FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 1 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

FCPC-CJETUTEQ

Fondo Complementario Previsional Cerrado de Cesantía y Jubilación Empleados y Trabajadores de Universidad Técnica Estatal de Quevedo (FCPC-CJETUTEQ)

MANUAL DE IMPLEMENTACION DE POLÍTICAS TICS

EMITIDO POR:	REVISADO POR:	APROBADO POR:
ANGÉLICA YÁNEZ NATA	EDISON LOZA FLORES	DIANA ESTUPIÑAN LOOR

VERSIÓN 1.1

Actualizado al: 30 de Noviembre del 2018

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 2 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

ÍNDICE

1.1. Generales	3
1.2. Específicos.....	3
2. ALCANCE	3
3. MARCO TEÓRICO	3
4. POLÍTICAS DE SEGURIDAD EN LA RED	6
4.1. Responsables	6
4.2. Políticas.....	6
5. POLÍTICAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.....	10
5.1. Responsables	10
5.2. Políticas.....	10
6. POLÍTICAS DE SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE	11
6.1. Responsables	11
6.2. Políticas.....	12
7. INVENTARIO DE EQUIPOS DE CÓMPUTO.....	16

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 3 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

1. OBJETIVOS GENERALES Y ESPECÍFICOS

1.1. Generales

Asegurar la integridad, confidencialidad y disponibilidad de los medios tecnológicos y las comunicaciones que se utiliza en el FCPC- de Cesantía y Jubilación de Empleados y Trabajadores de la Universidad Técnica Estatal de Quevedo.

1.2. Específicos

- a) Identificar los recursos tecnológicos que posee el Fondo
- b) Normalizar las políticas de uso de las Tecnologías de Información y Comunicaciones
- c) Organizar de forma documentada las políticas y procedimientos del uso del recurso tecnológico en el FCPC-CJETUTEQ.

2. ALCANCE

El manual y políticas de sistema integral informático va dirigido al personal que labora en el FCPC-CJETUTEQ.

3. MARCO TEÓRICO

- **Administrador de Red:** Es la persona encargada de la administración de la red. Entre sus actividades incluye la administración, mantenimiento y monitoreo de los equipos de comunicaciones y servidores que conforman la red: switches, routers, firewalls, entre otras.
- **Amenaza:** Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio.
- **Ancho de banda:** Nos indica la capacidad de comunicación, o la velocidad de transmisión de datos de una línea de conexión.
- **Antispam:** Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios.
- **Antivirus:** Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus.
- **Access Point o Punto de acceso inalámbrico:** (WAP o AP por sus siglas en inglés: Wireless Access Point) En una red de computadores, es un dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica. Normalmente un Access Point también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos.
- **Base de Datos:** (Data Base). Conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios, etc. Las bases de datos son uno de los grupos de aplicaciones de productividad personal más extendidos
- **Chat:** Comunicación simultánea de dos o más personas a través de Internet. Hasta hace poco tiempo sólo era posible la “conversación” escrita, pero los avances tecnológicos permiten ya la comunicación audio y video.
- **Cifrado:** un método que permite aumentar la seguridad de un mensaje o de un archivo mediante la codificación del contenido, de manera que sólo pueda leerlo la persona que cuente con la clave de cifrado adecuada para descodificarlo.

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 4 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

- **Correo electrónico:** (en inglés: e-mail), es un servicio de red que permite a los usuarios enviar y recibir mensajes (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos
- **Encriptación:** La encriptación es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos.
- **Firewall:** Mecanismo de seguridad en Internet frente a accesos no autorizados.
- **Hacker:** persona que realiza la acción de irrumpir o entrar de manera forzada a un sistema de cómputo o a una red.
- **Hub:** es el dispositivo que concentra los cables de una red local.
- **Infraestructura:** Conjunto de elementos o de servicios básicos para la creación y el funcionamiento de una organización o entidad.
- **Cookies:** es una pequeña información enviada por un sitio web y almacenado en el navegador del usuario, de manera que el sitio web puede consultar la actividad previa del usuario.
- **Copia de seguridad:** Salvaguarda del sistema o de datos en un momento concreto, que permite recuperar esos datos o el sistema en el estado en que se encontraban en el momento de realizarla.
- **Contraseña de Usuario:** Una contraseña de usuario o clave es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña normalmente debe mantenerse en secreto ante aquellos a quien no se le permite el acceso. Aquellos que desean acceder a la información se les solicitan una clave; si conocen o no conocen la contraseña, se concede o se niega el acceso a la información según sea el caso.
- **Dirección IP:** Dirección de 32 bits definida por el Protocolo de Internet. Se representa usualmente mediante notación decimal separada por puntos. Un ejemplo de Ip Address es: 193.127.88.567.
- **Intranet:** Red propia de una organización, diseñada y desarrollada siguiendo los protocolos propios de Internet; en particular el protocolo TCP/IP. Puede tratarse de una red aislada, es decir, no conectada a Internet.
- **IP (Internet Protocol):** Protocolo principal de comunicaciones a través de Internet. La transmisión de información ocurre mediante pequeños paquetes de "bits" que contienen la información que está siendo enviada y la dirección hacia la que se dirigen.
- **ISP:** (Internet Service Provider) (Proveedor de servicios de Internet): La institución que ofrece la conexión a Internet.
- **Log:** es un registro oficial de eventos durante un rango de tiempo en particular. Para los profesionales en seguridad informática es usado para registrar datos o información sobre quién, qué, cuándo, dónde y porqué (who, what, when, where y why) un evento ocurre para un dispositivo en particular o aplicación.
- **Modem:** Equipo utilizado para adecuar las señales digitales de una computadora a una línea telefónica o a una ISDN, mediante procesos denominados modulación (para transmitir información) y demodulación (para recibir información).
- **Política de Seguridad Informática:** Es una forma de comunicarse con los usuarios y los gerentes. Las PSI establecen en canal formal de actuación del personal, en relación con los recursos y servicios informa 'ticos, importantes de la organización.

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 5 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

- **Router:** es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.
- **Red:** Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos (computadoras y/o dispositivos) conectados por medio de cables, señales, ondas o cualquier otro método de transporte de datos, que comparten información (archivos), recursos (CD-ROM, impresoras, etc.), servicios (acceso a internet, e-mail, chat, juegos).
- **Red de datos:** Se denomina red de datos a aquellas infraestructuras o redes de comunicación que se ha diseñado específicamente a la transmisión de información mediante el intercambio de datos.
- **Seguridad Informática:** o seguridad de tecnologías de la información es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.
- **Sistemas de Control Interno:** es dentro del fondo un seguimiento y control de las actividades que se realizan en el seno de la misma. Corrigen errores y se asegura del cumplimiento de los objetivos. Cada área funcional de la empresa presentara un control interno de sus actividades. Estos sistemas de control buscan que el fondo tenga una mejor eficiencia.
- **Sistema de Información:** es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad u objetivo.
- **Sistema Operativo:** El software de nivel bajo que se encarga de organizar la operación de la computadora, asignar recursos, manejar la interfaz de los diversos periféricos, y comunicarse con el usuario. El sistema operativo es el software más importante de un computador, ya que sin él la operación del computador sería imposible. Algunos de los sistemas operativos más comunes son: Windows, MSDOS, MacOS, Linux y Solaris.
- **Spam:** Es cualquier mensaje destinado a una audiencia general (o sea, un comunicado de masas) que se envía a la gente por e-mail sin que lo soliciten. Generalmente las direcciones a las que llegan esos mails son robadas y la mayoría de las veces esos mails son publicidad o contiene algún virus. Representa una violación a la privacidad del usuario.
- **Swiches:** es un dispositivo analógico de lógica de interconexión de redes de computadores que opera en la capa 2.
- **TI:** Tecnología Informática
- **TIC:** Tecnologías de la Información y las Comunicaciones.
- **Usuario final:** En informática, el término usuario final designa a la persona o personas que van a manipular de manera directa un producto de software.
- **Vulnerabilidad:** Una vulnerabilidad es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas.
- **Virus:** Programa informático escrito para alterar la forma como funciona una computadora, sin permiso o conocimiento del usuario.
- **Web:** red informática y, en general a Internet, comprende aquellos sitios web que facilitan el compartir información, la interoperabilidad, el diseño centrado en el usuario y la colaboración en la World Wide Web.

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 6 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

4. POLÍTICAS DE SEGURIDAD EN LA RED

4.1. Responsables

Todos los usuarios que utilicen un sistema de información, un módulo de sistema de información, accedan a Internet, cuente con un correo electrónico, un equipo de cómputo en la institución.

4.2. Políticas

El objetivo de esta política es especificar la normatividad de seguridad de la red de comunicaciones en el FCPC-CJETUTEQ que responda a la confidencialidad, integridad y disponibilidad de la información en los usos requeridos por los usuarios tanto internos como externos. A continuación, se establecen los lineamientos generales para su cumplimiento:

1. Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de las redes y seguridad FCPC-CJETUTEQ deberán ser consideradas y tratadas como información confidencial.
2. Todas las conexiones a redes externas en tiempo real que accedan a la red interna del FCPC-CJETUTEQ, debe pasar a través del firewall previamente parametrizado con las políticas de navegación incluyendo antivirus de red, verificación de datos, detección de ataques, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuario(a)s, y bloqueo de sitios o intrusos.
3. Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo o documento de formalización.
4. La información es un componente esencial en la gestión de una institución, actualmente la información se maneja digital a través de sistemas de información. en la red a nivel internos y externos. Por tal razón, están expuestos a riesgos de seguridad, donde puede darse el acceso no permitido a la información para hacer daño. Entre las vulnerabilidades más relevantes esta "las puertas invisibles" descubiertas en los sistemas operativos, aplicaciones de software, browsers de Internet, protocolos de red, correos electrónicos y diferentes servicios informáticos. Por tanto, el principal objetivo de administrar riesgos, es garantizar la continuidad de una institución. En este sentido, el FCPC-CJETUTEQ, debe clasificar los servicios que presta a través de los sistemas de información, identificar las posibles amenazas. Entre los equipos de seguridad informática y protecciones que se brinda o recomiendan al FCPC-CJETUTEQ:

Firewall

Dispositivo con tecnología poderosa combinando hardware y software basado en uso de circuitos integrados de aplicación específica, brinda seguridad perimetral realizando control sobre el tráfico de las redes en tiempo real, garantizando protección completa a los sistemas de información que navegan en la red.

El nivel de seguridad que ofrece es muy alto, para lo cual presenta varias líneas de solución de seguridad en la red como es el permiso de terceros para navegar en la red de forma controlada, la restricción en la navegación a los usuarios internos, la configuración de antivirus para servicios en la red, control del ancho de banda, control de acceso, entre otros igualmente importantes.

Servidores

Para garantizar la seguridad de la información en la institución, debe propender porque los servidores manejen un volumen de gestión alto y estén en sitios especializados externos que brinden servicio de Cloud computing y para la gestión interna administrativa y financiera es recomendable que los servidores este en un sitio institucional ideal.

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 7 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

En este sentido, los servidores (Web, BD, Aplicaciones, entre otros.), de la Institución están respaldados en la navegación por firewall para seguridad perimetral, el mantenimiento físico y lógico especial de estos equipos y las políticas de navegación específicas que se establecidas. Otros controles que están presentes son las restricciones al espacio físico donde están ubicados los equipos servidores (aparte de los equipos de usuarios) para evitar el intento de acceso a la parte lógica.

Aplicaciones de Usuario

Para evitar la vulnerabilidad en las aplicaciones locales y de internet en los equipos de los usuarios, se deben tomar medidas de acuerdo al tipo de software, implementando otra clase de protecciones; como el antivirus corporativo, antivirus de red, administración de los usuarios donde se determine el acceso y las restricciones pertinentes, entre otras actividades que permitan mitigar el posible riesgo.

Protección física y digital de la información

El propósito es evitar riesgos potenciales a los activos de información institucionales que maneja el usuario, relacionados con su operar cotidiano, ya sean de manera accidental o intencionada, que puedan ocasionar la interrupción total o parcial, de las actividades de la institución.

En este apartado se definen lineamientos que deberán adoptarse al interior de la institución para la protección de la información, tanto física como digital y con acceso a través de los sistemas de cómputo, estos lineamientos deberán ser seguidos por todos y cada una de las áreas implicadas en estas actividades.

Para el FCPC-CJETUTEQ, es de vital importancia proteger información sensible, evitando que sea conocida por personas diferentes a aquellas que la requieren o que sea publicada de manera indistinta. Por tanto, los usuarios deberán cumplir lo siguiente:

- La información del fondo deberá mantenerse disponible a las personas autorizadas para ello en el momento en que se necesite, lo que hace que la información sensible se pueda encontrar en el puesto de trabajo de cada empleado durante su jornada, sin que esto deba ser entendido como admitir momentos en que la información NO esté debidamente protegida. A pesar que los niveles de protección y clasificación establecidos para la información de la institución son mantenidos en todo momento los usuarios con acceso a estos sistemas de información deberán estar pendiente que solo él sea el responsable de acceder al sistema de información
- Los usuarios dueños de la información son responsables, mientras tengan la información bajo su control, de mantener los niveles de protección y clasificación establecidos para la misma en todo momento, haciendo uso adecuado de los recursos a su disposición.
- Es responsabilidad de los usuarios el identificar riesgos relacionados al disponer de la información en su puesto de trabajo e iniciar las acciones para mitigarlos.
- Durante la jornada laboral, los usuarios deben propender por tener el Escritorio Limpio, los sistemas de información y elementos de procesamiento deberán ser adecuadamente protegidos, teniendo presente que se debe al menos guardar documentos confidenciales o elementos de almacenamiento de información (CDs, DVDs., Memorias USB, Discos móviles, asistentes personales, portátiles) en los cajones bajo llave, en todo momento que no los esté utilizando.
- Es responsabilidad de cada usuario la protección de los sistemas de información a su cargo, por lo que debe asegurar físicamente el computador portátil con cables de

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 8 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

seguridad en todo momento para evitar robos o si es equipo de escritorio tratar de asegurar el hardware y para el software colocar clave de acceso.

- Es responsabilidad de cada usuario la protección de la información a cargo, por lo que debe mantener presente NO publicar o dejar a la vista, documentos o datos confidenciales, delicados, confidenciales, por ejemplo:
 - Nombre de Usuario y Password
 - Direcciones IP
 - Contratos
 - Números de Cuenta
 - Listas de Clientes
 - Guía de Políticas Usuario Final
 - Propiedad Intelectual
 - Datos de Funcionarios
 - Cualquier cosa que no desea publicar
 - Dejar el Escritorio Limpio después de la jornada laboral y lo confidencial bajo llave.
 - Los usuarios deberán tomarse el tiempo necesario antes de abandonar la oficina para recoger y asegurar el material confidencial.
 - (Portátiles, Tablets, Memorias USB, entre otros.).
 - Cada usuario del fondo para mantener su computador bajo control, deberá bloquear la sesión al alejarse de su computador, aunque sea por poco tiempo, minimizando el tiempo que el equipo quedaría sin control ya que cualquier ausencia puede extenderse.

Protección contra software maligno

La intención en este punto es mencionar los controles que permiten minimizar el riesgo generado por el acceso a Internet y a redes públicas, el intercambio de medios de almacenamiento removibles, el intercambio de información con instituciones externas, entre otras, los cuales exponen los sistemas del FCPC-CJETUTEQ a la propagación interna y externa de software con código malicioso o nocivo, comprometiendo directamente la integridad, la disponibilidad y la confidencialidad de la información procesada por cada uno de los componentes de la red:

- Cualquier usuario que sospeche de una infección por un virus debe llamar al proveedor de TICs para ser guiado con instrucciones precisas en el procedimiento de eliminación del virus del computador.
- Los usuarios No deben transferir (bajar) software desde cualquier sistema que se encuentra por fuera de la red.
- Los usuarios No deben utilizar software obtenido externamente desde Internet o de una persona u organización diferente a los distribuidores confiables o conocidos, a menos que el software haya sido examinado en busca de código malicioso y que haya sido aprobado el proveedor de TICs.
- Antes de ser descomprimido, todo software transferido desde sistemas externos al FCPC-CJETUTEQ, debe ser analizado con un sistema antivirus aprobado.
- Antes que cualquier archivo sea restaurado en un computador de la institución, desde un medio de almacenamiento de respaldo, éste debe ser analizado con un sistema antivirus.
- Los usuarios intencionalmente no deben escribir, generar, compilar, copiar, almacenar, propagar, ejecutar o intentar introducir cualquier código de computador diseñado para auto replicarse, deteriorar o que dificulte el desempeño de cualquier sistema de la institución.

Protección durante la navegación en internet.

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 9 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

Esta política expresa los controles que permiten minimizar el riesgo generado por el acceso a Internet y a redes públicas, el intercambio de medios de almacenamiento móviles, el intercambio de información con instituciones externas, entre otros, los cuales dejan en riesgo los sistemas del FCPC-CJETUTEQ a propagación interna y externa de software con código malicioso o nocivo, comprometiendo directamente la integridad, la disponibilidad y la confidencialidad de la información procesada por cada uno de los componentes de la red.

El fondo con el objetivo de facilitar la realización de labores diaria administrativas, brinda acceso a Internet para navegación a los funcionarios autorizados, los cuales se ampararán en las políticas y formas de actuación expuestos en este documento.

- Los usuarios deberán abstenerse de visitar espacios en la Web restringidos por la institución, o sitios que afecten la productividad de la institución.
- Se deberá evitar el acceso desde el espacio institucional a sitios relacionados con la pornografía y fundamentalmente si éste involucra a menores de edad. Igualmente, se prohíbe la descarga y uso de software malicioso o documentos que brinden información sobre cómo atentar contra la seguridad de la información institucional.
- Los funcionarios deberán abstenerse de brindar cualquier tipo de información de la institución en sitios no autorizados o que no cuenten con mecanismos de seguridad que garanticen la confidencialidad de la información en tránsito.
- Los funcionarios de Institución No deben comprar bienes o servicios a través de Internet a nombre de Institución a menos que exista una aprobación previa de las directivas pertinentes.
- Los usuarios, deben evitar descargar y/o emplear archivos de imagen, sonido o similares que puedan estar protegidos por derechos de autor de terceros sin la previa autorización de los mismos.
- Los usuarios no deben instalar software en sus estaciones de trabajo o en otras máquinas, incluso si este software es libre o no licenciado; toda instalación de software debe hacerla un técnico autorizado, luego de la debida verificación y la autorización del proveedor de TICs.
- Los usuarios están conscientes de que toda la información (incluida la de navegación) que transite en la institución por ser para la labor diaria es propiedad de la misma y por ende puede ser monitoreada con objetivos de administración, seguridad o auditoría por personal autorizado de la institución.
- Los usuarios de los sistemas de navegación son conscientes de que estos, solamente deben ser utilizados para propósitos lícitos y en cumplimiento de las funciones específicas de su cargo, ya que toda actividad de navegación puede ser registrada por la Institución quien podrá revelar cualquier acceso cuando una autoridad judicial así lo requiera
- El personal de la Institución no debe utilizar el sistema de navegación para participar en grupos de discusión en Internet, listas de Correo, chats o cualquier otro foro público, a menos que su participación sea meramente con fines institucionales.
- La Institución facilita el acceso al uso de medios electrónicos para comercio electrónico como el pago de facturas, transacciones bancarias y lectura de correos personales que tengan acceso vía web, pero no asume ninguna responsabilidad por estas, ni recomienda el uso. Si el usuario hace uso de estos servicios de todas maneras asume que puede ser monitoreada toda la información que de este uso se derive como si fuese de la institución misma.

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 10 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

5. POLÍTICAS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN

5.1. Responsables

Todos los usuarios que utilicen un sistema de información, un módulo de sistema de información, accedan a Internet, cuente con un correo electrónico, un equipo de cómputo en la institución.

5.2. Políticas

Esta política nace como un instrumento del fondo para sensibilizar a los diferentes usuarios que hacen uso de los sistemas de información, con el fin de describirles la protección y el funcionamiento para la utilización adecuada y reconociéndolo como un canal de información que presta servicios integrales, confidenciales y direccionándolos a la prestación de un servicio eficaz, para lo cual establece las siguientes políticas:

Política de seguridad de los Sistemas de Información

El propósito de esta política es establecer límites que resguarden la información de ser liberada (deliberada o no deliberadamente) a las personas erradas. En el FCPC-CJETUTEQ la Información es un activo esencial para la prestación del servicio y la toma de decisiones, por lo cual existe un deber manifiesto de salvaguardar la propiedad más relevante como estrategia orientada a la continuación de la institución, la administración de peligros y el fortalecimiento de la cultura de seguridad.

Dentro de esta política se establecerá la protección de los activos de la información que cumple con la visión institucional:

- El Representante Legal del FCPC-CJETUTEQ dentro de sus responsabilidades velara por la actualización de la política de seguridad de la información, para lo cual realizara revisión y mejora continua.
- Los activos de información de la Institución, serán identificados, clasificados y socializados al personal de la institución, con el fin de instituir los elementos de protección necesarios.
- El fondo definirá e implementará controles para proteger la información y garanticen la disponibilidad solicitada por los usuarios de los servicios ofrecidos por la Institución.
- Se programarán auditorias y controles pertinentes a los sistemas de información existentes.
- Solo se permitirá software que se haya adquirido legalmente y el software libre que brinde seguridad y soporte.
- Los funcionarios y contratistas, como responsabilidad sobre la seguridad de la información, deberán comunicar los riesgos que identifique.
- El incumplimiento de las políticas será notificadas, reconocidas y monitoreadas.

Seguridad del comercio electrónico.

Esta política tiene como intención prevenir la revelación de información privada, el fraude en contra o en nombre de la institución privacidad de la información de cuentas y la seguridad de las transacciones realizadas a través de Internet o redes externas.

Toda información acerca de pagos, como números de cuentas corrientes entre otras debe ser acordada su transmisión con el banco a través de firmas digitales asignada al responsable de la actividad. La Institución debe informar al banco la IP de salida de la institución para que el banco permita a través de su firewall el acceso.

Logging o Registro Histórico de Actividades.

El propósito es contar con registros de los movimientos que se realizan dentro de los sistemas de información de la Institución, buscando evitar conductas inapropiadas y minimizar riesgos de seguridad en el uso de estos.

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 11 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

Todas las aplicaciones de producción que manejen información confidencial o sensible de la Institución, deben generar logs que muestren cada modificación, incorporación y borrado de la información.

Esto incluye modificaciones a los sistemas de producción y modificaciones a los sistemas fuente.

- Actividad que debe realizar el proveedor de cada sistema de información institucional (solicitarlo al desarrollador o al soporte externo), para estar monitoreando lo que es su responsabilidad.
- Los sistemas que manejen información valiosa, confidencial o crítica deben además contener y activar forzosamente el logs sobre todos los eventos o procesos relacionados con la seguridad de acceso a los mismos. Ejemplo: Varios intentos de contraseña, intentos de uso de privilegios no autorizados, entre otros.
- Los logs de procesos relevantes deben de proveer información suficiente para soportar auditorías y contribuir a la eficiencia y cumplimiento de medidas de seguridad.
- El período que debe activarse y depurarse un log es por lo menos cada mes. Durante este período, el administrador del sistema y/o dueño de la información, se debe asegurar que éste no sea modificado, y cerciorarse de que no sea leído por personal no autorizado. Estos aspectos son importantes para la corrección de errores, auditorías o huecos de seguridad.
- Debe realizarse supervisión a los sistemas de información, a sus administradores por lo menos cada tres meses (con ayuda de expertos), para evaluar el nivel de seguridad que realizan.
- Para evitar conductas inapropiadas, crear un sentido de responsabilidad del usuario, y permitir una administración adecuada de los sistemas, todas las actividades de los usuarios que afecten producción deben ser trazables desde el log.
- Las aplicaciones y otros manejadores de Bases de Datos, deben tener logs para las actividades de los usuarios y estadísticas relacionadas a estas actividades que les permitan identificar y detectar alarmas de posibles problemas o mal uso, y que reflejen eventos misionales de la institución sospechosos.
- Todos los sistemas de la Institución, incluyendo todos los computadores conectados a una red, siempre deben tener un mismo horario y calendario adecuado, utilizando sincronía con los servidores, cuando sea posible. Esto para facilitar actividades de rastreo mediante los logs de los sistemas.
- El manejo de Logs, los mecanismos para detectar y registrar eventos de seguridad significativos, deben ser resistentes a los ataques. Estos ataques incluyen intentos de desactivación, modificación, o borrado del software de log. Esto incluye tomar las medidas necesarias para que, aun cuando el log sea apagado o modificado, esta suspensión o modificación queden registradas en el mismo.
- Los logs de todos los sistemas y aplicaciones deben ser conservados de forma tal, que no puedan ser revisados o visualizados por personas no autorizadas.

6. POLÍTICAS DE SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

6.1. Responsables

Todos los usuarios que utilicen un sistema de información, un módulo de sistema de información, accedan a Internet, cuente con un correo electrónico, un equipo de cómputo en la institución.

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 12 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

6.2. Políticas

Infraestructura de la red eléctrica regulada

La infraestructura de la red eléctrica regulada deberá desarrollarse siguiendo las normas y estándares para este fin, permitiendo la seguridad del recurso humano, tecnológico y documental en la institución. De la misma manera, deberá asegurar el servicio, la protección de la información y de los equipos en las aéreas administrativas.

- **Responsabilidades de los usuarios:** Las diferentes áreas institucionales que están reguladas con una infraestructura eléctrica deben cumplir varias responsabilidades para garantizar la protección de la información que manejan y de los equipos, las cuales son:
- Los usuarios de las zonas reguladas eléctricamente deberán verificar que los equipos de cómputo en su responsabilidad estén conectados a la toma de batería (CPU y Pantalla).
- Los usuarios deben verificar que las impresoras, ventiladores, radios entre otros que No sean equipos de cómputo No estén conectados a tomas de batería.
- El usuario No deberá conectar cortapicos o reguladores a toma naranja para tratar de conectar más equipos.

Infraestructura de la red de datos

El FCPC-CJETUTEQ cuenta con infraestructura de red que comprende el, switches, routers permite la interconexión de equipos (computadores, impresoras) para el servicio de acceso a Internet, interacción entre usuarios a través de sistemas de información entre otros. A continuación, se detallan las políticas:

- **Centros de cableado:** El centro de cableado es el lugar o punto único donde se concentra el cableado de la red local y se conectan los dispositivos que permiten la interconexión para la comunicación interna y hacia internet. En este espacio solo está permitido el acceso al personal de soporte técnico institucional o externos que cumplan una labor contratada, para los diferentes usuarios está restringido el acceso. Los centros de cableado son los espacios donde se organiza el cableado, se ubican los dispositivos, router, transiver y demás que permitan la interconexión para el funcionamiento de la red local, estos al ser cerrados permiten brindar seguridad y protección contra el medio ambiente.

Equipos.

A continuación, se detallan las políticas con respecto a los equipos:

Inventario de equipos: Los equipos de cómputo de la institución son los activos indispensables para la interacción tecnológica en el FCPC-CJETUTEQ y para el control general debe relacionar los siguientes registros:

- Usuario responsable del equipo.
- Código de los equipos
- Dirección IP
- Confirmación hoja de vida
- Descripción general de las características técnicas del equipo (CPU).
- Marca
- Licencia Sistemas Operativo.
- Fecha de adquisición.
- Observaciones generales

Actividades relacionadas con el registro de equipos:

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 13 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

- Cada que ingrese un equipo nuevo debe registrarse en el inventario.
- Cada que el equipo cambie de usuario debe actualizarse el inventario.
- Anualmente elaborar estadística de los datos registrados: cantidad de equipos por sistema operativo y cantidad de equipos por licenciados y no licenciados.

Mantenimiento preventivo de equipos:

- Elaborar el cronograma anual para la programación del mantenimiento preventivo de los equipos de cómputo.
- De acuerdo al cronograma, planear semestralmente la realización del mantenimiento preventivo a equipos de cómputo institucionales y notificar por escrito a cada usuario responsable del equipo de cómputo con anticipación.
- Llevar el control del mantenimiento preventivo programado semestralmente.
- Elaborar informe técnico por insolencia de un equipo para el servicio, por daños o fallas graves.
- Elaborar el registro de equipos y parte para baja por insolencia de un equipo para el servicio, por daños o fallas graves.
- Antes de la ejecución del mantenimiento preventivo, explicar al usuario como elaborar la copia de seguridad de la información de los equipos en responsabilidad.
- Brindar soporte al usuario en el manejo de software legal en el equipo (sistema operativo y herramientas ofimáticas).
- Al entregar el equipo con el mantenimiento preventivo programado, solicitarle al usuario la verificación del funcionamiento general del equipo, así como de la información.

Seguridad de los equipos y protección contra virus: Para la instalación de software antivirus informático, se debe:

- Verificar la capacidad de los equipos de cómputo, antes de la instalación.
- Realizar pruebas de funcionamiento una vez instalado.

Software

A continuación, se detallan las políticas con respecto al software:

Plan de respaldo y recuperación: El respaldo y recuperación de la información que se maneja en la labor que se desempeña en la institución es de vital importancia, por lo cual para el FCPC-CJETUTEQ es fundamental para garantizar la continuidad del procesamiento de los datos, con la mínima dificultad posible ante una eventual alteración no deseada. Un responsable del FCPC-CJETUTEQ realiza respaldo de la información que manejan los usuarios en sus computadores al momento del mantenimiento preventivo programado y se le entrega al usuario, quien deberá verificarla y entregar una copia al archivo central. El mismo responsable es el encargado de realizar el respaldo de las bases de datos de los sistemas de información a los que tiene acceso directamente y solicitar a los que no tiene acceso.

Protección y respaldo de la información: El propósito es mostrar el estado actual de protección de la información en la institución y plantear estrategias para proteger y facilitar su utilización de acuerdo a las necesidades de prolongación trazadas a nivel de los procesos. En este documento se definen los parámetros que deberán seguirse al interior de la institución para el almacenamiento y recuperación de corto y largo plazo, así como de la recuperación de la información conservada a nivel de medios de almacenamiento para responder a los requerimientos de los procesos de la institución. Estos parámetros deberán ser atendidos por los

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 14 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

diferentes empleados que hacen parte del FCPC-CJETUTEQ. Para la Institución el mayor activo es la información, por lo cual se deben crear procedimientos que garanticen un apropiado uso durante el ciclo de vida de la información, principalmente para los asuntos que requieren conservar la disponibilidad de la misma, se deberá preservar la seguridad de la información dando cumplimiento a los principios de Confidencialidad, Integridad y Disponibilidad de la información de la institución.

- La información de la institución deberá mantenerse disponible a las personas autorizadas para ello en el momento en que se necesite.
- La institución deberá identificar mecanismos que permitan que las actividades de respaldo y recuperación de la información sean adecuadas costo / beneficio.
- Los niveles de protección y clasificación establecidos para la información de la institución deberán ser mantenidos en todo momento. Por lo tanto, se deben mantener los controles y medidas establecidas para esto.
- Los usuarios de la institución son responsables de la información institucional que manejan.
- Los usuarios respaldan y protegen la información que manejan, con medidas que eviten accesos de personas no autorizadas. Se deberán preservar los lineamientos de acuerdo a la sensibilidad y nivel de clasificación de seguridad.
- El archivo central de la institución deberá guardar los respaldos digitales de la información de gestión e históricos en sitios adecuados para la preservación que permitan la continuidad de la institución, de acuerdo a lo establecido en las tablas de retención documental.
- Una persona de la institución es la responsable del respaldo de las bases de datos a las que tenga acceso y deberá tener copia en varios espacios como garantía de continuidad de la institución.
- La institución deberá contar con el espacio en la nube para el respaldo de las bases de datos y otra información clasificada como relevante.
- Los usuarios de la institución deberán seguir los procedimientos de respaldo de la información y crear inventario de copias de la información de los medios donde se haya guardado la información local y enviada al archivo central, para facilitar el seguimiento de la actividad de seguridad y restauración.

Adquisición del software: La centralización de las necesidades tecnológicas entre ellas la adquisición de software, permiten beneficiar la institución en el control de costos por la puntualización de licencias correctas que causa descuentos, redistribución del software con otras dependencias, entre otras. Los usuarios y funcionarios que requieran la adquisición de software deberán presentar el requerimiento a la Gerencia e igualmente deberán quien se encargara de evaluar el tipo de software, los requerimientos de instalación, el tipo de licencia, entre otras características que permita analizar la viabilidad de la adquisición. Por otra parte, si lo que requiere el usuario o empleado es la instalación de software específico individual que sea propiedad de la Institución, deberá solicitarlo por escrito a la Gerencia para que sea esta quien verifique la capacidad de la licencia o si debe adquirirse una adicional. Si es software es para trabajo en equipo debe presentar la autorización de administrador de sistema de información. Sera una falta grave que se instalen cualquier tipo de software en sus computadoras conectado a la red de la Institución y que no esté autorizado previamente por el jefe inmediato y la Gerencia.

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 15 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

Controles de acceso físico

Entre los tipos de acceso, se encuentran los accesos físicos relacionados con permisos a empleados, terceros o proveedores y clientes, a oficinas, archivos confidenciales, áreas restringidas, entre otros.

A continuación, se detallan las políticas de controles de acceso físico

Ingreso a las instalaciones de la Institución: el FCPC-CJETUTEQ deberá proveer a sus empleados una identificación que los identifique como integrante de la institución. Las actividades realizadas por proveedores dentro de áreas seguras no deberán ser efectuadas, a menos que estén acompañados y/o sin supervisión por un empleado "identificable". Las puertas y ventanas deberán encontrarse cerradas cuando no exista personal.

Protección y ubicación de los equipos de cómputo: 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 del Jefe Inmediato, debiéndose solicitar a las mismas por escrito en caso de requerir este servicio. El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones asignadas al usuario del FCPC-CJETUTEQ. Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas entre otras instaladas y autorizadas en los equipos que utilizan, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas. Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos, a menos que sea en botellas de plástico. 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 aplastados al colocar otros objetos encima o contra ellos. Exclusivamente el proveedor de TICs podrá llevar a cabo los servicios y reparaciones a los equipos de cómputo, 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 considere relevante cuando el equipo sea enviado a mantenimiento o reparación y borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de mantenimiento o reparación. El usuario deberá dar aviso de inmediato a la Gerencia en caso de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su responsabilidad.

Daño de equipos: el equipo de cómputo o cualquier recurso tecnológico que sufra algún daño por maltrato, descuido o negligencia por parte del usuario comprobada, deberá cubrir el valor de la reparación o reposición del equipo o accesorio afectado.

Seguridad en el área de trabajo: una persona del FCPC-CJETUTEQ deberá tener en responsabilidad servidores, equipos, herramientas y partes tecnológicas debe ser un área restringida, por lo que sólo el personal autorizado por la Gerencia puede acceder al área debe tener aire acondicionado, que permita una temperatura adecuada para el recurso humano y tecnológico. Solo el personal autorizado ingresa al área de servidores. Solo los técnicos tendrán acceso a la herramienta, partes y equipos en reparación. En el área no debe ingresar ninguna persona que no sea del soporte técnico. No deben repararse, ni mucho menos cambiar partes a equipos que no sean institucionales. El mantenimiento preventivo y correctivo solo se realizará a equipos institucionales.

FONDO COMPLEMENTARIO PREVISIONAL CERRADO DE CESANTÍA Y JUBILACIÓN PARA EMPLEADOS Y TRABAJADORES DE LA UNIVERSIDAD TÉCNICA ESTATAL DE QUEVEDO – FCPC-CJETUTEQ	Código: FCPC-CJETUTEQ-02	
	Versión: 1	FECHA DE ELABORACIÓN: 30-09-2016
	Versión: 1.1	FECHA DE ULTIMA ACTUALIZACION: 30-11-2018
	Pág. 16 - 16	
RESPONSABLE DE APLICACIÓN:	TODAS LAS ÁREAS INMERSAS AL FCPC-CJETUTEQ	
RESPONSABLE MONITOREO:	CONSEJO DE ADMINISTRACIÓN BANCO DEL INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL	

7. INVENTARIO DE EQUIPOS DE CÓMPUTO

No.	Dependencia	Versión	Hardware	Software	Adicionales
1	Gerencia	00178-50282-02963-AA974	Intel(R) Core(TM) i5-2450M CPU @ 2.50 GHz, 2.50 Ghz,	Microsoft Windows 8 Pro, Fabricante del SOMicrosoft Corporation 2012 Microsoft Corporation	Laptop + Cargador +
1	Administrativo	00261-80423-51470-AA189	Intel(R) Core(TM) i5-3330 CPU @ 3.00 GHz, 3.00 Ghz,	Microsoft Windows 8.1 Pro, Fabricante del SOMicrosoft Corporation Nombre del sistema DESKTOP-LEG51LM	Monitor + Teclado+ Ratón + UPS + Impresora Epson L575 +
2	Contabilidad	6.1.7601 Service Pack 1 Compilación 7601	Intel® Core™ i7-2630QM CPU @ 2,00 GHz, 2001 Mhz 4 procesadores principales	Microsoft Windows 7 Home Premium	Laptop + Ratón + Cargador +