



DIA	MES	AÑO

**REGLAMENTO INTERNO DE OPERACIÓN PARA EL USO O UTILIZACIÓN DE LA RED DE DATOS (ANEXO 1)**

**CONTENIDO**

**OBJETIVO**

**ALCANCE**

**DEFINICIONES**

**POLÍTICA DE ASIGNACIÓN DE ACCESO A LA RED**

**DISPOSICIONES GENERALES**

- I. Altas de Cuentas de Usuarios**
- II. Vigencia de Cuentas**
- III. Uso de la Red CIJ**
- IV. De la Asistencia y Soporte Técnico**
- V. De las Sanciones**
- VI. De los Derechos de los Usuarios**
- VII. De las Responsabilidades de los Usuarios**
- VIII. Espacio en Disco Duro**
- IX. Impresión en Dispositivos de Propósito General**
- X. Computadoras de Escritorio, Computadoras Personales y Periféricos**
- XI. Servicios de Red**
- XII. Del Equipo y Paquetes de Software**
- XIII. De las Páginas de Internet del CIJ (web)**
- XIV. Transitorio**

**CONSENTIMIENTO**

**POLÍTICAS INTERNAS DE SEGURIDAD INFORMÁTICA**

- 6. Política de Seguridad Lógica (ANEXO 2)**
  - 5.2 Política de Seguridad Física (ANEXO 3)**



DIA	MES	AÑO

## REGLAMENTO INTERNO DE OPERACIÓN PARA EL USO O UTILIZACIÓN DE LA RED DE DATOS

### OBJETIVO

Establecer lineamientos, normar y reglamentar las actividades de los usuarios de Oficinas Centrales que ya cuentan con acceso a la Red de Datos Institucional o que son prospectos para contar con el acceso a red, a fin de que se responsabilicen del buen uso de ésta herramienta en los términos y condiciones que se establecen en el presente reglamento y políticas de seguridad (**ANEXOS 2 y 3**). El equipo de cómputo se conectará a la red CIJ de tal forma que el usuario contará con el acceso y utilización de la red para el desarrollo de sus funciones.

### ALCANCE

Al Departamento de Soporte Técnico y Mantenimiento y a todas las Áreas y Departamentos de Oficinas Centrales de Centros de Integración Juvenil, A.C.

### DEFINICIONES

10. **Red-CIJ:** Constituye un conjunto de facilidades y recursos informáticos, así como la infraestructura de voz y datos y los servicios asociados tanto local como remotos, a través del cual se pueden compartir recursos e intercambiar información.
- **Usuario de la Red:** Área, Departamento o Personal de la Institución a los que se les asignan **cuentas** de acceso a red en sus equipos de cómputo, aceptando los términos y condiciones establecidos en el presente reglamento y políticas de seguridad (**ANEXOS 2 y 3**).
  - **Equipo de Cómputo:** Bien informático propiedad de la Institución, que deberá cumplir con la capacidad y disponibilidad de recursos necesarios para su conexión a red.
  - **Cuenta de Acceso a Red:** Son los derechos otorgados a cada equipo de cómputo con acceso a red, el cual identifica a un usuario a través de: Nombre del Usuario y Clave o Código de Acceso.
  - ✓ **Nombre del Usuario (username):** Nombre acordado con el usuario como identificación propia para acceder a red. Este nombre puede ser diferente del nombre, departamento o área en el que se encuentra adscrito el usuario, la condición es que no exista, para poder ser generado.



DIA	MES	AÑO

## REGLAMENTO INTERNO DE OPERACIÓN PARA EL USO O UTILIZACIÓN DE LA RED DE DATOS

- **Clave o Código de Acceso (password):** Es un conjunto de letras y/o números determinado por el usuario, como una identificación personal para el acceso a red y a su correo electrónico.
- **Sesión de Red:** Solicitud de acceso y permanencia que realiza el usuario, para compartir recursos e intercambiar información en el desarrollo de sus funciones.

### POLÍTICA DE ASIGNACIÓN DE CUENTAS DE ACCESO A LA RED

La asignación, uso y permanencia de **cuentas** de acceso a la Red por parte del usuario, implica el conocimiento del presente reglamento y políticas de seguridad (**ANEXOS 2 y 3**), así como su aceptación y conformidad de acuerdo con lo siguiente:

#### Clasificación del personal autorizado para hacer uso de la Red

Toda persona que trabaje en la Institución de “planta” o “eventual”, esté inscrito como voluntario o esté cumpliendo con su servicio social, tiene derecho a solicitar el uso de los recursos de la red; adicionalmente y cuando la situación lo justifique, se podrá autorizar la creación de **cuentas** para usuarios externos. La clasificación de usuarios es la siguiente:

- Personal de la Dirección de Planeación
- Responsables de Informática de las áreas o departamentos
- Personal administrativo
- Personal Operativo
- Personas que realicen su servicio social en la Institución
- Usuarios Externos, previa validación y solo en caso necesario

### DISPOSICIONES GENERALES

Para tener cuenta de acceso a la red, los usuarios deberán contemplar que se cumpla con lo siguiente:

- ◆ Contar con servicio de voz o datos en sus áreas.
- ◆ Contar con el Vo.Bo. de la Subdirección de Desarrollo de Sistemas y Procesos Administrativos.
- ◆ Contar con el equipo de cómputo con la capacidad y disponibilidad de recursos necesarios para su habilitación en red.
- ◆ Estar conectado el equipo de cómputo preferentemente a la corriente regulada, para proteger al mismo de cualquier posible daño por descargas eléctricas.
- ◆ Conocer y aceptar las disposiciones generales del presente reglamento y políticas de seguridad, ya que su inobservancia no exonera de las responsabilidades asumidas por parte del usuario.



DIA	MES	AÑO

## REGLAMENTO INTERNO DE OPERACIÓN PARA EL USO O UTILIZACIÓN DE LA RED DE DATOS

- ♦ Los casos no previstos en el presente reglamento y políticas de seguridad, serán resueltos por la Dirección de Planeación, o entre el Comité de Informática y la Dirección General.

### I. Altas de Cuentas de Usuarios

- ♦ Para el uso de la Red-CIJ, se solicitará a través del SURS o vía memorándum a la Subdirección de Desarrollo de Sistemas y Procesos Administrativos la apertura de una **cuenta**.
- ♦ Dicha **cuenta** será personal e intransferible, y bajo ningún concepto puede ser prestada o compartida.
- ♦ El requerimiento formal no garantiza la apertura de la **cuenta**, sino hasta que sea analizado y validado previamente por el Departamento de Soporte Técnico y Mantenimiento y el resultado notificado al interesado, indicándole además, las características de su **cuenta** en caso de una resolución favorable.

### II. Vigencia de las Cuentas

Las **cuentas** creadas en la Red-CIJ tendrán una duración finita y quedarán determinadas por las siguientes reglas:

- Las **cuentas** creadas para personas que realicen su servicio social y becarios en la Institución, permanecerán durante el período que dure el programa, usualmente 6 meses a partir de la fecha de su creación.
- Las **cuentas** de las personas que trabajan en la Institución, se mantendrán mientras que el usuario no solicite su eliminación.
- Todas las **cuentas** que tengan 3 meses o más de no ser utilizadas se cancelarán.
- Los casos de las **cuentas** del personal que se encuentre de permiso, incapacidad o comisión serán analizados de manera individual.
- Las **cuentas** de los prestadores de servicios sociales o prácticas profesionales, así como voluntarios son de carácter temporal, por lo que su vigencia dependerá del programa al que estén inscritos.

### III. Uso de la Red-CIJ

- Los recursos de la Red-CIJ, únicamente deben ser usados de acuerdo con lo que establecen las normas y procedimientos de la Institución y la Administración Pública Federal al respecto.
- La infraestructura de la Red-CIJ, se utilizará únicamente para desarrollos de actividades institucionales, así como de investigación y administrativos.
- Ninguno de los recursos debe ser usado para recibir o enviar material ofensivo, ni realizar actos de difamación.



DIA	MES	AÑO

### REGLAMENTO INTERNO DE OPERACIÓN PARA EL USO O UTILIZACIÓN DE LA RED DE DATOS

- No se debe hacer uso de la red para transmitir información de carácter comercial o cualquier otra forma que represente un lucro o beneficio económico para la persona que lo origina o procura, excepto en caso de que CIJ se involucre en proyectos de éste tipo.
- Todos los usuarios que tengan bajo su cargo y responsabilidad equipo de cómputo, convienen en que éste es solo para uso institucional y que deberán de procurar su protección física y cuidar el consumo de energía eléctrica, así como de permitir el acceso al personal autorizado de la Subdirección de Desarrollo de Sistemas y Procesos Administrativos, para la verificación y realización de inventarios lógico y físico.
- Ningún usuario de la red está facultado para otorgar acceso a terceros y mucho menos a coaligarse con infractores cibernéticos.
- Todos los usuarios de la red deberán sujetarse a las “Políticas Internas de Seguridad Informática” (ANEXOS 2 y 3), establecidas y difundidas por la Dirección de Planeación.
- Ninguno de los recursos de la Red-CIJ deberá utilizarse con fines de proselitismo político ni religioso, y se respetarán en todo momento las preferencias y derechos individuales de cada persona.
- No se permite y será penalizada severamente, la transferencia de información que afecte los derechos de autor o propiedad intelectual de quién se trate.

#### IV. De la Asistencia y Soporte Técnico

- ◆ Único. La asistencia técnica y mantenimiento de los recursos de red, se apegarán a los procedimientos establecidos.

#### V. De las Sanciones

- ✓ La falta de cumplimiento de alguno de los incisos de éste reglamento, cuya sanción no esté especificada en los puntos 2, 3 ó 4 de éste apartado, conlleva en la primera ocasión, a que el usuario reciba un mensaje de amonestación sobre su falta, y la recomendación para enmendar su conducta.
- ✓ Aquel usuario que llegara a incurrir en el incumplimiento o infracción de alguno de los puntos considerados en el apartado **III. del Uso de la Red-CIJ** de éste documento, se le cambiará la clave de la **cuenta**, siendo necesario que solicite nuevamente la clave de acceso, que en base a sus atribuciones se decidirá si se otorga.
- ✓ Aquel usuario que reincida en las faltas señaladas en el inciso anterior, se le suspenderá el servicio de red por espacio de un mes. Si adicionalmente existiera una queja justificada y se comprueba que el usuario ha obrado de mala fe en cuanto a los incisos indicados con anterioridad, se le suspenderá definitivamente el servicio.



DIA	MES	AÑO

## REGLAMENTO INTERNO DE OPERACIÓN PARA EL USO O UTILIZACIÓN DE LA RED DE DATOS

- ✓ Si algún usuario incurre en el incumplimiento de alguno de los incisos de las políticas internas de seguridad informática (**ANEXOS 2 y 3**), establecidas y difundidas por la Dirección de Planeación , se le sancionará conforme a la normatividad establecida en dichas políticas.
- ✓ Algunos incisos del presente reglamento, describen delitos tipificados como del fuero común, y otros del orden federal, por lo que su observancia es obligatoria por parte de los usuarios.

### 5.1.1 De los Derechos de los Usuarios

- ✗ Los usuarios de CIJ pueden utilizar los recursos de la Red-CIJ, con las limitantes que se mencionan en el presente documento.
- ✗ A los usuarios externos se les faculta a utilizar únicamente los recursos que se les asigne y en la cantidad que se determine para cada caso.
- ✗ Los usuarios gozan de la privacidad de su información, con la salvedad de aquellos casos en que se detecten acciones que pongan en riesgo la seguridad de la Red-CIJ.

### VII. De las Responsabilidades de los Usuarios

- ◆ El correo electrónico es una comunicación directa y confidencial entre el que envía y el (los) que recibe (n), y no debe ser observado o reproducido por nadie mas que estos.
- ◆ El personal técnico del Departamento de Soporte Técnico y Mantenimiento que por razones de trabajo tenga acceso incidental al servicio de correo electrónico, deberá tratarlo con confidencialidad, y sujetarse a las normas y conducta de ética que su puesto conlleva.
- ◆ El usuario deberá acatar las disposiciones dictadas en el reglamento correspondiente, en cuanto al correo electrónico con dominio @cij.gob.mx
- ◆ El usuario deberá asegurarse de que sus archivos cuenten con las protecciones para escritura, lectura y ejecución adecuadas.
- ◆ El usuario deberá asegurarse de que los medios que introduzcan en la red de CIJ no contengan “virus”, acatando las disposiciones dictadas en las políticas de seguridad con respecto a éste tipo de protección informática.
- ◆ Los usuarios deben ser respetuosos del trabajo de los demás, absteniéndose de destruir, alterar o corromper información ajena.



DÍA	MES	AÑO

### REGLAMENTO INTERNO DE OPERACIÓN PARA EL USO O UTILIZACIÓN DE LA RED DE DATOS

- ◆ No se permite que programas ajenos a la red afecten su comportamiento, o hagan uso de los equipos de comunicación intensivamente y por consecuencia mermen su rendimiento.
- ◆ Es responsabilidad del usuario contribuir en la protección de su información, evitando dejar la computadora encendida mientras realice otra actividad por mas de 20 minutos.
- ◆ Es responsabilidad del usuario realizar los “respaldos” necesarios de su información.
- ◆ Es responsabilidad del usuario informarse sobre los detalles de los tipos de licencia y período de vigencia del software instalado en su equipo, mediante solicitud al Departamento de Soporte Técnico y Mantenimiento.
- ◆ Los envíos masivos de correo electrónico (“broadcasts”) y que incluyan todos los usuarios de la red, sólo podrán ser transmitidos si son autorizados por la Dirección de Planeación o Subdirección de Desarrollo de Sistemas y Procesos Administrativos
- ◆ La información que se envíe por correo electrónico, siempre debe responder a un comportamiento profesional y ético.

### DE LAS RESTRICCIONES

Siendo limitada la cantidad de recursos informáticos con que cuenta la Institución, también lo es la utilización que de ellos pueden hacer los usuarios, por lo que los límites establecidos para su uso, se estarán adecuando continuamente acorde a la demanda real de información de CIJ. Con la creación del presente reglamento, se tienen definidas las siguientes restricciones:

- **Espacio en Disco**

1. Al momento de la creación de una **cuenta**, se asigna como espacio de trabajo en disco una cantidad de 2.5 MB; de requerir mas espacio el usuario podrá solicitarlo y se evaluara la cantidad máxima.
2. Los usuarios podrán utilizar los espacios denominados “temporal\_x”, donde la x se refiere al nombre de la estación donde se encuentra el disco.



DIA	MES	AÑO

**REGLAMENTO INTERNO DE OPERACIÓN PARA EL USO O UTILIZACIÓN DE LA RED DE DATOS**

### **IX. Impresión en Dispositivos de Propósito General**

- Las impresoras de la sala de servicio que administra la Dirección de Planeación están a disposición de las áreas, previa solicitud..
- El número de impresiones de color será responsabilidad de cada área, en el entendido de que los recursos para “consumibles” son escasos.
- La impresión de acetatos de color se autorizará en base a las necesidades y justificación de cada usuario y de acuerdo con la reserva que se tenga de ellos, tomándose en consideración el costo involucrado.
- Los usuarios externos de otro inmueble o unidad que no cuentan con la opción de imprimir en la Red-CIJ; podrán hacer uso de éste servicio sólo bajo la autorización del Departamento de Soporte Técnico y Mantenimiento, siempre y cuando presenten una petición por correo ó intranet justificando la necesidad.
- Recomendamos no imprimir varias copias de un mismo documento.
- La impresión de manuales con será responsabilidad de cada área.
- La reproducción de documentos deberá realizarse de acuerdo a las reservas de Ley, respecto a derechos de autor y propiedad intelectual.

### **X. Computadoras de Escritorio, Computadoras Personales y Periféricos**

- ◆ Las computadoras y periféricos asignados a la sala de cursos del Departamento de Soporte Técnico y Mantenimiento, podrán ser utilizados por cualquier usuario de CIJ, con apego a lo establecido en éste reglamento. De registrarse una saturación continua de cursos o de alguna otra actividad, se establecerán horarios programados para el uso del equipo, los cuales se darán a conocer con oportunidad.
- ◆ El uso de las computadoras asignadas a proyectos específicos, estará regulado por los responsables del proyecto en conjunto con la Dirección de Planeación, Subdirección de Desarrollo de Sistemas y Procesos Administrativos y Departamento de Soporte Técnico y Mantenimiento.
- ◆ Está definida una prioridad en el uso de las máquinas y demás recursos de la red de acuerdo al orden siguiente: Director General, Directores Generales Adjuntos, Directores de Área, Subdirectores, Jefes de Departamento, Coordinadores, Subjefes y demás personal.
- ◆ Bajo condiciones especiales, tales como problemas en la comunicación, o la necesidad de prestar algún tipo de mantenimiento a la red, impresoras, etc., el personal del Departamento de Soporte Técnico y Mantenimiento tendrá la mayor prioridad en la utilización de la infraestructura informática de la Entidad.



DIA	MES	AÑO

## REGLAMENTO INTERNO DE OPERACIÓN PARA EL USO O UTILIZACIÓN DE LA RED DE DATOS

### XI. Servicios de Red

- x Los usuarios autorizados podrán utilizar libremente los servicios de red (ftp, mail, telnet, talk y sus variantes), pero en caso necesario, la Dirección de Planeación estará regulando el rendimiento de la red y propondrá – en caso de verse afectada la red – diversas formas de aprovechamiento óptimo de la misma.
- x No se permite la creación de servidores ajenos a la infraestructura del site que mermen la eficiencia de la red, en todo caso, se deberán presentar propuestas factibles, para su análisis y eventual autorización por parte de la Dirección de Planeación.

### XII. Del Equipo y Paquetes de Software

- ◆ Únicamente el personal del Departamento de Soporte Técnico y Mantenimiento y los Responsables de Informática de las áreas o departamentos, están autorizados para mover de lugar los equipos de cómputo y periféricos, así como de conectar y/o desconectar dichos bienes informáticos previos aviso.
- ◆ La adquisición de paquetes o licencias se determinará en base a la programación de necesidades de las áreas
- ◆ Sólo se permite instalar en los bienes informáticos software con licencia, ya sea de cobertura institucional, limitada o sin costo.
- ◆ La Dirección General, el Comité de Informática y la Dirección de Planeación, propiciarán la adquisición de licencias de “sitio”, ”institucionales”, de ”grupo” y otras modalidades que sean convenientes para la Institución.
- ◆ El Departamento de Soporte Técnico y Mantenimiento en conjunto con los Responsables de Informática, serán los encargados de vigilar y asegurar que solo software con licencia esté instalado en las computadoras y los mandos medios y superiores deberán colaborar con éste propósito para evitar el uso de software sin licencia en la Entidad.

### XIII. De las Páginas de Internet del CIJ (web)

- Soporte Técnico y Mantenimiento dedicara un servidor para la pagina Web de información para situarse en Internet.
- El material que aparezca en la página de Internet de la Entidad, debe ser aprobado por la Dirección General, respetando la propiedad intelectual (derechos de autor, créditos, permisos, protección, y todos los que se aplican a cualquier material de esta naturaleza).



DIA	MES	AÑO

## POLÍTICAS INTERNAS DE SEGURIDAD INFORMÁTICA

### XIV. Transitorio

Este reglamento entra en vigor a los \_\_\_\_ días del mes de \_\_\_\_\_ de 200.

Los casos no previstos en el presente reglamento serán analizados y resueltos por la Dirección de Planeación y de ser necesario, serán sancionados por el Comité de Informática para la resolución definitiva por parte de la Dirección General.

### Seguridad Lógica

#### Disponibilidad e Integridad

#### Objetivo

Asegurar que los cambios no autorizados a la información y comunicaciones sean detectables aunque no sean reversibles

#### Generales

- ◆ Efectuar de manera periódica respaldos de la información y mantenerlos en un lugar seguro fuera del sitio de comunicaciones.
- ◆ Se debe hacer una copia del software original para emplearse en las instalaciones. El software original y la documentación relacionada deberán mantenerse bajo resguardo.
- ◆ No se permite la existencia de software sin licencia en los bienes informáticos.
- ◆ No se permite la existencia de software diverso en los equipos de cómputo, tal como juegos o cualquier otro tipo de software de entretenimiento y quedan exentos aquellos que se estén generando o sea de operación.
- ◆ Se debe vigilar el uso de software mediante el empleo de inventarios de “disco duro”, a fin de evitar la existencia de software sin licencia en los equipos de cómputo
- ◆ Sólo personal del Departamento de Soporte Técnico y Mantenimiento, está autorizado para instalar el software con licencia.
- ◆ Se debe capacitar a los usuarios en el uso del software, e inducir el conocimiento del reglamento y éstas políticas de seguridad entre todo el personal de la Institución.



DIA	MES	AÑO

### POLÍTICAS INTERNAS DE SEGURIDAD INFORMÁTICA

- ◆ Instruir a los usuarios para que revisen todo medio de almacenamiento removible sea nuevo o no, así como cualquier archivo que accese al equipo vía medios de almacenamiento, red, correo o Internet.
- ◆ Se deben mantener instalados y actualizados los antivirus en todos los equipos de cómputo.
- ◆ Se debe regular el uso de “laptops” y cualquier otro equipo que se conecte a la red - como los equipos de proveedores - , los cuales deben de ser escaneados antes de conectarse a la misma.
- ◆ Todo proveedor o personal ajeno a las instalaciones de la Entidad que necesite conectarse a la red, deberá solicitar autorización al Departamento de Soporte Técnico y Mantenimiento para que el equipo se revise antes de conectarlo, y que en caso de ser necesario, se le instalarán los mecanismos de seguridad apropiados, a fin de cumplir con las políticas internas de seguridad informática existentes en la Institución.

#### Confidencialidad

#### Objetivo

Asegurar que la información que hayan sido interceptadas por programas o personas no autorizadas, no puedan ser utilizadas.

- ◆ El propietario de los archivos de información debe estar plenamente identificado.
- ◆ Toda la información debe ser clasificada de acuerdo a su confidencialidad.
- ◆ La información confidencial debe estar físicamente guardada de manera segura.
- ◆ El dueño de la información debe establecer los permisos adecuados de acceso a la misma.
- ◆ En el caso de terceros que por motivos relacionados con los proyectos de ciertas áreas, necesiten acceso a determinada información, deberán de comprometerse a la no difusión.
- ◆ La información confidencial que sea transmitida por la red debe “cifrase”.
- ◆ Las llaves de “cifrado” son confidenciales y personales, así como los passwords de acceso a equipos de cómputo, software y diversas aplicaciones, por lo que no se permite su difusión, en cuyo caso contrario, será bajo la estricta responsabilidad del propietario.
- ◆ Los algoritmos de “cifrado” deben cumplir con los estándares de la industria informática.
- ◆ Debe “cifrase” la información altamente confidencial almacenada en medios electrónicos.



DIA	MES	AÑO

### POLÍTICAS INTERNAS DE SEGURIDAD INFORMÁTICA

#### Control de Acceso

##### Objetivo

Evitar que sean utilizados programas, aplicaciones y/o recursos no autorizados.

- ◆ Todos los usuarios deberán de emplear controles de acceso lógico a los programas y aplicaciones, que limiten el acceso no autorizado a su información.
- ◆ Todos los usuarios deberán Únicamente ingresar a los recursos que requiere para desarrollar su trabajo.
- ◆ Todos los usuarios deberán firmar una carta – compromiso de uso de Software y Hardware, en donde se responsabilizan de su uso apropiado antes de que tengan acceso al equipo, red y sus recursos.
- ◆ Ningún usuario deberá proporcionar ningún tipo de información referente al equipo, red o institución, en cualquier pantalla ajena a la entidad
- ◆ Los usuarios no deberán divulgar información, ya que sólo el Responsable de Informática está autorizado para proporcionar información en determinados casos y bajo ciertos términos.
- ◆ Los usuario están limitados para conectarse a diversos equipos y recursos.
- ◆ Los usuarios deben entrar a la red y sus recursos, empleando su clave de acceso propia.
- ◆ Emplear “autenticación” fuerte para acceso a sistemas críticos.
- ◆ Deshabilitar cuentas de usuario después de un período de inactividad establecido y cancelarlas de acuerdo a un programa de temporalidad para la eliminación de cuentas.
- ◆ Seis (6) caracteres será la longitud mínima de password, así como la combinación de letras mayúsculas y minúsculas), números y signos. no utilizando información personal como nombres apellidos o fechas de nacimiento.
- ◆ Todo usuario deberá cambiar su password periódicamente, preferentemente cada 6 meses.
- ◆ Se cambiarán los passwords por omisión en la instalación de sistemas operativos, software y diversas aplicaciones.



DIA	MES	AÑO

### POLÍTICAS INTERNAS DE SEGURIDAD INFORMÁTICA

- ◆ El Departamento de Soporte Técnico y Mantenimiento segmentará la red para prevenir la interceptación de información.
- ◆ El Departamento de Soporte Técnico y Mantenimiento administrará y vigilará el funcionamiento de los equipos de seguridad (firewall's, Router, Switch, ) como parte de la solución de seguridad, y será el único punto de acceso entre la red interna y redes externas, para el cual se deberán emplear políticas de acceso.

#### Seguridad Física

##### **Objetivo**

Asegurar la capacidad de supervivencia de la Institución, ante eventos que pongan en peligro su existencia.

- ◆ Proteger y conservar los activos de la Entidad ante riesgos, desastres naturales, actos mal intencionados y/o diferentes eventos que amenacen su integridad física y patrimonial.
- ◆ Reducir la probabilidad de las pérdidas a un nivel mínimo aceptable, a un costo razonable y asegurar la adecuada y efectiva recuperación.
- ◆ Asegurar que existan los controles adecuados para regular las condiciones ambientales que reduzcan el riesgo por fallas o mal funcionamiento del equipo de cómputo, del software, de los datos y de los medios de almacenamiento.
- ◆ Controlar el acceso de agentes de riesgo a la entidad, para minimizar la vulnerabilidad potencial de la Institución.