POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL INSTITUTO MUNICIPAL DE CULTURA DE YUMBO

Tabla de contenido

POLICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL INSTITUTO MUNICIPAL DE CULTURA DE YUMBO 1

INTRODUCCIÓN 3

JUSTIFICACIÓN 4

2. ALCANCE Y APLICABILIDAD 5

3. POLÍTICA DE SEGURIDAD 5

3.1 POLÍTICAS DE CONTROL 6

3.1.1 Computadores, portátiles, servidores 6

3.1.2 Switches y routers 9

3.1.3 Correo electrónico institucional 10

3.1.4 Bases de datos 11

3.1.5 Red voz y datos 11

3.1.6 Contraseñas y control de acceso 12

3.1.8 Sistema de voz 13

INTRODUCCIÓN

Teniendo como base la constante evolución del ámbito tecnológico y la dinámica de las entidades, se plantea un marco de seguridad de la información para la prestación de servicios a los diferentes tipos de usuarios y ciudadanos a través de las tecnologías de la información, el cual deberá ser respaldado por una gestión y unos procedimientos adecuados, que resalten el papel de las personas como el primer eslabón de una compleja cadena de responsabilidades y que esté orientado a preservar los pilares fundamentales de la seguridad de la información.

La información es, en la actualidad, el elemento primordial de cualquier organización, de tal manera se hace importante la implementación de medidas que propendan por salvaguardar la integridad, la confidencialidad y la disponibilidad de la información que manejan las entidades, con el fin de asegurar la operación de las mismas.

Con el fin de implementar mecanismos de seguridad de la información se ha definido un conjunto de políticas que se debe cumplir según los criterios de estratificación particulares, sin embargo, estas políticas son generales y buscan dar directrices para lograr el aseguramiento de la información en todas sus formas.

JUSTIFICACIÓN

La información tiene valor para la entidad y por consiguiente debe ser debidamente protegida. El establecimiento y seguimiento de la aplicación de Política de Seguridad de la Información garantiza una protección frente a una amplia gama de amenazas. Con esta política se contribuye a minimizar los riesgos asociados de daño y se asegura el eficiente cumplimiento de las funciones sustantivas de la entidad apoyadas en un correcto Sistema de información.

La Política de Seguridad de la Información es la declaración general que representa la posición del INSTITUTO MUNICIPAL DE CULTURA YUMBO con respecto a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías de información incluido el hardware y el software).

El instituto municipal de cultura, para el cumplimiento de su misión, visión, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

Minimizar el riesgo en las funciones más importantes de la entidad.

Cumplir con los principios de seguridad de la información.

Cumplir con los principios de la función administrativa.

Mantener la confianza de sus clientes y funcionarios.

Apoyar la innovación tecnológica.

Proteger los activos tecnológicos.

Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices y clientes del instituto municipal de cultura.

2. ALCANCE Y APLICABILIDAD

Esta política aplica a toda la entidad, sus procesos estratégicos y de dirección, procesos misionales, procesos apoyo institucional, procesos evaluación y control.

Se espera el cumplimiento de las políticas de seguridad por todas las personas cubiertas por el alcance y aplicabilidad.

3. POLÍTICA DE SEGURIDAD

EL INSTITUTO MUNICIPAL DE CULTURA protegerá la información generada, procesada o resguardada por cada uno de los procesos.

EL INSTITUTO MUNICIPAL DE CULTURAL protegerá la información creada, procesada, transmitida o resguardada por sus procesos, con el fin de minimizar riesgos tales como financieros, operativos y legales que en manos de personal no autorizado pudiese ser catastrófico. Para ello es fundamental el uso de usuarios y contraseñas de red intransferibles y un excelente muro de protección por parte de los servidores.

EL INSTITUTO MUNICIPAL DE CULTURAL protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos.

EL INSTITUTO MUNICIPAL DE CULTURAL controlará la operación de sus procesos, garantizando la seguridad de los recursos tecnológicos y las redes de datos.

EL INSTITUTO MUNICIPAL DE CULTURAL Posee control de usuarios por medio de un id y contraseña del DOMINIO CULTURA, de igual forma dependiendo el ROL del usuario así mismo son los permisos y acciones otorgados de acceso a la información, sistemas y recursos de red.

Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática.

Es responsabilidad de cada usuario el equipo de cómputo y accesorios que fueron asignados.

Cada usuario es responsable de un id y pastor (usuario y contraseña de red) es intransferible.

Todo el personal nuevo de la Institución, deberá ser notificado al personal de Tecnología, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo).

Es Responsabilidad de los usuarios del instituto municipal respecto a la información que tiene acceso.

Es responsabilidad de los usuarios Realizar respaldo de la información cada día, en la unidad de red compartida (unidad mapiada)

Es responsabilidad de los usuarios modificar los nombres de carpetas, sub carpetas, documentos y archivos que estén demasiado largos, ya que a la hora de realizar el backup en el servidor no permite realizar esta copia, esto fue notificado en todos los procesos cuando se realizo las capacitaciones del uso de la carpeta compartida.

Es Responsabilidad de los usuarios del instituto municipal No descargar música, películas u otros archivos no legales.

Es Responsabilidad de los usuarios del instituto municipal No hacer clic en enlaces de mensajes no solicitados.

Es Responsabilidad de los usuarios del instituto municipal No visitar sitios web pornográficos o de contenido ilícito.

Es Responsabilidad de los usuarios del instituto municipal No proporcionar datos del instituto a desconocidos por e-mail.

Es Responsabilidad de los usuarios del instituto municipal No ocupar memoria y demás recursos para fines personales.

Es Responsabilidad de los usuarios del instituto municipal el No Uso de correo corporativo para fines personales.

3.1 POLÍTICAS DE CONTROL

3.1.1 Computadores, portátiles, servidores

Políticas

Los mecanismos de control de acceso físico para el personal de planta y contratistas deben permitir el acceso a las instalaciones y áreas restringidas

del Instituto Municipal de Cultura, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y de comunicaciones,

Los computadores de la Entidad sólo deben usarse en un ambiente seguro.

Controles

El usuario deberá reportar de forma inmediata al proceso en conjunto de sistemas TIC y/o MANTENIMIENTO, cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, alertas de incendio u otros.

El usuario tiene la obligación de proteger las unidades de almacenamiento interno y externo (memorias usb, dd extraibles) que se encuentren bajo su administración, aun cuando no se utilicen y contengan información reservada o confidencial de la institución; Es responsabilidad del usuario evitar en todo momento la fuga de la información de la Entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignado.

Cualquier persona que tenga acceso a las instalaciones del Instituto Municipal de Cultura , deberá registrar al momento de su entrada, Equipos de cómputo o cualquier tipo de dispositivos electrónicos, Herramientas que no sean propiedad de la Entidad, en el área de PORTERÍA con el guarda a cargo del turno, de igual manera deberá quedar en la minuta la entrada como la salida de computadoras personales y cualquier activo de tecnología de información, podrán salir de las instalaciones únicamente con la autorización de salida o ingreso del proceso de bienes e inventario(sistemas) , anexando el comprobante de salida del equipo debidamente diligenciado y firmado por el personal a cargo.

Los usuarios deben conocer que toda la información que necesita ser conservada, se deberá guardar en los servidores de la institución, desde las TIC, no se hace responsable por pérdidas de información que no se encuentren dentro del servidor (carpetas compartidas unidad mapeada).

En caso de que haya pérdida de información dentro del usuario de red podrán recuperar su información realizando la solicitud al correo sistemas@imcy.gov.co o de manera presencial dirigiéndose al área de las tic solicitando el formato FO-MA-16 de solicitud de servicio, indicando el nombre del archivo y la ruta del mismo para poder encontrarlo dentro de las copias de seguridad existentes.

Los centros de cómputo de la Administración, son áreas restringidas, por lo que sólo el personal autorizado por la Dirección de TIC puede acceder a ellos.

Los usuarios no deben mover o re ubicar los equipos de cómputo o de telecomunicaciones, instalar o des instalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Dirección, en caso de requerir este servicio deberá solicitarlo por escrito.

El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de la institución.

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 únicamente en la unidad de red del servidor o en la partición de disco que se le asigne ya que las otras están destinadas para archivos de programa y sistema operativo.

Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del computador. Se debe mantener el equipo informático en un entorno limpio y sin humedad.

Cuando se requieran realizar la re ubicación de lugares físicos de trabajo (computadores, escritorios, dispositivos, impresoras) éstos deberán ser notificados al área de TI, a través de una solicitud del formato FO-MA-16.

Esta rotundamente prohibido que los usuarios destapen o desarme los equipos de cómputo de la institución. Únicamente el personal autorizado del área de TI, podrá llevar a cabo los servicios y reparaciones al equipo informático.

Los usuarios deberán asegurarse de respaldar en el servidor la información que consideren relevante cuando el equipo sea enviado a mantenimiento y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de mantenimiento.

El usuario que tenga bajo su resguardo algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho

bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

El usuario deberá dar aviso inmediato a el proceso de bienes e inventario de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

Cualquier recurso de tecnología de información que sufra alguna averiá, maltrato, descuido o negligencia por parte del usuario, será evidenciado ante la Gerencia, con el respectivo concepto técnico.

Debe respetarse y no modificar la configuración de hardware y software establecida por el área de TI.

Deben protegerse los equipos de riesgos del medio ambiente (por ejemplo, polvo, incendio y agua).

Debe usarse el cableado estructurado de energía regulada o estabilizadores de energía eléctrica para los computadores y en los servidores, deben usarse fuentes de poder interrumpiles (UPS).

Es deber de los usuarios de la institución no cambiar la conexión de las tomas naranjas (regulados) donde se evidencia la conexión de equipos de cómputo e impresoras etc.

Los equipos o dispositivos tecnológicos deben marcarse con un numero único de activo fijo el cual indica que es propiedad de la institución.

3.1.2 Switches y routers

Política

El área de TIC es responsable del manejo de los dispositivos de red de los que dispone la institución, velando porque estén dispuestos en lugares seguros y protegidos a nivel físico así como también a nivel lógico.

Controles

Las contraseñas que traen por defecto los dispositivos nuevos, deben cambiarse inmediatamente al ponerse en servicio el dispositivo.

El personal de TI es el único debidamente autorizado para la manipulación de los dispositivos de red, tanto en el rack como instalados en las diferentes áreas de el instituto.

3.1.3 Correo electrónico institucional

Política

El correo electrónico es de carácter personal e intransferible, es deber de cada uno de los usuarios mantener el uso de este y de su contraseña siguiendo estas dos premisas y por ningún motivo se debe permitir a otra persona acceder a este recurso.

Controles

Los usuarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros.

Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de El Instituto municipal de Cultura Yumbo. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

Queda prohibido enviar mensajes de correo electrónico alterando la dirección electrónica del remitente para suplantar a terceros; identificarse como una persona ficticia o simplemente no identificarse.

Queda prohibido utilizar el servicio con fines comerciales o publicitarios no institucionales, propaganda o avisos que riñen con el fin del servicio de este medio de comunicación.

Queda prohibido acechar de cualquier forma, hostigar a otros usuarios de correo electrónico.

Queda prohibido recoger o recolectar datos personales acerca de otro usuario.

Queda prohibido permitir que terceros utilicen el servicio.

Queda prohibido utilizar el correo para fines personales.

3.1.4 Bases de datos

Política

Es obligación del Instituto Municipal de Cultura y en especial del administrador de la base de datos SQL SERVER 2014 del programa SCHOOL CONTROL y la base de datos del servidor ORFEO (Programador encargado) controlar todo tipo de manejo que se efectué sobre la base de datos y velar por mantenerla protegida; En caso de presentarse este tipo de situaciones deben aplicarse los procedimientos correctivos necesarios para restaurar el funcionamiento de la misma sin que ocurra perdida de información

Es política de la Entidad prohibir la divulgación, duplicación, modificación, destrucción, pérdida, mal uso, robo y acceso no autorizado de información propietaria.

Controles

La base de datos es manipulada unicamente por el programador encargado, el cual tiene acceso al servidor de manera local o remota con autorización del ingeniero de tic encargado.

La base de datos debe estar protegida contra fuego, el robo y otras formas de destrucción.

El personal de TI debe realizar el backup de la base de datos, a la hora de realizar el backup externo de la entidad.

3.1.5 Red voz y datos

Política

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

Controles

El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos en caso de que no se

cumpla solicitar un reacomodo de cables con el personal de soporte técnico del area de TI.

El acceso a Internet provisto a los usuarios de la institución es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

Todos los accesos a Internet tienen que ser realizados a través del MIKROTICK de la institución, ya que el es el encargado del direccionamiento y muros de seguridad en caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por el área de TI.

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.
- Saben que existe la prohibición al acceso de páginas no autorizadas.
- Saben que existe la prohibición de descarga de software sin la autorización del área de TIC.
- La utilización de Internet es para el desempeño de su función y no para propósitos personales.

Los servidores de red y los equipos de comunicación (Routers, switches, etc.) deben estar ubicados en lugares apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos lugares y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras, estas llaves se almacenan con el guarda de turno quien es responsable de velar por ellas y no darse a personal NO autorizado.

3.1.6 Contraseñas y control de acceso

Los usuarios no deben guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel o dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente. El cambio de contraseña implica realizar una solicitud al área de las TI por medio del formato FO-MA-16.

Nunca debe compartirse la contraseña o revelarla a otros. El hacerlo expone al usuario a las consecuencias por las acciones que los otros hagan con esa contraseña.

La contraseña inicial se crea entre el usuario y el encargado de las TIC

Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas de la institución, pudiendo ser causal de llamado de atención por parte de la gerencia

Para tener evidencias en casos de acciones disciplinarias y judiciales, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otro crimen que involucre los sistemas informáticos.

Uso de la red regulada y no regulada

El tomacorriente de color naranja, suministra energía eléctrica REGULADA a 110 voltios y se utiliza para conectar exclusivamente el computador (Monitor y CPU).

El tomacorriente de color blanco, suministra energía NO REGULADA a 110 voltios, se utiliza para conectar cualquier equipo o dispositivo electrónico diferente al computador (Ejemplo: Ventilador, impresora, scanner, etc.).

La toma de voz y datos de color blanco ubicado entre las tomas de color naranja y blanco, se usa para conectar los teléfonos y las comunicaciones de datos e internet por cable

3.1.8 Sistema de voz

Con el fin de garantizar la vida útil de los componentes de Voz, proteger la infraestructura tecnológica y los equipos y elementos de telecomunicaciones, el instituto municipal de cultura yumbo, establece como políticas de operación, las siguientes:

El teléfono se utiliza como medio de comunicación para asuntos institucionales y no personales, para tal fin, se establece como política de operación: Es responsabilidad del servidor público (fijos o contratistas) al cual se le ha asignado un aparato telefónico, realizar un uso medido del mismo no excediéndose en el tiempo de llamada ni en el número de llamadas, así como el cuidado físico del mismo.

Es responsabilidad del servidor público al cual se le ha asignado un aparato telefónico, contestar todas las llamadas que entren a la extensión asignada, se debe saludar de forma cortes seguido con el nombre de la dependencia y el servidor público que responde al teléfono.

Con el fin de contar con controles que le permitan al instituto dar seguridad y proteger la infraestructura tecnológica a la red de voz, se establece como política de operación: El área de TI es la única autorizada para la instalación y asignación de extensiones telefónicas dentro del instituto municipal de cultura.

En el evento en que el usuario de la extensión no se encuentre presente en el puesto de trabajo respectivo, el funcionario más cercano a ese puesto de trabajo deberá contestar las llamadas que entren, con el fin de atender a los usuarios tanto internos como externos.