**PLAN DE SEGURIDAD**  
**INFORMÁTICA**



**Dirección Municipal de Cultura**

**Cacocum**

**Ministerio de Cultura**

**2023**

**Cuba**

|  |  |  |  |
| --- | --- | --- | --- |
|  | Elaborado | Revisado | Aprobado |
| Nombre y Apellidos | Ing. Uliser Leyva Oliva | Oner E. Font Marrero | José Luis Rodríguez Aria |
| Cargo | Especialista B del GM JC | Técnico de Defensa y Seguridad y Protección | Director |
| Firma |  |  |  |
| Fecha |  |  |  |

Contenido

[1. Alcance del Plan de Seguridad Informática 4](#_Toc69783852)

[2. Caracterización del Sistema Informático 4](#_Toc69783853)

[3. Resultados del análisis de riesgos 5](#_Toc69783854)

[4. Políticas de Seguridad Informática. 6](#_Toc69783855)

[5. Responsabilidades 10](#_Toc69783856)

[6. Medidas y Procedimientos de Seguridad Informática. 12](#_Toc69783857)

[6.1 Clasificación y control de los bienes informáticos 13](#_Toc69783858)

[6.2 Del personal. 13](#_Toc69783859)

[6.3 Seguridad Física y Ambiental 15](#_Toc69783860)

[6.4 Seguridad de operaciones. 17](#_Toc69783861)

[6.5 Identificación, autenticación y control de acceso. 18](#_Toc69783862)

[6.6 Seguridad ante programas malignos. 20](#_Toc69783863)

[6.7 Respaldo de la Información. 22](#_Toc69783864)

[6.8 Seguridad en Redes. 22](#_Toc69783865)

[6.9 Gestión de Incidentes de Seguridad. 24](#_Toc69783866)

[7.Anexos 31](#_Toc69783867)

[7.1 Listado nominal de usuarios con acceso a los servicios de red. 34](#_Toc69783868)

[7.2 Registros 35](#_Toc69783869)

[7.3Modelo de solicitud de servicios de red 37](#_Toc69783870)

[7.4 Código de Ética para el uso del Correo Electrónico e Internet 38](#_Toc69783871)

[7.5Modelo Autorización de Permanencia fuera del horario laboral. 39](#_Toc69783872)

[7.6 Modelo de Autorización de Entrada/Salida de las Tecnologías Informáticas 40](#_Toc69783873)

[7.7 Base legal 41](#_Toc69783874)

[7.8 Control de cambios. 42](#_Toc69783875)

# Alcance del Plan de Seguridad Informática

El Plan de Seguridad Informática constituye el documento básico que establece los procedimientos y medidas a aplicar durante el procesamiento, intercambio, reproducción y conservación de la información a través de las Tecnologías Informáticas y de Comunicación (TIC) pertenecientes a la Entidad, siendo de obligatorio cumplimiento y conocimiento de todas las personas que participen en la elaboración, uso, aplicación, explotación y mantenimiento de las tecnologías informáticas a partir de la fecha en que entre en vigor.

La protección está dirigida fundamentalmente a prevenir, detectar y contrarrestar las acciones que pongan en peligro la confidencialidad, disponibilidad e integridad de la información que se procesa, intercambia, reproduce o conserva por medio de las TIC; según se establece resguardar los recursos relacionado con las TIC, independientemente de su importancia, pues estos se protegen contra alteraciones o sustracciones, ya sea de estas, de sus componentes o de la información que contienen, así como asegurar el área donde se ubican las tecnologías informáticas y de comunicaciones con herramientas de seguridad que las conviertan en más confiables. Resolución 360/2019 Ministerio de Las Comunicaciones, capítulo III Sección Tercera, seguridad Física.

El presente Plan de Seguridad Informática es aplicable en su totalidad en la Dirección Municipal de Cultura Cacocum, cito en calle Gilberto González # 1, Municipio Cacocum. Provincia Holguín

# 2. Caracterización del Sistema Informático

El sistema informático de la entidad, está soportado en los medios informáticos que se describen en el Anexo No.1, que incluyen computadoras de mesa, de las cuales 1 conectada en red.

En la empresa existe una red local que abarca los 9 locales incluyendo la dirección. Los locales destinados exclusivamente al trabajo de acuerdo a su especialidad. La PC de la dirección mantiene una comunicación con entidades externas mediante el empleo principalmente del correo electrónico.

El cableado de la red está soportado por cable UTP categoría 3 a 5, 100 Mb, con topología de árbol (Anexo No. 2), protegido con canaletas. Las estaciones de trabajo se agrupan todas en un edificio dividido en 2 locales a partir de 1 (router).

La conexión con el exterior se realiza a través ADSL con un ancho de banda de 2 Mbps. **NO SE TIENE ATERRAMIENTO FÍSICO EN LA ENTIDAD.**

El intercambio de información tanto interna como externa se realiza básicamente a través del correo electrónico y la nube de Cubarte, estos se producen con otras entidades del exterior y otras instituciones del gobierno cuando lo solicitan como por ejemplo el envío de informaciones, trasmitir datos, etc. También existen otras vías de intercambio empleando los soportes de información externos como son las memorias flash.

El paquete del Office se utiliza para la elaboración de informes y otros documentos*,* en las máquinas previstas para el trabajo interno en los locales destinados exclusivamente al trabajo de acuerdo a su especialidad.

La información que se procesa en la entidad es en su mayoría ordinaria y limitada en algunos casos. La información clasificada en la entidad se procesa en las máquinas de relaciones internacionales, recursos humanos, enseñanza artística, despacho, atención a la población. El resto de las informaciones son procesadas en las estaciones de trabajo de la reddonde cada trabajador opera sus sistemas y es el responsable del procesamiento, transmisión y conservación de la información; además de cumplir con la correcta aplicación de las políticas de seguridad definidas en este PSI.

La edificación se encuentra en el Centro de la Ciudad de Holguín, al lado de la Casa Iberoamericana en calle Arias, compuesta por un nivel. Tiene buenas condiciones constructivas, adecuadas tanto para la protección como para la preservación de los equipos, y la posibilidad de visibilidad de las pantallas desde el exterior es prácticamente nula. La mayoría de las puertas y las ventanas son de madera, poseen cierres seguros y están en buen estado. El personal que opera los equipos posee los conocimientos y la preparación necesaria para su empleo, y en la mayor parte de los casos tienen nivel medio o superior.

# 3. Resultados del análisis de riesgos

Los bienes informáticos más importantes a proteger en la empresa son:

* 9 PC (2 funcionando) 7 Almacén.
* Informaciones de VERSAT
* 2 router
* 1 teléfono corporativo

Las amenazas más importantes a considerar de acuerdo con el impacto que pudieran tener sobre la empresa son:

1. Ataque pirata a la red.
2. Tormentas eléctricas, ciclones.
3. Contaminación con virus informáticos
4. Entrada de ficheros (Imágenes, PowerPoint, Videos) desde medios extraíble.
5. Variación brusca del voltaje de la red eléctrica
6. Uso excesivo de los medios.
7. Fallo de la Red, o de las comunicaciones.
8. Fallo del Hardware, o del equipamiento.
9. Interrupción del servicio por causas fortuitas.
10. Deterioro físico del sistema.
11. Falta de mantenimiento periódico programado.
12. Hurto de la Tecnología Informática.

Las áreas sometidas a un mayor peso de riesgo y las amenazas que lo motivan son:

* Economía
* Acceso no autorizado.
* Pérdida de disponibilidad.
* Modificación de las configuraciones.
* Contaminación con programas malignos.
* Robo, hurto, traslado o pérdida.
* El local de la dirección.
* Acceso no autorizado.
* Pérdida de disponibilidad
* Fallas de comunicaciones
* Modificación de las configuraciones.
* Alteración o pérdida de datos.
* Contaminación con programas malignos
* Robo, Hurto, traslado o pérdida

El análisis de riesgo detallado se clasificó como **LIMITADO** y se encuentra bajo la custodia del responsable de Seguridad y protección.

# 4. Políticas de Seguridad Informática.

1. Las propuestas de iniciativas encaminadas a mejorar el sistema de Seguridad Informática se aprueban por el Consejo de Dirección.
2. El acceso a las tecnologías de la entidad es expresamente aprobado en cada caso y el personal tiene que estar previamente preparado en los aspectos relativos a la Seguridad Informática.
3. El Especialista de Seguridad Informática como máximo responsable de la Seguridad Informática de la instalación debe garantizar sistematicidad en el diseño del Sistema de Seguridad Informática, realizando actualizaciones en los análisis de riesgos cada vez que se produzcan cambios, aplicando los ajustes correspondientes.
4. El Plan de Seguridad Informática (PSI) es un documento de trabajo y como tal será accesible a todo el personal que requiera su utilización, por lo que la información incluida en este debe ser ordinaria y discutida con los trabajadores. El PSI será aprobado por el director (a) que exigirá su estricto cumplimiento.
5. Los usuarios de las tecnologías de la información y la comunicación responden por su protección y están en la obligación de informar cualquier incidente o violación que se produzca a su jefe inmediato superior.
6. El Técnico de Seguridad y Defensa, de conjunto con el Especialista de Seguridad Informática definirán las áreas o zonas controladas con requerimientos específicos que deban considerarse limitadas, restringidas o estratégicas y las medidas que deben aplicarse en las mismas.
7. Todos los bienes informáticos deben estar identificados, sellados e inventariados hasta nivel de componentes, implementándose un registro de inventario para cada medio aplicando el programa (Everest o Aida 64). El Especialista de Seguridad Informática guardará una copia actualizada para su control y dispondrá de otra copia para el usuario que opera cada estación de trabajo.
8. El sellado de las computadoras se realizará por el informático y mantendrá actualizado el registro de control de sellos, estableciendo un control semanal a los mismos.
9. Se establecen procedimientos que especifiquen quién y cómo se asignan y suspenden los derechos y privilegios de acceso a los sistemas de información.
10. Se prohíbe vincular cuentas de correo electrónico de la entidad a un servidor en el exterior del país con el fin de redireccionar y acceder a los mensajes a través de este.
11. En caso de violación de la Seguridad Informática, se comunica al jefe inmediato superior y a la Oficina de Seguridad para las Redes Informáticas y se crea una comisión encargada de analizar lo ocurrido y proponer la medida correspondiente.
12. Es responsabilidad de cada especialista el uso racional del equipamiento informático con que cuenta para el desarrollo de su trabajo.
13. La introducción de nuevas tecnologías informáticas como Software serán avalados por el Técnico de seguridad Técnica de la información en soporte informático antes de su utilización.
14. Cuando, por situaciones de trabajo, sea necesario el traslado de cualquier equipo informático debe ser aprobado por el Director, y realizar el movimiento de medios básicos.
15. El flujo de información interna y externa se realizará a través de la red, con predominio del correo electrónico o mediante dispositivos USB, con previa autorización por el jefe del departamento, el Especialista de seguridad informática y el director de la entidad.

16. Las PC de la entidad son instrumentos de trabajo, y como norma, no se mantendrá en ellas información no relacionada con el cumplimiento de las obligaciones funcionales. La tenencia de juegos, videos, imágenes y películas no relacionadas con el trabajo estará prohibida si no forma parte del contenido y función de trabajo.

17. El informático del centro se encargará de la adquisición de nuevas versiones de sistemas y/o aplicaciones, fundamentalmente a pedido de las diferentes áreas, y con el visto bueno del director. En cualquier caso, se tendrá en cuenta la capacitación del personal para su explotación.

18. En el centro no se desarrollan software, porque no hay personal destinado a ella. En todos los casos se adquiere a través de otra empresa.

19. Se realizarán auditorías semestralmente, para conocer la marcha del PSI y la preparación de los trabajadores en ese sentido.

20. 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 quienes tendrán acceso a determinado fichero y quienes no corresponde a los niveles superiores y no a su creador. Los usuarios no tendrán derechos administrativos, sólo el técnico en informática.

21. Es responsabilidad de cada trabajador del centro que todo soporte externo que salga de la misma no viole los requisitos, en lo que a materia de seguridad informática se refiere.

22. Se controlará a través del servidor de la Dirección Provincial de Cultura, el cumplimiento de la no difusión de información contraria al interés social, la moral, las buenas costumbres y la integridad de las personas; o que lesione la seguridad nacional. Las violaciones detectadas serán informadas oportunamente a las instancias pertinentes cuando se conecten las PC a una red.

23. Ningún usuario está autorizado para enviar mensajes de correo electrónico no solicitados a múltiples usuarios de forma indiscriminada (SPAM), ya sea de carácter informativo, cultural, comercial, social, con intenciones de engaño u otros.

24. Las salvas se realizan de forma cruzada en las máquinas y en soporte externo, dichas salvas son responsabilidad de cada operador que utilice la estación de trabajo, además de ser el Especialista de seguridad informático el máximo responsable.

25. Se tendrán al menos dos copias de la información que por su contenido se considere útil para la entidad, guardando una de ellas en una ubicación diferente con el fin de que no se pierda en caso de desastre en el lugar donde se emplea habitualmente. Se precisarán los procedimientos a ejecutar para su actualización, protección, conservación, verificación y utilización cuando se necesite.

26. El personal previo para ocupar cargos vinculados a la actividad informática, incluyendo personal eventual, estudiantes insertados y otros casos similares con acceso a sistemas críticos, a información de valor o a la supervisión y seguridad de los sistemas deberá ser seleccionado adecuadamente.

27. Los términos y condiciones del contrato de empleo incluirán la obligación del centro en cuanto a la preparación del contrato, así como la responsabilidad del trabajador hacia la seguridad informática, precisando este último aspecto mediante su vigencia una vez finalizada la relación laboral.

28. Constituye una violación grave de la seguridad la realización de acciones de comprobación de vulnerabilidades contra sistemas informáticos nacionales o extranjeros.

29. Todas las tecnologías de información, independientemente de su importancia, se protegerán contra alteraciones o sustracciones, ya sea de estas o sus componentes, así como de la información que contienen.

30. Los cables de alimentación o de comunicaciones se protegerán contra la intersección o el daño, además de estar separados para evitar la interferencia.

31. El Especialista de seguridad informático garantizará que el equipamiento reciba el mantenimiento correcto de acuerdo con los intervalos de servicios y recomendaciones por el fabricante, para asegurar su disponibilidad e integridad.

32. Se evitará que la información que contiene el equipamiento que cause baja o sea destinado para otras funciones pueda resultar comprometida.

33. Se apagarán y desconectarán los equipos en caso de alarma en el centro y al finalizar la jornada laboral.

34. En caso de ocurrencia de tormentas eléctricas se apagarán y desconectarán todas las tecnologías informáticas.

35. Todas las tecnologías informáticas y los tomacorrientes tendrán señalizado el voltaje a que trabajan.

36. El director, de conjunto con los jefes de departamento y la persona encargada de elaborar la información, serán los responsables de clasificarla, según el Decreto Ley 199/99 y la Lista Interna.

37. Existirá un registro de incidencias [**Registro No.5**](#_7.2_Registros), en el que se plasmará cualquier rotura de equipamiento, aparición de virus y programas malignos, intentos de accesos no autorizados, uso del equipamiento informático por personal ajeno al área.

38. Se designará a una persona, con las características de idoneidad requeridas para administrar la red y se precisarán documentalmente sus obligaciones y atribuciones quedando firmado su compromiso de cumplimiento.

39. La arquitectura y configuración de los diferentes componentes de seguridad de la red estarán en correspondencia con las políticas aprobadas por la máxima dirección, así como los servicios implementados. Para realizar cualquier modificación o incorporación de nuevos servicios se debe solicitar la aprobación del Director Nacional y no se procederá a su ejecución hasta no contar con el documento oficial que lo autoriza.

40. Se configurarán los sistemas operativos para garantizar la seguridad en las estaciones de trabajo, limitándose el acceso sólo para el personal autorizado; además de implementarse los mecanismos de monitoreo y auditoría de los principales eventos por un tiempo no menor de un año.

41. A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes y la correspondiente sincronización y verificación con fuentes externas.

42. Se instalarán cortafuegos (firewall) en cada una de las PC, que aseguren una barrera de protección para la conexión con otras redes externas, así como para la detección de potenciales intrusos.

43. Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y métodos utilizados. El especialista de seguridad informática, presentarán trimestralmente el informe al Consejo de Dirección, independientemente a esto deberán informar oportunamente a la OSRI sobre estos incidentes de seguridad.

44. El acceso a Internet se realizará a través de un servidor Proxy provincial, controlándose los usuarios autorizados y las reglas de acceso definidas. Ningún usuario está autorizado a realizar modificaciones o instalaciones de programas que vulneren las restricciones de este servicio.

45. Se prohíbe la adición de algún equipo o la introducción de cualquier tipo de software, ya sea a través de soportes removibles o mediante acceso a redes externas, sin la autorización de la Dirección, garantizando su compatibilización con las medidas de seguridad establecidas para la protección de las mismas.

Considerándose como una violación grave, el empleo de software no autorizado para transgredir las medidas de seguridad o realizar acciones que pongan en peligro la seguridad de las informaciones procesadas en las TIC.

46. Se prohíbe la administración remota de estas redes mediante conexiones conmutadas a través de las redes públicas de transmisión de datos.

47. El volumen de información desde o hacia la Entidad a través del correo electrónico, será restringido al igual que la generación de mensajes a múltiples destinatarios, con el fin de impedir la sobrecarga de los canales de comunicación.

48. Se establecerán controles de seguridad, e implementarán mecanismos técnicos, así como acciones de supervisión y monitoreo para detectar, obstaculizar, impedir e interrumpir la generación de cartas en cadenas.

49. Se realizarán los análisis de las trazas de navegación y de correo electrónico por parte del especialista de seguridad informática informando de los resultados al Director(a) tomándose las acciones para su esclarecimiento.

50. Se establecerán medidas y procedimientos que garanticen la continuidad, el restablecimiento y la recuperación de los procesos informáticos ante incidentes y violaciones de la seguridad. Incluirán las acciones de respuesta a realizar, la determinación de los responsables de su cumplimiento y los recursos necesarios en cada caso.

51. Se sancionará administrativamente a todo aquel que viole lo dispuesto en las políticas de seguridad informática, conforme a lo dispuesto por el reglamento disciplinario, y en caso de corresponder, se realizarán las acciones correspondientes ante los órganos del MININT.

# 5. Responsabilidades

Estructura de gestión de la Seguridad Informática del Centro Provincial de Superación para la Cultura.

**Director**

**Técnico de Seguridad y Protección**

**Técnico de Informática**

**Trabajadores**

**Funciones y Obligaciones de los Administradores de Sistemas, Aplicaciones y Bases de Datos de la Dirección Municipal de Cultura.**

**El Director del centro, como Jefe máximo del sistema de la Seguridad Informática, está obligado a cumplir lo dispuesto en la Resolución 128\_2019, siendo responsable, entre otras cuestiones, de garantizar:**

1) El diseño, la implantación y el mantenimiento del Sistema de Seguridad Informática a partir de la importancia de los bienes a proteger y de los riesgos a que están sometidos, con el fin de alcanzar los siguientes objetivos:

a) Minimizar los riesgos sobre los sistemas informáticos.

b) Garantizar la continuidad de los procesos informáticos.

2) La actualización de los Planes de Seguridad Informática, en lo adelante PSI, considerando para ello los siguientes factores:

a) La aparición de nuevas vulnerabilidades.

b) Los efectos de los cambios de tecnología o de personal, así como los cambios de la configuración o topología de la red.

c) La efectividad del sistema demostrada por la naturaleza, número y daños ocasionados por los incidentes de seguridad registrados.

3) La protección de los bienes informáticos que le han sido asignados, para lo cual deberá asegurar que se realicen las siguientes acciones:

1. Identificar los requerimientos de seguridad de los bienes informáticos bajo su responsabilidad y de las aplicaciones en desarrollo, determinar el nivel de acceso de los usuarios a los mismos y el cumplimiento y la vigencia de estos accesos.
2. Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática, en la parte que concierne a su esfera de acción y garantizar su cumplimiento.
3. Aplicar las medidas y procedimientos establecidos en su área de responsabilidad.
4. Especificar al personal subordinado las medidas y procedimientos establecidos y controlar su cumplimiento.
5. Participar en la elaboración de los procedimientos de recuperación ante incidentes de seguridad y en sus pruebas periódicas.
6. Imponer o proponer según lo establecido en el sistema, sanciones ante violaciones del sistema de seguridad, en correspondencia con su naturaleza y con los daños ocasionados.
7. Creará un equipo de trabajo que participará en el diseño e implementación del SGSI, recogido en el [Anexo No. 3](#_7._Anexos)

**El Especialista de seguridad informática se encargará de atender la actividad de Seguridad Informática. El mismo tendrá las siguientes obligaciones:**

1. Organizar y controlar la actividad de Seguridad Informática.
2. Participar en el diseño del Sistema de Seguridad y en la elaboración, evaluación y actualización del Plan de Seguridad Informática, supervisar su aplicación y disciplina en el cumplimiento.
3. Evaluar el estado de cumplimiento y aplicación de la base legal vigente en la materia.
4. Supervisar el trabajo del personal que responde por la Seguridad Informática en la entidad, y organizar su preparación.
5. Proponer medidas ante violaciones de la base legal establecida en la materia.
6. Verificar el cumplimiento de las medidas de Seguridad Informática a través de auditorías o controles realizados.
7. Realizar el análisis de las trazas de navegación y correo conjuntamente con el administrador de la red de la Dirección Provincial de Cultura mensualmente y enviar este informe al director del centro.

**El técnico de Informática tiene, en relación con la Seguridad Informática, las siguientes obligaciones:**

1. Garantizar la aplicación de mecanismos que implementen las políticas de seguridad definidas en la red.
2. Realizar el análisis sistemático de los registros de auditoría que proporciona el sistema operativo de la red.
3. Garantizar que los servicios implementados sean utilizados para los fines que fueron creados.
4. Comunicar a la dirección de la entidad los nuevos controles técnicos que estén disponibles y cualquier violación o anomalía detectada en los existentes.
5. 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.
6. Participar en la elaboración de los procedimientos de recuperación ante incidentes y en sus pruebas periódicas.
7. Informar a los usuarios de las regulaciones de seguridad establecidas y controlar su cumplimiento.
8. Participar en la confección y actualización del Plan de Seguridad Informática.
9. Informar a los usuarios de los controles de seguridad que hayan sido establecidos y verificar su utilización apropiada.
10. Controlar el acceso a los sistemas, aplicaciones y bases de datos en correspondencia con la política establecida para los mismos.
11. Garantizar la ejecución de los procedimientos de salva de programas y datos así como su conservación.
12. Detectar posibles vulnerabilidades en los sistemas y aplicaciones bajo su responsabilidad y proponer acciones para su solución.
13. Garantizar su mantenimiento y actualización y el registro de los sistemas y aplicaciones que lo requieran.

**Los trabajadores tienen en relación con la Seguridad Informática, las siguientes obligaciones**:

1. Adquirir la preparación necesaria y los conocimientos de Seguridad Informática imprescindibles para el desempeño de su trabajo.
2. Contar con la autorización expresa del jefe facultado, para obtener acceso a cualquiera de los bienes informáticos.
3. Utilizar las tecnologías de información sólo en interés de la entidad.
4. No transgredir ninguna de las medidas de seguridad establecidas.
5. 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.
6. No instalar ni utilizar en las tecnologías equipamientos o programas ni modificar la configuración de las mismas, sin la correspondiente autorización del jefe facultado.
7. Cumplir las reglas establecidas para el empleo de las contraseñas.
8. Informar al personal facultado de cualquier anomalía de seguridad detectada.

# 6. Medidas y Procedimientos de Seguridad Informática.

Con el objetivo de mantener actualizado el sistema diseñado de la Gestión del Sistema Informático, se revisarán las políticas para su adecuación

**Medida:** Aprobar en Consejo de Dirección, cada nueva política de seguridad surgida por cambios tecnológicos y/o nuevos riesgos.

**Procedimiento 1:** Actualización del PSI

1. Toda nueva política surgida como resultado de cambio de tecnología, será discutida con todos los trabajadores y aprobada en el Consejo de Dirección.
2. El monitoreo de cambios significativos en la exposición de los bienes informáticos a amenazas.
3. La evaluación de la idoneidad de los controles específicos de Seguridad Informática y la coordinación de su implementación para nuevos sistemas y servicios.
4. La revisión y el esclarecimiento de los incidentes de Seguridad Informática.
5. La nueva política aprobada será de uso obligatorio y tendrá alcance para todos los departamentos.
6. Será de conocimiento para todo el personal y confeccionarán un certifico, en el que se recoja la actualización del PSI y la discusión de dicha política por el personal.
7. Se confeccionará anualmente el Sistema de Gestión para la seguridad informática.

Responsable: Especialista de seguridad informático

1. Informar al director, los resultados de la actualización del PSI, con la nueva política puesta en vigor.

Responsable: Especialista de seguridad informático, en lo adelante ESI.

## 6.1 Clasificación y control de los bienes informáticos

**Medida:** El Especialista de seguridad informático del centro responde por la integridad de los medios informáticos.

**Procedimiento 2:** Control de medios informáticos.

1. La última semana de cada mes, el encargado de Seguridad Informática accederá a la herramienta (Everest) o (Aida) aplicándolo a las máquinas. Una vez que concluya este proceso, compara los resultados obtenidos con el anterior control realizado para detectar posibles cambios, confeccionando un informe que entrega al director.
2. El director es la única persona autorizada a permitir la entrada o salida.
3. Son los jefes de departamentos o el ESI, los responsables de consignar en el registro de entrada y salida de las tecnologías, todos los movimientos de los bienes bajo su custodia.
4. En caso de que el medio se mueva fuera del centro se hará con previo embalaje y en un medio de transporte de pocas vibraciones donde se evite la humedad, el polvo y el sol.
5. Realizar un resumen del resultado de cada control y conservarlo por un año.

**Responsable:** ESI

1. Esclarecer en caso de existir diferencia, las causas y responsabilidades.

**Responsable:** Director

## 6.2 Del personal.

**Medida:** Los jefes de departamentos determinarán, cómo utilizará el personal, las tecnologías informáticas de forma tal que se logre un uso racional de las mismas.

**Procedimiento 3:** Otorgar (retirar) acceso de personas a las TIC.

1. Para la autorización de las cuentas de acceso a las TIC y a las aplicaciones a los usuarios.

* Los jefes de departamento solicitan por escrito la creación de las nuevas cuentas, especificando las aplicaciones a que debe tener acceso, y los privilegios, en correspondencia con sus funciones.
* El director aprueba (modificándola de ser necesario) o deniega la solicitud realizada.
* Una copia de la planilla se le transfiere al ESI para la apertura de la cuenta.
* Si es un nuevo trabajador se entrega al mismo el código de ética para el acceso a las TIC, y se dan a conocer al mismo tiempo los elementos fundamentales del PSI.
* Se llena el modelo Acta de Compromiso del usuario individual de la red de datos, mediante la cual se compromete al cumplimiento de las regulaciones que rigen el uso de los servicios.
* Se abren las cuentas necesarias para el acceso del usuario a las aplicaciones aprobadas.
* El ESI archiva el documento que sirvió de base para la apertura de la cuenta y de la asignación de los privilegios otorgados.

1. Si un usuario causa baja del centro, el responsable de Seguridad Informática:

* Solicita eliminar la cuenta del usuario del servidor de dominio al Administrador de la red de la Dirección Provincial de Cultura.
* Elimina todos los directorios asociados al usuario que pudieran haber sido creados en la PC.
* Elimina las cuentas de los servicios a que tuviera derecho.
* Extrae del archivo el documento que sirvió de base para la apertura de la cuenta, y de la asignación de privilegios, y la guarda en un archivo histórico durante un período no menor de 2 años.

**Responsable:** ESI

1. Esclarecer en caso de existir diferencia, las causas y responsabilidades.

**Responsable:** Director.

**Medida:** El ESI establecerá el uso correcto del correo electrónico por parte de los usuarios.

**Procedimiento 4:** Autorización y denegación de los servicios a los usuarios.

1. Antes de transmitir una información adjunta, el usuario debe cerciorarse que no contenga programas malignos, chequeándolo con el software antivirus que se encuentre instalado en su equipo.
2. El personal que envía correo electrónico debe ser únicamente el autorizado.
3. Ante cualquier violación de las medidas establecidas se aplicará la suspensión del servicio al implicado.
4. Si el director entiende que un determinado buzón no es necesario, evaluará si se cancela el servicio.
5. Al recibirse un mensaje, si este posee ficheros anexos o adjuntos, se tendrán en cuenta las medidas antivirus (cuarentena técnica para programas y aplicaciones, “abrir sin macros”, para documentos de Office).
6. Es obligación de los jefes a los distintos niveles, garantizar el cumplimiento de las medidas de seguridad informática en su área, siendo esta una preocupación diaria.

**Responsable:** ESI.

**Procedimiento 5:** Acciones a realizar en caso de empleo no autorizado de las TIC y sus servicios.

Quien detecte tales acciones lo notifica al ESI del centro. Inmediatamente, se procede como se define para las incidencias de seguridad.

**Responsable:** Director

**Medida:** Los usuarios de las tecnologías informáticas están en la obligación de informar cualquier incidente, debilidad o amenaza que detecte en el sistema informático.

**Procedimiento 6:** Formas y medios mediante los cuales el usuario informa acerca de cualquier incidente de seguridad, debilidad o amenaza.

En caso de incidente el usuario notificará a su jefe de departamento, al ESI y al director.

En caso de debilidad o amenaza se evalúa su probabilidad y posible impacto para la entidad, adoptándose medidas inmediatas para tratar de eliminarla o contrarrestarla. Al concluir el análisis y en cuanto se determine las medidas a adoptar se organizará por parte del ESI, la actualización con los usuarios encargados de ponerlas en práctica para garantizar su cumplimiento adecuado. Se documentará el hecho en el acápite [**Control de Cambios**](#_7.3_Control_de) de este PSI.

**Responsable:** Director

**Medida:** Evitar la realización de acciones de comprobación de vulnerabilidades, así como la introducción, ejecución, distribución o conservación de programas para estos fines o información contraria al interés social, la moral y las buenas costumbres.

**Procedimiento 7:** Evitar la realización de acciones de comprobación de vulnerabilidades.

El ESI debe realizar chequeos semanales a los equipos conectados a la red local para comprobar vulnerabilidades propias en los sistemas o encontrar acciones con fines contrarios al interés social, la moral y las buenas costumbres, así mismo, tiene en su contenido de trabajo el chequeo del software instalados en cada PC (incluso máquinas independientes). Esto debe de realizarlo mensualmente y elaborar un informe el cual presentará en el consejo de Dirección.

**Responsable:** ESI

## 6.3 Seguridad Física y Ambiental

Clasificación y medidas específicas en las áreas controladas

|  |  |  |
| --- | --- | --- |
| Área controlada | Categoría | Medidas específicas |
| Dirección | Limitada | Acceso a Director, Especialistas de esas áreas; sello, cierre seguro en puertas, climatización y datos. |
| Economía | Limitada | Acceso físico limitado; separación de funciones; protección de copias de programas de datos. |

Medida: La entrada, salida y traslado de las tecnologías de información se realizará con autorización del Encargado de Seguridad Informática previamente autorizado por el Director en correspondencia con el Procedimiento 8, dejándose constancia de ello en el [Registro No. 1: Movimiento de Tecnologías de Información.](#_7.2_Registros)

**Procedimiento8:** Movimiento de las TIC

1. Solicitar autorización por escrito al Director de la entidad para el movimiento de las tecnologías que lo requieran, fundamentando en qué consiste el movimiento, los motivos y si es temporal el tiempo requerido.

**Responsable:** Jefe del área a que pertenece el medio a trasladar.

1. Autorizar si es procedente el movimiento de las tecnologías y darlo a conocer por escrito al Jefe del área que realizó la solicitud, al Jefe del área de Contabilidad y al Jefe del Departamento de Seguridad y Protección, especificando el tiempo de vigencia de la autorización.

**Responsable:** Director

1. Registrar en el sistema Contable el movimiento del medio básico autorizado a trasladar.

**Responsable:** Jefe del área de Contabilidad.

1. Revisar antes de su salida (entrada) de la entidad las tecnologías autorizadas a trasladar, precisando la existencia y estado de sus partes y componentes, si contienen información y de qué tipo, así como lo relacionado con el control antivirus. Constancia en [**Registro No. 1**](#_7.2_Registros).

**Responsable:** Jefe del área a que pertenece el medio a trasladar y ESI.

1. Se realizarán inspecciones sorpresivas para detectar las extracciones no autorizadas por el Responsable de la Actividad Informática.

**Medida:** Se hará un uso correcto de los soportes de información.

**Procedimiento 9:** Uso de los soportes de información

1. Los soportes existentes serán debidamente identificados
2. Las memorias flash de uso personal que se utilizan en función del trabajo se deben verificar periódicamente para el correcto uso de ellas.

**Responsable:** Jefe de cada área.

1. Para el control de estas se utilizará la herramienta MyUsbOnly, la cual genera información necesaria en los servidores para su control.

**Responsable:** ESI.

1. En caso de existir un medio del centro para el trabajo o salva de las trazas, al concluir la vida útil de este soporte, se borra la información que contiene y se le da baja del **Registro No 2: Control de Soportes**.
2. En caso que sea necesario el traslado de soportes se tendrá en cuenta que:

* El jefe de Dpto. es el único facultado para autorizar el traslado
* Se efectuará previamente el chequeo contra programas malignos

**Medida:** Los mantenimientos y reparaciones están contratados con TCP en reglamento y quedará la constancia del mantenimiento en **el Registro No 3. Mantenimiento a los equipos de cómputo**.

**Procedimiento 10:** Mantenimiento de las TIC

1. Velar porque los mantenimientos se efectúen en las fechas establecidas. Para evitar olvidos, se incluirá esta tarea como un punto en su Plan de Trabajo.

**Responsable:** ESI

1. Al realizarse el mantenimiento deberá estar presente la persona responsabilizada con dicho equipo.
2. En caso que sea necesario el traslado fuera de la entidad, la persona responsabilizada con el equipo de conjunto con el ESI se encargará después de verificar que existen las salvas correspondientes, de eliminar si fuera posible la información que éste posee, o en caso contrario exigir al Técnico la firma de un Acta donde se comprometa a no divulgar la información. También se realizarán las anotaciones en los registros correspondientes como se establece en el procedimiento de control de traslado de las TIC con vistas a controlar el medio básico.

## 

## 6.4 Seguridad de operaciones.

Procedimiento 11: Tratamiento dado a los Software nuevos que son adquiridos.

1. Para instalar un software nuevo, por la vía que se haya recibido tiene que estar aprobado por el director.
2. Antes de ser instalado tiene que ser verificado, con los antivirus establecidos.
3. Se registrará en el [Registro No.4 Registro de Software](#_7.2_Registros).

**Responsable:** Encargado de Seguridad Informática.

**Procedimiento 12:** Corrección de errores y brechas de seguridad.

1. Informar los resultados de las acciones de corrección de errores y brechas de seguridad al director cada vez que se realicen y preservar los registros en los soportes habilitados al efecto por un tiempo no menor de un año.

Responsable: ESI

1. Analizar los resultados de las acciones de corrección de errores y brechas de seguridad y proponer las acciones necesarias para su evaluación y determinación de las modificaciones requeridas para su eliminación.

Responsable: Encargado de Seguridad Informática.

1. Actualizar los cambios en el PSI.

Responsable: Encargado de Seguridad Informática.

## 6.5 Identificación, autenticación y control de acceso.

**Identificación de usuarios**

**Procedimiento 13:** Asignación de identificación de usuarios.

1. Cuando son recibidas las planillas de solicitud de los servicios para la creación de cuenta de usuarios, la misma es procesada por el administrador de la red de la Dirección Provincial de Cultura.
2. Si la planilla está correcta, el administrador de la red procede a entregarla al Especialista de Seguridad Informática de Cultura Provincial y éste a su vez procede a crear la cuenta.
3. Como norma para la identificación del usuario se tomará el primer nombre y el 1er apellido, con la siguiente estructura **<usuario@baibrama.cult.cu>**
4. En caso de existir similitud con algún otro usuario, se tomará el segundo nombre con el primer apellido o con el segundo apellido.
5. Se le da autorización de los servicios que va a recibir y es activada la cuenta.

Responsable: ESI

1. El ESI, le entrega la cuenta al usuario que ya ha sido creada en Cultura Provincial.
2. Se actualiza los cambios en el PSI.

Responsable: Encargado de Seguridad Informática.

Procedimiento 14: Inhabilitación de identificación de usuarios.

1. Cuando son recibidas las planillas de cancelación de los servicios de cuenta de usuarios, la misma es procesada por el administrador de la red de la Dirección Provincial de Cultura.
2. Si la planilla está correcta, el administrador procede a eliminar la cuenta.
3. Como norma para la cancelación de la cuenta se procede a la plataforma de administración de usuario y se inhabilita la cuenta **<usuario@baibrama.cult.cu>**
4. De esta manera se inhabilita todo lo referente a la cuenta del usuario

Responsable: ESI

1. El ESI verifica que se haya eliminado la cuenta del usuario.
2. Se actualiza los cambios en el PSI.

Responsable: Encargado de Seguridad Informática.

**Autenticación de usuarios**

**Procedimiento 15:** Autenticación de usuarios.

1. El servidor tendrá activadas contraseñas para la identificación y autenticación de los usuarios y estos serán los responsables de definir sus claves, si el usuario está convencido de que alguien ha detectado su palabra clave, se les permite cambiar la misma.

**Procedimiento 16:** Requerimientos de las contraseñas.

* 1. Tendrán un período de vigencia, con cuotas de 7 a 60 días. Aunque se permitirá cambiarlas fuera de estos términos en caso de ser necesario.
  2. Serán privadas e intransferibles, su estructura, fortaleza y frecuencia de cambios estarán en correspondencia según el nivel de información con la que se trabaja. Cambiarán en todos los casos letras y números sin un significado evidente, con una longitud mínima de 8 caracteres.
  3. Las claves de acceso se cambiarán por:
* cambio de usuarios (vacaciones o bajas)
* son conocidas por dos personas o más
* se utilizará refrescador de pantalla, con clave de acceso para proteger la entrada de usuarios no autorizados en los casos que sea necesario.

**Responsable:** todos los usuarios.

* 1. En cada PC se establecerá lo siguiente:
* Cuota mínima y máxima de duración de la contraseña, según se detalla al inicio de este procedimiento.
* Longitud mínima de la contraseña es de 8 caracteres.
* Bloqueo de cuentas, garantizando que el sistema inhabilite el acceso tras 3 intentos infructuosos de conexión.
  1. En el acta de compromiso que firma el usuario, que se incluye en su contrato de trabajo, consta que se comprometen a mantener confidencialidad sobre las contraseñas personales.

**Responsable:** El ESI.

**Procedimiento 17:** Cambio de contraseña de internet.

1. Para cambiar la contraseña del navegador de Internet se ejecutará desde la consola de administrador a través del Administrador de red de Cultura Provincial.
2. Es obligatorio que todos los usuarios cambien la contraseña.

**Responsable:** Todos los trabajadores

**Procedimiento 18:** Cambio de contraseña de correo.

1. Para cambiar la contraseña del correo, se ejecutará mediante la plataforma del administrador de red de Cubarte o el Sectorial Provincial de Cultura.
2. El trabajador asume la responsabilidad, de lo que pueda suceder con su cuenta y de lo que suceda no lo eximirá de responsabilidades.

**Responsable:** Todos los usuarios.

**Procedimiento 19:** Opción recordar contraseña en el navegador.

* 1. Cuando se está usando el Mozilla Firefox
* Ir a Menú Herramientas/Opciones/Pestaña seguridad.
* Desmarcar la casilla de verificación “recordar contraseña”
* Dar clic en aceptar.
  1. Cuando se está usando el Thunderbird.
* Ir a Menú Herramientas/Opciones/Pestaña seguridad.
* Desmarcar la casilla de verificación “recordar contraseña”
* Dar clic en aceptar.

Responsable: Todos los usuarios.

**Control de acceso a los bienes informáticos.**

Procedimiento 20: Acceso a las TIC.

* 1. Cada usuario tendrá acceso a la información imprescindible para el desarrollo de su trabajo.
  2. Todo lo que no está explícitamente permitido, queda prohibido.
  3. Los procedimientos para otorgar/retirar acceso a las TIC y sus servicios se describe en el [epígrafe 6.2](#_6.2_Del_personal.),en el [procedimiento 3](#_6.2_Del_personal.).

**Responsable:** Director.

## 6.6 Seguridad ante programas malignos.

**Medida:** El ESI está en la obligación de garantizar la instalación de los medios antivirus informáticos, en correspondencia con sus condiciones específicas.

***Medida: Usar como antivirus protector el Segurmática, para la plataforma Windows y Linux que es de factura Nacional.***

**Procedimiento 21:** Protección contra virus.

1. Poseer los productos antivirus certificados y actualizados.
2. Ejecutar el correspondiente chequeo a todos los soportes tecnológicos de información ajenos a la empresa, antes de su utilización.
3. Mantener protegidos contra escritura el software original (Sistemas operativos, utilitarios).
4. Establecer el chequeo previo y posterior de la computadora y los soportes tecnológicos de información si es objeto de traslado por cualquier razón, fuera de la empresa, antes de ser utilizados nuevamente, con el objetivo de evitar la posible propagación de virus informáticos.
5. Ante un indicio de contaminación por algún virus nuevo o desconocido, se deberá aislar el mismo o apagar y preservar el equipo infectado, debiendo reportarlo a una empresa especializada.
6. Queda totalmente prohibido el intercambio de códigos de virus entre personas.
7. Se creará para la PC objeto de este sistema de medidas, un disco inicio, con vistas a la restauración de los mismos, al producirse cualquier incidente que la afecte.
8. Se tendrá en cuenta lo siguiente:

* Deshabilitar la función autorun.
* Permitir que se muestren los archivos ocultos.
* Acceder a la raíz de los discos por la parte izquierda del explorador de Windows.

**Responsable:** ESI

Medida: Usar como antivirus el Segurmática, que es de producción nacional.

**Procedimiento 22:** Instalación Antivirus Segurmática

1. Instalar el antivirus Segurmática de factura Nacional, que se encuentra en el sitio C/Segurmática
2. Configurarlo para que se actualice manualmente desde el servidor ftp

ftp.baibrama.cult.cu/segurmatica/

1. Configurarlo para que elimine automáticamente los virus sin preguntar.

Responsable: Técnico en informática

**Medida:** El empleo del software no autorizado en la red estará sujeto a un estrecho control por parte del ESI.

**Procedimiento 23:** Tratamientos para los softwares no autorizados.

1. Ningún usuario está autorizado a usar o permitir conscientemente que se emplee en software de ningún tipo para:

* escanear la red.
* capturar o borrar contraseñas.
* ocultar información.
* verificar la seguridad de otra red.

1. Los softwares para estos fines estarán ubicados solamente en un lugar con acceso de los administradores.
2. En ninguna PC de trabajo en la entidad, los softwares con estas características estarán instalados, ni almacenados.

Responsable: ESI.

**Procedimiento 24**: Descontaminación de programas malignos.

1. Al detectar en una estación de trabajo indicios de contaminación detener la actividad que se esté realizando, desconectarla de la red e informar al jefe inmediato y al encargado de Seguridad Informática.

Responsable: Usuario de la estación de trabajo.

1. Identificar de qué tipo de programa maligno se trata.
2. Verificar que en el medio contaminado se esté ejecutando una versión actualizada del programa antivirus instalado y de no cumplirse, proceder a la actualización del programa antivirus y llevar a cabo la descontaminación. De ser exitosa la descontaminación, poner en operación el medio afectado.
3. Revisar los soportes y el resto de las tecnologías que pudieran haber sido afectadas.
4. Investigar las causas de aparición del código malicioso.
5. Realizarlas anotaciones pertinentes en el Registro de Incidencias: [**Registro No. 5**](#_7.2_Registros)

Responsable: ESI.

1. Reportar el incidente a su instancia superior.
2. Si es un programa maligno desconocido, proceder al aislamiento del fichero contaminado y remitirlo a la empresa Segurmática.

Responsable: ESI.

Procedimiento 25: Intercambio de sistemas y programas de aplicaciones.

* 1. Previamente al envío de información, se utilizará un programa identificador/ descontaminador de virus para revisar los ficheros y posteriormente a la recepción se someterán a los sistemas y programas de aplicaciones al proceso de cuarentena establecidos (en caso de documentos de Office se “abrirán sin macros”).

Medida: Para el Envío de anexos a través de correo electrónico es necesario que el remitente exprese al destinatario que le adjunta un fichero, y además su nombre y longitud en Byte. La persona que recibe un anexo debe exigir que se cumpla con esta condición.

## 6.7 Respaldo de la Información.

**Medida:** El ESI, conjuntamente con los jefes de departamentos y los administradores de sistemas que realizan las salvas, son los responsables de las mismas.

**Procedimiento 26:** Respaldo de información y aplicaciones.

1. En las PC de los usuarios.
2. Realizar la salva de la información y de los registros del sistema en el servidor identificando de la siguiente forma: Salva/XXX/N.

Donde XXX, corresponde a la fecha de efectuada la salva:

N, es el número consecutivo comenzando por 1.

**Responsable:** Especialista de seguridad informática**.**

1. Anotar en el modelo de registro establecido para las Salva, **Registro No.6**, el nombre de la salva, el soporte donde está el responsable, lugar de conservación, cual es el nivel de acceso y la firma del responsable.

**Responsable:** Especialista de seguridad informática**.**

1. Verificar integridad de la información salvada.

**Responsable:** Director

1. Guardar la primera salva de la información en el servidor y la segunda en la biblioteca provincial Alex Urquiola.

**Responsable:** Especialista de seguridad informática.

## 6.8 Seguridad en Redes.

Procedimiento 27: Auditoria de eventos del sistema operativo.

1. Realizar mensualmente la revisión y análisis de los registros de los eventos generados por el sistema operativo de la red de la Dirección Provincial de Cultura.
2. Investigar las causas de cualquier anomalía detectada y determinar si se está en presencia de un incidente de seguridad, actuando según lo establecido para esos casos.
3. Emplear, cuando se requiera, el software SAWMILL para la revisión de las trazas de auditoría conjuntamente al administrador de red de la Dirección Provincial de Cultura.
4. Anotar las acciones realizadas y sus resultados en el registro de auditorías de eventos del sistema operativo [**Registro No. 5**](#_7.2_Registros)
5. Mantener la disponibilidad y actualización de las herramientas que garantizan la auditoría de los eventos del sistema operativo.

**Responsable:** ESI.

1. Realizar una verificación trimestral del cumplimiento de este procedimiento.

Responsable: Encargado de Seguridad Informática.

**Procedimiento 28:** Registro y análisis de trazas

1. En cada máquina y aprovechando las posibilidades de SO Windows 7 y demás sistemas operativos, se habilitará la auditoría de al menos los principales eventos que pudieran comprometer la seguridad informática (dentro de las Herramientas Administrativas).

**Responsable:** ESI

1. Todos esos chequeos se realizarán mensualmente mediante inspecciones.
2. Después de realizar el análisis de las trazas, se hará la salva de todos los logs con periodicidad mensual, manteniéndolas duplicadas en distintas áreas de la entidad.

**Responsable:** ESI.

**Medida:** El Director de la entidad, para asegurarse de que funcionen correctamente las TIC, instaura un sistema de prueba, que realiza el ESI, lo cual contará en el [**Registro No 7**](#_7.2_Registros).

**Procedimiento 29:** Realización de inspecciones

Las inspecciones se realizarán al nivel de área en toda la Entidad.

Primero:

1. Chequeará las tareas funcionales que debe efectuar cada cual de acuerdo a su responsabilidad.
2. Interrogará a los jefes de departamentos en las distintas instancias, especialistas y demás personas que utilizan las TIC para comprobar que dominan cuáles son sus tareas en el PSI.
3. 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

Segundo:

1. Realizará inspecciones independientes a cada una de las máquinas, efectuando pruebas en las que trate de violentar las medidas de seguridad.
2. Chequeará al igual que en las auditorías internas lo siguiente:

* Que los equipos estén correctamente instalados según las normas correspondientes y que los locales cuenten con las condiciones requeridas tanto técnicas (ventilación, instalación eléctrica, línea de comunicaciones) como de protección física (cierres seguros).
* Que estén implantados los mecanismos de identificación y autenticación de usuarios y de control da acceso y que estos cumplan los requisitos establecidos.
* Que los equipos se utilicen en las funciones para los que fueron asignados.
* Que el equipo esté protegido con productos antivirus y que 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 en los casos necesarios y las demás regulaciones de protección contra virus informático.
* Que se tenga la información necesaria para la restauración del sistema informático.
* 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 empresa.

**Responsable:** Responsable de la Seguridad Informática.

## 6.9 Gestión de Incidentes de Seguridad.

**Procedimiento 30:** Interrupción en las comunicaciones.

1. Informar a la Dirección de la Empresa la situación que se ha presentado.
2. Identificar si la interrupción es causada por factores externos o internos.
3. Reportar la interrupción al proveedor del servicio (ETECSA) si el problema radica en la línea de comunicación.
4. Restablecer la operación y establecer las causas de la interrupción y determinar posibles acciones para evitar su reiteración una vez solucionado el problema.
5. Anotar las acciones realizadas y sus resultados en el registro de incidencias. [**Registro No 5**](#_7.2_Registros).
6. Reportar el incidente a la OSRI.

**Responsable:** ESI

**Medida:** Ante la ocurrencia de cualquier incidente el ESI garantizará su reporte a la Oficina de Seguridad para las Redes Informáticas enviándose un email y a la instancia superior de la entidad.

**Procedimiento 31:** Reporte de incidencia de Seguridad Informática

Este debe incluir:

1. En qué consistió el incidente o violación.
2. Fecha y hora de comienzo del incidente y de su detección.
3. Implicaciones y daños para la entidad y para terceros.
4. Acciones iniciales tomadas.
5. Evaluación preliminar.

**Responsable:** ESI

**Medida:** Se designará una comisión presidida por el ESI e integrada por Especialistas no comprometidos directamente con el incidente, que realizará las investigaciones necesarias con el fin de esclarecer lo ocurrido, determinar el impacto, precisar los responsables y proponer la conducta a seguir.

**Procedimiento 32:** Accesos no autorizado a la red.

1. Al detectar un acceso no autorizado se informará a la Dirección sobre la situación que se ha presentado.
2. También se informa al ESI.
3. Se analiza que situación fue la que propició el acceso no autorizado.
4. Se evalúa si hubo daño a la información o al SO y se procede a la recuperación.

**Responsable:** Especialista del área.

1. Anotar las acciones realizadas y sus resultados en el registro de incidencias.

[Registro No 5.](#_7.2_Registros)

**Responsable:** Especialista Seguridad Informática.

**Procedimiento 33:** Acciones de información, neutralización, recuperación y selección de recursos ante las amenazas.

1. Contaminación de Virus Informático

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | **ESI o Informático** | **Director** |
| Información | Informa al ESI | De ser necesario informa al Director y registra la incidencia |  |
| Neutralización | Apaga la máquina y alerta de que no se use la misma | Revisa la máquina, se procede a la descontaminación |  |
| Recuperación |  | Se le comunica al usuario cuándo puede trabajar y se analizan las causas que propiciaron la entrada de virus | Crea la comisión de investigación y si el virus es desconocido se informa a la OSRI |

|  |  |
| --- | --- |
| **Hecho No 1** | **Selección de recursos fundamentales y alternativos** |
| Recursos | Discos que contengan la salvaguarda de los sistemas fundamentales |
| Ubicación | Nodo de Comunicaciones |
| Responsable | Director, ESI |

1. Destrucción o modificación del Sistema Operativo

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | **RSI o Informático** | **Director** |
| Información | Informa al ESI o al Informático encargado de administrar la red | De ser necesario informa al Director y registra la incidencia |  |
| Neutralización |  | Procede con la restauración y análisis de los ficheros dañados o modificados. Antes debe realizar un chequeo de las trazas para determinar las causas del problema | Crea la comisión de investigación |
| Recuperación |  | Determina las causas y actualiza el PSI | Informa a la OSRI |

|  |  |
| --- | --- |
| **Hecho No 2** | **Selección de recursos fundamentales y alternativos** |
| Recursos | Discos con la instalación de los Sistemas Operativos utilizados en entidad |
| Ubicación | Nodo de Comunicaciones |
| Responsable | Director, ESI |

1. Pérdida de la información

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | **RSI o Informático** | **Director** |
| Información | Informa al ESI o al Informático encargado de administrar la red | De ser necesario informa al Director y registra la incidencia |  |
| Neutralización |  | En caso de pérdida de alguna información restaurar salvas anteriores | De ser necesario toma medidas con los involucrados |
| Recuperación |  | Restaurar los servicios |  |

|  |  |
| --- | --- |
| **Hecho No 3** | **Selección de recursos fundamentales y alternativos** |
| Recursos | Compra de soporte externo para hacer salvas |
| Ubicación | Nodo de Comunicaciones |
| Responsable | Director, ESI |

1. Desastres naturales

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | **RSI o Informático** | **Director** |
| Información | Situación conocida por todos | Informa al Director y a los usuarios de la situación |  |
| Neutralización |  | Verifica que el equipamiento informático se encuentre ubicado en los locales seguros y los que no, sean trasladados hacia los mismos. Informar a los usuarios la suspensión del servicio | Velar porque se cumplan las medidas del Plan contra catástrofes de la entidad. |
| Recuperación |  | Ubicar los medios informáticos en sus respectivos locales y evaluar los posibles daños. Restaurar el servicio | Crear la comisión de evaluación de daños |

|  |  |
| --- | --- |
| **Hecho No 4** | **Selección de recursos fundamentales y alternativos** |
| Recursos | Necesidad de instalar un sistema de aterramiento con pararrayos.  Medios de evacuación: cajas, sogas |
| Ubicación | Área contra incendios |
| Responsable | Director, Técnico de Seguridad y Protección, ESI. |

1. Deterioro físico

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | **RSI o Informático** | **Director** |
| Información | Informa al ESI o al Informático encargado de administrar la red | Informa al Director de ser necesario |  |
| Neutralización |  | Analizar para resolver el problema, de no ser posible hacer diagnóstico y proponer la sustitución del equipamiento | Solicitar la adquisición del recurso |
| Recuperación |  | De ser por desgaste, se procede al cambio | Revisar la conclusión de la reparación |

|  |  |
| --- | --- |
| **Hecho No 5** | **Selección de recursos fundamentales y alternativos** |
| Recursos | Equipamiento para reposición |
| Ubicación | Almacén |
| Responsable | Director, ESI. |

1. Robo o hurto de los bienes informáticos y sus componentes

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | **RSI o Informático** | **Director** |
| Información | Informa al ESI o al Informático encargado de administrar la red | Informa al Director y registra el hecho en el libro de incidencias | Informa a las autoridades pertinentes |
| Neutralización |  | Instalar los sistemas en otro equipo | Informa al MININT y a la OSRI |
| Recuperación |  | Puesta en marcha de los servicios | Crea comisión de investigación |

|  |  |
| --- | --- |
| **Hecho No 6** | **Selección de recursos fundamentales y alternativos** |
| Recursos | Estudiar mecanismo de seguridad adecuado: cómputo, anclajes, etc. |
| Ubicación | Almacén y locales de los medios informáticos |
| Responsable | Director, Técnico de Seguridad y Protección, ESI. |

1. Fallo de software

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | **RSI o Informático** | **Director** |
| Información | Informa al ESI o al Informático encargado de administrar la red | Informa al Director y registra el hecho en el libro de incidencias |  |
| Neutralización |  | Se analiza cual es el software o módulo que falló | De ser necesario crea comisión de investigación |
| Recuperación |  | Reinstalar el software que falló de ser posible, sino contactar con el administrador del mismo | Informa a la OSRI si se sospecha que el fallo fue intencional |

|  |  |
| --- | --- |
| **Hecho No 7** | **Selección de recursos fundamentales y alternativos** |
| Recursos | Discos con la instalación de los Sistemas Operativos utilizados en la Empresa |
| Ubicación | Nodo de comunicaciones |
| Responsable | Director, ESI. |

1. Fallo de Hardware

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | **RSI o Informático** | **Director** |
| Información | Informa al ESI o al Informático encargado de administrar la red | Informa al Director y registra el hecho en el libro de incidencias |  |
| Neutralización |  | Contactar con los técnicos para que solucionen el fallo | De ser necesario crea comisión de investigación |
| Recuperación |  | Restablecer los sistemas e instalar las aplicaciones en otra Pc de ser posible | Informa a la OSRI si se sospecha que el fallo fue intencional |

|  |  |
| --- | --- |
| **Hecho No 8** | **Selección de recursos fundamentales y alternativos** |
| Recursos | Según el caso: Hardware reservados para estos eventos, presupuesto reservado para piezas de repuesto para posible recambio.  Disco de instalación del Windows.  Discos que contengan la salvaguarda de los sistemas |
| Ubicación | Almacén |
| Responsable | Director, ESI. |

1. Fallas del fluido eléctrico

|  |  |  |  |
| --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | **RSI o Informático** | **Director** |
| Información | Informa al ESI o al Informático encargado de administrar la red | Informa al Director y registra el hecho en el libro de incidencias |  |
| Neutralización |  | Orienta apagar los equipos y se dejan con las UPS los necesarios |  |
| Recuperación |  | Verifica si existe afectación y si no hay, restaura el servicio | Toma las medidas pertinentes si es necesaria la compra de algún equipo |

|  |  |
| --- | --- |
| **Hecho No 9** | **Selección de recursos fundamentales y alternativos** |
| Recursos | Fuentes (UPS) y estabilizadores de voltaje |
| Ubicación | Almacén |
| Responsable | Director, ESI. |

1. Falla de comunicaciones.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | | **RSI o Informático** | **Director** | |
| Información | Informa al ESI o al Informático encargado de administrar la red | | Informa al Director y registra el hecho en el libro de incidencias |  | |
| Neutralización |  | | Trata de solucionar el error. De no tener solución, contacta con el proveedor de servicios, avisa a Dirección Provincial de Cultura. Si el problema es del equipamiento, lo informa | De ser necesaria la compra de algún componente, autoriza la compra | |
| Recuperación |  | | Se le informa a los usuarios de la restauración de las comunicaciones |  | |
| **Hecho No 10** | | **Selección de recursos fundamentales y alternativos** | | |
| Recursos | | Equipos y piezas necesarios para efectuar la reparación | | |
| Ubicación | | Almacén | | |
| Responsable | | Director, ESI. | | |

1. Acceso no autorizado

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Acción por etapas** | **Persona que detecta** | | **RSI o Informático** | **Director** | |
| Información | Informa al ESI o al Informático encargado de administrar la red | | Informa al Director |  | |
| Neutralización |  | | Cambia la clave a la máquina y a los sistemas, así como revisa los niveles de acceso | Crea la comisión de investigación | |
| Recuperación |  | | En caso de alteración en la información, reinstala con las salvas pertinentes | De ser necesario informa a la OSRI | |
| **Hecho No 10** | | **Selección de recursos fundamentales y alternativos** | | |
| Recursos | | Discos que contengan la salvaguarda de los sistemas fundamentales | | |
| Ubicación | | Nodo de comunicaciones | | |
| Responsable | | Director, ESI. | | |

**7.****Anexos**

**Anexo 1: Identificación de los bienes Informáticos.**

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Descripción** | **Tipo** | **Ubicación** |
| D1 | 9 PC | RD GD, HD | 1 en dirección, 1 economía, 1 Casa de Cultura, 1 en biblioteca y 5 depósito |
| D2 | Informaciones de VERSAT | OT,SW | Economía |
| D3 | 2 router | GD | 1 en dirección y 1 en biblioteca |
| D4 | 1 teléfonos corporativos | OT | 1 dirección |

RD-Redes de diferentes tipos.

GD-Sistemas de gestión de datos.

CP-Sistemas de control de procesos.

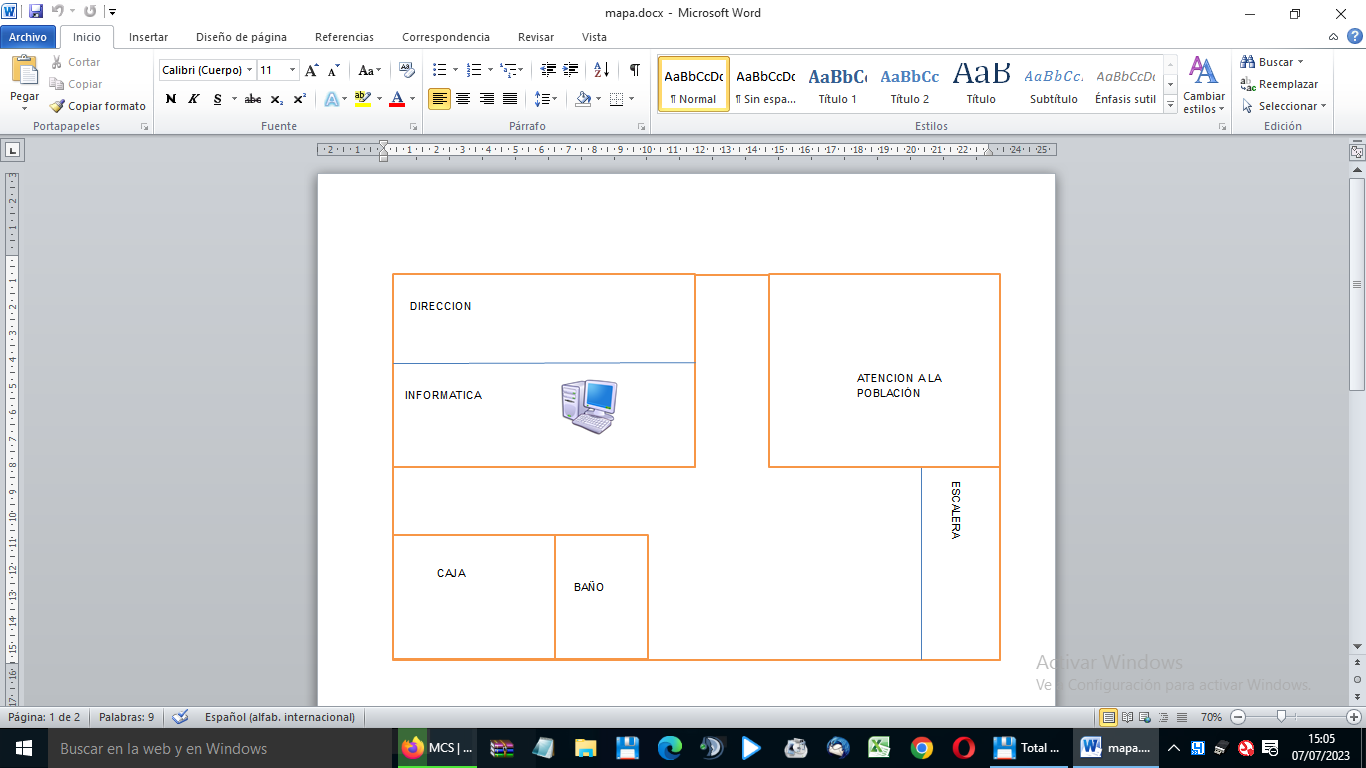
OT-Otros tipos de aplicaciones o sistemas.

HD-Hardware.

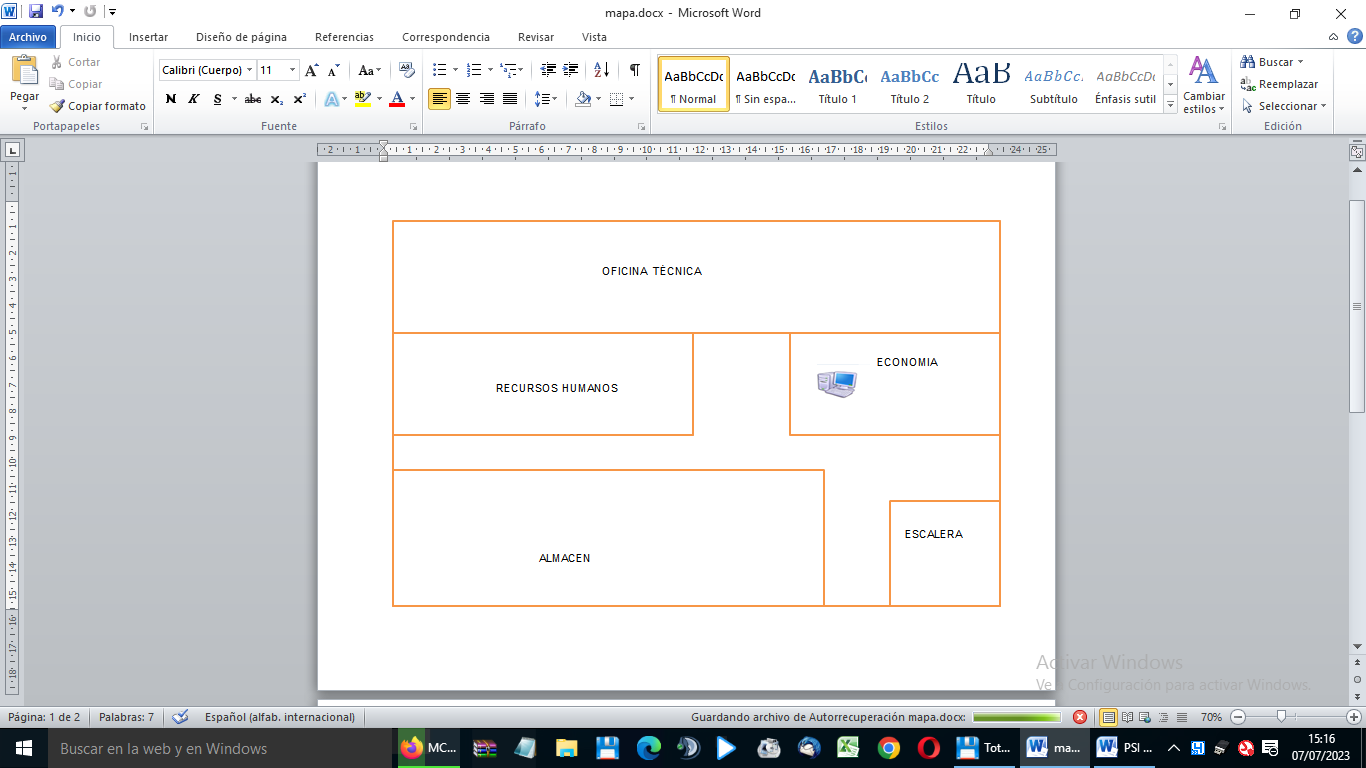
SW-Software

**Anexo 2: Diagrama de la Red**

**1er Nivel de la entidad**



**2do nivel de la entidad**



**Anexo 3: Equipo de trabajo para la implementación de la seguridad informática en la Escuela.**

|  |  |  |
| --- | --- | --- |
| **No** | **Nombre y Apellidos** | **Cargo** |
| **1** | José Luis Rodríguez Aria | Director |
| **2** | Oner E. Font Marrero | Técnico de Defensa y Seguridad y Protección |
| **3** | Aylen Bispo Trotman | Técnico en Informática |

## Listado nominal de usuarios con acceso a los servicios de red.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Nombre y Apellidos** | **Usuario** | **Correo** | | **Navegación** | |
| **Nacional** | **Internacional** | **Nacional** | **Internet** |
| Aylen Bispo Trotman | cacocum |  | X |  | X |

## 

## 7.2 Registros

**Registro No 1: Registro de entrada, salida y movimiento de tecnologías de información.**

**Área: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Datos del equipo: Tipo, Marca, Modelo, Configuración** | **No. Inventario** | **Fecha** | **Destino** | **Procedencia** | **Motivo del movto** | **Nombre del Funcionario que autoriza** | **Firma de quien autoriza** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Registro No 2: Control de soportes.**

**Área: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No. Consecutivo en el registro** | **Contenido Fundamental del soporte y clasificación** | **Trabajo para el que se destina el soporte** | **Nivel de acceso del soporte** | **Fecha y hora de alta** | **Fecha y hora de baja** | **Observaciones** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Registro No 3: Mantenimiento a los equipos de cómputo.**

**Área: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Equipos** | **Fecha del Mant.** | **Nombre del Técnico** | **Labor realizada** | **Observaciones** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Registro No 4: Registro de Software**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nombre del Software** | **Fecha de Adquisición** | **Vía utilizada** | **Soporte: tipo y cantidad** | **Nombre de quién lo adquirió** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**Registro No 5: Registro de Incidencias.**

**Área: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **No.** | **Fecha** | **Hora** | **Incidencia a registrar** | **Persona que detecta la incidencia** | **Observaciones** |
| **1** |  |  |  |  |  |
| **2** |  |  |  |  |  |
| **3** |  |  |  |  |  |

**Registro No 6:Registro de salvas**

**Área: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No** | **Nombre de la salva** | **Soporte** | **Responsable** | **Lugar de**  **conservación** | **Nivel de acceso** | **Firma** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**Registro No 7: Registro de Inspecciones**

**Área: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Equipo** | **Fecha de Inspección** | **Participantes** | **Situación detectada** | **Plan de medidas** | **Responsable del cumplimiento** | **Fecha de cumplimiento** |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

## 7.3Modelo de solicitud de servicios de red

**Datos del Solicitante Fecha:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

Nombre y Apellidos: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_C.I:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Centro/Institución: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Dpto: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Nombre de usuario: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SERVICIOS A SOLICITAR**

**Correo Electrónico: Navegación**

Nacional: \_\_\_\_\_ Internacional: \_ \_\_ WIFFI:\_\_\_ Nacional: \_\_\_\_\_\_\_ Internet: \_\_\_ Redes Sociales/Correo Exterior: \_\_\_\_\_\_\_\_

**Conectividad: Comunicación:**

**Conmutado (\*): \_\_\_\_ LAN: \_\_\_\_\_\_ ADSL:\_\_\_\_\_\_ WIFFI: \_\_\_\_\_\_**

**\* Telf: (2) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**RAZONES DE LA SOLICITUD**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Firma del solicitante:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Nombre y Apellidos Jefe de Area/Centro/Institc Autoriza:**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Firma y Cuño Firma y Cuño**

**Notas aclaratorias:**

* Este servicio será renovado a los dos años de solicitado.
* Al causar baja de la entidad el servicio será cancelado
* En el caso de los accesos conmutados solo se permitirá la conexión desde dos teléfonos que el usuario decida, estos serán objeto de verificación periódicamente y en caso de ocurrir violaciones se procederá a desconectar el servicio.
* Solo se aprobarán las solicitudes firmadas por el Director Provincial

## 7.4 Código de Ética para el uso del Correo Electrónico e Internet

**CÓDIGO DE ETICA DE LA RED CUBARTE**

El Código de Ética recoge un conjunto de normas de conducta tendentes a crear y preservar una cultura de uso de la red acorde con los principios de nuestra sociedad y estimula su utilización racional, sobre la base del respeto al resto de los usuarios y a los objetivos para los cuales fue creada.

Todos los nodos y usuarios del Sistema de la Cultura quedan sujetos al cumplimiento de las regulaciones establecidas por CUBARTE, entidad facultada por el Ministro de Cultura para establecer las regulaciones y controlar la conexión a la Red CUBARTE y a la Red Global Internet, de las instituciones culturales y usuarios finales del Sistema de la Cultura.

Con el objetivo de regular el uso de los sistemas y servicios instalados en la red de forma tal que cumpla la misión y objetivos de su creación se establece:

• El permiso de acceso a la red y los servicios personalizados (cuentas) en la misma deben ser utilizados para acceder a información cultural, científico - técnica y en general cualquier tipo de información en función de y para el desarrollo de la cultura. CUBARTE es, en esencia, un instrumento de trabajo para los trabajadores, escritores y artistas del Sistema de la Cultura.

• El permiso de acceso a la red y sus servicios es personalizado e intransferible. Ningún usuario está autorizado para transferir dichos servicios a terceras personas. La detección de algún tipo de transferencia de servicios, dígase cesión de acceso, por préstamo, alquiler o arrendamiento, conllevará a la cancelación inmediata del servicio.

• Dado el carácter agresivo del envío de mensajes anticubanos por parte de organizaciones contrarrevolucionarias y ante la ocurrencia de este tipo de hechos, se notificará inmediatamente a CUBARTE, a la dirección de correo proteccion@redcubarte.cult.cu. Este tipo de mensajes, no debe redistribuirse a ninguna otra cuenta o usuario. Por su parte, la administración de la red tomará las medidas necesarias para eliminar o minimizar la posibilidad de realización de esa actividad y se aplicará lo establecido en la ley penal vigente.

• La red CUBARTE ha sido concebida para producir, distribuir, divulgar, trasmitir y difundir la información cultural desde y hacia la República de Cuba cualquier información que no se avenga a tales propósitos no debe ser permitida. La integridad de la información que circule por la Red es de total responsabilidad del jefe del área o del usuario conectado a la Red.

• Toda actividad comercial que utilice la Red como vehículo de promoción deberá contar con las licencias comerciales correspondientes. La administración de la red velará por el cumplimiento de este precepto y aplicará, dadas las circunstancias de cada caso, tarifas comerciales que contribuyan a sufragar los gastos de mantenimiento y desarrollo.

• Todo usuario de la red debe respetar las opiniones del resto, en los foros de discusión y otras modalidades de debate, por lo que bajo ningún concepto deben utilizar frases agresivas o de desprecio.

• Los servicios que se ofrecen en la red CUBARTE, deben ser usados con racionalidad, ocupando el tiempo estrictamente necesario, sobre la base de que es un servicio de uso colectivo y en el que todos tienen iguales derechos.

• La utilización de la Red para diseminar información requiere ser regulada. La incorporación de revistas, boletines y otras formas similares de difusión informativa electrónica, deberán estar avaladas por el registro de publicaciones (ISSN) y su envío centralizado por los nodos de la Red. No se permitirá utilizar de forma indiscriminada la Red ni enviar información que no cuente con la autorización del destinatario.

• El uso de los servicios facilitados por la Red CUBARTE, deberá contribuir a preservar la imagen y reputación de cada institución, del Ministerio de Cultura y el país.

Es de obligatorio cumplimiento para todos los clientes y usuarios de la Red CUBARTE, lo dispuesto en el presente código de ética CUBARTE, como entidad responsable de la aplicación de la Informática del Ministerio de Cultura, tiene la facultad de monitorear toda cuenta electrónica en cumplimiento de su misión de velar por la integridad de la

Información que circula por la red CUBARTE, responsabilidad que comparte con los restantes nodos de la Red. Al detectarse cualquier violación, CUBARTE determinará la magnitud de la misma y tomará las medidas que correspondan, inhabilitándose de forma temporal o permanente la cuenta, de acuerdo al caso y de conformidad con lo dispuesto en el presente Código de Ética.

Firma: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## 

## 7.5 Modelo Autorización de Permanencia fuera del horario laboral.

A: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

De: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Se autoriza a los siguientes compañeros a permanecer en la escuela en el departamento de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ después de las \_\_\_\_\_\_\_\_ horas por problemas de trabajo.

El horario autorizado es: día \_\_\_\_\_\_\_\_\_\_, Desde: \_\_\_\_\_\_\_\_\_\_\_\_\_ Hasta: \_\_\_\_\_\_\_\_\_\_\_\_\_\_

Los compañeros son:

Firma y Cargo

## 7.6 Modelo de Autorización de Entrada/Salida de las Tecnologías Informáticas

EQUIPO (S): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FECHA: \_\_\_\_\_\_\_\_\_\_\_\_ HORA: \_\_\_\_\_\_\_\_\_\_\_\_ ENTRADA: \_\_\_\_\_\_\_\_ SALIDA: \_\_\_\_\_\_\_\_

TECNICO QUE REALIZA EL TRASLADO: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

SE AUTORIZA LA (ENTRADA/SALIDA) CON DESTINO A \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ PROCEDENTE DE \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ CON LOS SIGUIENTES PROPÓSITOS: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

NOMBRE Y APELLIDOS DE QUIEN AUTORIZA: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FIRMA: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

FECHA: \_\_\_\_\_\_\_\_\_\_ HORA: \_\_\_\_\_\_\_\_ ENTRADA: \_\_\_\_\_\_\_\_ SALIDA: \_\_\_\_\_\_\_\_\_

## 

## 7.7 Base legal

* Resolución 6/96 del MININT. Reglamento de Seguridad para las Tecnologías de Información.
* Decreto Ley 199/99 del Consejo de Estado sobre la Seguridad y Protección de la Información Oficial.
* Resolución 1/00 del MININT que pone en vigor el Reglamento sobre la Seguridad y Protección de la Información Oficial.
* Resolución Conjunta MIC-MFP 2004.
* Resolución 204/96 del SIME. Reglamento sobre la Protección y Seguridad Técnica de los Sistemas Informáticos.
* Resolución 128/11 del MIC. Reglamento sobre las redes privadas de Datos.
* Decreto Ley 370/18 Sobre la Informatización de la Sociedad en Cuba del CE.
* Decreto 360/19 Sobre la seguridad de las Tecnologías de la Información y la Comunicación y la Defensa del Ciberespacio Nacional, del CM.
* Resolución 126/19 del MC Aprueba el Reglamento que establecen las medidas de Control de Seguridad en las redes de datos.
* Resolución 128/19 del MC que establece el Reglamento de Seguridad de las Tecnologías de la Información y Comunicación.
* Resolución 129/19 del MC Metodología Para la Gestión de la Seguridad informática.
* Resolución 60/11 de la CGR. (NORMAS DEL SISTEMA DE CONTROL INTERNO.

## 7.8 Control de cambios.

En el siguiente registro se incluirán los cambios que se realicen, la fecha, la parte del plan que se modifica dejando bien claro todo lo que se realizó, el nombre de la persona que autoriza la modificación y el de la persona que la realiza y la firma.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Fecha** | **Parte del PSI que se modifica** | **Nombre del que autoriza la modificación** | **Nombre del realiza la modificación** | **Firma** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |