MANUAL DE PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DE LAS POLÍTICAS Y MEDIDAS REFERIDAS A LA SEGURIDAD INFORMÁRICA EN LA UNIVERSIDAD DE CIENCIAS PEDAGOGICAS ENRIQUE JOSÉ VARONA

Categoría de este documento

El presente manual de procedimientos tiene por objetivo facilitar a los diferentes usuarios y directivos las acciones a realizar para el uso de las tecnologías de la información y las comunicaciones de la Universidad.

Constituye un complemento a lo exigido en el Reglamento de Seguridad para las Tecnologías de la Información puesto en vigor por la Resolución 128 de 2019 del Ministro de la Informática y las Comunicaciones en cuanto a la obligación de diseñar, implantar y mantener actualizado un Sistema de Seguridad Informática y los procedimientos a partir de los bienes a proteger y de los riesgos a que están sometidos. Además de lo establecido en la Instrucción 1 del MES de 2016, que traza las políticas y procedimientos que se deben tener en cuenta para el uso y seguridad de los medios informáticos y los servicios de redes con que cuenta el Ministerio de Educación Superior y así cumplir con lo que establece dichas Resoluciones.

Objetivo.

Contar con un documento que regule el uso de los medios informáticos y el acceso a los servicios básicos que se brindan en la Red Informática de la Universidad de Ciencias Pedagógicas Enrique José Varona y la protección de la misma.

Alcance
Universidad de Ciencias Pedagógicas Enrique José Varona.
Índice de procedimientos.

7. Procedimiento para el registro de acceso de los usuarios de las PC de los laboratorios o computadoras ubicadas en oficinas independientes.
8. Procedimiento para el uso de dispositivos externos en las PC.
9. Procedimientos para actuar ante la presencia de un virus informático.
10. Procedimientos para el reporte de roturas de equipos y atención por parte del técnico.
11. Procedimiento para el control y reporte de incidentes de seguridad informática
12. Procedimiento para el control de los componentes internos de cada PC y los software instalados.
13. Procedimientos para la configuración de las contraseñas de autentificación en la Red y sus servicios.
14. Procedimiento para la actualización de los parches de seguridad de los sistemas operativos, y plataformas de educación a distancia y de los sitios Web.
15. Procedimiento para las salvas de información de los logs de navegación, plataformas de educación a distancia y los sitios Web.
16. Procedimiento para la actualización del antivirus y parches de seguridad del sistema operativo de las PC que se utilizan en la universidad.
17. Procedimientos para el escaneo de la Red de la Universidad.
18. Procedimientos para el sistema de control de la seguridad informática por los cuadros de dirección de la Universidad en sus áreas de responsabilidad.
19. Procedimiento al adquirir equipos informáticos en la Universidad.
20. Procedimiento para la salida y traslado de equipos informáticos fuera de la universidad.
21. Procedimiento: Control del uso de los dispositivos móviles
22. Procedimiento para el uso de los servicios Wifi.

Explicación de los procedimientos.

1. Caracterización del sistema informático del área.

Para realizar la caracterización del sistema informático de cada área se tuvieron en cuenta los siguientes elementos.

Objeto social del área.
Cantidad de PC con que se cuenta y locales donde están ubicadas.
Servicios que se prestan con el uso de las TIC.
Caracterización del personal en cuanto a su preparación en informática y en temas de seguridad informática.
Principales vulnerabilidades y riesgos al sistema informático, ordenados por nivel de importancia. Medidas, procedimientos y responsabilidades derivadas del análisis anterior. Sistema de control.

Para la realización del análisis anterior se tuvieron en cuenta los siguientes escenarios de acuerdo a la presencia de las PC, su utilización y responsabilidad o cargo del usuario que utiliza las PC.

Los escenarios son los siguientes:

1. PC por cada usuario (accede un solo usuario)
2. PC utilizada por varios usuarios (departamentos, otras oficinas, etc.).
3. Laboratorios

A partir de lo anterior las PC se agrupan por:

La información que se procesa
Cargo del usuario que la trabaja

Para el escenario 1 se incluyeron las 5 Clases, para el 2 se tuvieron en cuenta según sus funciones las clases B-C y F, donde se deben cumplir las siguientes condiciones para prevenir y preservar la información.

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.

Este grupo deberá cumplir con las siguientes condiciones de Seguridad Informática:

Nivel de acceso en la PC:

Administrador, usuario avanzado.
Debe estar habilitado la contraseña del SETUP
Debe inhabilitarse el inicio por torre de CD o DVD.

Nivel de acceso por los usuarios:

Solamente los cros. autorizados a procesar está información, técnicos informáticos e instaladores.

Las contraseñas de acceso a la PC deben cumplir con las siguientes características:

Más de 8 caracteres
Combinación de símbolos, números, mayúsculas, minúsculas y caracteres especiales.

Tipo de conexión:

Las PC que procesan información clasificada o limitada no puede estar conectada a la red.
Cada dirección que procese información clasificada o limitada, debe contar con una máquina destinada al tratamiento de la misma, independiente de la red.

Documentos compartidos:

No se podrán compartir carpetas en estas máquinas y los recursos que se compartan, como la impresora, deberán contar con contraseñas.

Privilegios de usuario:

Los usuarios de inicio de sesión que procesan esta información serán limitados, solo tendrán acceso los autorizados. **Salvas, periodicidad y cantidad de copias:**

En este caso se tendrá en cuenta lo establecido en la Resolución 127/07, en el Capítulo III, Sección V, Respaldo de la Información, artículos 54-56.

Para la protección de información en caso de salida del equipamiento de la instalación por reparación o rotura, se deberá en el caso de traslado interno o externo salvar la información a otro soporte como disco externo, memoria flash y otros aditamentos que sean necesarios.

En caso de la salida del equipamiento para mantenimiento o rotura, se deberá salvar la información en soporte extraíble u otro aditamento. En caso de no poder resguardar la información, se debe custodiar el disco duro por parte del usuario hasta el lugar donde se repare y realizar las salvas.

Soporte de almacenamiento:

Los dispositivos de almacenamiento para usarse en las máquinas serán solamente los autorizados y se anotarán en el registro de **Control de soportes extraíbles**.

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 económica.
4. PC con información de Proyectos con Instituciones Internacionales o con investigaciones sociales de gran impacto en la sociedad.

Este grupo deberá cumplir con las siguientes condiciones de Seguridad Informática: Nivel de acceso en la PC:

Administrador, usuario avanzado. **Nivel de acceso por usuario:**

Se crearán cuentas de usuarios como sean necesarias para los usuarios del área.

En el caso de personal ajeno al centro y debidamente autorizado se le creará una sesión de invitado.

Las contraseñas de acceso a la PC deben cumplir con las siguientes características:

Se tendrá en cuenta lo establecido en la Resolución 127/07, Capítulo III, Sección V, Identificación, autentificación y control de accesos, artículo 47. Más de 8 caracteres, combinación de símbolos, números, mayúsculas, minúsculas y caracteres especiales.

Tipo de conexión:

Las PC que se encuentran en este grupo pueden estar conectada a la red.

Documentos compartidos:

No se podrán compartir carpetas en estas máquinas y los recursos que se compartan, como la impresora, deberán contar con contraseñas.

Para el acceso a una información que sea de interés para el trabajo, se creará un lugar público controlado (FTP público del área, carpeta ubicada en la partición de trabajo), donde se ubicará dicha información para que pueda ser compartida.

Privilegios de usuario:

Los usuarios que procesan está información son simples.

Salvas, periodicidad y cantidad de copias:

En este caso se tendrá en cuenta lo establecido en la Resolución 127/07, en el Capítulo III, Sección V, respaldo de la información, artículos 54-56.

Para la protección de información en caso de salida del equipamiento de la instalación por reparación o rotura, se deberá en el caso de traslado interno o externo salvar la información a otro soporte como disco externo, memoria flash y otros aditamentos que sean necesarios.

En caso de la salida del equipamiento para mantenimiento o rotura, se deberá salvar la información en soporte extraíble u otro aditamento que sean necesarios. En caso de no poderse salvar, se debe custodiar el disco duro por parte del usuario hasta el lugar donde se repare y realizar las salvas.

Soporte de almacenamiento:

Los dispositivos de almacenamiento se revisarán contra virus y se anotarán en el registro de control de soportes extraíbles.

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.

Este grupo deberá cumplir con las siguientes condiciones de Seguridad Informática: Nivel de acceso en la PC:

Administrador, usuario avanzado **Nivel de acceso por usuario:**

Solamente los cros. autorizados a procesar está información.

Las contraseñas de acceso a la PC deben cumplir con las siguientes características:

Se tendrá en cuenta lo establecido en la Resolución 127/07, Capítulo III, Sección V, Identificación, autentificación y control de accesos, artículo 47. Más de 8 caracteres, combinación de símbolos, números, mayúsculas, minúsculas y caracteres especiales.

Tipo de conexión:

La PC que contenga este tipo de información no puede estar conectada a la red. **Documentos compartidos:**

Las carpetas compartidas tendrán contraseñas al igual que los recursos que se compartan, como la impresora. **Salvas, periodicidad y cantidad de copias:**

En este caso se harán dos copias y la periodicidad la determina el usuario, no mayor de tres meses.

Para la protección de información en caso de salida del equipamiento de la instalación por reparación o rotura, se deberá en el caso de traslado interno o externo salvar la información a otro soporte como disco externo, memoria flash y otros aditamentos que sean necesarios.

Soporte de almacenamiento:

Los dispositivos de almacenamiento se revisarán contra virus y se anotarán en el registro de Control de soportes extraíbles.

Clase D:

1. PC que trabajan o procesan información relacionada con la gestión contable y financiera. **Este grupo deberá**

cumplir con las siguientes condiciones de Seguridad Informática: Nivel de acceso en la PC:

Administrador, contador principal y usuario avanzado **Nivel de acceso por usuario:**

Solamente los cros. del área que estén autorizados, la Rectora y el Vicerrector de Economía y Servicios, no están autorizados usuarios que no sean trabajadores del área.

Las contraseñas de acceso a la PC deben cumplir con las siguientes características:

Más de 8 caracteres

Combinaciones de números, mayúsculas, minúsculas y caracteres especiales. **Tipo de conexión:**

La PC estarán fuera de la red de la entidad y conectada en una red local interna, con un switch independiente.

Documentos compartidos:

Las carpetas compartidas serán solamente entre los cos. del área.

Salvas, periodicidad y cantidad de copias:

Las establecidas en los registros correspondientes y cumpliendo con lo establecido en la Resolución 128/19, en el Capítulo III, Sección V, respaldo de la información, artículos 54-56.

En caso de salida del equipamiento de la instalación por reparación o rotura, se deberá en el caso de traslado interno o externo salvar la información a otro soporte como disco externo, memoria flash y otros aditamentos que sean necesarios.

Soporte de almacenamiento:

Los dispositivos de almacenamiento se revisarán contra virus y se anotarán en el registro de Control de soportes extraíbles.

Clase E:

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

Este grupo deberá cumplir con las siguientes condiciones de Seguridad Informática: Nivel de acceso en la PC:

Administrador, usuario avanzado **Nivel de acceso por usuario:**

Solamente los cros. autorizados

Las contraseñas de acceso a la PC deben cumplir con las siguientes características:

Más de 8 caracteres

Combinación de símbolos, números, mayúsculas, minúsculas y caracteres especiales.

Documentos compartidos:

No se podrán compartir carpetas en estas máquinas y los recursos que se compartan, como la impresora, deberán contar con contraseñas.

Salvas, periodicidad y cantidad de copias:

En este caso se tendrá en cuenta lo establecido en la Resolución 127/07, en el Capítulo III, Sección V, Respaldo de la Información, artículos 54-56.

En el caso de los servidores se cumplirá con lo que está establecido Soporte de almacenamiento:

Los dispositivos de almacenamiento se revisarán contra virus y se anotarán en el registro de control de soportes extraíbles.

Clase F:

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

Este grupo deberá cumplir con las siguientes condiciones de Seguridad Informática: **Nivel de acceso en la PC:**

Administrador, usuario limitado, invitado limitado

Nivel de acceso por usuario:

Usuarios comunes

Las contraseñas de acceso a la PC deben cumplir con las siguientes características:

Se tendrá en cuenta lo establecido en la Resolución 128/19, Capítulo III, Sección V, Identificación, autentificación y control de accesos, artículo 47.

Tipo de conexión:

La PC puede estar conectada a la red. **Documentos compartidos:**

Las carpetas compartidas tendrán contraseñas al igual que los recursos que se compartan, como la impresora. **Salvas, periodicidad y cantidad de copias:**

Información que sea necesaria mantener salvadas, dos copias y la periodicidad es determinada por el usuario. En caso Para la protección de información en caso de salida del equipamiento de la instalación por reparación o rotura, se deberá en el caso de traslado

interno o externo salvar la información a otro soporte como disco externo, memoria flash y otros aditamentos que sean necesarios.

Soporte de almacenamiento:

Los dispositivos de almacenamiento se revisarán ante virus y se anotarán en el registro de Control de soportes extraíbles.

2. Procedimiento para el uso del controlador de dominio.

El controlador de dominio es una medida técnica, que tributa aún mejor uso de los recursos y servicios de la Red informática de la Universidad, por ello será administrado desde el nodo central.

La administración del controlador de dominio será por el jefe del nodo y un administrador de red seleccionado. Se tendrá una clave de acceso para la administración del controlador de dominio, que será del conocimiento del jefe del nodo y del administrador de red designado.

En el caso de que un usuario necesite instalar o modificar el sistema de una PC o de las computadoras de un laboratorio por necesidades de trabajo, se realizará esta solicitud por la vía de su jefe administrativo, el cual notificará al Director del nodo o al administrador de red encargado del controlador de dominio para que haga las modificaciones o instalaciones necesarias y el tiempo que se necesitan mantener.

Una vez que la solicitud realizada para instalar o modificar el sistema de una PC o de las computadoras de un laboratorio, esté notificada al jefe del nodo o administrador encargado del controlador de dominio, tendrán 24 horas para implementar los cambios solicitados.

Una vez realizados los cambios, los usuarios tendrán disponible los servicios por el tiempo solicitado, al día siguiente del tiempo estipulado, serán cancelados por el administrador del nodo encargado de administrar en controlador de dominio.

El en caso del Centro de Software Educativo, por la variedad de sistemas y herramientas que utilizan para sus actividades de programación e implementación aplicaciones educativas, el jefe del Dpto., tendrá una clave de administración del controlador de dominio, que será personal e intransferible.

El Jefe del Centro de Software Educativo, con está clave, será la única persona autorizada a instalar o modificar las PC, de su Dpto., por motivos de trabajo, y dejará constancia de los cambios realizados en el registro de incidencias de su área.

3. Procedimiento para las salvas de información.

Es responsabilidad de cada usuario de las TI de la Universidad realizar las salvas de la información más importante de la actividad profesional que realiza, en el caso de las facultades, áreas y departamentos,

los jefes serán los máximos responsables de garantizar que las salvas de la información más importante de su área de responsabilidad se realicen con la calidad y periodicidad requerida, esto permitirá resguardar el patrimonio histórico de la Universidad, en formato digital y en copia dura (impresa).

Para ello todas las áreas realizarán lo siguiente:

- ✓ Seleccionaran y ubicarán la información más importante y que no se debe perder.

- ✓ Seleccionarán una persona responsable para realizar las salvas de la información seleccionada como importante e imprescindible resguardar.
- ✓ Todos los viernes cada 15 días, harán las salvas de la información en soporte digital CD o DVD y compactadas, habilitarles claves de lectura y escritura de acuerdo a su importancia y clasificación.
- ✓ Habilitar un local donde se guardarán las salvas de la información, con acceso restringido, solo a las personas autorizadas a tener acceso.
- ✓ Solicitar por escrito al Nodo de la Universidad, especio de FTP público o Privado para realizar salvas en el nodo central.
- ✓ Los jefes responsabilizarán por escrito la persona que tendrá acceso al FTP público o privado de la facultad y realizar las salvas, su actualización y borrado.
- ✓ Una vez habilitado este servicio del FTP, las áreas serán las responsables de lo que ocurra con la información contenida en ellos.
- ✓ Solo podrán ser subidos al FTP información compactada, no se admiten ficheros de música y vídeos.
- ✓ Se habilitará en cada área, facultad y Dpto. un registro de control de soportes de salvas que contendrá lo siguiente:

REGISTRO DE CONTROL DE SOPORTES DE SALVAS

No. Consecutivo

Contenido fundamental del soporte (Nombre de los ficheros salvados y extensión y las claves en caso que la tenga incorporada)

Trabajo para el que se destina el soporte (Se plasma si es en CD, CVD o FTP del Nodo) Nivel de acceso del soporte

Fecha y hora de realizada la salva y nombres y apellidos de la persona que realizó la salva. Fecha y hora de baja Observaciones

Se habilitará este registro y se mantendrá 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.

Las salvas se realizarán con una periodicidad mensual, en caso de que este tiempo sea menor o mayor será organizado por el jefe del área.

REGISTRO DE ENTREGA / RECEPCCIÓN DE SOPORTES MAGNÉTICOS CON SALVAS DE INFORMACIÓN O SOFTWARE.

No. del soporte magnético Contenido fundamental del soporte Entrega:

Nombre y firma de quien entrega el soporte Nombre y firma de quien recibe el soporte Objetivo

de utilización del soporte
Fecha y hora de entrega Recepción:
Nombre y firma de quien devuelve el soporte
Nombre y firma de quien recibe el soporte
Resultado de la comprobación contra la relación interna
Resultado de la revisión contra virus
Fecha y hora de recepción

Observaciones

4. Procedimiento para la habilitación de servicios a los usuarios de la Red.

Todo trabajador o estudiante que se incorpore a la Universidad, tiene los derechos de servicios que se establece en la Instrucción 1/2016 del Ministerio de Educación Superior, para que estos servicios sean habilitados, se procederá de la siguiente manera.

Para el caso de la incorporación de nuevos trabajadores, la Dirección de Recursos Humanos de la Universidad, al realizar la entrevista inicial con el trabajador y solicitarle la documentación establecida, incorporará el acta de compromiso del trabajador sobre el uso de los recursos informáticos de la Universidad, la cual será firmada por el trabajador y se incorpora a su expediente laboral.

Se coordinará con la DII, para que convoque una comisión que realizará una entrevista técnica al trabajador y comprobará sus conocimientos en informática y de seguridad informática, de ser suficientes sus conocimientos, se emite un documento por la DII que acredite que posee los conocimientos mínimos para utilizar los servicios de la Red de la Universidad, de no ser favorable los resultados de la entrevista, el trabajador debe recibir un curso de seguridad informática que lo habilite en estos contenido y será responsabilidad de la DII su organización y ejecución.

Si en trabajador recibe la certificación que lo acredita con los conocimientos mínimos, este documento lo presenta al jefe administrativo del área en la cual va a trabajar para que se proceda a la elaboración de la solicitud de servicios que le corresponde según Instrucción 1/2016 del MES .

El trabajador, entregará el documento recibido por la DII, que lo acredita que posee conocimientos mínimos de informática y de seguridad informática al Dirección de Recursos Humanos para que se archive en su expediente laboral.

El Jefe del área, Facultad o Departamentos, donde se incorpora el nuevo trabajador, elabora una carta dirigida a la DII firmada y acuñada, con los nombres y apellidos de las personas, solicitando la autorización de los servicios correspondientes de acuerdo a la resolución antes mencionada.

Una vez recibida la solicitud por la DII, de estar de acuerdo se firma y se acuña el documento, ubicando “estar de acuerdo” con lo solicitado, este documento, se envía al Nodo de la Universidad y será recibido por el cro (…….), el cual habilitará los servicios correspondientes y guardará en un file (archivo), la copia del documento de autorización en formato duro.

Este proceso se realizará cuando se comienza cada curso académico por parte de las áreas y el nodo central de la Universidad o en los momentos en que se incorpore un nuevo trabajador.

En el caso de los estudiantes, los Decanos de las Facultades, enviarán a la DII, la solicitud firmada y acuñada y adjuntan el listado con los datos de los estudiantes que se solicita dar servicios en la Red.

5. Procedimiento para la inhabilitación de servicios a los usuarios de la Red.

A los usuarios de la Red de la Universidad se les podrá inhabilitar los servicios, por haber cometido alguna indisciplina en el uso de la red y sus servicios asociados, por ejemplo, navegación por sitios no permitidos y que no tienen carácter educativo, utilización incorrecta del correo electrónico, utilizar PROXY anónimos para burlar los controles de seguridad del nodo, utilizar contraseñas de autentificación de otros usuarios. Los usuarios que sean detectados en alguna de las indisciplinas anteriores u otras, por parte de los administradores de la Red o los especialistas del grupo central de seguridad informática, se procederá de la forma siguiente:

Se notificará el hecho ocurrido por el personal del nodo o por los especialistas del Grupo Central de Seguridad Informática a la DII y al jefe administrativo de la persona involucrada, con imágenes tomadas del mismo y se plasmará en el registro de incidencias por vía correo ic@ucpejv.edu.cu. Se procederá de manera inmediata a inhabilitar y bloquearán los servicios que tiene asociada esa persona y los sitios por los cuales se encontraba navegando.
El jefe administrativo del usuario notificará en un tiempo no mayor de 72 horas a la DII las medidas tomadas por el hecho ocurrido.

Una vez notificada las medidas tomadas por el jefe administrativo a la DII, está orientará al nodo si es pertinente o no habilitar nuevamente los servicios correspondientes al usuario.

De no ser notificada las medidas administrativas tomadas con el usuario, por parte del jefe administrativo a la DII en el tiempo establecido, el personal del nodo inhabilitará totalmente la cuenta y los servicios de ese usuario.

6. Procedimiento para realizar la baja de los usuarios y sus servicios en la Red.

Las bajas de los trabajadores y estudiantes como usuarios de la Red, será responsabilidad en el caso de los estudiantes del Dpto. de Planeamiento y Estadística y en el caso los trabajadores del Dirección de Recursos Humanos de la Universidad. Para realizar este proceso se procederá de la siguiente manera.

Las Facultades y el Dpto. de Planeamiento y Estadística al inicio de cada curso académico (primera quincena de septiembre) entregarán al jefe del Nodo, el listado oficial de los estudiantes de su facultad, por carreras y año de estudio.
El jefe del Nodo con este listado comprobará la base de datos de los usuarios y dará bajas a todos aquellos que no aparezcan en el listado oficial entregado.

El Dpto. de Planeamiento y Estadística actualizará esta información mensualmente con el personal del nodo, En el caso de los trabajadores, el Dirección de Recursos Humanos de la Universidad al inicio de cada curso académico (primera quincena de septiembre) entregarán al jefe del Nodo, el listado oficial de bajas de los trabajadores de la Universidad.

El jefe del Nodo con este listado comprobará la base de datos de los usuarios y dará bajas a todos aquellos trabajadores informados en el listado oficial entregado.

La Dirección de Recursos Humanos actualizará esta información mensualmente con el personal del nodo.

7. Procedimiento para el 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.

N PC	NOMBRE Y APELLIDOS	NO DE INDENTIDAD	HORA ENTRADA	HORA SALIDA	FIRMA	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.

8. Procedimiento para el uso de dispositivos externos en las PC.

El uso de los dispositivos externos en la Universidad, es uno de los principales problemas que contribuyen en la diseminación de virus informáticos, con el objetivo de atenuar la proliferación de virus se establece lo siguiente. Procedimientos para el uso de dispositivos externos. El jefe máximo del área será el responsable de controlar que sean utilizados en las PC bajo su responsabilidad los dispositivos externos autorizados.

Solo podrán ser utilizados como dispositivos externos, las memorias flash, discos duros externos, cámaras de fotos digitales y HDD Player, teléfonos móviles, tablets ,laptops. No podrán ser utilizados otros dispositivos como, Ipoh, MP3, MP4.

En todas las áreas y laboratorios, se debe tener identificada una PC, como máquina de cuarentena, será la que se emplee, para revisar los dispositivos externos, antes de colocarlo en otro equipo.

Un usuario al llegar a un laboratorio o local independiente, el técnico del laboratorio o personal responsable del medio, será el máximo responsable de revisar minuciosamente el dispositivo externo autorizado, antes de colocarlo en una computadora.

Una vez comprobado que el dispositivo está limpio de virus, se autoriza al usuario a trabajar en la PC solicitada.

De comprobarse la presencia de un virus y no se pueda descontaminar, no se autoriza a utilizar el dispositivo en ninguna de las PC del local.

El hecho anterior se plasmará en el registro de incidencias del laboratorio o del local independiente, según el procedimiento que se establece para estos casos.

9. Procedimientos para actuar ante la presencia de un virus informático.

Todos los usuarios de los servicios de la Red de la Universidad, al detectar la presencia de un virus en la PC que está trabajando, debe informar de inmediato al técnico de laboratorio o al responsable del medio y en consecuencia actuar con el siguiente procedimiento.

Detener las conexiones en red de la PC infectada.

Reiniciar la PC y entrar con la opción de modo seguro o modo a prueba de fallo.

Si es posible, hacer copia de seguridad de sus archivos para poder compararlas con copias anteriores. Ejecutar un programa antivirus que este actualizado.

De no haber podido eliminar el virus, se debe formatear el disco duro a bajo nivel y si no le queda otra solución.

Para realizar esta operación debe hacerlo un especialista en informática, para ellos puede enviar su situación a la siguiente dirección 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.

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.

Plasmar el incidente en el Registro de incidencias y reportar al ic@ucpejv.edu.cu.

10. Procedimientos para el reporte de roturas de equipos y atención por parte del técnico..

Los administradores de las Facultades y de áreas serán los responsables de reportar las roturas de equipos por las siguientes vías.

Correo electrónico……

Utilizar el reporte de roturas habilitado en Portal de la Universidad

A partir del cúmulo de reportes recibidos, se establecerá un orden de prioridad en su atención por parte de la DII, teniendo en cuenta el nivel de importancia del equipo roto, afectaciones que produce y piezas de repuesto con que se cuente en ese momento.

Una vez establecidas las prioridades, el técnico tendrá 72 horas para dar respuesta a los reportes según la prioridad establecida.

Cada área llevará el siguiente **REGISTRO DE MANTENIMIENTOS A EQUIPOS** que será llenado por el técnico que realiza la tarea cada vez que se persone en el área y realice el mantenimiento o la reparación de algún equipo.

Equipo Fecha

Nombre del técnico
Labor realizada Observaciones

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).

11. Procedimiento para el control y reporte de incidentes de seguridad informática.

Todo trabajador o estudiante tiene el deber de informar cualquier incidente de seguridad, que atente contra resguardo e integridad de los recursos informáticos de la Universidad, para ellos se habilitará en todos los laboratorios y locales que posean PC independientes el registro de incidentes de seguridad informática, tiene la finalidad de controlar todo evento adverso que ponga en riesgo las computadoras y la Red de la Universidad.

Procedimiento para el control y reporte de incidentes de seguridad informática.

Se habilitará el registro de incidentes de seguridad informática según el siguiente formato.

REGISTRO DE INCDENCIAS DE SEGURIDAD INFORMÁTICA EN LABORATORIOS U OFICINAS

No. Consecutivo	Local o área	Fecha y hora en que se detecta el incidente	Local o PC del hecho detectado	Forma de detección y descripción del incidente	Medidas tomadas	Observaciones	Firma

Observaciones.

Por ejemplo se podrá plasmar en las medidas tomadas en correspondencia con el incidente, en el caso de alteración o rotura del sello de una PC, qué medidas se tomaron con la computadora y que indagaciones se realizan sobre el hecho.
En caso de un virus de alta incidencia destructiva, además de aislar la PC de la RED y pasarle el antivirus, se conserva este equipo en cuarentena y no podrá ser utilizado hasta que no sea
analizado por los especialistas correspondientes. Entre otras
El registro de control de incidentes será llenado cada vez que ocurra algún evento adverso que ponga en riesgo la integridad de los recursos informáticos y las redes de la Universidad. El incidente será reportado al correo ic@ucpejv.edu.cu

12. Procedimiento para el control de los componentes internos de cada PC y los software instalados. El control de los componentes internos de las PC, es un aspecto esencial que establece la RM 128/2019 del MIC, como vía para atenuar los robos de componentes de las computadoras y en caso de ocurrir hechos de robos, violación de sellos, la denuncia a la policía debe ir acompañada de la información detallada de los componentes de la PC afectada.
Por ello se establece como procedimiento que en todos los laboratorios y locales que exista la presencia de una PC lo siguiente.
Los técnicos de laboratorios, administradores de las áreas y jefes administrativos, no solo tengan en control del número de inventario del equipo, además sus componentes según el siguiente formato.

ASPECTOS QUE DEBEN SER CONTROLADOS EN CADA PC FECHA:_____
VCERRECTORIA:_____ ÁREA O DEPTO:_____ RESPONSABLE DEL EQUIPO:_____

Local	No Inv	Máquina			Placa Base	Fuente	Micro	Ram	HDD	CD	DVD	Qm	Monitor	Teclado	Mouse	Bocinas	UPS	Impresora	Direc Fis Tarj Red
		PIII	PIV	PV															

Estos datos de los componentes serán actualizados cada vez que sea cambiada una pieza por el técnico del taller.Para el control del software instalado en las PC se llevará el siguiente control.

REGISTRO 1

REGISTRO DE SOFTWARE DE AUTORIZADO

No consecutivo	Área y equipo	Relación de software autorizado a permanecer en el equipo	Nombres y apellidos del qu instala el software	Fecha de instalación	Nombre y apellidos del especialista o activista de seguridad informática

13. Procedimientos para la configuración de las contraseñas de autentificación en la Red y sus servicios. Las contraseñas de los usuarios de las PC y los servicios de la Red en la Universidad, deberán cumplir con los siguientes requisitos de las contraseñas según el artículo 47 de la RM 128/2019 del MIC.

Para la utilización de contraseñas como método de autenticación de usuarios, se cumplirán los siguientes requisitos:

a) Serán privadas e intransferibles.
b) Su estructura, fortaleza y frecuencia de cambio estarán en correspondencia con el riesgo estimado para el acceso que protegen.
c) Combinarán en todos los casos letras y números sin un significado evidente, con una longitud mínima de 8 caracteres.
d) No pueden ser visualizadas en pantalla mientras se teclean.
e) No pueden ser almacenadas en texto claro (sin cifrar) en ningún tipo de tecnologías de información. Es responsabilidad de los usuarios cambiar su contraseña cada cierto periodo de tiempo.

Los usuarios protegerán la información más importante y confidencial que posean para su trabajo, con contraseñas fuertes y seguras de apertura y escritura.

14. Procedimiento para la actualización de los parches de seguridad de los sistemas operativos, y plataformas de educación a distancia y de los sitios Web.

Los sistemas operativos, aplicaciones y plataformas utilizadas para la elaboración de los sitios Web y los Cursos a Distancia de la Universidad, por motivos de seguridad, periódicamente se ofrecen actualizaciones y parches de seguridad que tienen como objetivos, cerrar brechas o fisuras de seguridad que poseen estos sistemas, por ellos se establece como procedimiento lo siguiente.

1. Los administradores de Red del nodo de la Universidad y los administradores de las plataformas utilizadas para los sitios Web y los Cursos a Distancia, semanalmente descargarán las actualizaciones y parches de seguridad de las versiones de los sistemas que utilizan.
2. Implementarán las políticas de seguridad definidas para el sitio que administran.
3. Realizarán análisis y monitoreo sistemático del sitio.
4. Garantizar que los servicios implementados en el sitio cumplan con las normas de seguridad (Chat, blog, entre otros y sean utilizados para los fines que fueron creados.
5. Comunicar al Grupo de Seguridad Informática y la DII cualquier violación o anomalía detectada en el sitio.

15. Procedimiento para las salvas de información de los logs de navegación, plataformas de educación a distancia y los sitios Web.

Con el objetivo de garantizar la recuperación de la Red y sus servicios en la Universidad, ante cualquier evento adverso que perjudique la integridad de los servidores donde están alojados estos servicios, se establecen los siguientes procedimientos.

Los administradores de los servidores del nodo, de los sitios y de la plataforma de educación a distancia, realizarán salvas correspondientes de los servidores donde están alojados estos sitios, además de los log de navegación, trazas y de los sitios con una periodicidad semanal.

Las salvas se guardarán en HDD externo o CD, DVD, se ubicarán en un local o lugar resguardado con acceso restringido.

Se habilitará una libreta de control, para que se refleje las fechas en que se realizaron las salvas, la hora y la persona responsable de realizarla.

Los jefes correspondientes controlarán la realización de las salvas realizadas y su debido resguardo y funcionabilidad.

16. Procedimiento para la actualización del antivirus y parches de seguridad del sistema operativo de las PC en la universidad.

Con el objetivo de garantizar la actualización de los parches de seguridad de los sistemas operativos instalados en las PC de la Universidad, la actualización de la base de datos de los antivirus, se garantizará al acceso a través de los servicios de la Red, las actualizaciones correspondientes a los usuarios. Por ello se establece como procedimiento lo siguiente.

Los administradores del nodo habilitarán en el ftp de la universidad el servicio de actualizaciones y de los parches de seguridad de los sistemas operativos que se utilizan Windows XP SP3, Ubuntu y Debian, W-7, W-8, W8.1, W-10 así como las bases de datos de las actualizaciones de los antivirus que se utilizan en la Universidad Segurmática Antivirus Corporativo 1.72, Nod 32, V4 o V5, V7, V8

Los jefes administrativos velarán y son responsables de que las PC instaladas en sus áreas de responsabilidad tengan actualizado los parches de seguridad del sistema operativo y actualizado el antivirus que se utiliza. Los técnicos de laboratorios y personal responsable de las PC en oficinas independientes serán los encargados de actualizar las PC bajo su responsabilidad.

Estas actualizaciones podrán ser realizadas de manera automática o manual.

17. Procedimientos para el escaneo de la Red de la Universidad.

La auditoría del comportamiento de los servicios de la Red es responsabilidad de los administradores del

Nodo y de grupo central de especialistas de seguridad informática, para realizar este auditoria se realizarán los siguientes procedimientos.

Se escanearán los servicios de navegación, donde se incluye el uso de ancho de banda, sitios visitados, la gestión de correos y vulnerabilidades en la Red.

El escaneo de la Red será sistemático y con carácter aleatorio, a determinados servicios, facultades o áreas y usuarios o cuentas que resulten sospechosas.

Se emitirá cada 15 días el Boletín del comportamiento de la seguridad informática en la Universidad, el cual tendrá carácter limitado (Anexo boletín).

Los resultados del escaneo del comportamiento de la Red, al encontrarse una violación, será informado de manera inmediata a los jefes de las áreas administrativas correspondientes y a la DII, para que se tomen las medidas pertinentes.

Como resultado del escaneo de los servicios de la Red, los usuarios que se detecten en violaciones, serán cerradas sus cuentas y servicios según lo incluido en el procedimiento 4.

Las violaciones detectadas, se tomarán imágenes como muestras de las evidencias de las mismas.

18. Procedimientos para el sistema de control de la seguridad informática por los cuadros de dirección de la Universidad en sus áreas de responsabilidad.

El sistema de control hacia las actividades relacionadas con la seguridad informática, constituyen una vía esencial para mantener una disciplina de los usuarios en este sentido, para ello se establecen los siguientes procedimientos.

Los jefes tienen que incluir en el sistema de control de sus áreas las actividades referidas a la seguridad informática, donde se incluye el cumplimiento de los procedimientos establecidos.

El sistema de control incluye, la coordinación con el Nodo Central para saber el comportamiento del uso de la Red y sus servicios por parte del personal que dirigen y controlan.

Como resultado de los controles que se realizan, se actualizará el sistema de seguridad informática del área o facultad, documento que establece las políticas medidas, procedimientos y responsables de las actividades que garantizan la seguridad informática de cada área.

19. Procedimiento al adquirir equipos informáticos en la Universidad.

La Universidad recibe equipamiento informático por diferentes vías, es decir de forma centralizada por asignaciones del Ministerio de Educación Superior, donaciones recibidas por organizaciones o instituciones, compras que se realizan con financiamientos de proyectos, entre otras.

Con el objetivo de establecer una organización a esta actividad se establecen los siguientes procedimientos. Todo equipo informático que entre a la Universidad, será inventariado según establece los procedimientos contables.

Además se procederá a tomar toda la información de sus componentes internos y formará para del expediente de cada equipo.

Al llegar el equipo a la Universidad, será comprobado su funcionamiento por el técnico del taller de servicios técnicos o personal especializado designado por la DII.

Los equipos deben ser recibidos con su documentación técnica completa, discos de instalación de los sistemas o driver, cables y otros dispositivos, comprobando que estén completos.

Si los equipos de forma inmediata no serán ubicados en los locales para ser utilizados y van para un almacén, sus cajas serán selladas, se firmará un acta con toda la información del equipo de sus componentes internos, marcas y número de serie.

Esta acta será constancia del jefe administrativo que posteriormente recibirá el equipo.

Los administradores de las áreas que reciben el equipo o el módulo deben comprobar su funcionamiento y estado de uso, así como las partes que lo componen, calves y otros aditamentos.

20 Procedimiento para la salida y traslado de equipos informáticos fuera de la universidad.

Con el objetivo de mantener controlado los recursos informáticos que por motivos de trabajo deban salir de la Universidad, será responsabilidad del jefe administrativo del área cumplir con los procedimientos contables establecidos.

Desde el punto de vista de la seguridad informática se procederá a controlar los siguientes aspectos:

Fecha

Datos del Equipo: Tipo, Marca, Modelo, Configuración y componentes internos. Procedencia Destino

Motivo del movimiento Nombre de quien autoriza Firma de quien autoriza

21. Procedimiento: Control del uso de dispositivos móviles

Dada la existencia de dispositivos móviles en la universidad, se establece este procedimiento con el objetivo de regular su uso.

- La persona responsabilizada con estos equipos debe firmar un Acta de responsabilidad material, garantizando su uso correcto, en función del objeto social de la entidad y estrictamente para el trabajo según los fines definidos por la administración.
- En cualquier caso, de utilizarse por más de una persona se tendrá en cuenta el uso de perfiles de usuario si el sistema operativo instalado lo permite, o el trabajo en soportes magnéticos removibles con vistas a mantener la confidencialidad e integridad de la información.

- La persona responsabilizada con el equipo responde por la existencia en la misma de softwares antivirus actualizados.
- En caso de ausencia temporal de la entidad se deberá entregar el equipo al Jefe de Área.
- Estos equipos deben recibir los mantenimientos establecidos, y por tanto estarán incluidos en la programación que al respecto existe en la entidad. Es responsabilidad del Jefe de Área exigir porque éstos se cumplan.
- Al igual que cualquiera de las otras tecnologías informáticas de la entidad, existirá para cada uno de estos equipos la Relación de Software autorizado, partes y componentes, asimismo durante las inspecciones y auditorias o a solicitud del Jefe de Área, la persona que la posea está en el deber y la obligación de dejarla disponible para su chequeo.

22. Procedimiento para el uso de los servicios Wifi.

Procedimiento para la habilitación de los servicios para el personal de la Universidad que posee laptop, teléfonos móviles, tablets con estas prestaciones.

1. Los jefes administrativos del usuario que posee dispositivo y desea este servicio, realizarán una solicitud por escrito a la DII para su habilitación y garantizarán que el usuario firme el código de ética para el uso de la red y sus servicios en la Universidad.
2. Una vez aprobada la solicitud por la DII, se enviará la respuesta al nodo de la Universidad y al técnico de laboratorio del área correspondiente a la que pertenece el usuario.
3. El técnico de laboratorio del área, obtendrán la dirección física de la tarjeta de red del dispositivo (MAC)

(laptop, tablet, celular y enviarán esta información al nodo)

4. Con esa información los técnicos del nodo identificarán la PC correspondiente, el nombre de usuario y contraseña serán las mismas que posee con anterioridad para utilizar los servicios de la red.
5. El usuario deberá garantizar que, en su dispositivo, estén instalados los softwares correspondientes para este tipo de servicios, ya que este tipo de software varía según las marcas de los dispositivos, de no tenerlo instalado no podrá utilizar estos servicios.
6. En el caso de personal extranjero en pasantías, maestrías, doctorados, la secretaría de postgrado o Relaciones Internacionales, enviará una solicitud oficial a la NODO solicitando este servicio.

9. Con esa información los técnicos del nodo identificarán la PC correspondiente, en este caso por ser una nueva incorporación se les asignará un nombre de usuarios y contraseña para utilizar los servicios de la red.

10. En el caso anterior por ser la primera vez se habilitará un nombre de usuario y contraseña genérica que será cambiada cada 15 días y el usuario será el máximo responsable en realizar estos cambios, coordinado con los técnicos del nodo.

11. Se controlará el uso de la Wifi con el mysar u otro software de control de usuarios por parte de los técnicos del nodo y el grupo de seguridad informática, los que emitirán cada 15 días un reporte de las principales incidencias en caso de que existan.

14. El usuario que incurra con violaciones de la seguridad informática con estos dispositivos y servicios, serán analizados con los procedimientos administrativos correspondientes y le serán suspendidos los servicios de forma inmediata.

15. Los jefes administrativos, técnicos de laboratorio y personal responsable del lugar donde sea ubicada la antena Wifi, serán los responsables de su cuidado y conservación, así como desconectarla de la corriente los fines de semana y en momentos de lluvias y tormentas eléctricas, solo podrán cambiarla de lugar o realizar otro tipo de manipulación los técnicos del nodo.

16. Los jefes administrativos deberán comunicar de forma inmediata y por escrito a los cros del nodo, aquellas personas bajo su responsabilidad ya sean profesores de la universidad o personal extranjero, que fueron autorizadas a utilizar los servicios de la red wifi y causaron bajas o ya no se encuentran trabajando en la universidad, para efectuar la cancelación de los servicios correspondientes 17. Solo, podrá registrarse un solo dispositivo móvil por usuario

Total de usuarios de la red de la UCP EJV: 1600
De ellos estudiantes: 835 Trabajadores en general: 2435

1. Gráfico del comportamiento del ancho de Banda asignado a la Universidad.

2. Listado de los 10 sitios más visitados en la etapa:

Dirección del sitio	Dirección del sitio

3. Listado de los 10 sitios menos visitados en la etapa (No educativos)

Dirección del sitio	Dirección del sitio

4. Listado de los 10 sitios educativos más visitados en la etapa (Dirección del sitio)	5. Listado de los 10 sitios educativos menos visitados en la etapa (Dirección del sitio)

6. Listado de sitio Web internacionales dudosos o no confiables que se intento tener accesos y fueron bloqueados.

Dirección del sitio	Dirección del sitio

7. Comportamiento del tráfico de correo electrónico.

Gestión de mensajería	Total	MB utilizados en la mensajería
Correos recibidos	-	-
Correos enviados	-	-

Total de correos	-	-

8. Listado de los 10 servidores de correos que más recibe la UCP.

Direcciones de correo	Lugar	MB utilizados en la mensajería

9. Listado de los 10 servidores de correo que reciben la mensajería de la UCP.

Direcciones de correo	Lugar	MB utilizados en la mensajería

Listado de las 10 áreas de la UCP que más correos recibieron.

Direcciones de correo	Lugar	MB utilizados en la mensajería

10. Listado de las 10 áreas de la UCP que más correos enviaron.

Direcciones de correo	Lugar	MB utilizados en la

		mensajería

11. Resumen de las incidencias de seguridad.

Total de cuentas bloqueadas por sospecha de ser utilizadas por suplantación de identidad: ___
Total de cuentas bloqueadas por navegar en sitios dudosos o no confiables: ___ Facultades o áreas que más se reiteran en estos incidentes: _____

12. Resumen de las principales deficiencias detectadas por el grupo seguridad informática de la UCP en visitas realizadas a las áreas de la Universidad.

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.

10HECHO: 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.		

11Hecho: 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.

12Hecho: 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.	

13Hecho: 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.

CLASIFICACIÓN DE LOS INCIDENTES DE CIBERSEGURIDAD Y CATEGORIZACIÓN DE LOS SISTEMAS DE TRABAJO ACCIONES A EJECUTAR EN LAS DIFERENTES ETAPAS ANTE UN INCIDENTE DE CIBERSEGURIDAD

Etapa 1: Prevención y protección En esta etapa se incluyen:

1. Establecer las bases normativas regulatorias para garantizar la implementación de las políticas de Ciberseguridad.
2. Garantizar el diseño, establecimiento, control y mejora continua de las medidas de protección que permitan la prevención, detección, contención y respuesta ante la ocurrencia de incidentes.
3. Compatibilizar, homologar y certificar la seguridad de las infraestructuras y servicios, según su propósito y clasificación, de acuerdo con la legislación vigente.
4. Promover el desarrollo de soluciones integradas, protegidas y propias para la seguridad tecnológica.
5. Realizar ejercicios de Ciberseguridad para la comprobación de las capacidades reactivas, tanto organizativas como tecnológicas, ante posibles incidentes.
6. Implementar, como parte de la cooperación nacional, el intercambio con entidades especializadas en materia de Ciberseguridad.
7. Realizar campañas comunicacionales para fomentar la cultura de Ciberseguridad y elevar la percepción de riesgo.

Etapa 2: Detección, evaluación y notificación En esta etapa se realizan las acciones siguientes:

1. Realizar una evaluación preliminar del daño y de las causas y condiciones que ocasionaron o propiciaron el incidente, realizar la clasificación del incidente según peligrosidad, de acuerdo con lo establecido en la presente Resolución.
2. Preservar las evidencias digitales del lugar del hecho y las informaciones sobre los eventos de seguridad detectados por los sistemas de supervisión existentes. Esto puede incluir el aislamiento del objeto afectado de la infraestructura y la paralización parcial o completa de servicios.
3. Notificación a los niveles correspondientes de acuerdo con el Artículo 22.
4. Analizar y recolectar, para su revisión posterior, todos los eventos registrados por los sistemas de supervisión, los resultados de auditorías, diagnósticos integrales y ejercicios de Ciberseguridad efectuados. Buscar antecedentes del hecho.
5. Dar seguimiento al flujo informativo en las sucesivas etapas del modelo.

Etapa 3: Investigación

En esta etapa se ejecutan las acciones siguientes:

1. Comprobar el incidente a través de la caracterización del fenómeno, se identifican las causas y condiciones.
2. Realizar análisis retrospectivos para la reconstrucción de los hechos, así como la ejecución de diagnósticos reactivos para complementar las investigaciones.
3. Generar hipótesis sobre el hecho para su posterior comprobación y validación.

4. Determinar la responsabilidad administrativa, jurídica y penal, cuando corresponda, sobre el hecho investigado.
5. Documentar y legalizar los elementos probatorios que permitan establecer la identidad y objetivos, víctimas y modo de operar.
6. Informar a los niveles superiores de las personas jurídicas involucradas en el incidente sobre los daños y su repercusión política, económica y social, así como el impacto tecnológico y sus consecuencias.

Etapa 4: Mitigación y recuperación

Esta etapa comprende las siguientes acciones:

1. Diseñar e implementar soluciones tecnológicas para su erradicación.
2. Resolver las problemáticas detectadas en el estudio de causas y condiciones que permitieron que el ataque fuera efectivo.
3. Evaluar la pertinencia de restablecer gradualmente los entornos afectados y restablecerlos en tanto no entorpezcan el curso de la investigación.
4. Notificar por el órgano encargado de la gestión de la Ciberseguridad del Ministerio de Comunicaciones a las instituciones externas al país implicadas en el incidente, y se solicita su posición oficial, cuando corresponda.

ANEXO III

MODELO DE INFORMACIÓN PARA REPORTAR LOS INCIDENTES DE CIBERSEGURIDAD

<table>
<tr><th colspan="5">DATOS DEL INFORMANTE</th></tr>
<tr><td colspan="5">Nombres y apellidos:</td></tr>
<tr><td>Organismo:</td><td>Entidad:</td><td colspan="3">Cargo:</td></tr>
<tr><td colspan="2">Dirección:</td><td>Provincia:</td><td>Municipio:</td><td>País:</td></tr>
</table>

Correo electrónico:	Teléfono donde contactar:	Fax:	
Vía del reporte:	Fecha:	Hora:	
Otros datos de interés:			
DATOS DE LA ENTIDAD AFECTADA			
Organismo:	Dependencia:	Entidad:	
A quien contactar (nombres y apellidos):			
Dirección:	Provincia:	Municipio:	País:
Correo electrónico:	Teléfono:	Fax:	
Otros datos de interés:			
DATOS DEL INCIDENTE			
Categoría del incidente:		Clasificación nivel de seguridad/ peligrosidad en la entidad:	
Fecha de detección:	Hora de detección:	Sistema operativo:	

Origen del incidente (si se conoce):	
Descripción del incidente:	
Recursos afectados:	
Contramedidas aplicadas:	Otra información de interés: