CENTRO DE INVESTIGACIONES Y ESTUDIOS SUPERIORES
EN ANTROPOLOGÍA SOCIAL

MANUAL DE POLÍTICAS Y ESTÁNDARES DE SEGURIDAD INFORMÁTICA PARA USUARIOS

Subdirección de Informática

Elaboró	Aprobó	Autorizó
L.I.. Roberto de J. González Dávila *Coordinador de Sistemas*	*Ing. Gabriel Canizales Castillo* *Titular de la UTIC*	*Mtro. Fabián Elí García Becerril* *Director de Administración*

Contenido

Introducción

El Centro de Investigaciones y Estudios Superiores en Antropología Social, CIESAS, como toda organización actual que requiere del aprovechamiento de las tecnologías de la Información y la Comunicación (TIC) para llevar a cabo sus objetivos institucionales, obteniendo de éstas sus beneficios al facilitar las funciones administrativas, confiables y verificables entre otros, requiere a su vez contar con políticas, bases claras, así como procesos con estándares que aseguren el debido manejo de la información, así como su adecuado resguardo, en el amplio concepto que hoy se identifica como "Seguridad Informativa".

Entendiendo que las TIC son una innovación mundial de reciente generación, los temas a su alrededor también se han venido creando conforme se generan las necesidades, entre otros la Seguridad Informática, la cual es entendida actualmente como: *"El conjunto de normas, mecanismos, herramientas, procedimientos y recursos orientados a brindar protección a la información resguardando su disponibilidad, integridad y confidencialidad"*, es una tarea en la que se deben identificar, evaluar y administrar los riesgos, basados en políticas y estándares que cubran las necesidades del CIESAS en ésta materia.

El presente documento tiene como objetivo establecer las políticas y bases que permitan generar un ambiente de seguridad informática en CIESAS, para lo cual se organiza en seis dominios generales de seguridad, orientados a los usuarios de la informática a través de los siguientes puntos:

- Seguridad Física y Ambiental.
- Administración de Operaciones de Cómputo.
- Controles de Acceso Lógico.
- Seguridad de Personal.
- Cumplimiento.
- Continuidad del Negocio

Estas políticas en seguridad informática se encuentran alineadas con el Estándar ISO/IEC 27002:2013 que proviene del Estándar Británico BS 7799.

Objetivo

El presente instrumento tiene como finalidad definir y difundir las políticas y estándares de Seguridad Informática que deberán observar los usuarios de servicios de tecnologías de información

TIC, para la protección y aprovechamiento de los activos tecnológicos y la información del Centro de Investigaciones y Estudios Superiores en Antropología Social, CIESAS, siendo de carácter obligatorio su cumplimiento y seguimiento.

Alcance

Se describen las políticas y los estándares de seguridad que deberán ser observadas de forma obligatoria por todos los usuarios para el buen uso del equipo de cómputo, aplicaciones y servicios informáticos del CIESAS.

Marco Jurídico

Los ordenamientos jurídicos referidos en este apartado, se citan de manera enunciativa y no limitativa.

1. Constitución Política de los Estados Unidos Mexicanos.
2. Código Penal Federal.
3. Ley de Ciencia y Tecnología
4. Ley Orgánica de la Administración Pública Federal.
5. Ley Orgánica de la Procuraduría General de la República.
6. Ley General de Bienes Nacionales.
7. Ley Federal de las Entidades Paraestatales.
8. Ley Federal de Presupuesto y Responsabilidad Hacendaria.
9. Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.
10. Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.
11. Ley Federal de Manejo de Datos Personales
12. Ley Federal de Responsabilidades Administrativas de los Servidores Públicos.
13. Ley Federal de Telecomunicaciones.
14. Ley Federal sobre Metrología y Normalización.
15. Ley Federal de Archivos.

16. Ley de Seguridad Nacional.

17. Ley de Firma Electrónica Avanzada.

18. Ley del Sistema de Horario en los Estados Unidos Mexicanos.

19. Reglamento de la Oficina de la Presidencia de la República.

20. Reglamento Interior de la Secretaría de Gobernación.

21. Reglamento Interior de la Secretaría de la Función Pública.

22. Reglamento de Ley Federal de las Entidades Paraestatales.

23. Reglamento de la Ley Federal de Presupuesto y Responsabilidad Hacendaria.

24. Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

25. Reglamento de la Ley de Firma Electrónica Avanzada.

26. Reglamento para la Coordinación de Acciones Ejecutivas en Materia de Seguridad Nacional.

27. Plan Nacional de Desarrollo 2013-2018.

28. Programa para un Gobierno Cercano y Moderno 2013-2018.

29. Decreto que establece las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal.

30. Lineamientos para la aplicación y seguimiento de las medidas para el uso eficiente, transparente y eficaz de los recursos públicos, y las acciones de disciplina presupuestaria en el ejercicio del gasto público, así como para la modernización de la Administración Pública Federal.

31. Lineamientos de Protección de Datos Personales, expedidos por el entonces Instituto Federal de Acceso a la Información Pública.

32. Recomendaciones sobre medidas de seguridad aplicables a los Sistemas de Datos Personales, emitidos por el entonces Instituto Federal de Acceso a la Información Pública.

33. Acuerdo por el que se establece el Esquema de Interoperabilidad y de Datos Abiertos de la Administración Pública Federal.

34. Acuerdo que tiene por objeto crear en forma permanente la Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico.

35. Lineamientos para la operación, funcionalidad, comunicación y seguridad de los sistemas automatizados de control de gestión.

36. Documento Técnico para la Interoperabilidad de los Sistemas Automatizados de Control de Gestión.

37. ACUERDO por el que se modifican las políticas y disposiciones para la Estrategia Digital Nacional, en materia de tecnologías de la información y comunicaciones, y en la de seguridad de la información, así como el Manual Administrativo de Aplicación General en dichas materias.

Justificación

La Subdirección de Informática tiene el compromiso y la responsabilidad de definir políticas y estándares en materia de informática a fin de dar cumplimiento a lo establecido en el proceso ASI del MAAGTIC-SI derivado del acuerdo para la Estrategia Digital Nacional, además de ofrecer un marco adecuado para el control y seguridad de todos los elementos informáticos del Centro.

Sanciones por incumplimiento

El cumplimiento de lo establecido en el presente Manual es de carácter obligatorio para todo el personal, estudiantes y usuarios de las TIC en CIESAS.

El incumplimiento puede ser causa de responsabilidad Administrativa o Penal en consideración a su naturaleza y gravedad, por parte de las Autoridades competentes.

Beneficios

Las políticas y estándares de seguridad informática establecidas dentro de este documento son la base para la protección de los activos tecnológicos e información del CIESAS.

1.- SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

Los recursos humanos de cualquier organización deben considerarse como un elemento básico en su funcionamiento. Derivado de lo anterior, los usuarios del CIESAS, deberán cumplir con lo establecido en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios, a fin de aportar de forma específica en una operación informática orientada al aprovechamiento y seguridad de la información y activos tecnológicos con que se cuenta.

Obligaciones de los usuarios

Es responsabilidad de los usuarios de activos y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.

Entrenamiento en seguridad informática

Todos los empleados y funcionarios del CIESAS de nuevo ingreso deberán contar con la inducción sobre el Manual de Políticas y Estándares de Seguridad Informática para Usuarios, a cargo de la Subdirección de informática a quien compete dar a conocer las obligaciones para los usuarios y las sanciones que pueden incurrir en caso de incumplimiento.

Medidas disciplinarias

- En los casos que la Subdirección de Informática identifique como incumplimiento al presente Manual, procederá a remitir el reporte o denuncia correspondiente al Órgano Interno de Control, para los efectos de su competencia.
- Cuando el incumplimiento se detecte por parte de usuarios no empleados o funcionarios del CIESAS, procederá a remitir el reporte a la Dirección Académica y/o Director Regional del CIESAS, para los efectos de su competencia y atribuciones.
- El robo, daño, divulgación de información reservada o confidencial del CIESAS, o de que presuma la comisión de un delito de carácter informático, se considerará en todos los casos como grave procediendo a dar aviso a la Dirección de Administración para que por su conducto se formulen las denuncias ante las autoridades correspondientes.

2. CONTROL DE ACCESOS

Cada usuario es responsable de sus identificadores de usuario y contraseñas necesarios para acceder a la información y a la infraestructura tecnológica del CIESAS, por lo cual deberá mantenerlo de forma confidencial.

Controles de acceso lógico

- El acceso a la infraestructura tecnológica del CIESAS para personal externo debe ser autorizado al menos por un Director de área del CIESAS, quien deberá notificarlo a la Subdirección de Informática quien dará su visto bueno y lo habilitará.
- Todos los usuarios de servicios de información son responsables por el Identificador de Usuario y contraseña que recibe para el uso y acceso de los recursos
- Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la Subdirección de Informática antes de poder usar la infraestructura tecnológica del CIESAS.
- Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del CIESAS, a menos que se tenga la autorización del dueño de la información y de la Subdirección de Informática.
- Cada usuario que acceda a la infraestructura tecnológica del CIESAS debe contar con un Identificador de Usuario único y personalizado. Por lo cual no está permitido el uso de un mismo Identificador de Usuario por varios usuarios.
- Los usuarios son responsables de todas las actividades realizadas con su Identificador de Usuario. Los usuarios no deben divulgar ni permitir que otros utilicen sus identificadores de usuario, al igual que tienen prohibido utilizar el de otros usuarios.

Administración de privilegios

Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso a la infraestructura tecnológica del CIESAS, deberán ser notificados a la Subdirección de Informática con el visto bueno de su Director de área.

Administración y uso de Contraseñas

- La asignación de la contraseña debe ser realizada de forma individual, por lo que el uso de contraseñas compartidas está prohibido.
- Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá enviar un reporte a la Subdirección de Informática para que se le proporcione una nueva contraseña y una vez que lo reciba deberá cambiarlo en el momento en que acceda nuevamente a la infraestructura tecnológica.
- La obtención o cambio de una contraseña debe hacerse de forma segura, el usuario deberá acreditarse ante la Subdirección de Informática como empleado del CIESAS.
- Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

- Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.
- Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus Contraseñas:
  - Deben estar compuestos de al menos ocho (8) caracteres y máximo diez (10), estos caracteres deben ser alfanuméricos y de preferencia deben contener una mayúscula y un carácter especial (/,#,$,&,=, etc).
  - Deben ser difíciles de adivinar, esto implica que las Contraseñas no deben relacionarse con el trabajo o la vida personal del usuario, y no deben contener caracteres que expresen listas secuenciales y caracteres de control.
  - No deben ser idénticos o similares a contraseñas que hayan usado previamente.

- La contraseña tendrá una vigencia de 180 días, finalizando este periodo el usuario recibe una solicitud electrónica de cambio de contraseña.
- Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarlo inmediatamente.
- Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.
- Los cambios o desbloqueo de contraseñas solicitados por el usuario a la Subdirección de Informática serán notificados con posterioridad por correo electrónico al solicitante con copia al Director de área correspondiente, de tal forma que se pueda detectar y reportar cualquier cambio no solicitado.
- En el momento de que cualquier empleado del CIESAS deje de prestar sus servicios en el Centro, el responsable de su área de adscripción, deberá de dar aviso al Departamento de Recursos Humanos y a la Subdirección de Informática para solicitar dar de baja o inhabilitar, según sea el caso, las cuentas de usuario pertenecientes a este usuario.
- Cada 6 meses, la Subdirección de Informática procederá a revisar la vigencia de las cuentas de acceso existentes y los privilegios otorgados para su actualización.
- Las claves de acceso a todos los equipos de cómputo personal deberán ser registrados y resguardados por el jefe responsable de cada área.

Control de accesos remotos

- Está prohibido el acceso a redes externas vía dial-up, cualquier excepción deberá ser documentada y contar con el visto bueno de la Subdirección de Informática.
- La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y de la Subdirección de Informática.

3.- SEGURIDAD FÍSICA Y AMBIENTAL

Los mecanismos de control de acceso físico a las instalaciones del CIESAS sólo deberán permitir el acceso del personal y terceros autorizados, en el entendido que los accesos a las áreas restringidas sólo estarán permitidas para el personal que cuente con las autorizaciones específicas, a fin de salvaguardar los equipos de cómputo y de comunicaciones, en especial las instalaciones y el centro de cómputo del CIESAS.

Resguardo y protección de la información

- Todos los usuarios están obligados a reportar de forma inmediata a la Subdirección de Informática, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser entre otros: fugas de agua, conatos de incendio, etc.
- Los usuarios tienen la obligación de proteger los discos, memorias, unidades de disco externas, etc., que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial.
- Es responsabilidad del usuario evitar en todo momento la fuga de la información del CIESAS que se encuentre almacenada en los equipos de cómputo personal que tenga asignados, siendo responsables en todo momento por el uso indebido de información reservada o confidencial a su cargo, en términos de la legislación aplicable.

Controles de acceso físico

- Toda persona que tenga acceso a las instalaciones del CIESAS, está obligada a registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad del CIESAS, el cual deberá retirar el mismo día, registrando su salida. En caso que los equipos o bienes deban permanecer en la institución por un plazo mayor, deberán tramitar e informar el caso específico, para su debido control.
- Las computadoras personales, las computadoras portátiles y cualquier activo de tecnología de información propiedad o bajo la custodia del CIESAS, podrá salir de las instalaciones del CIESAS únicamente con la autorización de salida de la Jefatura de Recursos Materiales. En las unidades académicas, a través de la autorización que brinde el director regional o el administrador de la sede.

Seguridad en áreas de trabajo

El centro de cómputo del CIESAS es área restringida, por lo que sólo el personal autorizado por la Subdirección de Informática puede acceder a él.

Protección y ubicación de los equipos

- Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Subdirección de Informática, en caso de requerir este servicio deberán solicitarlo a la Subdirección de Informática o a la Coordinación de Sistemas.
- La Jefatura de Recursos Materiales será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Subdirección de Informática.
- El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones del CIESAS.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Es responsabilidad de los usuarios almacenar su información en las carpetas de "Documentos" o en las creadas por él para este efecto, respetando las que están destinadas para archivos de programa y sistema operativo.
- Mientras se opera el equipo de cómputo, deberá evitarse el consumo de alimentos o bebidas.
- Se debe evitar colocar objetos encima del equipo o cubrir los conductos de ventilación del monitor o del CPU.
- Se debe mantener el equipo informático en un entorno limpio y sin humedad
- El usuario debe asegurarse que los cables de conexión no sean pisados o maltratados al colocar otros objetos encima o contra ellos.
- Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación a la Subdirección de Informática a través de un plan detallado de movimientos debidamente autorizados por el director del área que corresponda.
- Queda prohibido que el usuario abra o desarme los equipos de cómputo.

Mantenimiento de equipo

- Únicamente el personal autorizado por la Subdirección de Informática podrá llevar a cabo los servicios y reparaciones al equipo informático, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

- Los usuarios deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación. En caso de no poder realizarlo personalmente por cualquier razón, deberá solicitar a la Subdirección de Informática el apoyo para realizarlo.

Pérdida o extravío de equipo

- Los equipos entregados en forma personal bajo custodia a personal de CIESAS, deberá ser devueltos a la Subdirección de Informática en los casos que dejen de ser útiles o necesarios para los fines asignados, lo que permite reducir el riesgo para el responsable y la reasignación en su caso a áreas demandantes.
- El usuario que tenga bajo su resguardo algún equipo de cómputo, es responsable de su uso debido y custodia; en consecuencia, responderá por el bien de acuerdo a la normatividad vigente en los casos de robo, extravío, daño doloso o por negligencia inexcusable y por pérdida o extravío del mismo.
- El resguardo para las laptops, tiene el carácter de personal y es de carácter intransferible. Por tal motivo, queda prohibido su préstamo o entrega bajo ningún tipo, a personal de CIESAS o tercero ajeno. El incumplimiento a lo señalado genera responsabilidad de servidor público que deberá ser calificada por el órgano interno de control.
- El usuario de un equipo TIC bajo su custodia deberá dar aviso inmediato a la Subdirección de Informática, Órgano Interno de Control y Departamento de Recursos Materiales de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo. Entendido por inmediato, tan pronto como tenga noticia de la desaparición. El incumplimiento de esta disposición agrava la responsabilidad, que en su caso, se hubiera incurrido.

Equipo desatendido

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla (screensaver) previamente instalados y autorizados por la Subdirección de Informática cuando no se encuentren en su lugar de trabajo.

Uso de dispositivos especiales

- Queda prohibido el uso de (ANTENAS WI-FI, SWITCHES) sin la previa consulta y autorización de la Subdirección de Informática.

- Si algún área por requerimientos muy específicos del tipo de aplicación o servicio de información tiene la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por su responsable de área (Subdirector o Director).

Daño del equipo

El equipo de cómputo o cualquier recurso de tecnología de información que sufra alguna descompostura por maltrato, descuido o negligencia por parte del usuario quien resguarda el equipo, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado. Para tal caso la Subdirección de Informática determinará la causa de dicha descompostura.

4.- SEGURIDAD Y ADMINISTRACIÓN DE OPERACIONES DE CÓMPUTO Y TELECOMUNICACIONES

Los usuarios deberán utilizar los mecanismos institucionales para proteger la información que reside y utiliza la infraestructura tecnológica del CIESAS. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser almacenada o transmitida, ya sea dentro de la red interna del CIESAS o hacia redes externas como Internet.

Los usuarios del CIESAS que hagan uso de equipo de cómputo, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus o malware.

Uso de medios de almacenamiento

- Los usuarios deberán respaldar diariamente la información sensitiva y crítica que se encuentre en sus computadoras asignadas.
- En caso de que por el volumen de información se requiera algún respaldo en un disco externo, este servicio deberá solicitarse por escrito a la Subdirección de Informática y con la firma del Director o Subdirector del área correspondiente.
- Los usuarios de informática del CIESAS deben conservar los registros o información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial, de conformidad a las disposiciones que emita el Comité de Información del CIESAS, en términos de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.

- Las actividades que realicen los usuarios en la infraestructura de Tecnología de Información del CIESAS son registradas y susceptibles de auditoria.
- Es responsabilidad de los usuarios hacer respaldo de su información periódicamente en los modelos de servicios locales o en la nube que proporcione el Centro.
- Es responsabilidad de los usuarios que manejen softwares especializados realizar respaldos del contenido de los datos en los servicios que proporcione el Centro.

Instalación de software.

- Los usuarios que requieran la instalación de software que no sea propiedad del CIESAS, deberán justificar su uso y solicitar su autorización a la Subdirección de Informática, a través de un oficio firmado por su Dirección de adscripción, indicando el equipo de cómputo donde se instalará el software y el período de tiempo que permanecerá dicha instalación.
- Se considera una falta grave el que los usuarios instalen cualquier tipo de programa (software) en sus computadoras, servidores, o cualquier equipo conectado a la red del CIESAS, incluso de carácter gratuito que no esté autorizado por la Subdirección de Informática.

Identificación de incidentes

- El usuario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo de inmediato a la Subdirección de Informática, indicando con la mayor claridad posible los datos por los cuales lo considera un incidente de seguridad informática.
- Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el usuario informático deberá notificar a su Director de adscripción.
- Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del CIESAS debe ser reportado a la Subdirección de Informática.
- Es responsabilidad del usuario al dar aviso de incidente el guardar copia del reporte a fin de facilitar el deslinde de responsabilidades en que se pudo haber incurrido.

Administración de la configuración

- Los usuarios de las áreas del CIESAS no tienen autorización para establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro

tipo de protocolo para la transferencia de información empleando la infraestructura de red del CIESAS, sin la autorización de la Subdirección de Informática.

- La configuración de las conexiones de red de los equipos del CIESAS sólo podrá ser modificada por el personal del área de informática o mediante una autorización específica al respecto por parte de la Subdirección de Informática.

Seguridad para la red

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por la Subdirección de Informática, en la cual los usuarios realicen la exploración de los recursos informáticos en la red del CIESAS, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

Uso del Correo electrónico

- La asignación de una cuenta de correo electrónico, deberá solicitarse por escrito a la Subdirección de Informática, atendiendo lo especificado para este efecto en el procedimiento correspondiente y señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del Director del área que corresponda.
- Los usuarios de cuentas de correo institucional al aceptar su uso, aceptan expresamente que están utilizando un medio de comunicación de una institución de carácter público Federal y por lo mismo, deberán abstenerse de utilizarla para actividades o con contenidos de carácter estrictamente personal.
- Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al CIESAS, a menos que cuente con la autorización de la Dirección de adscripción.
- Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información propiedad del CIESAS. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
- Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptada y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y atribuciones y en el marco de las funciones y atribuciones que tiene asignadas por el CIESAS.
- El CIESAS se reserva el derecho a acceder y revelar todos los mensajes enviados por este medio para cualquier propósito y revisar las comunicaciones vía correo electrónico de personal, a fin de garantizar la seguridad del sistema y el cumplimiento de las políticas y

bases establecidas, así como la no comisión de conductas que puedan resultar calificables como delitos informáticos en términos de la legislación aplicable.

- Los usuarios de las TIC de CIESAS también deberán abstenerse de utilizar los mismos como medio para el uso de correos personales, y en especial para la recepción de información ajena a las actividades que tiene asignadas en la institución.
- El usuario debe de utilizar el correo electrónico del CIESAS única y exclusivamente a los recursos que tenga asignados y las facultades que le hayan sido atribuidas para el desempeño de su empleo, cargo o comisión, quedando prohibido cualquier otro uso.
- Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.
- Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

Controles contra código malicioso

- Para prevenir infecciones por virus informático, los usuarios del CIESAS deberán abstenerse en todo tiempo de hacer uso de cualquier clase de software que no haya sido proporcionado o previamente validado por la Subdirección de Informática.
- Los usuarios del CIESAS deben verificar que la información y los medios de almacenamiento, considerando al menos memorias flash, CD's, discos externos, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Subdirección de Informática.
- Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.
- Ningún usuario del CIESAS debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o en otros casos impedir el funcionamiento de cualquier memoria de computadora, archivos de sistema, o software. Mucho menos probarlos en cualquiera de los ambientes o plataformas del CIESAS. El incumplimiento de este estándar será considerado una falta grave.
- Ningún usuario, empleado o personal externo, podrá descargar o "bajar" software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Subdirección de Informática.
- Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar a la Subdirección de Informática para la detección y erradicación del virus.

- Cada usuario que tenga bajo su resguardo algún equipo de cómputo personal portátil, será responsable de solicitar a la Subdirección de Informática periódicamente las actualizaciones del software antivirus.
- Los usuarios no deberán alterar o eliminar, las configuraciones de seguridad para detectar y/o prevenir la propagación de virus que sean implantadas por el CIESAS en: Antivirus, Outlook, office, Navegadores u otros programas.
- Debido a que algunos virus son extremadamente complejos, ningún usuario del CIESAS debe intentar erradicarlos de las computadoras.

Internet

- El acceso a Internet provisto a los usuarios del CIESAS es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.
- La asignación del servicio de Internet, deberá solicitarse por escrito a la Subdirección de Informática, señalando los motivos por los que se desea el servicio. Esta solicitud deberá contar con el visto bueno del subdirector del área correspondiente.
- Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el CIESAS.
- El personal que visita CIESAS cuando lo solicite, se le podrá autorizar en forma personal la conexión a internet de la Institución (mediante la clave de acceso) en su equipo; no obstante, el permiso otorgado no implica autorización alguna para que pueda a través de sistemas o dispositivos compartir con terceros el uso de internet que le fue concedido.
- Los usuarios de Internet del CIESAS tienen que reportar todos los incidentes de seguridad informática a la Subdirección de Informática inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.
- Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que:
  - Serán sujetos de monitoreo de las actividades que realiza en Internet.
  - Son sabedores que existe la prohibición al acceso de páginas no autorizadas, como son todas aquellas que promueven o facilitan la propagación de la pornografía en todas sus formas, la propaganda política (en épocas electorales), la propagación o promoción de cualquier forma de discriminación, violencia social y familiar, entre otros, salvo los casos que se utilice como medio para investigación social conforme a un protocolo debidamente registrado.
  - Son sabedores que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados.
  - Son sabedores que existe la prohibición de descarga de software sin la autorización de la Subdirección de Informática.
  - La utilización de Internet es para el desempeño de su función y puesto en el CIESAS y no para propósitos personales.

- El acceso a Internet se encontrará sujeto al filtrado de contenidos que defina la Subdirección de Informática.

5.- CUMPLIMIENTO DE SEGURIDAD INFORMÁTICA

La Subdirección de Informática tiene como parte de sus funciones, proponer y revisar el cumplimiento de normas y políticas de seguridad que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como de la información existente en general.

Derechos de propiedad intelectual

- Está prohibido por las leyes de derechos de autor y por el CIESAS, realizar copias no autorizadas de software, ya sea adquirido o desarrollado por el CIESAS.
- Los sistemas desarrollados por personal interno o externo que controle la Subdirección de Informática son propiedad intelectual del CIESAS.

Revisiones del cumplimiento

- La Subdirección de Informática realizará acciones de verificación del cumplimiento del Manual de Políticas y Estándares de Seguridad Informática para Usuarios.
- La Subdirección de Informática podrá implantar mecanismos de control que permitan identificar tendencias en el uso de recursos informáticos del personal interno o externo, para revisar la actividad de procesos que ejecuta y la estructura de los archivos que se procesan. El mal uso de los recursos informáticos que sea detectado será reportado conforme a lo indicado en la política de Seguridad ligada a los recursos humanos.
- Los dueños de los procesos establecidos en el CIESAS deben apoyar las revisiones del cumplimiento de los sistemas con las políticas y estándares de seguridad informática apropiadas y cualquier otro requerimiento de seguridad.

Violaciones de seguridad Informática

- Queda prohibido el uso de herramientas de hardware o software que tengan como objetivo en forma directa o indirecta violar los controles de seguridad informática establecidos, salvo los casos expresamente autorizados por la Subdirección de Informática.
- Queda prohibido realizar pruebas a los controles de los diferentes elementos de Tecnología de Información. Ninguna persona que accese a los TIC del CIESAS está autorizada para

probar o intentar comprometer los controles internos, salvo la aprobación expresa de la Subdirección de Informática y los privilegios que por ley tienen los Órganos Fiscalizadores.

- Ningún usuario del CIESAS debe probar o intentar probar fallas de la Seguridad Informática identificadas o conocidas, a menos que estas pruebas sean controladas y aprobadas previa y expresamente por la Subdirección de Informática.
- Queda prohibido realizar en forma intencional escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos ó caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del CIESAS. Los eventos que sean detectados serán puestos de conocimiento a la Dirección de Administración para la presentación de las denuncias correspondientes ante el Órgano Interno de Control y las autoridades en materia penal que corresponda.

6.- SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La continuidad del negocio, debe definir los lineamientos a seguir, antes, durante y después de una interrupción en las operaciones del CIESAS, que respondan asertiva y oportunamente ante eventos que afecten los servicios del centro, así como gestionar la continuidad y restauración de sus procesos, buscando el mínimo impacto en las operaciones.

Planificación de la continuidad

La Subdirección de Informática identificará todos los activos críticos de la operación informática del centro y analizará el impacto de interrupción que se puede generar.

Para estas actividades deberán definirse y asignarse roles y responsables de coordinar y gestionar los procesos de continuidad del centro.

Se debe definir una estrategia de prevención y recuperación, siendo necesario asignar y organizar todos los recursos necesarios en los siguientes puntos:

- Plan de Prevención de Riesgos
- Plan de Gestión de Emergencias
- Plan de Recuperación

Glosario de términos

Para un mejor entendimiento de este manual, se presenta a continuación algunos términos técnicos o palabras con un significado específico para los temas o conceptos que se presentan. El objetivo del mismo es que se manejen los mismos significados y evitar cualquier confusión en el documento. Se utiliza un orden alfabético para facilitar su consulta con descripciones claras y breves.

Término	Significado
Acceso	Es el resultado positivo de la interacción entre un usuario y un activo informático que resulta en intercambio de información de uno a otro.
Acceso físico	Acción de ingresar a un área.
Acceso lógico	Acción de establecer comunicación a un activo tecnológico para su uso.
Acceso remoto	Conexión de dos activos tecnológicos ubicados en diferentes lugares físicos por medio de líneas de comunicación que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.
Antivirus	Programa que detecta y elimina los virus informáticos que pueden haber infectado un disco duro, o cualquier sistema de almacenamiento electrónico de información.
Ataque	Es un intento organizado e intencionado propiciado por una o más personas para causar daño o problemas a un sistema informático o red.
Archivo	Colección identificada de registros relacionados.
Autorización	Proceso de asignar a los usuarios permisos para realizar actividades específicas.
Base de datos	Colección almacenada de datos relacionados, requeridos por las organizaciones e individuos para que cumplan con los requerimientos de proceso de información y recuperación de datos.
CD	Medio de almacenamiento de información.
Código malicioso	Hardware, software o firmware que es intencionalmente introducido en un sistema con un fin malicioso o no autorizado. Un troyano es ejemplo de un código malicioso.

Computadora	Dispositivo electrónico capaz de recibir, almacenar y procesar información de forma útil, siguiendo instrucciones almacenadas en programas.
Confidencialidad	Se refiere a que la información no sea divulgada a personal no autorizado para su conocimiento.
Contraseña	Secuencia de caracteres utilizados para determinar que un usuario específico tiene permitido el acceso a una computadora personal, sistema, aplicación o red en particular.
Control de acceso	Es un mecanismo de seguridad diseñado para prevenir, salvaguardar y detectar acceso no autorizado y permitir acceso autorizado a un activo tecnológico.
Correo Electrónico o Email	Es un servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos.
Descargar	Se refiere a la transferencia de archivos informáticos a un aparato electrónico a través de un canal de comunicación.
Dial-up	Es una forma de conexión a Internet por medio de una línea telefónica.
Disponibilidad	Se refiere a que la información esté disponible en el momento que se requiera.
Estándar	Son acuerdos (normas) documentados que contienen especificaciones técnicas u otros criterios precisos para ser usados consistentemente como reglas, guías, o definiciones de características, para asegurar que los materiales productos, procesos y servicios se ajusten a su propósito.
FTP	Protocolo de transferencia de Archivos. Es un protocolo estándar de comunicación, que proporciona un camino simple para extraer y colocar archivos compartidos entre computadoras sobre un ambiente de red.
Gusano	Programa de computadora que puede replicarse a sí mismo y enviar copias de una computadora a otra a través de conexiones de la red. Además de la propagación, el gusano desarrolla en los sistemas de cómputo funciones no deseadas.

Hardware	Se refiere a las partes físicas tangibles de un sistema informático; sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.
Impacto	Magnitud del daño ocasionado a un activo en caso de que se materialice una amenaza.
Incidente de seguridad	Cualquier evento que represente un riesgo o impedimento de la operación normal de las redes, sistemas o recursos informáticos y que afecte la adecuada conservación de la confidencialidad, integridad o disponibilidad de la información utilizada.
Integridad	Es la propiedad que busca mantener los datos sin pérdida o deficiencia en su autorización, totalidad o exactitud. Es un principio de seguridad que asegura que la información y los sistemas de información no sean modificados de forma intencional o accidental.
Internet	Es una red de redes que permite la interconexión descentralizada de computadoras en donde cualquier usuario puede consultar información.
Maltrato, descuido o negligencia	Son todas aquellas acciones que de manera voluntaria o involuntaria el usuario ejecuta y como consecuencia de ellos daña los recursos tecnológicos a los que tiene acceso.
Mecanismos de seguridad o de control	Es un control manual o automático para proteger la información, activos tecnológicos, instalaciones, etc. que se utiliza para disminuir la probabilidad de que una vulnerabilidad exista, sea explotada, o bien ayude a reducir el impacto en caso de que sea explotada.
Medios de almacenamiento	Son todos aquellos medios en donde se pueden almacenar cualquier tipo de información (CDs, Memorias USB, Discos externos, Tarjetas de memoria, etc.).
Normatividad	Conjunto de lineamientos que deberán seguirse de manera obligatoria para cumplir un fin dentro de una organización.
Respaldo	Copia de datos, procedimientos o aplicaciones disponibles para ser utilizados en caso de una falla o pérdida, si los originales se destruyen o quedan fuera de servicio.
Riesgo	Es el potencial de que una amenaza tome ventaja de una debilidad de seguridad (vulnerabilidad) asociadas con un activo, comprometiendo la

	seguridad de éste. Usualmente el riesgo se mide por el impacto que tiene y su probabilidad de ocurrencia.
Servidor	Es una computadora y sus programas, que está al servicio de otros equipos o computadoras. El servidor atiende y responde a las peticiones que le hacen los otros equipos.
Software	Término que hace referencia a un programa o conjunto de programas de cómputo que incluye datos, procedimientos y pautas que permiten realizar distintas tareas en una computadora.
Software antivirus	Ver Antivirus.
Switch	Es un dispositivo de interconexión de redes informáticas.
Usuario	Término utilizado para distinguir a cualquier persona que utiliza algún sistema, computadora personal, o dispositivo.
Virus	Programas o códigos maliciosos diseñados para esparcirse, copiarse y generar problemas o daños de una computadora a otra por medio de los enlaces de telecomunicaciones o al compartir archivos o medios de almacenamiento portátiles.
Vulnerabilidad	Es una debilidad de cualquier sistema informático que puede ser utilizada para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.