POLÍTICAS DE SEGURIDAD DE ACTIVOS DE INFORMACIÓN.

Objetivo de Control: Proveer dirección y soporte a la administración para la seguridad de información.

1.1 Protección y respaldo de la información

1.1.1 Propósito:

Presentar la posición de la institución frente a la protección de la información y dar lineamientos para mantener la disponibilidad de la información de acuerdo a las necesidades de continuidad planeadas a nivel de los procesos y por ende de la institución.

Esta guía define lineamientos 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 mantenida a nivel de medios de almacenamiento (cintas, discos ópticos, etc.) para responder a los requerimientos de los procesos de la institución. Estos lineamientos deberán ser seguidos por todos los funcionarios y cada una de las direcciones involucradas en estas actividades.

1.1.2 Declaración:

Para la Universidad Tecnológica de Pereira la información es considerada como un activo de valor estratégico, por esta razón se deberán implementar los mecanismos necesarios que garanticen un adecuado tratamiento en el ciclo de vida de la información, especialmente para los casos que requieren mantener 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. (Acceso, toma de respaldo, backup, transporte, recuperación, otros). Por lo tanto se deben mantener los controles y medidas establecidas para esto.

Los usuarios de la institución son responsables de alojar la información que necesita ser respaldada en los lugares establecidos para ello.

Los usuarios respaldarán y protegerán, con medidas que eviten accesos de personas no autorizadas, aquellos activos digitales de información que estén almacenados en elementos de TI de uso personal, que les hayan sido asignados. Se deberán preservar los lineamientos de acuerdo a la sensibilidad y nivel de clasificación de seguridad.

Los usuarios son responsables de aplicar los controles para la protección de la información según su nivel de clasificación. Así mismo deberán alertar al área del CRIE y la División de Sistemas cuando un activo digital de información requiera medidas especiales de protección.

Los funcionarios de la institución deberán seguir los procedimientos de respaldo de la información y realizar su seguimiento a partir de una bitácora de respaldos a la información personal.

1.2 Escritorio Limpio y Bloqueo de sesión

1.2.1 Propósito:

Evitar riesgos potenciales a los activos de información de la Universidad Tecnológica de Pereira, asociados a su accionar cotidiano y ya sean de manera accidental o intencionada, que puedan ocasionar la interrupción total o parcial, de las actividades de la institución.

Esta guía define lineamientos que deberán seguirse al interior de la institución para la protección de la información, tanto física como digitalizada y con acceso a través de los sistemas de cómputo, estos lineamientos deberán ser seguidos por todos y cada una de las áreas involucradas en estas actividades.

1.2.2 Declaración:

Para la Universidad Tecnológica de Pereira, es crucial proteger información sensitiva, evitando que sea conocida por personas diferentes a aquellas que la requieren o que sea publicada de manera indiscriminada.

Teniendo presente que las oficinas son visitadas frecuentemente por proveedores, consultores, clientes, personal de limpieza y otros compañeros de trabajo, se define esta buena práctica que se traduce como mantener su escritorio lo más limpio y organizado posible, ya que si está desordenado, es muy probable que usted no se de cuenta de que le hace falta algo.

La información de la institución deberá mantenerse disponible a las personas autorizadas para ello en el momento en que se necesite, lo que hace que 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.

Los niveles de protección y clasificación establecidos para la información de la institución deberán ser mantenidos en todo momento.

Los usuarios 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 asociados a disponer de la información en su puesto de trabajo e iniciar las acciones para mitigarlos.

Sobre el Escritorio Limpio durante la jornada laboral

Los sistemas de información y elementos de procesamiento deberán ser adecuadamente protegidos, teniendo presente que se debe al menos guardar documentos sensitivos o elementos de almacenamiento de información (CDs, Vds., Memorias portátiles, Discos Portátiles, 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 su computador portátil con cables de seguridad en todo momento para evitar robos.

Es responsabilidad de cada usuario la protección de la información a su cargo, por lo que debe mantener presente NO publicar o dejar a la vista, documentos o datos sensitivos, por ejemplo:

- Nombre de Usuario y Passwords
- Direcciones IP
- Contratos
- Números de Cuenta
- Listas de Clientes

- Propiedad Intelectual
- Datos de Funcionarios
- Cualquier cosa que no desea publicar

Sobre el Escritorio Limpio después de la jornada laboral

Los usuarios de la institución deberán tomarse el tiempo necesario antes de abandonar la oficina para recoger y asegurar el material sensitivo.

Los usuarios de la institución deberán tomarse el tiempo necesario antes de abandonar la oficina para de ser posible cerrar bajo llave gabinetes, cajones y oficinas.

Los usuarios de la Universidad Tecnológica de Pereira deberán tomarse el tiempo necesario antes de abandonar la oficina para Asegurar equipo costoso o almacenes de información sensible (Portátiles, PDAs, Memorias USB, etc.).

Sobre el Bloqueo de la estación de Trabajo

Para la institución es importante que una estación de trabajo se mantenga en control, aún cuando su usuario no se encuentre frente a ella, por lo que se requiere que se encuentra bloqueada cuando el usuario se retire de su lugar, pues el no hacerlo potencia el riesgo de utilizar los sistemas sin los privilegios adecuados, expone la información de la institución de manera innecesaria y se considera un uso inadecuado de los recursos.

Como apoyo para aquellas eventualidades que ocasionan el dejar la estación de trabajo desatendida y sin bloquear, La Universidad Tecnológica de Pereira en los equipos que están bajo su control programará el bloqueo automático de la sesión, pero esta acción debe entenderse como un complemento al deber del funcionario de mantener su

estación y su puesto de trabajo bajo su control, lo que será reforzado con capacitaciones y sensibilizaciones en el uso del bloqueo de los equipos.

Cada usuario de la institución para mantener su estación de trabajo bajo control, deberá bloquear la sesión al alejarse de su computador, aunque sea por poco tiempo, minimizando el tiempo que la estación quedaría sin control ya que cualquier ausencia puede extenderse.

1.3 Protección contra software nocivo.

1.3.1 Propósito:

En este numeral se pretende formular controles que permitan 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, etc., los cuales exponen los sistemas de la Universidad Tecnológica de Pereira a la propagación interna y externa de software con código malicioso o nocivo, el cual puede comprometer directamente la integridad, la disponibilidad y la confidencialidad de la información procesada por cada uno de los componentes de la red.

1.3.2 Declaración:

Cualquier usuario quien sospeche de una infección por un virus debe apagar inmediatamente el computador involucrado, desconectarlo de cualquier red, llamar al grupo de soporte de la división de sistemas y procesamiento de datos y no hacer ningún intento de eliminar el virus

Solamente el grupo de soporte de la división de sistemas y procesamiento de datos debe enfrentar una infección por virus de computador.

Los usuarios no deben intentar eliminar el virus, a menos que sigan instrucciones precisas de los Administradores de sistemas.

Los usuarios no deben transferir (bajar) software desde cualquier sistema que se encuentra por fuera de La Universidad Tecnológica de Pereira.

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 por El CRIE y la División de Sistemas.

Antes de ser descomprimido, todo software transferido desde sistemas externos a la Universidad Tecnológica de Pereira, debe ser analizado con un sistema antivirus aprobado, después de que el usuario haya terminado su sesión y se haya terminado con todas sus conexiones de red.

Siempre que algún software o archivos hayan sido recibidos de una entidad externa, este material debe ser probado para buscar software no autorizado en una máquina aislada de desarrollo (no producción), antes de ser utilizado en los sistemas de información de la Universidad Tecnológica de Pereira.

Debe certificarse que todo el software, archivos o ejecutables, se encuentran libres de virus antes de ser enviados a una entidad externa a La Universidad Tecnológica de Pereira.

Cualquier archivo encriptado suministrado por instituciones externas a la Universidad Tecnológica de Pereira, debe ser desencriptado antes de ser sometido al análisis con sistemas antivirus.

Cualquier sistema de almacenamiento como disquetes, CD-ROMs, cartuchos ópticos, cintas DAT, etc., provistos por instituciones externas no deben ser utilizados en los sistemas de la Universidad Tecnológica de Pereira, a menos que éstos medios hayan

sido analizados con sistemas antivirus por personal autorizado y hayan recibido una etiqueta que certifique que no se encontraron virus.

Antes que cualquier archivo sea restaurado en un sistema de la Universidad Tecnológica de Pereira, desde un medio de almacenamiento de respaldo, éste debe ser analizado con un sistema antivirus actualizado.

Los usuarios no deben intencionalmente escribir, generar, compilar, copiar, almacenar, propagar, ejecutar o intentar introducir cualquier código de computador diseñado para auto replicarse, deteriorar o que obstaculice el desempeño de cualquier sistema de la Universidad Tecnológica de Pereira o de cualquier institución externa a ella.

1.4 Protección durante la navegación en internet.

1.4.1 Propósito:

En esta política se pretende formular controles que permitan minimizar el riesgo generado por el acceso a Internet y a redes públicas, el intercambio de medios de almacenamiento portátiles, el intercambio de información con instituciones externas, etc., los cuales exponen los sistemas de la Universidad Tecnológica de Pereira a la propagación interna y externa de software con código malicioso o nocivo, el cual puede comprometer directamente la integridad, la disponibilidad y la confidencialidad de la información procesada por cada uno de los componentes de la red.

1.4.2 Declaración:

La Universidad Tecnológica de Pereira con el objetivo único de facilitar la realización del trabajo contratado brinda acceso a Internet para navegación a sus funcionarios y contratistas autorizados, los cuales se acogen a las políticas y formas de actuación dictados en esta guía.

La institución adelantará campañas dirigidas a todos los usuarios de la navegación para garantizar que las personas estén informadas sobre los peligros de descargar archivos de Internet (el software espía, los troyanos y los atacantes externos), acceder a sitios desconocidos o de baja confianza y aceptar los mensajes sobre instalación de software que brinde el navegador, así como el contenido relevante de ésta guía.

La institución buscará garantizar de manera técnica que se controla el acceso a sitios que puedan afectar la productividad de la institución, la seguridad de su información o su personal.

Los usuarios deberán Abstenerse de visitar sitios restringidos por la institución de manera explicita o implícita, o sitios que afecten la productividad de la institución. Especialmente se deberán evitar el acceso desde la institución a sitios relacionados con la pornografía y fundamentalmente si este involucra a menores de edad. Así mismo, esta prohibida la descarga y uso de software malicioso o documentos que brinden información sobre como atentar contra la seguridad de la información corporativa

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 transito

Los funcionarios de La Universidad Tecnológica de Pereira no deben comprar bienes o servicios a través de Internet a nombre de La Universidad Tecnológica de Pereira, a menos que exista una aprobación previa.

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 descargar software de Internet bajo ninguna circunstancia.

Los usuarios no deben instalar software en sus estaciones de trabajo, en los servidores de la red, o en otras máquinas, incluso si este software es libre o no licenciado; toda instalación de software debe hacerla un técnico luego de la debida verificación y la autorización previa del CRIE y la División de Sistemas.

El software residente en sitios mirror de Internet no debe ser descargado a ningún sistema de La Universidad Tecnológica de Pereira a menos que sea recibido directamente de una fuente confiable y conocida y que se hayan empleado herramientas como verificación de firmas digitales.

Los servidores disponibles en Internet no deben ser utilizados para almacenar información de las actividades del La Universidad Tecnológica de Pereira.

Los usuarios están consientes de que toda la información (incluida la de navegación) que transite en la institución por ser para el trabajo es propiedad de la misma y por ende puede ser monitoreada con objetivos de administración, seguridad o auditoría por personal autorizado por la institución.

Los usuarios de los sistemas de navegación son concientes 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 Universidad Tecnológica de Pereira, quien podrá revelar cualquier acceso cuando una autoridad judicial así lo requiera.

El personal de La Universidad Tecnológica de Pereira no debe utilizar el sistema de navegación de la UTP para participar en grupos de discusión en Internet, Listas de Correo, chats o cualquier otro foro público, a menos que su participación haya sido expresamente autorizada formalmente por la universidad.

Los usuarios de Internet, podrán emplear este recurso para su propia capacitación previa autorización de su jefe directo y en horarios no laborales

La institución facilita el acceso al uso de medios electrónicos para comercio electrónico como el pago de facturas, transacciones bancarias de sus funcionarios y lectura de correos personales que tengan acceso vía web, pero no asume ninguna responsabilidad por estas, ni recomienda su 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.

1.5 Manejo y Seguridad de Medios.

1.5.1 Propósito:

Este rubro pretende prevenir la revelación de documentación relacionada con los sistemas de la Universidad Tecnológica de Pereira a terceros que puedan utilizarla en contra de la institución.

1.5.2 Declaración:

Toda la documentación que describe los sistemas de información o los procedimientos de sistemas de la Universidad Tecnológica de Pereira, debe ser revisada y aprobada por El CRIE y la División de Sistemas, antes de ser liberada a terceras partes.

Toda la documentación relacionada con los sistemas de la Universidad Tecnológica de Pereira, es considerada confidencial y no debe ser conservada por los funcionarios que dejen de laborar en la institución.

1.6 Seguridad del comercio electrónico.

1.6.1 Propósito:

Esta política pretende prevenir la revelación de información privada, el fraude en contra o en nombre de la Universidad Tecnológica de Pereira la privacidad de la información de cuentas y la seguridad de las transacciones realizadas a través de Internet o redes externas.

1.6.2 Declaración:

Todos los contratos originados a través mensajes de ofertas y aceptaciones electrónicas deben ser formalizados y confirmados por medio de documentos en papel, dentro de las siguientes dos semanas a partir de su aceptación.

Toda información acerca de pagos, como números de cuentas corrientes y de tarjetas de crédito, debe ser encriptada mientras esté almacenada en computadores accesibles desde Internet o desde redes externas.

Toda información acerca de pagos, como números de cuentas corrientes y de tarjetas de crédito, debe permanecer encriptada cuando no sea utilizada para propósitos de la institución y cuando sea transmitida o almacenada en medios de respaldo y transporte.

1.7 Seguridad del correo electrónico.

1.7.1 Propósito:

Esta política pretende asegurar la privacidad de los mensajes de correo electrónico, el buen uso del sistema y el compromiso inherente de la Universidad Tecnológica de Pereira al suministrar este servicio a su personal.

1.7.2 Declaración:

La información secreta y no encriptada no debe ser trasmitida por correo electrónico, a menos que una persona con autoridad directiva, de acuerdo a su cargo autorice específicamente cada ocurrencia.

El personal de la Universidad Tecnológica de Pereira no puede emplear direcciones de correo electrónico diferentes a las cuentas oficiales para atender asuntos de la institución.

Todos los mensajes de correo electrónico que utilizan los sistemas de la Universidad Tecnológica de Pereira, deben contener el nombre y apellidos del remitente, su cargo, dirección y número telefónico.

Todas las comunicaciones de mercadeo realizadas por correo electrónico, dirigidas a clientes o usuarios encontrados en la base de datos de contactos de la Universidad Tecnológica de Pereira , deben incluir instrucciones de cómo los destinatarios pueden ser removidos rápidamente de la base de datos de contactos y detener comunicaciones, correos o mensajes posteriores.

Los usuarios no deben reenviar correo electrónico a direcciones externas al Universidad Tecnológica de Pereira, a menos que exista autorización previa de quien origina el mensaje o que la información sea pública por naturaleza.

Un mensaje de correo electrónico debe ser retenido y conservado para futuras referencias solamente si contiene información relevante para a finalización de una transacción, si contiene información de referencia potencialmente importante o si tiene valor como evidencia de una decisión administrativa de la Universidad Tecnológica de Pereira.

Todos los mensajes de correo electrónico que contengan información concerniente, pero no limitada a, números de tarjetas de crédito, claves de acceso, información de

investigación y desarrollo e información sensible de entidades externas, debe ser encriptados antes de ser transmitidos.

El personal de la Universidad Tecnológica de Pereira NO puede monitorear los sistemas de correo electrónico para asegurar el cumplimiento de políticas, a menos que haya autorización judicial o de autoridad competente.

La Universidad Tecnológica de Pereira debe notificar a todos los usuarios que los sistemas de correo electrónico solamente deben ser utilizados para propósitos de la institución, todos los mensajes enviados por correo electrónico constituyen registros de la Universidad Tecnológica de Pereira, quien se reserva el derecho de acceder y revelar cualquier mensaje para cualquier propósito sin previo aviso y los administradores pueden revisar el correo electrónico del personal para determinar si han roto la seguridad, han violado la política de la Universidad Tecnológica de Pereira o han realizado actividades no autorizadas

Los usuarios no pueden crear, enviar, o retrasmitir mensajes de correo electrónico que puedan constituir acoso o que puedan contribuir a un ambiente de trabajo hostil.

El personal de la Universidad Tecnológica de Pereira no puede enviar o distribuir cualquier mensaje a través de los sistemas de la Universidad Tecnológica de Pereira, el cual pueda ser considerado difamatorio, acosador o explícitamente sexual o que pueda ofender a alguien con base en su raza, género, nacionalidad, orientación sexual, religión, política o discapacidad.

El personal no debe utilizar los sistemas de la Universidad Tecnológica de Pereira para la transmisión de cualquier correo masivo no solicitado.

En todos los mensajes de correo electrónico salientes, debe agregarse un pié de página que indique que el mensaje puede contener información confidencial, que es para el uso de los destinatarios nombrados, que ha sido registrado para propósitos de archivo, que puede ser analizado por otras áreas de la Universidad Tecnológica de Pereira y que no

constituye necesariamente una oficial representación de la Universidad Tecnológica de Pereira.

El personal de la Universidad Tecnológica de Pereira no debe emplear versiones digitalizadas de sus firmas manuscritas en los mensajes de correo electrónico.

El personal no debe abrir archivos adjuntos a los correos electrónicos, a menos que hayan sido analizados por el software antivirus aprobado.

El personal de la Universidad Tecnológica de Pereira no debe utilizar las cuentas de correo oficiales para participar en grupos de discusión en Internet, Listas de Correo o cualquier otro foro público, a menos que su participación haya sido expresamente autorizada por El CRIE y la División de Sistemas.

1.8 Logging o Registro Histórico de Actividades.

1.8.1 Propósito:

Contar con registros de los movimientos que se realizan dentro de los sistemas de la Universidad Tecnológica de Pereira, buscando evitar conductas inapropiadas y minimizar riesgos de seguridad en el uso de estos sistemas.

1.8.2 Declaración:

Logs de aplicaciones sensibles

Todas las aplicaciones de producción que manejen información sensible de la Universidad Tecnológica de Pereira, 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.

Los sistemas que manejen información valiosa, sensible o crítica deben además contener y activar forzosamente el log 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. Es importante que La división de sistemas y procesamiento de datos o el CRIE acuerde con el Propietario de la Información cualquier característica especial que estos logs deban incluir, de acuerdo a requerimientos internos o con autoridades externas.

Todos los comandos emitidos por los operadores de sistemas deben ser rastreables o identificables para especificar su uso individual.

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 brechas de seguridad.

La división de sistemas y procesamiento de datos, el CRIE o una persona asignada por ellas (que no tenga el rol de administrador de sistemas) debe revisar, por lo menos cada tres meses, uno o más registros relevantes a las actividades de los usuarios responsables administradores de la información (administradores de servidores y aplicaciones) para asegurarse que estén manejando con responsabilidad sus acciones con respecto a los sistemas de cómputo.

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 Universidad Tecnológica de Pereira, incluyendo todas las PC's conectadas 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.

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, aún 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. Los funcionarios autorizados deben contar con una autorización de La división de sistemas y procesamiento de datos, el CRIE, el Comité de Seguridad de la Información, o el dueño de la información en cuestión para realizar tal acceso.

Comentarios

Los logs son una herramienta muy valiosa que pueden ayudar a identificar y a solucionar muchas incidencias no contempladas. De esta forma, los archivos log son útiles para el personal de Control Interno, el Comité de Seguridad de la Información, Propietarios de la información, para detectar errores, modificaciones no autorizadas, transacciones no válidas, regeneración de archivos y restablecimiento de procesos.

El objetivo es que todos los movimientos que se realizan dentro de las operaciones críticas o sensibles de la institución, sean registrados, para detectar y reducir el riesgo de violación o fraudes. Estas herramientas sirven como evidencia y apoyo para la detección de la fuente del problema ocasionado, identificando sus posibles causas y posibles soluciones.