PLAN DE SEGURIDAD INFORMÁTICA
2020

BENEFICENCIA DEL VALLE DEL CAUCA EICE

JEFATURA DE SISTEMAS

JEFE DE SISTEMAS
DIEGO FERNANDO CUERO HURTADO

Contenido

I. GENERALIDADES

Dentro del plan de Seguridad Informática de la Beneficencia del Valle del Cauca EICE (en adelante La Entidad), las normas y políticas expuestas sirven de referencia, en ningún momento pretenden ser normas absolutas por lo que están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad. Se han elaborado siguiendo el esquema normativo de seguridad ISO 27000, tomando como lineamientos principales cuatro criterios:

- **Seguridad Organizacional**
- **Seguridad Lógica**
- **Seguridad Física**
- **Seguridad Legal**

Esta normativa deberá ser revisada y actualizada conforme a las exigencias de la empresa, o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica de la Red BENEVALLE.

II. INTRODUCCION

El plan de seguridad informática de la Beneficencia del Valle del Cauca EICE, está fundamentado bajo la norma ISO/IEC 27000, alineado con las normas y procedimientos de BENEVALLE y comprende:

1. **Seguridad Organizacional:** Dentro de este, se establece el marco formal de seguridad que aplica para la Entidad, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, responsabilidades y actividades complementarias como respuesta ante situaciones anómalas relativas a la seguridad. Consta de:
   1.1. Seguridad Organizacional
   1.2. Políticas de Seguridad
   1.3. Clasificación y Control de Activos
      1.3.1. Responsabilidad por los Activos
      1.3.2. Clasificación de la Información
   1.4. Seguridad Relacionada con el Personal
   1.5. Capacitación de Usuarios
   1.6. Respuestas a Incidentes y Anomalías de Seguridad

2. **Seguridad Lógica:** Establece e integra los mecanismos y procedimientos que permitan monitorear el acceso a los activos de información, procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, control de software malicioso.
   Comprende:
   2.1. Administración del Acceso de Usuarios
   2.2. Responsabilidades del Usuario
   2.3. Uso de Correo Electrónico
   2.4. Seguridad en Acceso de Terceros
   2.5. Control de Acceso a la Red

2.6. Control de Acceso al Sistema Operativo
2.7. Control de Acceso a las Aplicaciones
2.8 Mantenimiento de Sistemas y Equipos de Cómputo
2.9 Manejo de Copias de Seguridad

3. **Seguridad Física:** Identifica las características mínimas que se deben cumplir en cuanto a elementos físicos de seguridad, de forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas físicas con base en la importancia de los activos.
   Incluye:
   3.1. Seguridad Física y Ambiental
   3.2. Seguridad de los Equipos
   3.3. Controles Generales

4. **Seguridad Legal:** Integra los requerimientos de seguridad que deben cumplir todos los empleados y usuarios de La Entidad bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos de La Entidad, haciendo especial énfasis en el licenciamiento de software.
   4.1. Licenciamiento de Software
   4.2. Revisión de Políticas de Seguridad y Cumplimiento Técnico

III. DEFINICIÓN DE TÉRMINOS UTILIZADOS EN ESTE DOCUMENTO

Activo Informático: Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos. Bienes de información y procesamiento que posee La Entidad.

Administración Remota: Forma de administrar los equipos informáticos o servicios de BENEVALLE, a través de equipos remotos, físicamente separados de La Entidad.

Amenaza: Evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Archivo Log: Archivos de registro o bitácoras de sistemas, en los que se registran las actividades realizadas (ingreso de un usuario, acciones en la conexión, horarios de conexión, terminales o IP´s involucradas en el proceso, etc.)

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.
Confidencialidad: Calidad de la información para prevenir su revelación no autorizada.

Cuenta: Mecanismo de identificación, acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático.

Desastre o Incidencia: Interrupción de la capacidad de procesamiento de la información necesaria para la operación normal de un negocio

Disponibilidad: Condición que permite que los recursos informáticos sean accesibles cuando se necesitan.

Encriptación: Es el proceso mediante el cual cierta información es cifrada de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.

IEC:(Comisión Electrotécnica Internacional) Junto a la ISO, desarrolla estándares que son aceptados a nivel internacional.

Integridad: Condición que garantiza que la información no sufre alteraciones

Impacto: Consecuencia de la materialización de una amenaza

ISO: (Organización Internacional de Estándares) Institución acreditada para normar en temas de estándares.

Normativa de Seguridad ISO/IEC 27000: (Código de buenas prácticas, para el manejo de seguridad de la información) Estándar o norma internacional que vela por que se cumplan los requisitos mínimos de seguridad, que propicien un nivel de seguridad aceptable y acorde a los objetivos institucionales desarrollando buenas prácticas para la gestión de la seguridad informática.

Outsourcing: Contrato por servicios a terceros, tipo de servicio prestado por personal ajeno a La Entidad.

Responsabilidad: En términos de seguridad, significa determinar que individuo en La Entidad, es responsable directo de mantener seguros los activos de cómputo e información.

Servicio: Conjunto de aplicativos o programas informáticos que apoyan los procesos diarios de La Entidad.

SGSI: Sistema de Gestión de Seguridad de la Información

Riesgo: Posibilidad de que se produzca un evento determinado en un activo, en un dominio o en toda la organización.

Terceros: Proveedores de hardware, software o servicios que tengan vínculos profesionales con La Entidad.

Usuario: Cualquier persona jurídica o natural que utilice los servicios informáticos de la red corporativa de La Entidad (BENEVALLE).

Vulnerabilidad: Posibilidad de ocurrencia de una amenaza sobre un activo

IV. DEFINICIÓN DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA

OBJETIV O

Dotar de la información necesaria a los empleados de La Beneficencia del Valle del Cauca EICE, sobre las normas y mecanismos que deben cumplir para proteger el hardware, software y la información que es procesada y almacenada en la red BENEVALLE. Establecer un conjunto de lineamientos, reglas, recomendaciones y controles con el propósito de dar respaldo a las políticas de seguridad a través de funciones, responsabilidades y otras técnicas, acorde con las necesidades de seguridad establecidas para la red BENEVALLE.

1. NIVEL DE SEGURIDAD ORGANIZATIVA

1.1. Seguridad Organizacional

1.1.1. Los recursos informáticos y de comunicaciones sólo podrán ser utilizados por las personas que, en su calidad de trabajadores, aprendices, contratistas o bajo cualquier otra modalidad, estén vinculados a La Entidad.

1.2. Políticas de Seguridad

1.2.1. Toda persona que utilice los servicios que ofrece la red, deberá conocer y aceptar el reglamento vigente sobre su uso, plasmado en el documento AA-DO-003 Políticas de Seguridad Informática, el desconocimiento del mismo, no exonera de responsabilidad al usuario ante cualquier eventualidad que involucre la seguridad de la información o de la red de BENEVALLE.

1.2.2. Todo usuario de la red BENEVALLE, gozará de absoluta privacidad sobre su información, o la información que provenga de sus acciones, salvo en casos, en que se vea involucrado en actos ilícitos o contraproducentes para la seguridad, sus servicios o cualquier otra red ajena a BENEVALLE.

1.2.3. La Entidad se reserva el derecho de divulgar la información personal de los usuarios de la red institucional, si estos se ven envueltos en actos ilícitos.

1.2.4. El usuario acatará las disposiciones expresas sobre la utilización de los servicios informáticos de la red.

1.2.5. Los usuarios tendrán el acceso a Internet, siempre y cuando se cumplan los requisitos mínimos de seguridad para acceder a este servicio y se acaten las disposiciones de conectividad de la Jefatura de Informática.

1.2.6. El jefe de Informática, dará de alta y baja a usuarios y revisará las cuentas para estar seguros de que no hay usuarios ficticios.

1.2.7. El Jefe de Informática hará respaldos periódicos de la información, así como la depuración de los discos duros, de acuerdo con la IT-GAF-005-J Copias de Seguridad.

1.3. Clasificación y Control de Activos Informáticos

1.3.1. **Responsabilidad por los activos informáticos**

1.3.1.1. Cada persona es responsable de los activos informáticos asignados para el desarrollo de sus actividades y velará por la salvaguarda de ellos (hardware y medios magnéticos), activos de información (Bases de Datos, archivos, documentación de sistemas, procedimientos operativos, configuraciones), activos de software (aplicaciones,

herramientas y programas de desarrollo)

1.3.1.2. Cada usuario debe guardar la información referente al desempeño de sus funciones en la carpeta “Mis Documentos”.

1.3.1.3. El Jefe de Informática, es el responsable de la seguridad de la información almacenada en los servidores

1.3.2. **Clasificación de la Información**

1.3.2.1. Los activos de información de mayor importancia para La Entidad deberán clasificarse por su nivel de exposición o vulnerabilidad

1.3.2.2. Los niveles de seguridad se clasifican como nivel de seguridad alto, nivel de seguridad medio y nivel de seguridad bajo

1.3.2.3. De forma individual, los procesos de La Entidad, son responsables de clasificar la información de acuerdo con su nivel de importancia

1.3.2.4. Se tomarán los siguientes criterios, como niveles de importancia, para clasificar la información:

- Confidencial
- Interna
- Pública

1.3.2.5. La información confidencial es propiedad absoluta de La Entidad, el acceso a ésta es permitido únicamente a personal directivo

1.3.2.6. La información interna, es propiedad de cada proceso y de La Entidad, en ningún momento intervendrán en su manipulación personas ajenas al proceso.

1.3.2.7. La información pública puede ser visualizada por cualquier persona dentro o fuera de La Entidad.

1.4. Seguridad Relacionada con el Personal

1.4.1. Se entregará al personal contratado toda la documentación necesaria para ejercer sus labores dentro de La Entidad, anexando o divulgando el documento AA-DO-003 Políticas de Seguridad informática, en el momento en que se de por establecido su contrato laboral.

1.4.2. La información procesada, manipulada o almacenada por el empleado es propiedad exclusiva de La Entidad.

1.4.3. La información que maneja o manipula el empleado, no puede ser divulgada a terceros o fuera del ámbito de laboral.

1.4.4. El empleado no tiene ningún derecho sobre la información que procese dentro de las instalaciones de La Entidad.

1.4.5. Los usuarios son responsables de las acciones causadas por sus operaciones con el equipo de la red institucional

1.4.6. La Entidad no se hace responsable por daños causados provenientes de sus empleados a la información o activos de procesamiento en equipos informáticos externo

1.5. Capacitación de Usuarios

1.5.1. Los usuarios de la red BENEVALLE, serán capacitados en temas de seguridad de la información, de acuerdo con el proceso al que pertenezcan y en función de las actividades que desarrollen en el.

1.5.2. Se deben tomar todas las medidas de seguridad necesarias, antes de realizar una capacitación a personal ajeno o propio de La Entidad, siempre y cuando se vea implicada la utilización de los servicios de red o se exponga

material de importancia considerable para La Entidad.

1.5.3. En cada capacitación se revisarán los dispositivos de conexión de servicios involucrados en la capacitación.

1.5.4. Las capacitaciones deben realizarse fuera de las áreas de procesamiento de información.

1.5.5. Entre los deberes y derechos de los empleados y los terceros, se encuentran acatar o respetar las disposiciones sobre capacitaciones y por ende asistir a ellas sin excepción alguna, salvo casos especiales.

1.6. Respuesta a incidentes y anomalías de seguridad

1.6.1. La Entidad debe contar con respaldos de la información ante cualquier incidente.

1.6.2. Se realizarán respaldos de la información, que se utilizará en caso de fallas tal como está en el documento AA-DO-003 Políticas de Seguridad informática.

1.6.3. Los respaldos se utilizarán únicamente en casos especiales dada la importancia de su contenido

1.6.4. Los respaldos de información deberán ser almacenados en un sitio aislado, libre de cualquier daño o extracción por terceros y en lo posible fuera de las instalaciones de La Entidad.

1.6.5. Cualquier situación anómala y contraria a la seguridad deberá ser documentada, posterior revisión de los registros o Log del sistema, con el objetivo de verificar la situación y dar una respuesta congruente y acorde con la incidencia.

1.6.6. Se deben respaldar los archivos de logs o registro de los sistemas

1.6.7. La Jefatura de Informática tendrá la responsabilidad de priorizar una situación de la otra en cuanto a los problemas en las estaciones de trabajo de acuerdo con:

1.6.7.1. Urgencia

1.6.7.2. Tendencia

1.6.7.3. Impacto

1.6.8. En situaciones de emergencia que impliquen suspensión del servicio, la prioridad para el restablecimiento será en el orden siguiente.

1.6.8.1. Procesos Misionales

1.6.8.2. Procesos Gerenciales

1.6.8.3. Procesos de Apoyo

1.6.9. En caso de requerir evacuación se prioriza la información catalogada como confidencial

1.6.10. Se llevará a cabo lo estipulado en los documentos AA-DO-004 plan de continuidad del negocio y AA-IN-006 Instructivo de contingencia

2. NIVEL DE SEGURIDAD LOGICA

2.1. Administración del Acceso de Usuarios

2.1.1. Son usuarios de la red todas aquellas personas que, en su calidad de

empleados, aprendices, contratistas o bajo cualquier otra modalidad, estén vinculados a La Entidad.

2.1.2. Se consideran usuarios externos o terceros, cualquier entidad o persona natural, que tenga una relación con La Entidad fuera del ámbito mencionado en el ítem anterior

2.1.3. El acceso a la red por parte de terceros es de carácter restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad hacia La Entidad y compromiso con el uso exclusivo del servicio para el que le fue provisto el acceso.

2.1.4. La asignación de usuario y contraseña se realizará por solicitud escrita del jefe del proceso

2.1.5. Los eventos de restauración de contraseña se harán previa autorización del jefe directo del solicitante

2.1.6. No se proporcionará el servicio solicitado por un usuario o proceso sin antes haberse autorizado por su jefe directo.

2.1.7. Toda cuenta nula u olvidada, se inactivará del sistema previa verificación o asignación de una nueva cuenta al usuario involucrado

2.1.8. Los usuarios darán un seguimiento estricto sobre las políticas de creación de contraseñas, acatando lo establecido en AA-DO-003 Políticas de Seguridad informática

2.2. Responsabilidad del Usuario

2.2.1. Las cuentas de usuario son personales, en ningún momento deben ser utilizadas por personal ajeno al que le fue asignada.

2.2.2. El usuario será responsable del uso que se haga de su cuenta de acceso a los sistemas o servicios.

2.2.3. El usuario es responsable de eliminar cualquier rastro de documentos proporcionados por el área de informática, que contenga información que pueda facilitar a un tercero la obtención de la información de su cuenta de usuario.

2.2.4. El usuario es responsable exclusivo de mantener a salvo su contraseña, esta debe ser memorizada desde el mismo momento en que le es asignada.

2.2.5. Se debe evitar el guardar o escribir las contraseñas en cualquier papel o superficie o dejar constancia de ellas

2.2.6. No se debe guardar las contraseñas en papel adherido al monitor o áreas cercanas al equipo de trabajo

2.2.7. Es importante que el usuario establezca contraseñas fuertes y desligadas de su vida personal o de su entorno familiar, no empleando formatos comunes de fechas o números, ni palabras que existan en el diccionario.

2.2.8. El usuario deberá proteger su equipo de trabajo, evitando que personas ajenas a su cargo puedan acceder a la información almacenada en el, mediante una herramienta de bloqueo temporal (protector de pantalla),

protegida por una contraseña, el cual deberá activarse en el momento en que el usuario se ausente

2.2.9. El servidor de dominio deberá bloquear cualquier estación de trabajo con un protector de pantalla, que tenga un tiempo de inactividad mayor a quince minutos.

2.2.10. Cualquier usuario que detecte una falla de seguridad en los sistemas informáticos de BENEVALLE, está obligado a reportarlo como una incidencia a la mesa de ayuda y a la Jefatura de Informática

2.3. Uso de correo electrónico

2.3.1. El sistema de correo electrónico y utilidades asociadas de La Entidad deben ser usados únicamente para el ejercicio de las funciones de competencia de cada empleado y de las actividades contratadas en el caso de los contratistas

2.3.2. El correo electrónico institucional es de uso exclusivo, para los empleados de La Entidad.

2.3.3. Es responsabilidad del usuario hacer un correcto empleo del correo electrónico y será responsable de la información que sea enviada con su cuenta

2.3.4. El correo electrónico es un medio de comunicación directo y confidencial entre el emisor del mensaje y el receptor o receptores del mismo, por ende deberá ser visto o reproducido sólo por las personas implicadas en la comunicación.

2.3.5. Las cuentas de correo que no cumplan con la normativa de seguridad o los fines para los que fueron creadas, pierden automáticamente su característica de privacidad

2.3.6. El usuario es responsable de respetar la ley de derechos de autor, por lo tanto no se debe distribuir de forma ilegal licencias de software o reproducir información sin conocimiento del autor

2.3.7. Se considera un mal uso del correo electrónico:

2.3.7.1. Enviar o contestar cadenas de correo (chistes, oraciones, denuncias, etc.)

2.3.7.2. La no depuración de su bandeja de entrada (dejar correos por largos periodos de manera innecesaria)

2.3.7.3. Hacer uso de la cuenta para fines diferentes a los laborales

2.3.7.4. Uso de un lenguaje inapropiado en sus comunicaciones.

2.3.7.5. Incumplir los términos dados en el contrato de trabajo sobre normativas y políticas de seguridad.

2.3.8. El servidor de correo está configurado para bloquear archivos adjuntos o información nociva como archivos .exe o de ejecución de comandos como applets java, javascript o archivos del tipo activeX o IFrame

2.3.9. La información y el software tienen la característica de ser propiedad intelectual, La Entidad no se responsabiliza por el uso del correo electrónico de parte de sus empleados violentando la ley de derechos de autor.

2.4. Seguridad en Acceso de Terceros

2.4.1. El acceso de terceros será concedido siempre y cuando se cumplan con los requisitos de seguridad establecidos en el contrato de trabajo, el cual deberá estar firmado por las entidades involucradas en el mismo.

2.4.2. Los servicios accedidos por terceros acataran las disposiciones generales de acceso a servicios por el personal interno de La Entidad, además de los requisitos expuestos en su contrato específico con La Entidad

2.4.3. Todo usuario externo, estará facultado a utilizar única y exclusivamente el servicio que le fue asignado, y acatar las responsabilidades que devengan de la utilización del mismo.

2.4.4. El no cumplimiento de las disposiciones de seguridad y responsabilidad sobre sus acciones en la red BENEVALLE, acarrea la suspensión de su cuenta de usuario

2.5. Control de Acceso a la Red

2.5.1. El departamento de informática deberá emplear dispositivos de red para el bloqueo, enrutamiento, o el filtrado de tráfico evitando el acceso o flujo de información, no autorizada hacia la red interna o desde la red interna hacia el exterior.

2.5.2. Se utilizarán mecanismos y protocolos de autenticación como, ssh, IPsec, Claves públicas y privadas, autenticación usuario/contraseña, cualquiera de ellos será válido para la autenticación

2.5.3. Se registrara todo acceso a los dispositivos de red, mediante archivos de registro o Log, de los dispositivos que provean estos accesos

2.5.4. Los archivos de registro o logs de sucesos de los sistemas de aplicación y de operación, se mantienen siempre activos y en ningún momento deberán ser deshabilitados

2.5.5. Cualquier alteración del tráfico entrante o saliente a través de los dispositivos de acceso a la red, será motivo de verificación y tendrá como resultado directo la realización de una auditoria de seguridad

2.6. Control de Acceso al Sistema Operativo

2.6.1. El acceso a la configuración del sistema operativo de los servidores, es únicamente permitido al Jefe de Informática.

2.6.2. Los servidores estarán debidamente configurados, evitando el acceso de personal extraño a la administración de estos

2.6.3. No le está permitido al usuario final ejecutar actividades de configuración del sistema

2.6.4. Se deshabilitarán las cuentas creadas con privilegios de sistema, (cuentas del servidor de aplicaciones, cuentas de herramientas de auditoría, etc.) evitando que estas corran sus servicios con privilegios nocivos para la seguridad del sistema.

2.6.5. Todo servicio instalado en los servidores, correrá o será ejecutado bajo cuentas restrictivas.
2.6.6. La finalización de la jornada laboral, termina con cualquier actividad que se desarrolla en ese momento, lo cual implica guardar todo cuanto se utilice y apagar equipos informáticos antes de salir de las instalaciones.
2.6.7. Al terminar una sesión de trabajo, el usuario evitará dejar encendido el equipo

2.7. Control de Acceso a las Aplicaciones

2.7.1. Tienen acceso total a las aplicaciones y sus archivos, los usuarios que lo ameriten por su cargo dentro de La Entidad, siempre que sea aprobado por el comité de seguridad.
2.7.2. El usuario tendrá los permisos de aplicaciones necesarios para ejercer su trabajo.

2.8. Mantenimiento de Sistemas y Equipos de Cómputo

2.8.1. Ningún usuario está facultado a intervenir física o lógicamente ninguna estación de trabajo
2.8.2. Cualquier falla detectada en las aplicaciones o equipos de cómputo debe ser reportada como incidencia a la jefatura de informática
2.8.3. La jefatura de informática realiza las revisiones hechas a los equipos de cómputo y quedan registradas en el formato AA-FO-005 Mantenimiento Equipo de Cómputo.

2.9. Manejo de Copias de Seguridad

2.9.1. Las copias de seguridad se realizarán de acuerdo con AA-DO-003 Políticas de Seguridad informática
2.9.2. Las copias de seguridad de La Entidad serán etiquetadas de acuerdo con la información que almacenan u objetivo que suponga su uso, haciendo alusión a su contenido.
2.9.3. Las copias deben ser manipulados única y exclusivamente por el personal encargado de hacer los respaldos y el personal encargado de su salvaguarda.
2.9.4. Una segunda copia será resguardada fuera de las instalaciones de la BENEVALLE

3. SEGURIDAD FÍSICA

3.1. Seguridad Física y Ambiental

3.1.1. Los centros de procesamiento de datos o data center son zonas restringidas únicamente accesibles por personal autorizado
3.1.2. Todo ingreso a la sala de servidores deberá ser autorizada por el jefe de informática.
3.1.3. La sala de servidores debe estar separada de las oficinas mediante una división física
3.1.4. Las líneas de alimentación de energía externa deberán estar protegidas con filtros de protección para rayos
3.1.5. Solo el personal autorizado es el encargado exclusivo de intervenir físicamente los recursos de la red institucional.

3.1.6. No esta permitida la intervención física de los usuarios sobre los recursos de la red BENEVALLE (cables, enlaces, estaciones de trabajo, dispositivos de red).

3.2. Seguridad de los Equipos

3.2.1. Los equipos o activos críticos de información deberán ubicarse en áreas aisladas y seguras, protegidas con un nivel de seguridad verificable y manejable por las personas autorizadas

3.2.2. Deberá llevarse registro del mantenimiento preventivo o correctivo que se les haga a los equipos AA-FO-005 Mantenimiento Equipo de Cómputo

3.2.3. El cableado de red se instalará físicamente separado de cualquier otro tipo de cables como los de energía eléctrica, para evitar interferencias.

3.2.4. El suministro de energía eléctrica debe hacerse a través de un circuito exclusivo para los equipos de cómputo

3.3. Controles Generales

3.3.1. Toda área de trabajo debe poseer elementos como, extintores, etc., necesarias para salvaguardar los activos informáticos

3.3.2. Las instalaciones deben contar con un adecuado respaldo para los fallos en el suministro de energía eléctrica (UPS, Plantas)

3.3.3. Periódicamente se hará una revisión de los equipos de respaldo de energía (UPS, Plantas) verificando de manera práctica su capacidad y correcto funcionamiento, se registrará cada revisión en una lista de chequeo de control y funcionamiento de los equipos.

3.3.4. Los equipos de oficina, como radios, lámparas, aires acondicionados, entre otros no deben estar conectados al mismo circuito que los sistemas informáticos.

3.3.5. Está prohibido el ingreso de bebida(s) o alimento(s) de cualquier tipo a los centros de cómputo.

4. SEGURIDAD LEGAL

4.1. Licenciamiento de Software

4.1.1. La Entidad rechaza por completo la utilización de software pirata o no licenciado, en las estaciones de trabajo, servidores y equipo informático personalizado, que sea parte de sus inventarios informáticos

4.1.2. La Entidad se reserva todo derecho al utilizar software licenciado en sus equipos de cómputo, bajo ninguna circunstancia se aprueba la utilización de software sin licencia en sus instalaciones.

4.1.3. Ningún empleado de La Entidad esta facultado a obtener software para BENEVALLE

4.1.4. La Jefatura de Informática llevará un control detallado sobre el inventario de software instalado

4.1.5. El contrato de licencia de usuario final tanto de software comercial con derechos de copyright, como de software libre con derechos de copyleft, son respetados en su totalidad por La Entidad, sus empleados no pueden utilizar software de este tipo sin su respectiva licencia

4.2. Revisión de Políticas de Seguridad y Cumplimiento Técnico

4.2.1. Toda violación a las políticas de licenciamiento de software será motivo de sanciones aplicables de acuerdo con la normatividad vigente

4.2.2. Cualquier violación a la seguridad por parte del personal que labora para La Entidad, así como terceros que tengan alguna relación o contrato con La Entidad se harán acreedores a sanciones aplicables de ley.

4.2.3. Todos los empleados o usuarios de la red BENEVALLE deberán tener pleno conocimiento de la documentación de seguridad y apegarse a ella en todo sentido

4.2.4. El medio exclusivo de soporte para la seguridad en el tratamiento de la información de BENEVALLE, lo constituyen el AA-DO-003-Políticas de seguridad informática y este documento.

Referencias.

[1]. ISO/IEC 17799 Code of Best Practice for Information Security Management
[2]. Certified Information Systems Security Professional (CISSP)
[3]. RFC 1244, Site Security Handbook
[4] Normativas PROACTIVA MEDIO AMBIENTE
[5] Sistema de Gestión Integrado BENEVALLE