos de la entidad.
k. Que se utilice INTERNET con los fines para los que se ha concebido, que efectivamente sólo las personas autorizadas hagan uso de las tecnologías con acceso a INTERNET y que se cumplan todas las medidas establecidas en este sentido.
l. Que se cumpla con el procedimiento para el uso de las laptops, incluyendo el Acta de responsabilidad para los usuarios que la poseen.
m. La fortaleza de las contraseñas de los usuarios.

Como resultado de las auditorías se elaborará un "Informe de Auditoría" donde se detallarán las violaciones detectadas y se calificará el resultado de las mismas (Excelente, Satisfactorio y No Satisfactorio) así como se propondrá un Plan de Acciones para solucionar las dificultades encontradas con los responsables y tiempo máximo para ello.

FORMATO DEL INFORME DE AUDITORIA.

No.	EQUIPO	MEDIDA DE SEGURIDAD	VIOLACION DETECTADA

FORMATO DEL PLAN DE ACCIONES.

No.	EQUIPO	ACCION A DESARROLLAR	PLAZO	RESPONSABLE

El activista y el especialista de Seguridad Informática, en coordinación con el jefe Administrativo responderán por la ejecución integral de dicho Plan.

Las auditorías internas se harán semestralmente durante el primer año de implantación del Plan de Seguridad. Se coordinará asimismo por parte del especialista de Seguridad Informática, con el MINED para en este período realizar una auditoría externa.

Después las auditorías internas serán anuales.

5.2.4.- De recuperación ante contingencias.

Estas tienen en cuenta las amenazas y vulnerabilidades a las que están expuestas las tecnologías informáticas en la entidad. Aunque se concentra en aquellos riesgos que tienen solución en el propio centro.

De materializarse un riesgo cuya recuperación implique la necesidad del traslado a otra entidad para continuar utilizando las tecnologías informáticas en el resto de los procesos, han decidido prescindir de éstas.

La Universidad y en particular la Dirección de Informatización cuenta con un plan de recuperación ante contingencias y catástrofes, que se asume ante hechos de tales magnitudes, este plan de recuperación debe mantenerse actualizado, siendo la Vicerrectoría de Tecnología, la Vicerrectoría de Economía y Servicios, el Director de Nodo y el especialista de Seguridad Informática, los encargados de que así sea.

Se cuenta con un plan de aviso en el área que es el siguiente:

5.2.4.1.- Determinación de Vulnerabilidades.

En el análisis de riesgo de la UCP Enrique José Varona realizado anteriormente están expuestos los activos críticos más importantes de la universidad, donde también se ven afectadas las tecnologías, así como las acciones a realizar, los recursos a utilizar y el personal a emplear en caso de que se degrades o inutilicen los recursos y servicios informáticos del centro.

En caso de que la contingencia inhabilite totalmente el sistema informático de la universidad se prescindirá de los servicios de mensajería e internet hasta tanto no se normalicen las condiciones de trabajo.

Tomado en consideración el análisis de riesgo realizado en el pto. 3 de este plan se prevé que los hechos que causarían la puesta en marcha de este plan de recuperación ante contingencia son:
No desarrollamos las acciones a tomar ante incendios porque las respuestas a este hecho deben encontrarse en otro plan de la entidad.

1. Acceso no autorizado
2. Modificación o divulgación de información no autorizada
3. Contaminación por programas malignos
4. Fuga de información
5. Fallo de software
6. Fallo de hardware
7. Fallo de energía eléctrica
8. Error de operación
9. Robo o hurto parcial o total de TI
10. Deterioro físico y obsolescencia técnica
11. Falla de comunicación
12. Modificación de los controles de seguridad
13. Tormentas eléctricas severas

A continuación, detallamos algunas de las acciones a tomar en cada caso:

1 Hecho: Acceso no autorizado.

Acción por etapas	Persona que detecta	Activista o especialista de Seguridad Informática y administrador de la Red
Información	Informa al activista de Seguridad Informática del área	
Neutralización	El activista de Seguridad Informática informa al jefe del área	El especialista de seguridad informática de la universidad y el administrador de red desconectan la PC de la Red y determinan la cuenta burlada y la bloquea desde el servidor Se analiza con el jefe del área y el usuario correspondiente los hechos. Se informa al MINED y la OSRI Se anota en el libro de incidencia del área donde ocurre el hecho. Se crea una comisión para investigar los hechos
Recuperación		Al analizar los hechos se analiza se mantiene la cuenta y servicios y se cambia nombre de usuario y la contraseña.

Nota: El Responsable es **e**l especialista de la universidad y el activista de Seguridad Informática del área realiza las anotaciones en el Registro de Incidencias

2 Hecho: Modificación o divulgación de información no autorizada.

Acción por etapas	Persona que detecta	Activista o especialista de Seguridad Informática, jefe del área y administrador de red
Información	Informa al activista de Seguridad Informática del área, de la Universidad y al jefe del área El especialista de SI de la Universidad informa a la VRTE y la Rectoría.	
Neutralización	El especialista de SI informa al MINED y la OSRI	Si levantada la evidencia. Se procede a borrar la información y o corregirla cuando sea posible Se informa al MINED y la OSRI Se anota en el libro de incidencia del área donde ocurre el hecho.

		Se crea una comisión para investigar los hechos y las personas involucradas en el hecho y tomar las medidas disciplinarias correspondientes.
Recuperación		Se procede a borrar la información y o corregirla cuando sea posible.

Nota: El jefe del área, el especialista o activista de Seguridad Informática realiza las acciones correspondientes y son anotadas en el Registro de Incidencias

3 Hecho: Contaminación con programas malignos.

Acción por etapas	Persona que detecta	Activista o especialista de Seguridad Informática y administrador del nodo
Información	Informa al activista de Seguridad Informática del área y al Informa al Jefe de Área del hecho	
Neutralización	Se analiza la PC para detectar la contaminación y posible procedencia Apaga la máquina y alerta que no se use la misma.	Se desconecta la PC de la Red y todas las que tengan problemas. Si estaba levantada la Protección Permanente en el Antivirus y este no detectó el virus, revisar su actualización. Si el antivirus instalado no neutraliza, probar con otro de los autorizados. De no tener solución se aísla (según procedimiento) e informa a Segurmatica (878-2665 ó 870-3536) y al MINED y la OSRI.
Recuperación		-Procede a descontaminar -Revisa disquetes o flash, si existe posibilidad de que estén infectados. -Informa de ser exitosa la descontaminación que se puede usar la máquina. -Informa al Jefe de Área de la solución -Investiga causas de aparición del virus y responsables -Realiza las anotaciones en el Libro de Incidencias.

Nota: El especialista o activista de Seguridad Informática realiza las anotaciones en el Registro de Incidencias.

4 HECHO: FUGA DE INFORMACIÓN

Acción por etapas	Persona que detecta	Especialista de Seguridad Informática	Director del Nodo de la Red	Dirección de Informatización
Información	Informa al Jefe de Área correspondiente y al activista de Seg. Informática.	Informa al Administrador de la Red y jefe del nodo		
Neutralización		Analizan de conjunto el problema, determinando: cómo conservar la evidencia o prueba, analizar posibles consecuencias de tal hecho e implicados.		
Recuperación		Estudian posible fisura de seguridad que posibilitó el hecho y cómo solucionarla. La Vicerrectoría analiza propuestas de sanciones a los implicados. El especialista de Seguridad Informática realiza anotaciones en el Libro de Incidencias		

5 Hecho: Falla de Software.

Acción por etapas	Persona que detecta	Administrador de la red ó especialista designado	Suministrador del Software
Información	Informa al Administrador de la Red y al Jefe de Área		
Neutralización	Apaga la máquina y alerta que no se use la misma	Administrador o especialista designado investigan lo ocurrido. Si el software es adquirido o comprado, avisa al suministrador.	Acude y revisa el software que falló.
Recuperación		Administrador ó Especialista designado restaura utilizando los softwares originales o copias de los mismos. Informa al Jefe de Área lo sucedido y al usuario que la máquina esta lista para continuar sus labores.	Efectúa los arreglos necesarios o reinstala software y prueba su funcionamiento. Avisa que ya el software puede usarse de nuevo.

6 Hecho: Falla de Hardware.

Acción por etapas	Persona que detecta	Administrador del área y especialista designado para atender el fallo	Técnico del taller de Empromave
Información	Informa al Administrador de la Red y al Jefe de Área y al administrador del área		
Neutralización		Revisa el equipamiento afectado y trata de solucionar el problema. De no ser posible coordina con el administrador del área para enviar el equipo al Taller.	Si es factible realiza la reparación, si no, dictamen técnico e informa a afectados.
Recuperación		-De no poderse solucionar de inmediato, en coordinación con el Jefe de Área, disponen de ser urgente continuar el uso de las tecnologías informáticas, el traslado a lugar de hardware de similares características (previa instalación del software necesario).	

		-De reportarse la imposibilidad de solucionar el problema, de conjunto con el técnico del taller harán las propuestas de una posible para solucionar al problema.	

7 Hecho: Fallo de de energía eléctrica

Acción por etapas	Persona que detecta	Activista de Seguridad Informática	Administrador de la red y jefe del Nodo y personal jefes del área	Administrador de red
Información	Informa al activista. de Seguridad Informática y al Jefe de Área	Informa al administrador de la red.	Investiga si se trata de una falla interna o si es un apagón en la zona, así como el tiempo de duración.	
Neutralización	Salva la información.	Contacta al técnico que se encarga de las reparaciones eléctricas	Garantizan la salva de la información contenida en los servidores y las PC. Desconecta los equipos. .	Soluciona problema u ofrece diagnóstico y posible solución
Recuperación	Reanuda el trabajo	Realiza anotaciones en el Registro de Incidencias	Restablecen las comunicaciones externas e internas y levanta los Servidores.	

8 Hecho: Errores de operación.

Acción por etapas	Persona que detecta	Administrador de la red ó activista de seguridad informática del área	Especialista o personal Afectado	Jefe del Área
Información	Informa al administrador de la red o al Jefe de Área	Administrador atiende el fallo ó si se trata de una aplicación específica, el Jefe de área designa especialista que deberá atender el fallo		
Neutralización		Analizan qué se debe hacer para eliminar el problema. Existen dos posibilidades: 1ro. Corrigen el error. 2do. Orientan al afectado los pasos a seguir para solucionar el problema.	Acata o aplica las medidas orientadas	Controla el cumplimiento de las medidas.
Recuperación		Si el error se ocasionó por desconocimiento se procede a la capacitación del involucrado. En caso contrario notifica al Jefe del Área.	Reanuda el trabajo	Analiza posibilidad de sanción.

Nota: El especialista o activista de Seguridad Informática realiza las anotaciones en el Registro de Incidencias.

9 HECHO: ROBO O HURTO PARCIAL O TOTAL DE TI

Acción por etapas	Persona que detecta	Especialista de Seguridad Informática	Jefe del área	Dirección de Informatización
Información	Informa al Jefe de Área correspondiente y al activista de Seg. Informática y a grupo de Seg y Protección.	Informa al Administrador de la Red y jefe del nodo y a la VRTE y al jefe de Seg y Protección.	Preserva el área	De conjunto con el jefe de protección física informa a las autoridades policiales de ser necesario

Neutralización		Analizan de conjunto el problema, determinando: cómo conservar la evidencia o prueba, analizar posibles fallas de seguridad y consecuencias de tal hecho e implicados.
Recuperación		Estudian posible fisura de seguridad que posibilitó el hecho y cómo solucionarla. La Vicerrectoría analiza propuestas de sanciones a los implicados. El especialista de Seguridad Informática realiza anotaciones en el Libro de Incidencias De lograrse la recuperación del equipo, tras la revisión se procede a restablecer las condiciones iníciales, de no ser posible evaluar la posibilidad de su sustitución o adquisición de otro.

10 HECHO: DETERIORO físico y obsolescencia técnica

Acción por etapas	Persona que detecta	Especialista de Seguridad Informática	Administrador y jefe del área y Taller de servicios técnicos y VRES	Dirección de Informatización Y VRES
Información	Informa al Jefe de Área, al activista de Seg. Informática y al administrador del área	Informa al Administrador del área a la VRTE y VRES.	Preserva el equipo. Taller realiza dictamen técnico	De conjunto con el administrador, el técnico del taller y la VRES analizan los resultados del dictamen técnico.
Neutralización		Analizan de conjunto el problema, determinando: cómo proceder con el equipo desde el punto de vista contable para su baja técnica, lugar de almacenamiento hasta su traslado para materias primas.		
Recuperación		Proceder con la baja desde el punto de vista contable del equipo y su traslado para materias primas.		

11 Hecho: Falla de las Comunicaciones.

Acción por etapas	Persona que sufre la falla	Administrador de la red / administrador del área	Personal Especializado del Nodo o técnico del taller
Información	Informa al administrador de la red		
Neutralización		Trata de detectar el error y solucionarlo. De no ser posible de inmediato, lo informa al afectado y contacta personal especializado. Comprueba si la falla está en el lado del Proveedor, llamando a RIMED. Se analiza si la falla es por un problema de tarjeta de red en el caso de una PC o del sistema operativo. De ser este tipo de falla se reporta al técnico del taller por el administrador del área	Reparan la avería si existe. Si es el proveedor, solucionan el problema e informan. Si es por problemas de tarjeta de red o software el técnico del taller soluciona el problema
Recuperación		Hasta que no se elimine el problema, realiza las coordinaciones para continuar el trabajo, de ser posible y necesitarse con urgencia implementando una solución temporal. De no ser posible continuar el procesamiento en la entidad, puesto que no hay posibilidades de sustituir el componente afectado, el Jefe del Nodo lo informa a la Dirección de Informatización	El administrador del nodo de conjunto con el técnico del taller Informa a los interesados cuando restauran las condiciones iniciales.

12 Hecho: Modificación o alteración de los controles de seguridad

Acción por etapas	Persona que detecta	Activista de Seguridad Informática	Director del Nodo	Vicerrectoría de Tecnología
Información	Informa al activista o al especialista de Seguridad Informática	Informa al Administrador de la Red y jefe del Nodo y al jefe del área	Informa a la Dirección de Ihformatizaciònsi lo considera necesario por la gravedad del incidente	
Neutralización		Procede a sacar de la red la máquina desde donde se efectuó el acceso y bloquear la cuenta de usuario.	Elimina de inmediato el acceso. Administrador de la red analiza grieta de seguridad que lo permitió y la corrige de inmediato.	Se crea una comisión para investigar los hechos
Recuperación		Realiza anotaciones en el Libro de Incidencias	Administrador de la red reanuda el servicio.	Analiza posibilidad de sanción.

Como parte del HECHO: Modificación o alteración de los controles de seguridad **se toma en cuenta las alteraciones de la configuración de Servidores y PC**

Acción por etapas	Persona que detecta	Especialista de Seguridad Informática	Técnicos y especialista de SI y jefe del Nodo	Dirección de informatización
Información	Informa al Jefe de Área, al activista de Seg. Informática y al administrador de la red	Informa al Dtor del nodo, administrador de la red y la VRTE.	Preserva el equipo. Realizan análisis de los logs para determinar si es interno o externo la procedencia del ataque para alterar la configuración Realizan dictamen técnico	De conjunto con los especialistas analiza los resultados del dictamen técnico.
Neutralización		Se informa al MINED y la OSRI	Investigan las causas del hecho, implicados y fallas de seguridad. Analizan de conjunto el problema, determinando: cómo proceder para su recuperación.	
Recuperación		Proceder con la recuperación del equipo en sus estados iníciales Se crea comisión para determinar medidas disciplinarias de ser necesario.		

13 Hecho: Tormentas eléctricas severas

Acción por etapas	Director del Nodo	Dirección de informatización	Activista de Seguridad Informática
Información	Informa a la Dirección de informatización sobre la interrupción de los servicios para proteger los equipos dada la gravedad del incidente	Informa a los jefes administrativos y a los activistas de seguridad informática sobre la interrupción hasta tanto no se restablezcan las condiciones normales y que se proceda a desconectar todo el	Informa a las áreas y proceden a desconectar todo el equipamiento de la alimentación eléctrica

		equipamiento de la alimentación eléctrica	
Neutralización	Se desconecta todo el equipamiento de la alimentación eléctrica, en caso de algún hecho que ocurra por no cumplir lo orientado para estos casos se crea una comisión para investigar los hechos de ser necesario. Se investigan las causas de los hechos y se comunica al técnico que se encarga de las reparaciones eléctricas Se procede a restaurar la información con la copia de seguridad.		
Recuperación	Realiza anotaciones en el Libro de Incidencias y el administrador de la red reanuda los servicios y se comunica a los activistas de seguridad informática, jefes administrativos y usuarios.		

Se anexa Plan de respuesta ante contingencias del Nodo de Comunicaciones (ANEXO 7)

5.2.4.3.- Pruebas y Mantenimientos.

El especialista de Seguridad Informática se reunirá con todos los implicados en el cumplimiento de este Plan de recuperación ante contingencia instruyendo a cada uno qué hacer en cada caso.
En primera instancia debe explicar la organización de la recuperación, definiendo sus funciones y responsabilidades una vez que se materializa la amenaza.

En caso de producirse cambios en el mismo lo deberá informar de inmediato a la parte afectada, precisando cuales son las novedades que se incorporan a lo ya conocido, y de hecho cómo queda a partir de ese momento.

Las pruebas son el único método de asegurar que los procedimientos de recuperación están completos y se pueden llevar a cabo, los medios alternativos están disponibles y se pueden usar, las salvas son las adecuadas y el personal está correctamente entrenado.
Para mantener actualizado el Plan de Contingencia se realizarán pruebas periódicas y como resultado de éstas se procederá a los ajustes que sean convenientes de forma tal que se pueda asegurar la operatividad del mismo en caso de producirse alguna de las contingencias previstas.

Se prevén dos niveles de prueba:

1º Semestralmente se realizará una revisión de esta documentación, se probará la factibilidad de las respuestas propuestas para cada una de las contingencias y se comprobará la existencia y accesibilidad de los softwares y aplicaciones necesarias, así como disponibilidad de hardware.

2º Una vez al año se realizará la prueba comprobando incluso los medios de comunicación y utilizando otros locales y/o hardware, así como software, salvas e insumos (según sea necesario para el tipo de contingencia que se haga la prueba), que se planifiquen usar para estos fines en caso de una verdadera emergencia.

Las pruebas descritas (aunque deben incluir la efectividad de respuesta a todos los riesgos analizados) no se realizarán masivamente, sino que se harán seleccionando cada vez una contingencia o un área determinada. Resulta válido aclarar que, no obstante, en el año se tienen que realizar pruebas que abarquen todas las contingencias.

El especialista de Seguridad Informática en coordinación con las personas que intervienen en la recuperación, seleccionarán la fecha y hora de las pruebas, preferiblemente en horario nocturno, fines de semana o períodos en que no se realice un procesamiento crítico.
Durante las pruebas, la persona que esté al frente de la misma, designará a otra, a la que llamaremos observador, que no participe de ella, y sólo observe y anote aspectos que los participantes no notan u olvidan.
Una vez concluida cada prueba se reunirá todo el personal que participó, el observador y el activista o especialista de Seguridad Informática para analizar y discutir los sucesos acaecidos durante la misma.

De las conclusiones que se obtengan, se nutrirá el Plan de Contingencia de posibles adecuaciones.

MEDIDAS EDUCATIVAS Y DE CONCIENTIZACIÓN.

Divulgación de aspectos claves para garantizar la seguridad informática.
Los activistas de Seguridad Informática serán los mayores divulgadores de este plan de Seguridad, deben leerlo, estudiarlo y extraer lo más importante. En función de ello organizarán seminarios.

Es importante resumir los aspectos más importantes de forma diferenciada, según las personas o el grupo de personas que tengan que cumplimentar tareas similares.
Los activistas de Seguridad Informática de las áreas imprimirán y circularán entre las personas que deban cumplir con este Plan de Seguridad Informática el resumen elaborado con aquellos aspectos importantes que deban ser de dominio general.

El especialista de Seguridad Informática de la universidad deberá en no más de dos cuartillas y de forma concreta referir las tareas que debe acometer el primer nivel de dirección.
Además, se fijarán en lugares visibles en los locales donde se encuentran las microcomputadoras, aquellas medidas que resulten de vital importancia cumplimentar, en ese puesto de trabajo, para el éxito del Plan de Seguridad.
Se impartirá un curso de seguridad informática a todos los trabajadores que tengan a su disposición una computadora para realizar sus actividades profesionales, además firmarán el compromiso de empleo de las tecnologías informáticas y sus servicios en la universidad, el resultado de dicho curso y el compromiso de empleo de las tecnologías será archivado en el expediente laboral del trabajador.
Todos los trabajadores firmarán el código de ética para el uso de las tecnologías informáticas y los servicios de las redes en la Universidad.

Programas de preparación.

El personal responsabilizado de la Seguridad Informática en la universidad debe estar actualizado en esta materia y participar en cursos, conferencias o seminarios que se impartan.
Una vez aprobado el Plan de Seguridad Informática, el especialista de Seguridad Informática de la universidad planificará tres cursos de capacitación, uno para el primer nivel de Dirección, otro para los especialistas de Seguridad Informática de las áreas, quienes a su vez lo harán para el resto de los trabajadores vinculados con el uso de las tecnologías informáticas y otro para los técnicos de laboratorios y personal de secretaria y otros trabajadores.
En el curso de capacitación al primer nivel de dirección se tratará de ser conciso y explicar los objetivos del Plan y responsabilidades y como debe ser controlada las actividades de la seguridad informática como parte del sistema de trabajo.
En los cursos orientados al resto del personal, se definirán las tareas orientadas al tema de la seguridad informática en que tienen que concentrar sus trabajos los que laboran con las Tecnologías Informáticas y se sentarán las bases para el trabajo posterior. Se tendrá en cuenta:

i. Capacitación General sobre Seguridad Informática y Protección de Datos. Medidas a cumplimentar por todos los trabajadores en el Plan de Seguridad Informática.
ii. Capacitación diferenciada, en algunos casos de forma personal, sobre las tareas específicas de cada cual.

Sanciones.

El personal sujeto al cumplimiento de este Plan de Seguridad Informática que viole en alguna medida lo aquí dispuesto puede ser objeto, de acuerdo a la gravedad de los hechos y el criterio de la comisión disciplinaria que analice el caso, de alguna de las siguientes medidas:

- Aplicación del Decreto Ley 92 por la Responsabilidad material
- Amonestación Pública.
- Amonestación privada
- Retiro de los servicios por 3 mese, 6 meses o un año.
- Separación Temporal de su cargo.
- Separación Definitiva del cargo.

MEDIDAS LEGALES

Se cumplen en este Plan de Seguridad con las medidas que sobre la Seguridad Informática se expresan en la Resolución No.127 del año 2007 del MIC así como el Acuerdo No. 6058 del Comité Ejecutivo del Consejo de Ministros, de fecha 9 de julio del sobre los Lineamientos para el Perfeccionamiento de la Seguridad de las Tecnologías de la Información en el país. Asimismo, se respetan los procedimientos, modelos y medidas ya establecidas en el Institución Central para la protección y cuidado de las tecnologías informáticas y de comunicaciones y la seguridad de la información, así como la protección física.

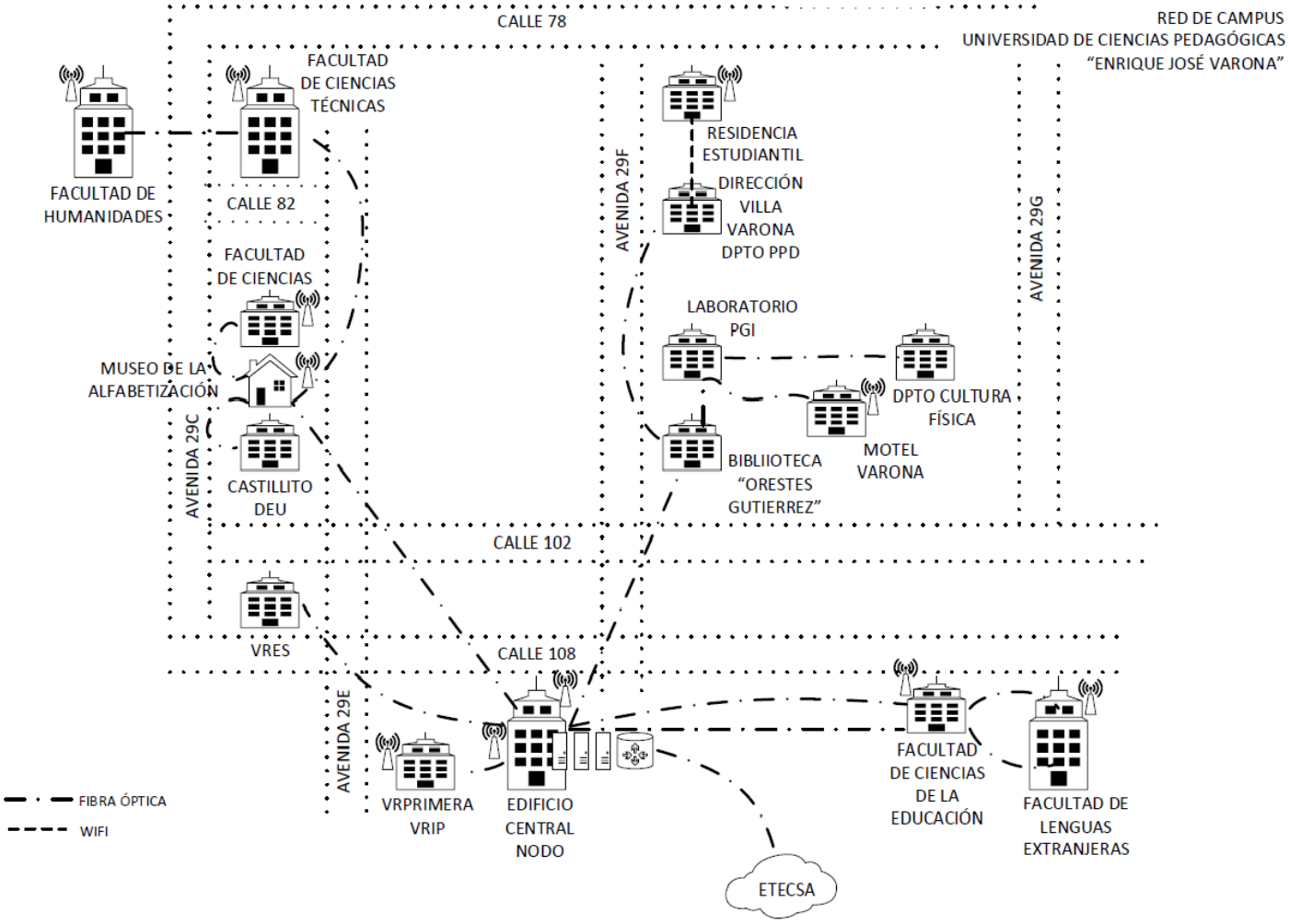
MEDIDAS GENERALES

En los servidores:

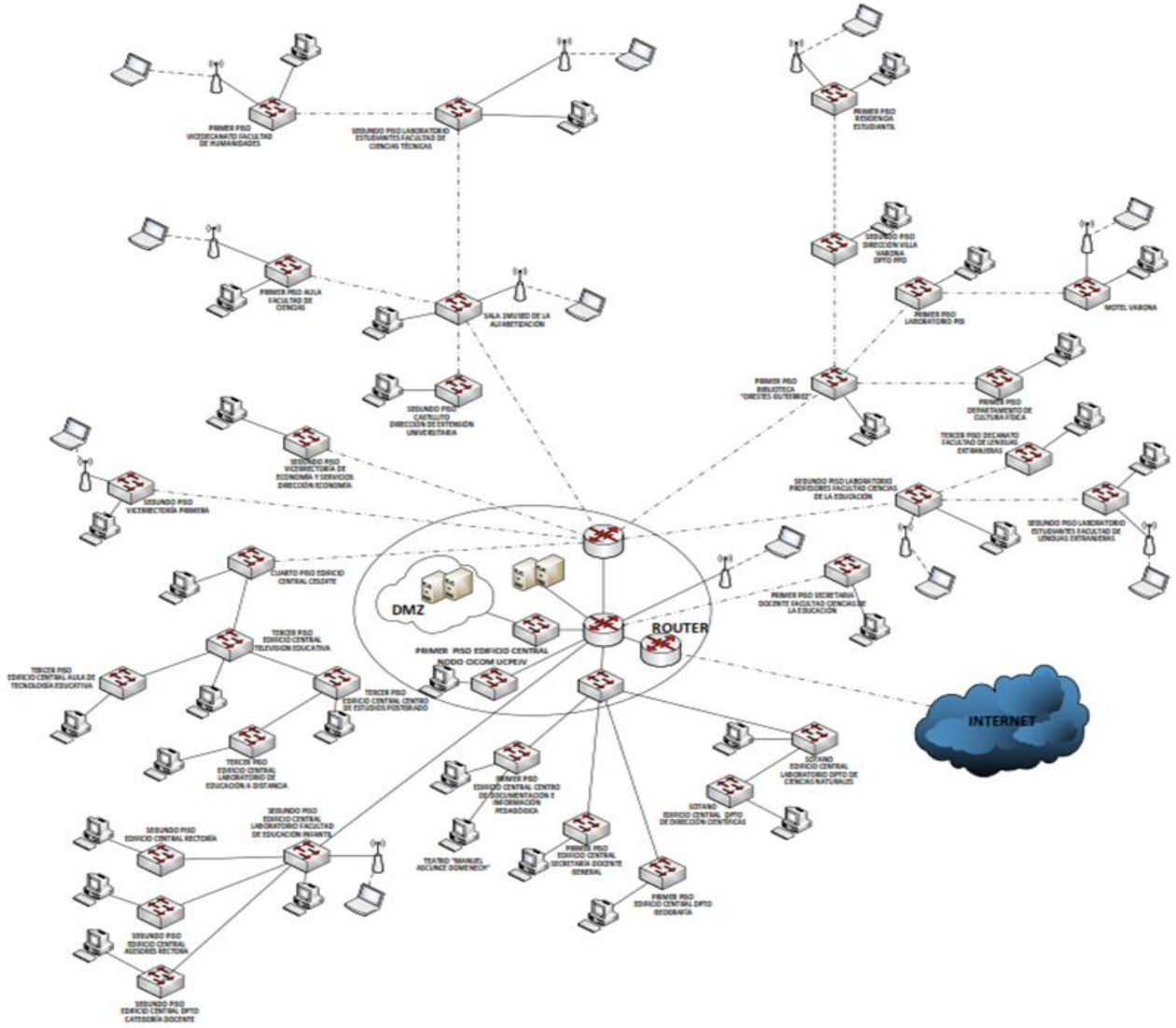
El administrador de la red utilizará dos cuentas: una como usuario normal y otra como administrador (que renombrará). Todo ello en aras de la seguridad. Mientras inicia una sesión como usuario normal no podrá modificar accidentalmente aspectos que sólo puede cambiar como administrador. Al renombrar la cuenta enmascara su identidad, lo que es útil ya que sabemos que la cuenta implícita de los administradores no puede ser cerrada por intentos de contraseñas no válidas ni tampoco puede ser desactivada, por lo que está expuesta a ataques de fuerza brutal para adivinar la contraseña.

ANEXO 1

ORGANIGRAMA



Anexo 1a



ANEXO 2

ADMINISTRADORES DE RED Y PERSONAL AUTORIZADO A PROCESAR INFORMACION SENSIBLE

1. José Vasco Capote (Director)
2. Pedro Juan Morales Alfonso
3. Joel Pérez Vargas
4. Osmaro Alberto González Falcón
5. Manuel Alejandro Aguilar Díaz
6. Milagros Midiela Collazo Salcedo

ANEXO 3

COMPROMISO PARA EL EMPLEO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y SUS SERVICIOS POR LOS USUARIOS DE LA RED DE LA UCPEJV.

SOLICITUD SERVICIOS TELEMÁTICOS
FORMULARIO DE SOLICITUD DE SERVICIOS
PARA LA RED INFORMÁTICA UCPEJV

Día	Mes	Año

Fecha de Solicitud

Datos Personales y Laborales

Nombre(s) y Apellidos:		Universidad de Ciencias Pedagógicas "Enrique José Varona"	Calle 108, # 29E08 / 29E y 29F Ciudad Escolar Libertad, Marianao
Número Carné de Identidad	Cargo que Ocupa	Facultad/ Área / Departamento	
☐ Docente ☐ Licenciado ☐ Master ☐ Doctor ☐ Instructor ☐ Asistente ☐ Auxiliar ☐ Titular ☐ No Docente ☐ Estudiante			

Datos del Servicio

Tipo de Solicitud	**No. Solicitud**
☐ Creación de usuario **NO** existente	**No. Consecutivo** / **Año**
☐ Modificación de Privilegios de un usuario existente ☐ Renovación del Servicio a un usuario existente	

Tipo de Servicios		**Nombre de Usuario**: (Nodo Central)
☐ Correo Electrónico Nacional ☐ Correo Electrónico Internacional ☐ Navegación Nacional ☐ Navegación Internacional	☐ Navegación REUNIV ☐ Servicio Conmutado	**Contraseña Temporal**: No. Carnet Identidad **http://acceso.ucpejv.edu.cu**

Dirección Particular (Solo para Servicio Conmutado (PAP))

Calle	No.	Apto	Entre	Y
Reparto	Municipio		Provincia	
Teléfono				

Manifiesto que los datos arriba expuestos se ajustan a la realidad y regirán mi comportamiento como usuario de la Red UCPEJV. Doy fe de que he leído y entendido el Código de Ética al dorso de éste formulario y que por lo tanto acataré todo lo expresado por la letra de dicho documento, así como también las disposiciones que estipule su administración. Me comprometo además a no divulgar o usar a través de la RED hacia el exterior, ninguna información confidencial, clasificada, de importancia estratégica o que pueda constituirse patrimonio de la institución. **Firma del Solicitante**: _____	**Funcionario que Autoriza** Nombre y Apellidos Cargo Firma y Cuño **Director Nodo UCPEJV** / **Ejecutado por** Firma / Firma

Normas de Ética para el uso de los Servicios Telemáticos Red UCPEJV, cualquiera que sea su alcance.

Queda prohibido el envío por correo electrónico de juegos, programas ejecutables, correos cadenas (correos que se envía a grupos de personas instando a su distribución masiva) y cualquier otro tipo de información que no sea de interés para el trabajo investigativo, docente o de extensión de los usuarios.

En caso de recibir información no solicitada como la descrita en el punto anterior, se le debe informar al remitente que cancele al envío de la misma.

En caso de recibir información de tipo subversiva usted debe:

1. Informar de inmediato a la Seguridad Informática de su entidad.
2. No responda al remitente ni reenvíe el mensaje a nadie.
3. No reproduzca por ningún medio dicha información.
4. No divulgue ni haga exclamaciones al respecto.

Las búsquedas en Internet deben limitarse a las temáticas relacionadas con las líneas de investigación, la actividad docente que realiza, y su superación. El servicio de Internet no es para utilizar en correo electrónico con servidores internacionales, ni para el chat, para los casos anteriores deberá estar autorizado por el jefe inmediato superior, el que informará su decisión al Director del Centro de Informática y Comunicaciones, al hacerse responsable el que autoriza del flujo de información por los mismos. Las descargas no anónimas de otros servidores FTP deberán ser autorizadas por el jefe inmediato superior e informadas al Director del Centro de Informática y Comunicaciones.

No se podrá compartir u ofrecer la información de la cuenta (usuario y contraseña) de los servicios telemáticos con otras personas y deberá utilizar el servicio desde el dispositivo autorizado a tales efectos, en caso contrario el usuario deberá informar al Director del Centro de Informática y Comunicaciones o al Responsable de Seguridad Informática de la entidad.

Se prohíbe el acceso y descarga de páginas de contenido pornográfico o que agredan la ética y moral de la revolución, se sugiere a los usuarios que trabaje con configuraciones seguras en su navegador y en caso de accesos involuntarios informe del hecho al Responsable de Seguridad Informática de la entidad.

Se debe utilizar adecuadamente y según lo normado por el MES la cuota asignada a cada usuario según su clasificación, grado académico y científico.

Una vez realizadas las búsquedas se deben seleccionar las páginas a solicitar y no se deben marcar hipervínculos sin tener la certeza que los mismos serán útiles.

Queda prohibido descargar de Internet TODO TIPO DE PROGRAMAS EJECUTABLES o solicitar a alguna persona el envío de los mismos, si es de interés para su docencia o investigación diríjase a los técnicos de informática de su área.

Queda prohibido utilizar programas para escanear la red o utilizar los servicios de la misma de manera irregular como los casos de aceleradores de descargas, proxys anónimos, proxys virtuales y otros con la misma finalidad.

Para reducir el tamaño de los mensajes a enviar los mismos deberán ser elaborados fundamentalmente en modo de texto. El mensaje que va a enviar no debe exceder los límites asignados por el servidor (4 MB).

El uso del correo electrónico es para envío de mensajería de contenido profesional, afín a los intereses de la institución docente, su proceso docente y a la actividad investigativa que realiza el usuario autorizado. En ningún caso el buzón podrá ser utilizado por otra persona ajena al autorizado, no pudiéndose dar contraseña, prestar o vender el servicio a terceros.

No se podrá suscribir a ningún tipo de lista internacional considerada ajena a la actividad profesional, aun requiriendo esta de autorización por parte de la autoridad facultada por el Director del Centro de Informática y Comunicaciones.

Se prohíbe el envío de información con carácter clasificado y se explica que para otros tipos de información se procederá según la legislación emitida a los efectos.

Igualmente se responsabiliza a los usuarios titulares con todo el contenido en su buzón, así como la información que se intercambia, y con el mantenimiento del mismo (20 MB límite de espacio máximo del buzón de correo); lo que implica además la prohibición de envío de códigos malignos en la información adjunta.

El uso de los buzones de correo electrónico, así como la navegación tiene como exigencia, el cumplir con lo estipulado por el Código de Ética para el trabajo en la Red, el de uso del correo electrónico y de cuantas resoluciones y reglamentos se emita al efecto.

El usuario titular del correo estará conforme, para poder recibir el servicio, y aprobará la realización de auditorías sorpresivas a su buzón y mensajería que intercambia según la legislación y reglamentaciones vigentes presentes y futuras, estando presente o no en la auditoria del sistema.

En caso de violación de algunas de estas medidas, se le cancelarán temporal o definitivamente los servicios telemáticos al infractor.

Grupo de Seguridad Informática UCPEJV

Centro de Informática y Comunicaciones CICOM UCPEJV

ANEXO 4

NORMAS ÉTICAS GENERALES PARA EL USO Y EXPLOTACION DE LOS SERVICIOS DEL CORREO ELECTRONICO E INTERNET EN LA UCP EJV.

Objetivos y alcance de las normas:

Artículo 1: Las siguientes normas tienen por objetivo establecer los principios éticos que deben ser observados por los estudiantes, trabajadores y personal en general de la UCP EJV en el uso de los servicios disponibles en el Correo Electrónico e Internet.

COMPROMISO PARA EL EMPLEO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y SUS SERVICIOS POR LOS USUARIOS DE LA RED DELA UCPEJV.

ANEXO AL CONTRATO LABORAL No. _____

DATOS PERSONALES

Nombres y apellidos: _____ CI: |__|__|__|__|__|__|__|__|__|__|__|

Área de trabajo: _____

Ocupación: _____

Por este medio declaro que conozco y asumo la responsabilidad en cuanto a la Seguridad Informática en el uso de las Tecnologías de la Información y la Comunicación para el desempeño de mis funciones laborales como se expresa en la Resolución 127/2007 del MIC, y otras circulares que se emitan el Ministerio de Educación Superior y la Universidad.

Como usuario de las Tecnologías de la Información y la Comunicación en la entidad asumo las siguientes obligaciones:

a) Usar y conservar correctamente las tecnologías y sus sistemas automatizados en interés de las funciones de mi cargo.

b) Responder por el uso de las cuentas que me han asignado y cumplir con la política establecida para la gestión de identificadores y claves de acceso.

c) Utilizar solamente los servicios establecidos y de la forma en que los mismos han sido configurados.

d) No utilizar el correo electrónico e Internet para trasmitir, acceder, o difundir información pornográfica, terrorista, contrarrevolucionaria, o en general con fines lesivos a los intereses de la sociedad, de la institución o de terceros.

e) No utilizar las tecnologías de la información con fines lucrativos o de carácter personal.

f) No identificarme ante otras Instituciones para recibir algún servicio a nombre del MES sin una autorización expresa para ello.

g) Abstenerme de realizar cualquier tipo de acciones de comprobación de redes sin autorización, así como el envío o reenvío de mensajes masivos con información intrascendente, de supuestos alertas, cartas cadenas, etc.

h) No acceder a servidores de correo electrónico externos sin previa utilización, ni desde máquinas utilizadas para el empleo propio en el puesto de trabajo, ni procesar o conservar información interna en terminales previstas para el acceso a INTRANET e INTERNET.

i) No enviar a través de INTRANET e INTERNET o del correo electrónico documentos clasificados o de importancia para el trabajo de la Universidad y del MES.

j) De ser necesario descargar programas ejecutables existentes en INTRANET e INTERNET, aplicar los procedimientos establecidos para ello.

k) Cumplir las políticas establecidas en el MES y la Universidad para la protección contra virus informáticos, así como para la recepción y envío de ficheros anexos a mensajes electrónicos.

l) Mantener actualizado el antivirus en la estación de trabajo asignada para realizar mis labores.

m) Utilizar para los servicios que me fueron aprobados, una contraseña segura y no permitir su uso indebido por otros usuarios.

n) Informar de inmediato al Asesor de Seguridad Informática del área y al Grupo de Seguridad Informática de la Universidad de la recepción de mensajes no demandados o que ocasionan molestias, así como los mensajes contrarrevolucionarios o con otros fines, que no guarden relación con la política del MES y la Universidad.

o) Cumplir con las regulaciones establecidas para el empleo de las redes informáticas emitidas por la Dirección de Informatización, el grupo de Seguridad Informática y las que se deriven de las resoluciones ministeriales y rectorales.

p) Adquirir la preparación y los conocimientos de Seguridad Informática imprescindibles para el desempeño de su trabajo.

q) Contar con la autorización expresa del jefe facultado, para obtener acceso a cualquiera de los bienes informáticos.
r) No transgredir ninguna de las medidas de seguridad establecidas.
s) Proteger las tecnologías o la terminal de red que le ha sido asignada y colaborar en la protección de cualquier otra, para evitar que sea robada o dañada, usada la información que contiene o utilizado de manera impropia el sistema al que esté conectada.
t) Proteger y respetar los derechos de autor y otras licencias de la entidad.
u) No instalar ni utilizar en las tecnologías equipamientos o programas ni modificar la configuración de las mismas, sin la correspondiente autorización del jefe facultado.
v) Se prohíbe la difusión a través de las redes públicas de transmisión de datos de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas; o que lesione la Seguridad Nacional, por cualquier persona natural o jurídica. Las entidades instalarán los controles y mecanismos que permitan detectar y obstaculizar este tipo de actividades. Las violaciones detectadas serán informadas oportunamente a las instancias pertinentes.
Ninguna persona natural o jurídica está autorizada para enviar mensajes de correo electrónico no solicitados a múltiples usuarios de forma indiscriminada (spam), ya sean de carácter informativo, comercial, cultural, social, con intenciones de engaño (hoax) u otros.
Y para que así conste, firmo a los ___ días del mes de _____ de _____

_____ _____
Jefe de **Dirección de Recursos Humanos J´ de área** Trabajador

Artículo 2: Los trabajadores encargados de brindar los servicios del Nodo de la UCP EJV, además de las normas referidas a los usuarios cuando actúen como tales, deberán cumplir las normas siguientes:
a) Mantener la discreción en cuanto a la administración y uso de la tecnología empleada en la prestación de los servicios de Correo Electrónico e Internet.
b) Proteger los derechos de autor y otras licencias de la entidad.
c) Usar y conservar correctamente los sistemas automatizados, así como los datos en ellos contenidos.
d) Monitorear el sistema sólo en los casos de mantenimiento, administración, correcciones de errores y otros aspectos similares relacionados con el comportamiento y disponibilidad del sistema.
e) No acceder a la información de otro trabajador o estudiantes sin la presencia de éste o sin previa autorización del jefe inmediato superior.
f) No divulgar logins, ni contraseñas propias de los usuarios a nadie, orientando y velando por que los mismos sean de uso estrictamente personal.
g) Habilitar los servicios a los usuarios, sólo con la aprobación previa del Director del Centro de Informática y Comunicaciones, por escrito, que la emitirá a partir del modelo de solicitud de cuenta de correo electrónico del área interesada.
h) Operar los servidores de forma que el acceso a cada uno de los servicios que se brinde quede limitado exclusivamente a los usuarios, tanto internos como externos, autorizados por escrito por el Director del Centro de Informática y Comunicaciones.
i) Velar por los aspectos de la seguridad informática, garantizando que los servidores estén configurados y operados en forma correcta para evitar, en la medida de las posibilidades del software y del hardware disponible, tanto la fuga de información no autorizada como la penetración de intrusos que puedan causar daños.
j) Resolver tan pronto como sea posible cualquier anomalía que se detecte en el funcionamiento de los servidores, informarlo inmediatamente al nivel superior y reflejarlo en el libro de incidencias, incluyendo un análisis sobre la afectación de la seguridad informática que pudiera haber ocurrido.
k) El administrador procederá a la apertura de las Cuentas de Correo Electrónicas aprobadas y la confirmará a los usuarios
l) El administrador está en la obligación de garantizar que la información que se genere o se reciba cumpla lo regulado.
m) El administrador realizará el mantenimiento de las Cuentas de Correos autorizadas, respondiendo a las solicitudes de actualización de cuentas y códigos de
n) identificación, así como a otras necesidades que presentan los usuarios en el uso del servicio.

ANEXO 5

ESPECIALISTA DE SEGURIDAD INFORMATICA DE LA UNIVERSIDAD

Issel Luis Puig González

Integrantes del grupo central de seguridad informática de la universidad.

- Iniel Linares Gutiérrez
- Pedro J. Morales Alfonso
- Roberto Jorge Pérez Lombard

Activistas de Seguridad Informática por áreas

Relación del Grupo Central de Informática				
Nombre	**Apellidos**	**Representa**	**Área**	**Correo**
Raúl Ernesto	Nodarse Silveira	Seg. Innf	Humanidades	raulens
Carlos Alberto	Lavín Ruiz	Asesor TIC	Humanidades	carlosalr
Ricardo	Méndez Lorenzo	Asesor TIC	FCT	ricardoml
Iniel	Linares Gutiérrez	Seg. Inf	Ciencias	iniellg
Dayamith	Menéndez Mendoza	Asesor TIC	Ciencias Educ.	dayamithbmm
Celia Yunek	Prado Laffita	Asesor TIC	FEI	celiaypl
Mebis Esther	Hernández Ruíz	Seg. Inf	FEI	mebisehr
Joel	Fuentes Domínguez	Asesor TIC	VRFP	joelfd
Mario L.	Chacón Gallarfo	Seg. Inf	Ciencias	mariolchg
Yisely	Afá Gonzalez	Seg. Inf	FLEX	yiselyag
Cristina de la C.	Bueno Mojena	AsesorTIC	FLEX	cristinacbm
Héctor Alejandro	Pérez Moya	Seg. Innf	Ciencias Educ.	hectorapm
Lagos Torres	Rebeca	Seg. Innf	Dir Comunic.	rebecalt

ANEXO 6

Plan de respuesta ante contingencias del Nodo de Comunicaciones:

Los Preparativos. - Medidas y acciones que aseguran una respuesta óptima e incluye la elaboración de las decisiones y los planes de reducción de desastres y su actualización. Comprende además las actividades que se desarrollan antes del impacto de una amenaza, con el objetivo de reducir sus daños. Dentro de estos tenemos.

Contingencias que se pueden presentar: Ciclones tropicales, Huracanes, intensas lluvias, tormentas eléctricas locales severas, sismos, incendios en áreas del CICOM, falla eléctrica o cortacircuitos.

En el Centro de Informática y Comunicación (CICOM) se cuenta con un plan de aviso, el cual está articulado de la manera siguiente. Al ocurrir algún incidente en el Centro de Informática y Comunicación, el puesto de mando de la universidad se comunica con el Director del CICOM y este a su vez debe comunicarle a la vicerrectora correspondiente.

#	Contingencia	Recuperación	Tiempo de Respuesta de puesta en Marcha
1	**Ciclones tropicales:** -Se apagan todos los servicios menos el correo para que el puesto de Dirección tenga comunicación con el MES, y demás Órganos de dirección del municipio y provincia. Una vez establecidas las condiciones iníciales comienza la recuperación.	-Se ponen en marcha todos los servicios y en caso de estar algún servicio corrupto, se recupera con la salva o mediante la reinstalación del mismo.	- Esta dado por el tiempo que dure el evento meteorológico, y se restablezca el fluido eléctrico -El tiempo que pueda llevar esta acción desde 1hora en adelante.
2	**Huracanes:** -Se apagan todos los servicios menos el correo para que el puesto de Dirección tenga comunicación con el MES, y demás Órganos de dirección del municipio y provincia. Una vez establecidas las condiciones iníciales comienza la recuperación.	-Se ponen en marcha todo los servicios y en caso de estar algún servicio corrupto, se recupera con la salva o mediante la reinstalación del mismo.	- Esta dado por el tiempo que dure el evento meteorológico, y se restablezca el fluido eléctrico -El tiempo que pueda llevar esta acción desde 1hora en adelante.
3	**Intensas lluvias:** -Se apagan todos los servicios menos el correo para que el puesto de Dirección tenga comunicación con el MES y demás Órganos de dirección. Una vez establecidas las condiciones iníciales comienza la recuperación.	-Se ponen en marcha todo los servicios y en caso de estar algún servicio corrupto, se recupera con la salva o mediante la reinstalación del mismo.	- Esta dado por el tiempo que dure el evento meteorológico, y se restablezca el fluido eléctrico -El tiempo que pueda llevar esta acción desde 1hora en adelante.
4	**Tormentas eléctricas locales severas:** **Se apagan todos servicios.** Una vez establecidas las condiciones iníciales comienza la recuperación.	-Se ponen en marcha todo los servicios y en caso de estar algún servicio corrupto, se recupera con la salva o mediante la reinstalación del mismo.	- Esta dado por el tiempo que dure el evento meteorológico, y se restablezca el fluido eléctrico -El tiempo que pueda llevar esta acción desde 1hora en adelante.
5	**Sismos:** **Se apagan todos servicios.** Una vez establecidas las condiciones iníciales comienza la recuperación.	-Se verifica que la construcción no ofrece peligro para la vida, ni para los recursos materiales. Se ponen en marcha todo los servicios y en caso de estar algún servicio corrupto, se recupera con la salva o mediante la	- Esta dado por el tiempo que dure el acceso al local, y el restablecimiento del fluido eléctrico -Esta acción va desde 1hora en adelante.

		reinstalación del mismo.	
6	**Incendios en áreas:** Se comunica al servicio de bomberos y al puesto de dirección. Se comunica a la brigada contra incendios, se aplica el extintor según sea fuego y por lo que fue provocado Se procede a desconectar el equipamiento y de ser posible evacuar los servidores y el resto del equipamiento.	- Se ponen en marcha todo los servicios y en caso de estar algún servicio corrupto, se recupera con la salva o mediante la reinstalación del mismo.	Esta dado por el tiempo que dure el acceso al local, y el restablecimiento de las condiciones. -Esta acción va desde 1hora en adelante.
7	**Falla eléctrica o cortacircuitos**: Se apagan todos servicios y se comunica al servicio de mantenimiento los hechos. Una vez establecidas las condiciones iníciales comienza la recuperación.	- Se ponen en marcha todo los servicios y en caso de estar algún servicio corrupto, se recupera con la salva o mediante la reinstalación del mismo.	El tiempo que pueda llevar esta acción desde 1hora en adelante.
8	**Falla en la climatización**: Se apagan todos servicios y se comunica al servicio de mantenimiento los hechos. Informar a la dirección de informatización y la Dirección institucional. Dejar funcionando solo los servidores que garanticen el flujo de correos, el resto apagarlos hasta tanto se restablezcan las condiciones. Una vez establecidas las condiciones iníciales comienza la recuperación.	- Se ponen en marcha todo los servicios y en caso de estar algún servicio corrupto, se recupera con la salva o mediante la reinstalación del mismo.	El tiempo que pueda llevar esta acción desde 1hora en adelante.

ANEXO 7

Reglamento interno para los laboratorios de informática, oficinas y departamentos.

REGLAMENTO INTERNO PARA LOS LABORATORIOS DE INFORMÁTICA, OFICINAS Y DEPARTAMENTOS.

Con el objetivo de prevenir posibles violaciones de la seguridad informática en la Institución y de optimizar el uso de los recursos informáticos puestos a nuestro servicio, se dispone el siguiente reglamento:

1. Laboratorios de Informática.

1.1 Las PC deben cumplir los siguientes requisitos:

- Todas las Pc ubicadas en el laboratorio están en función de la docencia como prioridad. (No hay Pc privativas para el uso de los técnicos)
- Tener configurado el SETUP para que arranque sólo desde el disco duro y a su vez esté protegido por contraseña. (Esta contraseña estará en poder del técnico, el decano de la facultad y el equipo de seguridad informática de la Institución).
- Tener instalados un solo sistema operativo. Tendrán más de uno cuando la actividad relacionada con la docencia lo exija (previa autorización del Jefe de Departamento).
- Tener creados sólo dos sesiones de usuarios para el trabajo.
  - Sesión Usuario “administrador”. Este usuario será para el uso exclusivo del técnico de laboratorio, responsable del servicio técnico de la Pc o la red y del equipo de seguridad Informática de la Institución.
  - Usuario “estudiante”. Este usuario tendrá propiedades de usuario de avanzada y se utilizará para la docencia y los servicios.

  (En el caso que la actividad docente lo requiera el trabajo con usuarios que posean privilegios administrativos, el técnico previa coordinación, garantizará la creación del mismo y finalizada la actividad lo inhabilitará.)
- Tener instalado, configurado y actualizado correctamente un software antivirus (el acordado por nuestro Ministerio). Para ello se recomienda utilizar los Antivirus Segurmática, NOD32 o KAV, el software y actualizaciones periódicas que se publican en el FTP del portal Varona o RedUniv.
- Tener actualizado sistemáticamente el sistema operativo que utiliza con los parches de seguridad. Para ello podrá descargarlo del FTP del Nodo de la Universidad.
- Al recibir un laboratorio el técnico y el personal designado por el jefe del área, se debe solicitar los discos de instalación de Drivers, Sistemas Operativos y aplicaciones y la contraseña de las PC, la que estará bajo la custodia del propio técnico, el decano y el asesor de la seguridad informática del área.
- Si un equipo resulta infestado se deben realizar las siguientes acciones.
  - Desconectar el equipo inmediatamente de la red y hacer una revisión minuciosa con el software antivirus instalado en él.
  - Reiniciar la PC y entrar con la opción de modo seguro.

- Si es posible, hacer copia de seguridad de sus archivos para poder compararlas con copias anteriores.
- Ejecutar un programa antivirus.
- De no ser efectiva la desinfección o eliminación del programa maligno y le sea imposible instalar otro programa antivirus que neutralice la amenaza sin poner en riesgo otros equipos, contacte al equipo de seguridad informática de la Institución. en la siguientes direcciones de correo electrónico: asesor_si@ucpejv.edu.cu o a través del número telefónico 72607952.
- **Instalar** nuevamente el sistema operativo y restaurar las copias de seguridad

- No pueden instalarse software que violen o intenten violar los servicios de seguridad y trabajo que brinda CICOM (el nodo central).
- Se prohíbe la instalación, así como el uso de los medios informáticos para almacenamiento, ejecución o reproducción de juegos, música, videos, u otro material que no tengan que ver con la actividad docente e investigativa docente, laboral e investigativa de nuestra Institución.
- Tener instalados, configurado y protegido correctamente todo el soporte de Sistema Operativo y de navegación para el trabajo con la Pc del laboratorio.
- Tener instalados el software que se emplean directamente en la docencia, el desempeño laboral o la investigación. El paquete de office, enciclopedias, software educativo, utilitarios y herramientas de programación entre otros.

1.2 Funciones y exigencias que deben cumplir los técnicos de laboratorio.

- Deben tener una preparación adecuada en cuanto a conocimientos técnicos informáticos.
- Deben controlar diariamente los recursos Informáticos que están bajo su custodia y hacer marcado énfasis en la integridad de los sellos de seguridad que coloca el taller central, COPEXTEL u otra entidad que brinde servicios de mantenimiento.
- Para la docencia, debe facilitarle al profesor, el uso de todos los medios informáticos disponibles en el laboratorio y le servirá de apoyo en el desarrollo del proceso docente educativo. Y fiel custodio de la Información almacenada en las Pc por docentes y estudiantes previa coordinación y autorización.
- Debe brindar asesoramiento y protección a los usuarios que acceden a la conectividad y la mensajería electrónica (Intranet, Internet y el correo de la Institución) desde el laboratorio.
  - Evitar que las cuentas y contraseñas de acceso a INTERNET o correo electrónico queden registradas de forma automática en los exploradores de Internet.
  - Garantizar que no existan instalados KEYLOGGER o programas piratas que obtienen esta información.
- Deben revisar con programas antivirus los medios extraíbles que se pretendan introducir en el laboratorio para evitar que sea contaminado por programas malignos.
- Deben apagar y desconectar de la corriente la PC y demás dispositivos de conectividad en caso de descargas eléctricas y posibles tormentas.

- Deben realizar mantenimiento informático y físico sistemático a los medios de cómputos para garantizar el correcto funcionamiento de los mismos, aumentar su eficiencia y rendimiento.
  - Limpiar registros, ficheros temporales, historial de navegación por Internet y contraseñas guardadas.
  - Desfragmentar
  - Quitar elementos innecesarios del menú inicio. Así como información innecesaria (Liberación de espacio en disco)
  - Usar temas y apariencias del sistema operativo acordes con la institución y que no malgasten recursos de memoria.
- Evitar que se introduzcan alimentos en laboratorio, prohibido fumar y mantener una higiene adecuada dentro del mismo.
- No colocar paquetes ni bultos encima de las mesas y/o equipos. Garantizar un área para la colocación de los mismos.
- Controlar y reportar cualquier incidente de seguridad al grupo central de seguridad informática al especialista Issel Puig vía correo electrónico asesor_si@ucpejv.edu.cu
- Mantener un control estricto sobre las personas que acceden al laboratorio, no permitir que personal ajeno al área de informática y mucho menos a la Institución, instale o configure equipos u opciones en la PC. registrando los siguientes datos en una libreta diseñada para este fin.
  - Nombre y apellidos del usuario.
  - Hora de entrada y salida.
  - Nombre o Nº del equipo que utilizó.
  - Firma.
- Asegurar puertas y ventanas, así como la desconectividad eléctrica al concluir la sesión de trabajo.
- Configurar las aplicaciones ofimáticas, el navegador de Internet y el gestor de correo con las opciones de seguridad apropiadas.
- Escribir en el libro o libreta de incidencias cualquier desperfecto o irregularidad detectada e informarlo a la instancia de dirección que se corresponda.

2. Oficinas, departamentos y otros lugares con presencia de recursos informáticos.

2.1 Las PC deben cumplir los siguientes requisitos:

- Tener configurado el SETUP para que arranque sólo desde el disco duro y a su vez esté protegido por contraseña. (Esta contraseña estará en poder del propietario del equipo y el grupo de seguridad informática de la Universidad).
- Tener creados sólo dos usuarios.
  - Usuario “administrador”. Este usuario será para el uso exclusivo del equipo de seguridad Informática.

- Usuario “nombre elegido por el responsable del equipo”. Este usuario tendrá propiedades administrativas para garantizar la instalación de software, mantenimiento del equipo, etc.

❖ Tener instalado, configurado y actualizado correctamente un software antivirus. Para ello se orienta utilizar los antivirus Segurmática, NOD32, KAV, los software y actualizaciones periódicas que se publican en el FTP de la Universidad.

❖ Tener actualizado sistemáticamente el sistema operativo que utiliza con los parches de seguridad. Para ello podrá descargarlo del FTP del Nodo de la Universidad.

❖ Si un equipo resulta infestado se deben realizar las siguientes acciones.

➢ Desconectar el equipo inmediatamente de la red y hacer una revisión minuciosa con el software antivirus instalado en él.

➢ Reiniciar la PC y entrar con la opción de modo seguro.

➢ Si es posible, hacer copia de seguridad de sus archivos para poder compararlas con copias anteriores.

➢ Ejecutar programa antivirus.

➢ De no ser efectiva la desinfección o eliminación del programa maligno y le sea imposible instalar otro programa antivirus que neutralice la amenaza sin poner en riesgo otros equipos, contacte al equipo de seguridad informática de la Institución. en la siguientes direcciones de correo electrónico: asesor_si@ucpejv.edu.cu o a través del número telefónico 72607952.

- **Instalar** nuevamente el sistema operativo y restaurar las copias de seguridad

❖ No pueden instalarse software que violen o intenten violar los servicios que brinda CICOM (el nodo central de la universidad).

❖ Se prohíbe el uso de los medios informáticos para almacenamiento, ejecución o reproducción de juegos, música y videos que no tengan que ver con el objeto social de la oficina o departamento.

❖ Al recibir una PC en una oficina o local independiente, se realizarán las pruebas correspondientes a su funcionamiento y será recibida por la persona responsable del medio asignado.

2.2 Exigencias que debe cumplir el responsable del equipo.

❖ Deben tener una preparación adecuada para el uso del medio informático.

❖ Deben controlar diariamente los recursos Informáticos que están bajo su custodia y hacer marcado énfasis en la integridad de los sellos de seguridad que coloca el taller central o COPEXTEL.

❖ Debe brindar protección a los usuarios que acceden a INTERNET y al correo de la Universidad desde su equipo.

- Evitar que las cuentas y contraseñas de acceso a INTERNET o correo electrónico queden registradas de forma automática en los exploradores de Internet.

- Exigir a los diferentes usuarios que sus contraseñas sean seguras y cumplan las normas para su confección.

- Garantizar que no existan instalados KEYLOGGER o programas piratas que obtienen esta información.

- Deben revisar con programas antivirus los medios extraíbles que se pretendan introducir en su equipo para evitar que sea contaminado por programas malignos.
- Deben realizar mantenimiento sistemático al equipo para aumentar su rendimiento.

- Limpiar registros, ficheros temporales, historial de navegación por Internet y contraseñas guardadas.
- Desfragmentar
- Quitar elementos innecesarios del menú inicio. Así como información innecesaria (Liberación de espacio en disco)
- Usar temas y apariencias del sistema operativo acordes con la institución y que no malgasten recursos de memoria.

2.3 Exigencias que debe cumplir el responsable del equipo respecto a las salvas de información

- Realizar todos los viernes de cada semana, copias de seguridad de la información más importante almacenada en su equipo en CD, DVD y en el espacio del FTP habilitado en los servidores del nodo de la universidad.

Este reglamento forma parte del plan de seguridad informática aprobado para nuestra Universidad. El cumplimiento del mismo será motivo de análisis en los encuentros mensuales del grupo de seguridad informática y se tomará como base para las inspecciones que se realicen a los diferentes laboratorios oficinas y departamentos de la Universidad.

Aprobado por:

_____ _____

Lic. Issel Puig González — Especialista de Seguridad Informática

Dr. C Alejandro Miguel Rodríguez Cuervo — Director de Informatización

_____

Dr. C Deysí Fraga Cedré
Rectora

ANEXO 8

PROGRAMA DE SEGURIDAD INFORMÁTICA.

El programa de Seguridad Informática que se ha concebido tiene previstas las siguientes tareas:

1.- Actualización e implantación del Plan de Seguridad Informática.
Responsable: Rectora
Participa: Director de informatización, especialista y activistas de Seguridad Informática de las áreas y director del nodo.
Plazo: septiembre 2017.

2.- Dar a conocer, según corresponda, las Medidas de Seguridad Informática y de Recuperación al personal que trabaja con las Tecnologías de la Información.
Responsable: Director de informatización, Director de Economía y Servicio
Participan: Director del nodo, especialista y activistas de Seguridad Informática de las áreas y Jefes y administradores de las áreas.
Plazo: Durante el curso escolar

3.- Elaboración del Plan de Auditoria de la Seguridad Informática.
Responsable: Especialista de Seguridad Informática
Participa: Director de informatización, Equipo Auditor
Plazo: octubre 2017.

4.- Elaboración e implantación de los Registros definidos en el Plan de Seguridad Informática.
Responsable: Especialista y activistas de Seguridad Informática de las áreas.
Participa: Especialista y activistas de Seguridad Informática de las áreas.
Plazo: noviembre 2017.

5.- Elaboración del Plan de Capacitación y de reuniones con el personal en materia de seguridad informática, incluyendo la capacitación personal activista de Seguridad Informática.
Responsable: Director de informatización y especialista de Seguridad Informática
Participan: Especialista de Seguridad Informática y Director del nodo.
Plazo: Junio-julio 2018

6.- Elaboración del Plan del presupuesto sobre las necesidades del nodo, para ser incluidos en el plan de la Universidad.
Responsable: Jefe del nodo
Participa: Administradores de la Red.
Plazo: Enero.

7.- Coordinar con otro centro o unidad de la misma entidad, el almacenamiento de las salvas externas mediante la firma de un convenio por escrito.
Responsable: Director de Economía y Servicios, Especialista de Seguridad y Protección.
Participa Especialista de Seguridad y Protección
Plazo: Junio-Julio

8.- Resolver los problemas de desactualización y falta de parches de seguridad existentes en los Sistemas Operativos de los servidores y estaciones de trabajo, así como las actualizaciones de las aplicaciones utilizadas en la universidad.
Responsable: Jefe del nodo y Administrador de la Red designado.
Participa: Administrador de la Red designado
Plazo: Enero-junio 2018

13.- Completar la incipiente Base de Software, incluyendo las copias de discos de rescate, discos de sistemas operativos y aplicaciones que se utilizan en la entidad.
Responsable: Jefe del nodo, Administrador de la Red designado y especialista de seguridad informática
Participa: Especialista de Seguridad Informática, Jefe del nodo y taller de servicios técnicos
Plazo: julio 2018

ANEXO 9

REGISTROS.

REGISTRO No. 1
REGISTRO DE SOFTWARE DE NUEVA ADQUISICION.

No. Consecutivo
Nombre del Software
Fecha de Adquisición
Vía utilizada para ello
Soporte: tipo y cantidad
Nombre de quién lo adquirió

El especialista de Seguridad Informática en la medida que se vayan adquiriendo los softwares, tendrá que anotar el número consecutivo que le corresponda (se inicia en 1), nombre de los mismos, la fecha en que llegan a la entidad, la vía por la que llegaron, ya sea una compra, donación, a través de terceros, etc.
Igualmente se hará constar en que soporte llegó: disquete, disco compacto, etc. y la cantidad de ellos.
Por último, consignará el nombre de la persona que lo adquirió (ya sea el que hizo la compra o el que lo trajo).

REGISTRO No. 2
REGISTRO DE ACCESO DE LOS USUARIOS DE LAS PC DE LOS LABORATORIOS O COMPUTADORAS UBICADAS EN OFICINAS INDEPENDIENTES.
Todo trabajador o estudiante o personal ajeno a la Universidad y autorizado por el jefe del área que hagan uso de las PC de los laboratorios o computadoras ubicadas en oficinas independientes, en estos locales se contará con un registro de acceso a la computadora que corresponda, tiene la finalidad de controlar a todo el personal que haga uso de las computadoras.
Procedimiento para el control de acceso a las computadoras.

- Se habilitará el registro de control de acceso según el siguiente formato.

Local o Laboratorio

Nombre y apellidos	No Identidad	Hora de entrada	PC en la que trabaja	Hora de salida	Firma del Usuario	Observaciones

Observaciones: se anotan por el técnico de laboratorio o responsable del medio, al observar las actividades que realiza el usuario.
Por ejemplo:

- Uso correo electrónico.
- Búsqueda y descarga de información en Internet o la Intranet cubana o Portal Varona.
- Preparación de presentaciones electrónicas.
- Trabajo en tesis de Maestría o Doctorado.
- Preparación de artículos científicos.
- Análisis de materiales digitalizados (revistas, tesis, libros).

Entre otras.

- Es registro de control de acceso será llenado de forma sistemática en todos los locales que posean recursos informáticos.

REGISTRO No. 3
REGISTRO DE CONTROL DE SOPORTES

No. Consecutivo
Contenido fundamental del soporte
Trabajo para el que se destina el soporte

Nivel de acceso del soporte
Fecha y hora de entrada
Fecha y hora de baja
Observaciones

Se habilitará este registro que se encontrará junto a los soportes en el lugar donde se almacenan. En el control de soportes se deben identificar los correspondientes a la Base de Software y los de la salva de información.
En ellos se consignará el número del soporte, que debe coincidir con el que se encuentra en su etiqueta, el contenido fundamental del soporte (nombres de ficheros y archivos que contenga), que también coincidirá con los que tiene en la etiqueta, trabajo para el que se destina el soporte (ya sea copia de software originales, salva diaria, etc.). Asimismo, anotará el nivel de acceso del soporte (clasificación según Decreto Ley 199/99 sobre la Seguridad y Protección de la Información Oficial del Consejo de Estado) y la fecha y hora de entrada del soporte.
Dado que el soporte se deteriore a tal grado que implique su baja, se hará constar en el registro.

En Observaciones se anotará cualquier dato que no se recoja en las anotaciones anteriores y se considere importante. Las anotaciones sobre el contenido del soporte deben hacerse a lápiz, con vistas a que se pueda actualizar en caso necesario.

REGISTRO No. 4
REGISTRO DE ENTRADA, SALIDA Y MOVIMIENTO DE TECNOLOGIAS DE INFORMACION.

Fecha
Datos del Equipo: Tipo, Marca, Modelo, Configuración
Procedencia
Destino
Motivo del movimiento
Nombre de quien autoriza
Firma de quien autoriza

Se habilitará un registro que tendrá que llenarse por el activista o especialista de Seguridad Informática cada vez que se realice un movimiento de las tecnologías informáticas hacia o desde fuera del centro.
Se debe consignar la fecha del movimiento, datos del equipo objeto del movimiento, de qué lugar se extrae o proviene y a qué lugar se lleva, motivo por el que se realiza el movimiento (ejemplo: evento, exposición, reparación, etc.).
Por último, la persona que autoriza el movimiento escribirá su nombre y estampará la firma.

REGISTRO No. 5
REGISTRO DE MANTENIMIENTOS A EQUIPOS.

Área
Equipo
Fecha
Nombre del técnico
Labor realizada
Observaciones

Deberá ser llenado por el técnico que realiza la tarea cada vez que se persone en la entidad y realice el mantenimiento o la reparación de algún equipo.
Consignará el equipo específico que es objeto del trabajo, la fecha en que realiza la labor, su nombre y apellidos y la tarea realizada.
En observaciones agregará cualquier dato que pueda resultar importante. Por ejemplo: En caso de que sea necesario sacar el equipo del local se hará constar aquí ese movimiento (independientemente que se deban realizar a su vez anotaciones en el Registro de entrada, salida y movimiento de Tecnologías de Información).

REGISTRO No. 6
REGISTRO DE INCIDENCIAS.

No. consecutivo
Fecha
Hora
Área
Hecho detectado
Forma de detección
Medidas tomadas
Observaciones

Se creará un registro por el Responsable de Seguridad Informática donde se anotarán los hechos considerados como incidencias para la seguridad informática. Es como un historial de cómo se comporta la actividad de Seguridad Informática.
Aunque normalmente será actualizado por el Responsable de Seguridad Informática, también se concibe que el administrador de la red realice anotaciones en el mismo.
Cada hecho detectado recibirá un número consecutivo que se inicia en 1, anotándose la fecha y hora en que se descubrió.
Se describirá lo más explícitamente posible las características del hecho detectado, asimismo quedará claro la forma en que se detectó: durante una inspección, auditoría, reportado por alguna persona, casualmente).
Finalmente se mencionarán las medidas tomadas para corregir o enmendar el error, y en Observaciones se hará constar cualquier otro dato adicional que aporte elementos para el análisis del hecho.

REGISTRO No. 7

REGISTRO DE SALVAS.
Área:
No.
Fecha y Hora de la Salva
Sistema/software o Información salvada
Identificación del disquete, CD, flash u otro soporte
Realizada por:
Se habilitará este registro en cada lugar donde se realicen salvas de información. La persona que realiza la actividad se encargará de mantenerlo actualizado.
La primera columna corresponde a un número consecutivo que comienza en 1. A continuación se consigna la fecha y hora en que se realiza la salva, el nombre del sistema, software o información específica salvada y los datos que permitan identificar el soporte en que se realiza la salva.
Por último, se consignará el nombre de la persona que realiza la operación.

REGISTRO No. 8
REGISTRO DE INSPECCIONES

Fecha de la Inspección.
Área objeto de la inspección
Participantes
Situaciones Detectadas
Plan de Medidas
Responsables del Cumplimiento
Fecha de cumplimiento

Cada vez que el Responsable de Seguridad Informática realice una prueba de inspección anotará la fecha, el área objeto de la misma, las personas que participan de la inspección (de creerse necesario invitar alguna persona para ello).

En la columna Situaciones Detectadas, escribirá lo más detalladamente posible los problemas encontrados durante el desarrollo de la inspección.
En las columnas siguientes sólo consignará datos de haber encontrado algún problema. Ellas son:

- Plan de Medidas: Aquí enumerará las medidas que considera oportunas para eliminar la situación detectada. Tratará de no ser general, sino todo lo contrario: en caso de que existan varias personas afectadas, dirá qué tiene que hacer cada cual.
- Responsables del cumplimiento: Mencionará las personas responsables de cumplir con la medida.

Fecha de cumplimiento: Se refiere a la fecha tope en que el problema tiene que ser resuelto

REGISTRO No. 9
REGISTRO DE SOFTWARE AUTORIZADO.

Equipo: _____

Relación de software autorizado a permanecer en dicho equipo
Nombre y apellidos de quien instala el software
Fecha de Instalación
Firma del Responsable de Seguridad Informática

Para cada una de las máquinas, el Responsable de Seguridad Informática, relacionará los softwares autorizados a permanecer en ésta, después que se haya decidido de forma colegiada con el Jefe de Área. Para cada software se debe especificar el nombre de la persona que lo instaló y la fecha en que lo hizo. Este registro, inicialmente y para cobrar validez, debe ser avalado por el Responsable de Seguridad Informática, quien será el encargado de incorporar posteriormente los nuevos softwares que se autoricen en cada una de las máquinas bajo su custodia.

LICENCIA No: 10738
VALOR: 100 CUP
NP: 622-0283

REPÚBLICA DE CUBA

MINISTERIO DE COMUNICACIONES

Unidad Presupuestada Técnica de Control del Espectro Radioeléctrico

Conforme a lo establecido en la Resolución No. 128/11 del Ministro de la Informática y las Comunicaciones, de fecha 16 de Agosto de 2011 se expide la presente licencia, que autoriza la operación de una Red Privada de Datos a la entidad:

Universidad de Ciencias Pedagógicas "Enrique José Varona"

Inscrita en el Registro de Proveedores de Servicios en el Entorno de Internet de este Ministerio con el Expediente No 6,528. Dicha red es de alcance Local o de Campo, con ubicación de su nodo principal en Centro de Informática y Comunicaciones CICOM, Calle 108 No. 29E08 e/29E y 29F Ciudad Escolar Libertad, Marianao. Edificio Central, Primer Piso.

Esta Licencia se concede por un término de dos (2) años, a partir de la fecha de su expedición y deberá ser renovada dentro de los treinta (30) días hábiles anteriores a su vencimiento.

Dado en La Habana, a los 7 días del mes de Junio del 2017

Director del Centro de Control de Trámites
UPTCER La Habana

Recibe: Jesús Ramón Vasco Capote
No. CI o Pasaporte: 57060/10/27
Fecha: 29/6/2017

OSC

El Ministro de Educación Superior

Lectura ETECSA

La Habana, 27 de abril de 2017
"Año 59 de la Revolución"

Fc. Walter 3/5/17

Ca Mayra Arevich Marin
Presidenta
ETECSA

Estimada compañera

Por medio de la presente y debido a los cambios ocurridos en la denominación de algunas de nuestras instituciones y en sus direcciones, estamos renovando la solicitud del acceso a los servicios de Internet, de nuestro Ministerio de Educación Superior

Debido a la importancia que tiene el acceso a Internet para el desarrollo de los procesos sustantivos de la Educacion Superior y las caracteristicas de gestión de nuestro ministerio, faculto a cada Rector(a) y Director(a) que aparece en la siguiente lista para la firma de los respectivos contratos con su empresa

1 Universidad de Pinar del Rio - (UPR)
Rector: York Mayor Hernández

2 Universidad de Artemisa - (UART)
Rector: Carlos E. Suarez Ponciano

3 Universidad de La Habana - (UH)
Rector: Gustavo Jose Cobreiro Suárez

4 Universidad Tecnologica de La Habana José Antonio Echeverria - (Cujae)
Rectora: Alicia Alonso Becerra

5 Universidad de Ciencias Informaticas - (UCI)
Rectora: Miriam Nicado Garcia

6 Escuela Superior de Cuadros del Estado y del Gobierno - (ESCEG)
Rectora: Mercedes Delgado Fernández

7 Universidad de las Ciencias de la Cultura Fisica y el Deporte - (UCCFD)
Rector: Héctor Noa Cuadro

624
2/5/17

El Ministro de Educación Superior

8 Universidad de las Ciencias Pedagógicas Enrique José Varona (UCPEJV)
Rectora: Deysi Fraga Cedré

9 Instituto Superior de Diseño – (ISDi)
Director General: Sergio Peña Martínez

10 Instituto Superior de Tecnología y Ciencias Aplicadas – (INsTEC)
Directora General: Bárbara Garea Moreda

11 Universidad de la Isla de la Juventud - (UIJ)
Rector: Leonardo Cruz Cabrera

12 Universidad Agraria de La Habana - (UNAH)
Rectora: Adianez Taboada Zamora

13 Instituto Nacional de Ciencias Agrícolas - (INCA)
Directora General: María del Carmen Pérez Hernández

14 Instituto de Ciencia Animal - (ICA)
Director General: José Andrés Díaz Untoria

15 Centro Nacional de Sanidad Agropecuaria - (CENSA)
Directora General: Ondina León Díaz

16 Universidad de Matanzas - (UM)
Rector: Lewis Finalé de la Cruz

17 Estación Experimental de Pastos y Forrajes Indio Hatuey - (EEPFIH)
Director General: Giraldo Jesús Martín Martín

18 Universidad de Cienfuegos - (UCf)
Rector: Juan B. Cogollo Martínez

19 Universidad Central Marta Abreu de Las Villas - (UCLV)
Rector: Andrés Castro Alegría

20 Universidad de Sancti Spíritus - (UNISS)
Rectora: Naima Ariatne Trujillo Barreto

21 Universidad de Ciego de Ávila - (UNICA)
Rectora: Anisia Ruiz Gutiérrez

El Ministro de Educación Superior

22 Universidad de Camaguey - (UC)
Rector: Santiago Lajes Choy

23 Universidad de Las Tunas - (ULT)
Rectora: Aurora del Carmen Ramos de Las Heras

24 Universidad de Holguin - (UHO)
Rector: Reynaldo Velázquez Zaldivar

25 Instituto Superior Minero Metalurgico de Moa - (ISMMM)
Rector: Angel Oscar Columbié Navarro

26 Universidad de Granma - (UG)
Rectora: Narcy Bueno Figueras

27 Universidad de Oriente - (UO)
Rectora: Martha del Carmen Mesa Valenciano

28 Universidad de Guantanamo - (UG)
Rector: Alberto Turro Breff

28 Organo Central
Director: Mario Manuel Ares Sánchez

Fraternalmente.

Jose Ramón Saborido Loidi

Ref RS OM 645
tmd

UCP

UNIVERSIDAD DE CIENCIAS PEDAGOGICAS
"ENRIQUE JOSÉ VARONA"

CONVENIO DE COLABORACIÓN INSTITUCIONAL.

DE UNA PARTE: La Universidad de Ciencias Pedagógicas Enrique José Varona, (UCPEJV), representada por la Dr. C Deysi Fraga Cedré Rectora con correo electrónico, rectorado@ucpejv.edu.cu, Telf. 72671083, de conformidad con el nombramiento expedido a su favor por Resolución Rectoral No. 66/16 de fecha 30 de agosto de 2016, en términos por los cuales se encuentra facultada para firmar el presente Convenio con domicilio legal de la (UCPEJV) en calle 108, No 2E089, e/ 29F y 29E, Ciudad Escolar, municipio Marianao, provincia, La Habana.

DE LA OTRA PARTE: La Dirección Provincial de Educación de La Habana, con domicilio legal en calle 22, No. 111 e/ 1era y 3era, municipio Playa, provincia La Habana, representada en este acto por Yanet Hernández Pérez en su carácter de Directora Provincial de Educación, teléfono 7-206-4232, correo electrónico yanet@pd.rimed.cu,

AMBAS PARTES:Considerando el interés de las instituciones que representan y de mantener las relaciones de cooperación entre ellas, pactan el siguiente **Convenio de Colaboración Institucional**, reconociéndose mutuamente el carácter y facultades con que comparecen, convienen y acuerdan las siguientes **Cláusulas**:

Cláusula Primera: El presente Convenio tiene por objeto brindar por parte de la Universidad de Ciencias Pedagógicas "Enrique José Varona (UCPEJV), los servicios en el campo de la informática que han venido utilizando dependencias que pertenecen a la Dirección Municipal de Educación.

Cláusula Segunda: La Universidad de Ciencias Pedagógicas "Enrique José Varona (UCPEJV), se compromete a brindar el servicio en el campo de la informática a las dependencia que pertenecen a la Dirección Municipal de Educación del municipio Marianao: tales como la Biblioteca Orestes Gutiérrez Escalona, la Residencia de Profesores Villa Varona y la Escuela Especial Dora Alonso.

Cláusula Tercera: Los servicios referidos están regulados por lo dispuesto en la Resolución No 127/07 de fecha 30 de julio de 2007 Reglamento de Seguridad para la Tecnologías de la Información del Ministerio de la Informática y las Comunicaciones, que trata todo lo relacionado con la Seguridad Informática, así como todo lo dispuesto por la Resolución Rectoral No. 20/2017, de fecha 13 de febrero de 2017 que regula, a todo lo relacionado con el uso de nuestra red informática por los diferentes usuarios, que sean autorizados, por la autoridad competente a este nivel.

Cláusula Cuarta: Es responsabilidad de la Dirección Municipal de Educación del municipio Marianao, **cuidar y brindar la debida seguridad y protección a los equipos propiedad de la Universidad de Ciencias Pedagógicas "Enrique José Varona", (UCPEJV)**, que son usados por los usuarios de esa Dirección, en el lugar donde están ubicados, cualquier sustracción o deterioro que sufran los equipos mencionado, da lugar al total retiro de este, sin posterior reposición del mismo.

Cláusula Quinta: Cualquier violación de la Seguridad Informática, se viole el equipamiento o se sustraigan sus componentes, por parte de los usuarios de estas dependencias, que controla y regula la referida Dirección Municipal, se retirará automáticamente totalmente este servicio.

Cláusula Sexta: El presente Convenio tendrá vigencia por cinco (5) años a partir de la firma del mismo, que consta de tres (3) ejemplares del mismo valor y fuerza legal.

Y para que así conste, se firma el presente a los 4 días del mes de septiembre de 2017, "año 59 de la Revolución".

Por la UCPEJV.

Dr.C Deysi Fraga Cedré
Rectora.

RECTORIA

Por la DPE.

Yanet Hernández Pérez
Directora Provincial de Educación