INSTITUTO DE EDUCACIÓN TÉCNICA PROFESIONAL
DE ROLDANILLO, VALLE - INTEP

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

GESTIÓN DE INFRAESTRUCTURA

ABRIL, 2016

1. ASPECTOS GENERALES

Los computadores y la red proporcionan acceso y recursos, dentro y fuera del ámbito del INTEP y nos permiten la comunicación con usuarios en todo el mundo. Este privilegio acarrea unas responsabilidades a los usuarios, que han de respetar los derechos de los otros usuarios, la integridad del sistema y de los recursos físicos y respetar las leyes y regulaciones vigentes. Los motivos que han llevado a la redacción de estas políticas, son:

Actualmente los usuarios a nivel general que utilizan los recursos tecnológicos e informáticos en el INTEP, no se les ha definido directrices de seguridad en cuanto al uso de los sistemas de información, que les permitan adoptar políticas y planes que ayuden a que los mismos usuarios hagan un uso adecuado de este tipo de herramientas.

Sumando a esto, la infraestructura informática y de cableado estructurado, no cuenta con la seguridad, soporte y cobertura necesarios para su adecuada utilización, con lo cual aspiramos que de acuerdo a las políticas, se solucionen los problemas actuales de seguridad informática, y uso de la información con que se trabaja y finalmente los usuarios puedan tener un manual de trabajo para realizar de la manera correcta todos sus recursos de tipo tecnológicos en el INTEP.

2. OBJETIVOS

Garantizar que la seguridad sea parte del proceso de planificación de la información.

Promover la difusión y apoyo a la seguridad de la información dentro de la institución.

Revisar y proponer la Política de Seguridad de la Información.

Acordar y aprobar metodologías y procesos específicos.

Evaluar y coordinar la implementación de controles específicos.

Coordinar el proceso de administración de la continuidad de la operatividad de la Institución.

Monitorear cambios significativos en los riesgos.

Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

3. ALCANCE DE LAS POLÍTICAS

Las políticas definidas en el presente documento aplican a todos los funcionarios públicos, contratistas, pasantes y monitores del INTEP, personas de contratación temporal y relacionada con terceras partes que utilicen recursos informáticos de la institución.

4. DESCRIPCIÓN DE LAS POLÍTICAS

4.1 ACCESO A LA INFORMACIÓN

Todos los funcionarios públicos, contratistas, pasantes y monitores que laboran para el INTEP deben tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas al INTEP, se debe autorizar sólo el acceso indispensable de acuerdo con el trabajo realizado por estas personas, previa justificación.

El otorgamiento de acceso a la información esta regulado mediante las normas y procedimientos definidos para tal fin.

Todas las prerrogativas para el uso de los sistemas de información de la entidad deben terminar inmediatamente después de que el trabajador cesa de prestar sus servicios a la entidad

Proveedores o terceras personas solamente deben tener privilegios durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

Para dar acceso a la información se tendrá en cuenta la clasificación de la misma al interior de la entidad, la cual deberá realizarse de acuerdo con la importancia de la información en la operación normal de la entidad.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento a los accesos realizados por los usuarios a la información de la entidad, con el objeto de minimizar el riesgo de pérdida de integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la

información se deberán documentar y realizar las acciones tendientes a su solución.

4.2 ADMINISTRACIÓN DE CAMBIOS

Todo cambio (creación y modificación de programas, pantallas y reportes) que afecte los recursos informáticos, debe ser requerido por los usuarios de la información y aprobado formalmente por el responsable de la administración del mismo, al nivel de jefe inmediato o a quienes estos formalmente deleguen. El responsable de la administración de los accesos tendrá la facultad de aceptar o rechazar la solicitud.

Bajo ninguna circunstancia un cambio puede ser aprobado, realizado e implantado por la misma persona o área.

Para la administración de cambios se efectuará el procedimiento correspondiente definido por el INTEP, de acuerdo con el tipo de cambio solicitado en la plataforma tecnológica.

Cualquier tipo de cambio en la plataforma tecnológica debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros debe realizarse de tal forma que no disminuya la seguridad existente.

4.3 SEGURIDAD DE LA INFORMACIÓN

Los funcionarios públicos, contratistas, pasantes y monitores del INTEP son responsables de la información que manejan y deberán cumplir los lineamientos generales y especiales dados por la entidad, por la Ley 594 de 2000 para protegerla y evitar pérdidas, accesos no autorizados, exposición y utilización indebida de la misma.

Los funcionarios públicos, contratistas, pasantes y monitores no deben suministrar cualquier información de la entidad a ningún ente externo sin las autorizaciones respectivas; de igual manera, los jefes de dependencia deberán suministrar a los pasantes o monitores la información estrictamente necesaria para cumplir con sus funciones.

Todo funcionario que utilice los recursos informáticos, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje, especialmente si dicha información está protegida por reserva legal o ha sido clasificada como confidencial y/o crítica.

Los funcionarios, contratistas, pasantes y monitores deben firmar y renovar cada año, un acuerdo de cumplimiento de la seguridad de la información, la confidencialidad, el buen manejo de la información. **Después de que el trabajador deja de prestar sus servicios a la entidad, se compromete entregar toda la información respectiva de su trabajo realizado**. Una vez retirado el funcionario, contratistas, pasantes y monitores del INTEP deben comprometerse a no utilizar, comercializar o divulgar los productos o la información generada o conocida durante la gestión en la entidad, directamente o través de terceros, así mismo; borrar las cuentas de usuarios y privilegios que tenían las personas que ya no pertenecen a la institución. Los funcionarios públicos que detecten el mal uso de la información esta en la obligación de reportar el hecho a de control interno.

Como regla general, la información de políticas, normas y procedimientos de seguridad se deben revelar únicamente a funcionarios y entes externos que lo requieran, de acuerdo con su competencia y actividades a desarrollar según el caso respectivamente.

4.4 SEGURIDAD PARA LOS SERVICIOS INFORMÁTICOS

El sistema de correo electrónico, grupos de charla y utilidades asociadas de la entidad debe ser usado únicamente para el ejercicio de las funciones de competencia de cada funcionario y de las actividades contratadas en el caso de los contratistas, pasantes y monitores.

Los correos electrónicos institucionales serán realizados según el instructivo de creación de usuarios sistemas de información.

La entidad no podrá acceder a los mensajes enviados por medio del sistema de correo electrónico para proteger los derechos a la privacidad de los funcionarios de la entidad; solo se pueden acceder a estos, si un ente de control o fiscal lo pida por medio de un oficio a la entidad.

Los funcionarios públicos, contratistas, pasantes no deben utilizar versiones **escaneadas de firmas hechas a mano** para dar la impresión de que un mensaje de correo electrónico ó cualquier otro tipo de comunicación

electrónica haya sido firmado por la persona que la envía. Por seguridad para la firma digital se debe realizar una diferente a los documentos impresos.

La propiedad intelectual desarrollada o concebida mientras el trabajador se encuentre en sitios de trabajo alternos, es propiedad exclusiva de la entidad o como se haya pactado con la entidad en un acto administrativo. Esta política incluye patentes, derechos de reproducción, marca registrada y otros derechos de propiedad intelectual según lo manifestado en memos, planes, estrategias, productos, programas de computación, códigos fuentes, documentación y otros materiales.

Los funcionarios públicos, contratistas, pasantes y monitores que hayan recibido aprobación para tener acceso a Internet deberán aceptar, respetar y aplicar las políticas y prácticas de uso de Internet.

Si los usuarios sospechan que hay infección por un virus, deben inmediatamente llamar a la oficina de infraestructura tecnológica o a soporte técnico, no utilizar el computador y desconectarlo de la red. Ver instructivo eliminación de virus informáticos.

El intercambio electrónico de información se realizará con base en estándares de documentos electrónicos y mensajes de datos de dominio público, regidas por organismos idóneos de carácter nacional e internacionales, y utilizando mecanismos criptográficos de clave pública que garanticen la integridad, confidencialidad, autenticidad y aceptación de la información. Cuando se considere necesario, los servicios de intercambio de información también incluirán garantías de "no repudio".

El encargado de la seguridad informática en conjunto con la oficina de comunicaciones y mercadeo debe proveer material para recordar regularmente a los funcionarios acerca de sus obligaciones con respecto a la seguridad de los recursos informáticos.

Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

Administración de usuarios: Establece cómo deben ser utilizadas las claves de ingreso a los recursos informáticos.

Rol de Usuario: Los sistemas operacionales, bases de datos y aplicativos deberán contar con roles predefinidos o con un módulo que permita definir roles, estableciendo las acciones permitidas por cada uno de estos. También deben admitir que un rol de supesusuario administre el sistema; se debe cumplir con las siguientes características:

Longitud de las contraseñas, debe ser de mínimo 8 caracteres combinando mayúsculas, minúsculas, números y caracteres especiales.

Por seguridad la contraseña debe ser cambiada mensualmente.

Los períodos de vigencia del **usuario** deben ser de 1 año para personal de planta y para el personal de contrato, docentes hora cátedra, pasantes y monitores, su duración es de acuerdo al tiempo de labores.

Los tipos de usuarios para los sistemas de información son:

1. **Cuentas de usuarios de equipos de cómputo**: el nombre de la dependencia, si hay varios equipos con un consecutivo, y la cuenta limitada.

2. **Cuentas de correo electrónico**: la estructura debe ser la siguiente:

2.1 El dominio para los correos serán: @intep.edu.co para dependencias, administrativos, docentes y estudiantes.

2.2 Dependencias: Nombre de la dependencia

Ejemplo: rectoría@intep.edu.co

3.3 Administrativos: Inicial de los nombres seguido del primer apellido completo.

Ejemplo: afbermudez@intep.edu.co

Si hay nombres y apellidos repetidos: Se colocara la inicial del segundo apellido.

Ejemplo: afbermudezr@intep.edu.co

2.4 Docentes: Inicial de los nombres seguido del primer apellido completo.

Ejemplo: afbermudez_docente@intep.edu.co

Si hay nombres y apellidos repetidos: Se colocara la inicial del segundo apellido.

Ejemplo: afbermudezr_docente@intep.edu.co

2.3 Estudiantes: Inicial de los nombres seguido del primer apellido completo.

Ejemplo: afbermudez_usistemas@intep.edu.co
afbermudez_uadmon@intep.edu.co
afbermudez_ucaya@intep.edu.co

Si hay nombres y apellidos repetidos: Se colocara la inicial del segundo apellido.

Ejemplo: afbermudezr_usistemas@intep.edu.co
afbermudezr_uadmon@intep.edu.co
afbermudezr_ucaya@intep.edu.co

Esta nomenclatura se realiza para tener control en quien envía información en los correos institucionales.

3. Cuentas a sistemas de información: según la necesidad de cada dependencia.

3.1 Para Gestión Documental y Ventanilla Única, la estructura debe ser la siguiente:

Inicial de los nombres seguido del primer apellido completo.

Ejemplo: afbermudez

Si hay nombres y apellidos repetidos: Se colocara la inicial del segundo apellido.

Ejemplo: afbermudezr

Para la creación de cualquier tipo de usuario se utiliza el formato de solicitud de creación o modificación de usuarios.

La configuración de las cuentas de correo, usuarios a equipos de cómputo y aplicativos (Paquetes contable, Sistema de Registro y Control, Sistema de Biblioteca, Pasantías, Egresados, Extensión, Calificación Docentes, Prestamos Audiovisuales, Gestión Documental, Ventanilla Única, SIABUC 9, entre otros) serán realizados por el funcionario que designe las directivas de la institución mediante un oficio.

Plan de auditoría: Hace referencia a las pistas o registros de los sucesos relativos a la operación. Para esto se debe definir las auditorías para los diferentes aplicativos y módulos.

Las puertas traseras: Las puertas traseras son entradas no convencionales a los sistemas operacionales, bases de datos y aplicativos. Es de suma importancia aceptar la existencia de las mismas y efectuar las acciones preventivas necesarias para contrarrestar la vulnerabilidad que ellas generan.

El control de acceso a todos los sistemas de computación de la entidad debe realizarse por medio de códigos de identificación y palabras clave o contraseña única para cada usuario.

Las palabras clave o contraseñas de acceso a los recursos informáticos, que designen los funcionarios públicos, contratistas, pasantes y monitores del INTEP son responsabilidad exclusiva de cada uno de ellos y no deben ser divulgados a ninguna persona.

Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.

Se prohíbe tener identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos.

Todo sistema debe tener definidos los perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

El nivel de superusuario de los sistemas críticos debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema (jefe de infraestructura o quién designe la dirección)**.**

Toda la información del servidor de base de datos que sea sensible, crítica o valiosa debe tener controles de acceso y sometida a procesos de ciframiento para garantizar que no sea inapropiadamente descubierta, modificada, borrada o no recuperable.

Antes de que un nuevo sistema se desarrolle o se adquiera, los jefes de oficina, en conjunto con el encargado de seguridad informática, deberán definir las especificaciones y requerimientos de seguridad necesarios.

La seguridad debe ser implementada por diseñadores y desarrolladores del sistema desde el inicio del proceso de diseño de sistemas hasta la conversión a un sistema en producción.

Los ambientes de desarrollo de sistemas, pruebas y producción deben permanecer separados para su adecuada administración, operación, control y seguridad y en cada uno de ellos se instalarán las herramientas necesarias para su administración y operación.

Las contraseñas o password de acceso a los recursos informáticos del INTEP serán entregadas vía oficio o correo electrónico y el sistema debe permitir que al primer ingreso se cambie la clave, esto se realiza por seguridad y privacidad de la información.

4.5 SEGURIDAD EN COMUNICACIONES

Las direcciones internas, topologías, configuraciones e información relacionada con el diseño de los sistemas de comunicación, seguridad y cómputo de la entidad, deberán ser consideradas y tratadas como información confidencial.

Todas las conexiones a redes externas de tiempo real que accedan a la red interna de la entidad, deben pasar a través de los sistemas de defensa electrónica que incluyen servicios de cifrамiento y verificación de datos, detección de ataques cibernéticos, detección de intentos de intrusión, administración de permisos de circulación y autenticación de usuarios.

En caso de requerirse que los computadores del INTEP sean conectados de manera directa con computadores de entidades externas a conexiones seguras, deber autorizado por el representante legal de la Institución

Toda información secreta y confidencial que se transmita por las redes de comunicación de la entidad e Internet deberá estar cifrada.

Se Anexa protocolo de seguridad en redes inalámbricas.

4.6 EL USO DEL CORREO ELECTRÓNICO

Estas Políticas son de carácter general y de cumplimiento obligatorio para todos los usuarios del INTEP que tienen asignada una cuenta de correo en el dominio **intep.edu.co.**

Cuentas

Disposiciones Generales

1. La cuenta de correo electrónico es personal e intransferible, por lo que queda estrictamente prohibido dar a otros la posibilidad de uso. O según el manejo que le den internamente las dependencias.

2. La cuenta de correo identifica de manera única a cada usuario y es a través de ella que puede enviar y recibir mensajes de otros usuarios.

3. Las cuentas personales se darán de baja en el momento que el usuario deje de pertenecer al INTEP. Las cuentas de correo electrónico para administrativos, docentes estarán vigentes hasta que haya un vínculo con la institución y los estudiante al terminar su carrera pueden seguir con este como egresados, pero si al cabo de 2 años no lo usa será eliminada la cuenta.

4. Si un usuario tiene un problema relacionado con su cuenta de correo, deberá tratarlo personalmente, escribiendo un correo a webmaster@intep.edu.co, y no a través de terceros.

5. Tener en cuenta que son cuentas solo para recibir o enviar información de tipo institucional.

6. Las cuentas de correo electrónico serán administradas en la plataforma de Gmail, estos estarán regidos por las clausulas de manejo y privacidad de este; pero cumpliendo también las políticas de la institución.

7. La firma para los correos de administrativos, docente debe contener lo siguiente:

   Nombres y apellidos completos en mayúscula
   Cargo
   Instituto de Educación Técnica Profesional - INTEP
   Carrera 7 # 10-20
   Teléfono 2298586 Ext.
   Roldanillo - Valle del Cauca
   www.intep.edu.co

8. Para la confidencialidad de la información se colocará el siguiente mensaje al final de correo:

CONFIDENCIALIDAD: Este correo electrónico es correspondencia confidencial del Instituto de Educación Técnica Profesional - INTEP. Si Usted no es el destinatario, le solicitamos informe inmediatamente al correo electrónico del remitente o a webmaster@intep.edu.co, así mismo por favor bórrelo y por ningún motivo haga público su contenido, de hacerlo podrá tener repercusiones legales.

Si Usted es el destinatario, le solicitamos tener absoluta reserva sobre el contenido, los datos e información de contacto del remitente o a quienes le enviamos copia y en general la información de este documento o archivos adjuntos, a no ser que exista una autorización explícita a su nombre.

9. Para cumplir con la norma de cero papel se colocara el mensaje:

Sea amable con el medio ambiente: no imprima este correo electrónico a menos que sea estrictamente necesario.

Asignación de Cuentas

1. La cuenta de correo electrónico (nombre de usuario y contraseña) se entrega únicamente al titular de la misma, no se puede entregar a través de otra dirección de correo o por teléfono, por motivos de seguridad

2. Se asignará solamente una cuenta por usuario.

3. Las cuentas de los correos para docentes y estudiantes serán creados por la oficina de comunicaciones con la asesoría del grupo Webmaster y en colaboración de Vicerrectoria Académica, Registro y Control Académico para suministrar el listado de los usuarios nuevos.

Obligaciones del Usuario

En el Instituto de Educación Técnica Profesional de Roldanillo, Valle se prohíben las siguientes conductas:

- El usuario es completamente responsable de todas las actividades realizadas con su cuenta de correo proporcionada por el INTEP.

- Una vez que el usuario haya recibido su cuenta de correo electrónico (nombre de usuario y contraseña), deberá cambiar su contraseña por motivos de seguridad.

- No suplantar cuentas de usuarios para acceder a información que no es de su competencia para proteger los derechos de privacidad.

- Usar los equipos de cómputo de la entidad para enviar mensajes de amenaza o acoso a los usuarios de la institución o personas externas, lo cual será comunicado a las autoridades correspondientes para su investigación.

- El envío de correos de tipo spam o con comunicaciones fraudulentas desde las cuentas institucionales, que originen daños a la imagen de la institución; tampoco está permitido. Remitir correos con mensajes, imágenes o videos obscenos o inmorales desde o hacia la institución.

- Usar identidades falsas en mensajes de correo electrónico institucionales, ya sea con direcciones ficticias o con una identidad que no sea la propia asignada por la institución (cuenta de correo personal).

- Utilizar las comunicaciones electrónicas para violar los derechos de propiedad de autores, revelar información privada sin el permiso explícito del dueño, dañar o perjudicar de alguna manera los recursos disponibles electrónicamente, para apropiarse de los documentos de la institución.

- El uso de correo institucional para participar en cadenas de correos, se debe borrar este tipo de mensajes en el momento de recepcionarlos.

Sobre los mensajes

1. El tamaño máximo de un mensaje de correo (incluyendo archivos anexos) que puede enviar y/o recibir un alumno es de 15 MB.

2. El usuario no interferirá con el buen funcionamiento y la distribución del correo del servidor, por lo tanto generará sus listas de direcciones de correo con un máximo de 80 cuentas.

3. El envió de correo masivo a cualquiera de los grupos objetivos de la comunidad académica como docentes, estudiantes y funcionarios solo se puede realizar del correo electrónico de la oficina de comunicaciones y mercadeo o Webmaster previa autorización de está.

Alias

Uso de Alias

1. Todo alias debe tener un propósito específico y su uso debe ser congruente con éste, por lo que debe ser utilizado sólo con fines institucionales.

2. Es responsabilidad del dueño del alias hacer uso correcto del mismo.

Generación de Alias

1. Únicamente los Directores de Unidades o de Dirección podrán solicitar la generación de un alias. Para ello deberán enviar un correo a la cuenta webmaster@intep.edu.co mencionando los siguientes datos:

Nombre del alias: la cual no debe exceder de 15 caracteres y no contener caracteres especiales como ‘ñ’, acentos, ‘/’, etc.

Cuenta de correo: incluir cuenta de correo a la cual se redireccionarán los mensajes.

Responsable del alias: es la persona que podrá solicitar altas o bajas de la cuenta a la que se redireccionan los mensajes.

2. La generación de un alias se realizará únicamente con fines Institucionales. De ninguna manera se procederá a elaborar un alias con fines personales.

3. La vigencia del alias será por período de un año. Se le notificará al solicitante de la lista antes de dos semanas del vencimiento, el cual puede enviar un mensaje a la cuenta webmaster@intep.edu.co para pedir su renovación, de lo contrario al vencer el período el alias se dará de baja.

4. Cualquier baja o alta de la cuenta a la que se redireccionan los mensajes no se realiza de forma automática. El responsable deberá solicitar cualquier cambio que se desee vía correo electrónico a la cuenta webmaster@intep.edu.co.

5. En caso de desear la baja del alias el responsable deberá enviar un mensaje a la cuenta webmaster@intep.edu.co.

Todas las políticas incluidas en este documento son aplicables al correo electrónico institucional. El correo electrónico debe usarse de manera profesional y cuidadosa, tomando especial cuidado en evitar el envío a destinatarios dudosos ó destinatarios colectivos. Las leyes de derechos de autor y licencias de software también aplican para el correo electrónico.

Los mensajes de correo electrónico institucional (dominio **intep.edu.co**) deben ser eliminados una vez que la información contenida en ellos ya no sea de utilidad, vaciando la papelera.

También ver anexo de política de privacidad del correo electrónico.

4.7 EL ACCESO A INTERNET Y A OTROS SERVICIOS WEB

En el Instituto de Educación Técnica Profesional de Roldanillo, Valle se prohíben las siguientes conductas:

- El uso de los recursos de internet con fines personales no académicos o administrativos.

- El acceder a internet con fines comerciales o recreativos (juegos, chat, radio por internet, blogs de música y video para descargar o escuchar en línea, conversación en tiempo real) esta restringido solo para uso académico o administrativo.

- Usar cualquier tipo de conversación en línea, sin el requerimiento respectivo y el permiso expreso de la dependencia respectiva.

- Degradar el ancho de banda de la conexión de red e Internet, mediante la descarga de archivos de música, imágenes, videos, entre otros, o el empleo de radio o video en línea.

El responsable de los sistemas de información acogiendo las directivas del INTEP determinará los estándares para los contenidos considerados como oficiales para uso educativo y de investigación así como los necesarios para el desempeño de la labor académica y administrativa. Cualquier otra página o sitio web puede ser bloqueado sin necesidad de comunicación al usuario.

El encargado(a) del diseño y mantenimiento de la web institucional o Webmaster, que manipule información referente a la entidad debe acogerse a las políticas del INTEP incluyendo derechos de autor, leyes sobre obscenidad, calumnia, difamación y piratería de software y privacidad de la

información recopilada. El contenido debe ser revisado periódicamente para asegurar su veracidad. Ver Políticas de privacidad y Copyright.

4.8 CONTROL DE ACCESO REMOTO

La persona encargada de la infraestructura tecnológica es la responsable de proporcionar el servicio de acceso remoto y las normas de acceso a los recursos informáticos disponibles.

Para el caso especial de los recursos de informático a terceros deberán ser autorizados por el funcionario que cumpla estas funciones, previa solicitud por escrito o correo electrónico.

El usuario de estos servicios deberá sujetarse al reglamento de uso de la red institucional y en concordancia con los lineamientos generales de uso de Internet.

El acceso remoto que realicen personas ajenas a la institución deberá cumplir las normas que emite la persona encargada de la infraestructura tecnológica.

4.9 CONTROL DE ACCESO DESDE DISPOSITIVOS EXTERNOS

Para realizar el control a la lectura de cualquier dispositivo externo se debe seguir siguientes indicaciones:

Desactivar la reproducción automática de los equipos de cómputo.

Chequear con un antivirus los CD's, DVD's ingresados en nuestro computador sólo una vez, al comprarlos o adquirirlos y marcarlos para certificar el chequeo. Esto solo es válido en el caso de que nuestros CD's no sean procesados en otros computadores y sean regrabables.

Revisar todo diskette, memoria USB, tarjeta de memoria que provenga del exterior, es decir que no haya estado bajo nuestro control, o que haya sido ingresado en la multi-lectora o puerto USB.

Si nos entregan un CD´s, DVD´s, memoria USB, tarjeta de memoria o diskette y nos dicen que está revisado, NO CONFIAR NUNCA en los procedimientos de otras personas que no seamos nosotros mismos. Nunca sabemos si esa persona sabe operar correctamente su antivirus. Puede haber revisado sólo un tipo de virus y dejar otros sin controlar durante su

escaneo, o puede tener un módulo residente que es menos efectivo que nuestro antivirus.

4.10 SEGURIDAD PARA USUARIOS TERCEROS

Los dueños de los recursos Informáticos que no sean propiedad de la institución y deban ser ubicados y administrados por ésta, deben garantizar la legalidad del recurso para su funcionamiento. Adicionalmente debe definir un documento de acuerdo oficial entre las partes.

Los usuarios terceros tendrán acceso a los recursos informáticos, que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados por quien será el jefe inmediato o coordinador. En todo caso deberán firmar el acuerdo de buen uso de los recursos Informáticos.

Si se requiere que un equipo con módem, este equipo no podrá en ningún momento estar conectado a la red al mismo tiempo.

La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada y certificada por el área de seguridad informática con el fin de no comprometer la seguridad de la información interna de la institución.

Los equipos de usuarios terceros que deban estar conectados a la red, deben cumplir con todas las normas de seguridad informática vigentes en la entidad.

La entidad se reserva el derecho de monitorear estos sistemas de terceros sin previo aviso para evaluar la seguridad de los mismos. La institución se reserva el derecho de cancelar y terminar la conexión a sistemas de terceros que no cumplan con los requerimientos internos establecidos por la institución.

4.11 SOFTWARE UTILIZADO

Todo software que utilice el INTEP será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos específicos de la institución o reglamentos internos.

El software de manejo de datos que utilice el INTEP dentro de su infraestructura informática, deberá contar con las técnicas más avanzadas de la industria para garantizar la integridad de los datos.

Debe existir una cultura informática al interior de la entidad que garantice el conocimiento por parte de los funcionarios públicos, contratistas, pasantes y monitores de las implicaciones que tiene el instalar software ilegal en los computadores del INTEP para esto se definen las estrategias:

- Crear usuarios limitados en los equipos de las oficinas y salas de cómputo.
- La instalación de un software debe ser solicitado por escrito siguiendo el instructivo control de software.
- Realizar un listado de los programas que se entregan instalados a cada oficina.
- Verificar periódicamente los equipos para verificar el listado de software instalado.
- La creación de usuarios administradores en oficinas debe se solicitado por escrito y justificando su creación y asumiendo las responsabilidades legales que se puedan presentar si instala software sin licencia en el equipo.

Está prohibido la instalación o uso de software de espionaje, monitoreo de tráfico o programas maliciosos en la red de datos que originen: violaciones a la seguridad, interrupciones de la comunicación en red, que eviten o intercepten la autenticación del usuario (inicio de sesión en el dominio) por cualquier método, o que busquen acceder a recursos de los que no se les ha permitido expresamente el acceso.

Toda instalación, desinstalación o traslado de software incluyendo los de "dominio público" o de "distribución libre" desde y hacia un equipo informático de la entidad requiere autorización y coordinación previas de infraestructura tecnológica.

Cualquier software o aplicación instalado en un equipo informático que no cumpla con lo estipulado anteriormente, será desinstalado sin aviso previo y sin que ello origine ninguna responsabilidad del personal de infraestructura o de la propia entidad.

Existirá un inventario de las licencias de software del INTEP que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

Deberá existir una reglamentación de uso para los productos de software instalado en demostración a los computadores del INTEP.

Ver Instructivo de control de software.

4.12 ACTUALIZACIÓN DE HARDWARE

Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, adición de memoria o tarjetas) debe tener previamente una evaluación técnica y autorización del área responsable.

La reparación técnica de los equipos, que implique la apertura de los mismos, únicamente puede ser realizada por el personal autorizado.

Los equipos de microcomputadores (computadores, servidores, LAN entre otros) no deben moverse o reubicarse sin la aprobación previa del administrador, jefe o coordinador del área involucrada.

4.13 ALMACENAMIENTO Y RESPALDO

La información que es soportada por la infraestructura de tecnología informática del INTEP deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

Debe existir una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo.

La entidad definirá la custodia de los respaldos de la información que se realizará externamente.

El almacenamiento de la información deberá realizarse interna y/o externamente a la entidad, esto de acuerdo con la importancia de la información para la operación del INTEP. Cumplir con el protocolo de copias de seguridad institucional.

Los funcionarios públicos son responsables de los respaldos de su información en los computadores, siguiendo las indicaciones técnicas dictadas por la dependencia encargada; esta será la autorizada para realizar el seguimiento y control de esta política.

4.14 SEGURIDAD FÍSICA

En un futuro si se hace necesario la entidad deberá contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y circuitos cerrados de televisión en las dependencias que la entidad considere críticas.

Se debe colocar señalización que identifique cuales son las áreas controladas, de igual manera los visitantes de las oficinas de la entidad deben ser escoltados durante todo el tiempo por un funcionario autorizado, mientras este en el área señalada; esto incluye clientes, antiguos empleados, miembros de la familia del trabajador.

Siempre que un funcionario se de cuenta que un visitante no escoltado se encuentra dentro de áreas restringidas de la entidad, el visitante debe ser inmediatamente cuestionado acerca de su propósito de encontrarse en área restringida e informar a las responsables de la seguridad del edificio.

Toda persona que se encuentre dentro de la entidad deberá portar su identificación en lugar visible.

En los centros de cómputo o áreas que la entidad considere críticas deberán existir elementos de controles para:

Fuego

En todos los centros de procesamiento, sin excepción, deberán existir detectores de calor y humo, instalados en forma adecuada y en número suficiente como para detectar el más mínimo indicio de incendio. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento.

Se deben tener extintores de incendios debidamente probados, y con capacidad de detener fuego generado por equipo eléctrico, papel o químicos especiales. Las centrales de conexión o centros de cableado deben ser catalogados como zonas de alto riesgo, con limitación y control de acceso.

Explosivos

Por ninguna razón se debe tener material explosivo dentro, o en sitio cercano a áreas definidas como seguras por el INTEP. (Por ejemplo químicos especiales, pólvora o gases explosivos)

Inundación

Las salas de procesamiento de la información deberán estar ubicadas en pisos a una altura superior al nivel de la calle a fin de evitar inundaciones.

Las cañerías de desagüe de dichas salas y ubicadas en el piso, deberán poseer válvulas de retención de líquidos en flujo inverso a fin de que no sirvan como bocas de inundación ante sobre-flujos.

Interferencia Eléctrica y/o Radiación electromagnética.

El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.

Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.

Las áreas en donde se tenga equipos de procesamiento de información, no se permitirá fumar, tomar ningún tipo de bebidas o consumir alimento.

Equipos fuera de las instalaciones: El uso de equipos de procesamiento de la información o software, fuera de las instalaciones del INTEP, debe ser autorizado por el jefe o director del área donde el empleado dependa.

Esto aplica para Computadores personales, Agendas electrónicas, Memorias USB, teléfonos móviles, entre otros.

Las siguientes recomendaciones deben ser consideradas:

- No dejar los equipos abandonados en zonas publicas.
- Los computadores personales deben evitar su apariencia y ser llevados como equipaje de mano.
- Las especificaciones del fabricante deben ser consideradas.
- El trabajo remoto debe estar sujeto a controles especiales, considerando las recomendaciones aplicadas cuando su uso es de tipo interno.
- Se debe considerar el uso de seguros contra robo, perdida etc.

Todos los computadores portátiles, módems y equipos de comunicación se debe registrar su ingreso y salida y no debe abandonar la entidad a menos que esté acompañado por la autorización respectiva y la validación de supervisión de la oficina encargada.

Todos los visitantes deben mostrar identificación con fotografía y firmar antes de obtener el acceso a las áreas restringidas controladas por la entidad.

Los equipos como (computadores, servidores, de comunicaciones, entre otros) no deben moverse o reubicarse sin la aprobación previa de infraestructura tecnológica con el fin de garantizar que no se deterioren o sean conectados a fuentes de energía no regulada.

Los funcionarios públicos se comprometen a NO utilizar la red regulada de energía para conectar equipos eléctricos diferentes a su equipo de cómputo, como impresoras, cargadores de celulares, grabadoras, electrodomésticos, fotocopiadoras y en general cualquier equipo que generen caídas de la energía.

Los particulares en general, entre ellos, los familiares de los funcionarios públicos, no están autorizados para utilizar los recursos informáticos de la entidad.

4.15 ESCRITORIOS LIMPIOS

Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD´s, DVD´s, USB, tarjetas de memoria y disquetes, con fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

5. ADMINISTRACIÓN DE LA SEGURIDAD

La evaluación de riesgos de seguridad para los recursos informáticos en producción se debe ejecutar al menos una vez cada dos años. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

Cualquier brecha de seguridad o sospecha en la mala utilización en Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el funcionario que la detecta, en forma inmediata y confidencial a la persona responsable del proceso.

Los funcionarios públicos, contratistas, pasantes y monitores del INTEP que realicen las labores de administración del recurso informático son responsables por la implementación, permanencia y administración de los controles sobre los recursos computacionales. La implementación debe ser consistente con las prácticas establecidas por la infraestructura informática.

La persona responsable del proceso divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento al cumplimiento de las políticas de seguridad y reportara a la secretaria General, los casos de incumplimiento con copia a la oficina de control interno.

6. CONTINGENCIA

La alta Dirección debe preparar, actualizar periódicamente y probar en forma regular un plan de contingencia que permita a las aplicaciones críticas y sistemas de cómputo y comunicación estar disponibles en el evento de un desastre de grandes proporciones como terremoto, explosión, terrorismo, inundación entre otros. (Ver Matriz de riesgo).

7. AUDITORÍA

Todos los sistemas automáticos que operen y administren información sensitiva, valiosa o crítica para la entidad, como son sistemas de aplicación en producción, sistemas operativos, sistemas de bases de datos y telecomunicaciones deben generar pistas (adición, modificación, borrado) de auditoria.

Todos los archivos de auditorias deben proporcionar suficiente información para apoyar el monitoreo, control y auditorias.

Todos los archivos de auditorias de los diferentes sistemas deben preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

Todos los archivos de auditorias deben ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas; los usuarios que no estén autorizados deben solicitarlo al área encargada de su administración y custodia.

Todos los computadores de la entidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

8. INCUMPLIMIENTO DE LAS POLÍTICAS

El INTEP hará responsable al usuario de las consecuencias derivadas por el incumplimiento de las políticas y normas establecidas en este documento. La Institución se reserva el derecho de evaluar periódicamente el cumplimiento de estas.

Cualquier acción disciplinaria derivada del incumplimiento de la misma (tales como llamadas de atención, suspensiones, expulsiones o despidos), será considerada de acuerdo a los procedimientos establecidos por el INTEP y en estricto acato a la normatividad interno y externa que rige a la Institución.

El usuario que no cumpla con el uso correcto del software será directamente responsable de las sanciones legales derivadas de sus propios actos y de los costos y gastos en que pudiera incurrir el INTEP en defensa por el uso no autorizado o indebido de licencias de software.

9. NOTIFICACIÓN DEL REGLAMENTO

Estas políticas serán socializadas a través de la oficina de Comunicaciones y Mercadeo en colaboración de la persona encargada del proceso.

El INTEP establecerá un **Acta de Compromiso** que firmarán todos los usuarios al momento de recibir el presente reglamento.

10. APLICACIÓN Y CUMPLIMIENTO

Esta política aplica a todos los integrantes de la Institución, sean docentes, estudiantes o personal administrativo. Cualquier usuario que viole este reglamento será objeto de sanción disciplinaria pertinente, sea su relación de cualquier tipo (laboral, académica, entre otros).

11. DEFINICIONES

Entiéndase para el presente documento los siguientes términos:

INTEP: Instituto de Educación Técnica Profesional de Roldanillo - Valle

Política: son instrucciones mandatarias que indican la intención de la alta gerencia respecto a la operación de la organización.

Recurso Informático: Elementos informáticos (base de datos, sistemas operacionales, redes, sistemas de información y comunicaciones) que facilitan servicios electrónicos.

Información: Puede existir en muchas formas. Estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación. Cualquiera que sea la forma de adquirir la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

Usuarios Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios del INTEP, pero que por las actividades que realizan en la entidad, deban tener acceso a Recursos Informáticos

Ataque cibernético: Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones perturbadoras y perjudiciales.

Brecha de seguridad: deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Criptografía de llave pública: Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Cifrar: quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama “descodificar" o “descifrar". Los sistemas de ciframiento se llaman “sistemas criptográficos".

Certificado Digital: un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor

No repudio: este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.

Activos de software: Son elementos tales como: Aplicaciones de software, herramientas de desarrollo, y utilidades adicionales.

Activos físicos: Se consideran activos físicos elementos tales como: Computadores, laptops, modems, impresoras, maquinas de fax, Equipos de Comunicaciones, PBX, cintas, discos, UPS, muebles etc.

Versión No.	Fecha de Aprobación	Descripción del Cambio	Solicitó
1	2011-05-28	Modificar y organizar el capítulo de correos institucionales.	Líder del Proceso de Infraestructura

	Nombre	Cargo	Firma	Fecha
Elaborado	Victor Elias Ruiz Vargas	Auxiliar Administrativo		2015-04-29
Revisado	William Gómez Valencia	Líder del Sistema Integrado de Gestión		2015-04-29
Aprobado	German Colonia Alcalde	Rector		2015-04-29