TRIBUNAL REGISTRAL ADMINISTRATIVO

Marco de Políticas de Seguridad de la Información

(APROBADO EN SESIÓN ORDINARIA N°. 42-2018 DEL 01 DE NOVIEMBRE DE 2018)
(ACUERDO N°. 396-2018)

TRIBUNAL REGISTRAL ADMINISTRATIVO

Control del Documento

Información del documento

Nombre del documento: Marco de Políticas de Seguridad de TI

Fecha de recepción definitiva: 26/10/2017

Elaborado por: PwC Costa Rica

Cambios del documento

Fecha	Realizado por	Rol	Descripción	Versión
26/10/2017	Jennifer Cordero Hernández	Consultora	Versión Final	Final
24/10/2018	Ronald Vargas Bermúdez	Encargado	Actualización política #4	V.1.

Entrega del documento

Elaborado por	Jennifer Cordero Hernández Consultora	Firma	
Recibido por	Ronald Vargas Bermúdez Comisión Normas TIC	Firma	
	Leonardo Villavicencio Cedeño Comisión Normas TIC	Firma	
	Vanessa Rodríguez Mora Comisión Normas TIC	Firma	

TRIBUNAL REGISTRAL ADMINISTRATIVO

Tabla de Contenidos

Marco de Políticas de Seguridad de TI

Introducción

Conforme las tecnologías se han esparcido, la severidad de daños y su frecuencia las han transformado en un continuo riesgo, que obliga a las entidades a crear medidas de control y políticas definitivas para contrarrestar estos posibles ataques.

La seguridad de las instituciones en muchos de los países se ha convertido en cuestión de seguridad nacional, por ello contar con un Marco de Políticas de Seguridad en Tecnologías de Información (TI) es imprescindible, y debe plasmar mecanismos confiables que con base en la política institucional proteja los activos y la información de la institución.

Los requerimientos de seguridad que involucran las tecnologías de la información, en pocos años han cobrado un gran auge, y más aún con las de carácter globalizador como los son la de Internet y en particular la relacionada con la Web, la visión de nuevos horizontes explorando más allá de las fronteras naturales, situación que ha llevado la aparición de nuevas amenazas en los sistemas computarizados.

De esta manera, las políticas de seguridad de TI del Tribunal Registral Administrativo (TRA) emergen como el instrumento para concientizar a sus miembros acerca de la importancia y sensibilidad de la información y servicios críticos, de la superación de las fallas y de las debilidades, de tal forma que permiten al Tribunal cumplir con su misión.

El proponer esta política de seguridad requiere un alto compromiso con la institución, agudeza técnica para establecer fallas y deficiencias, constancia para renovar y actualizar dicha política en función del ambiente dinámico que nos rodea

Alcance

Lo enunciado en las diferentes políticas que conforman este Marco de Políticas de Seguridad de Tecnologías de Información (TI) aplica a todos los funcionarios del Tribunal Registral Administrativo(TRA) así como para todo el personal de las empresas que prestan servicios por medio de contrato, que por sus funciones tenga acceso a los equipos de cómputo, a las bases de datos institucionales, a los sistemas y aplicaciones de cómputo, a las instalaciones que resguardan el centro de cómputo y en general a todos los recursos de Tecnología de Información.

Objetivo General

Cumplir con la implementación de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información emitidas por la Contraloría General de la República para garantizar de manera razonable, la confidencialidad, integridad y disponibilidad de la información.

Objetivos Específicos

- Colaborar en el cumplimiento de las regulaciones legales o técnicas emitidas por el ente regulador respecto al proceso de Tecnologías de Información como lo son el decreto 37549-JP Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central y las normas de Control interno de la Contraloría General de Republica enfocado hacia los sistemas de información.

- Comunicar a todo el personal un principio fundamental: la información es un activo muy valioso para la institución y es responsabilidad de todos protegerla y garantizar la confidencialidad, disponibilidad e integridad de la misma.

- Promover el uso de las mejores prácticas de seguridad informática en el trabajo, para proteger el uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.

Sobre la actualización de estas políticas

Todas las políticas que conforman este marco tienen vigencia por un año a partir de la fecha de su oficialización, pasado este lapso se realizará una revisión anual para actualizarlo conforme lo establece al artículo 15 Actividades de Control de la Ley General de Control Interno #8292. Publicado en la Gaceta 169 del 04 de setiembre de 2002.

Políticas de Seguridad de la Información

La política de seguridad de la información establece el canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la institución garantizando de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizada, daño o pérdida u otros factores disfuncionales, esta política se encuentra en el documento *Política de Seguridad de la Información – Tribunal Registral Administrativo*.

A continuación se indican las políticas que responden a esta política general y que permiten el cumplimiento de la misma:

Política #1. Uso de Recursos Tecnológicos

Responsabilidades

- Auditoría Interna: Velar por el cumplimiento de lo estipulado en esta política.
- Funcionarios, terceros y usuarios de recursos tecnológicos: Conocer e implementar lo estipulado en esta política.

Normas

Sobre los equipos fijos y portátiles

1. El Analista Programador en coordinación con el encargado de bienes de la institución, deberá tener un registro o inventario actualizado de todos los equipos de cómputo propiedad del TRA.

2. Los usuarios deben conocer y tener un listado de las características técnicas del hardware del equipo asignado a su persona.
3. Los usuarios no deben ingerir alimentos cerca del equipo de cómputo.
4. Los usuarios deben tomar las precauciones necesarias con el fin de proteger su equipo tecnológico asignado, como no colocarlo en bases inestables, no exponerlo a condiciones ambientales que puedan afectarle y en caso de presentar fallas informar al Analista Programador inmediatamente.
5. Queda totalmente prohibido que el usuario abra o desarme los equipos de cómputo.
6. El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos, en caso de que no se cumpla solicitar un reacomodo de cables al Analista Programador.
7. Ningún usuario de estación de trabajo está autorizado para almacenar material pornográfico, u ofensivo en ningún medio de almacenamiento de la estación de trabajo o dispositivo periférico, o en ningún otro medio de almacenamiento disponible en la red institucional, y mucho menos propagarlo o distribuirlo a otras personas.
8. El usuario deberá asegurarse de tener la autorización respectiva para el uso del equipo fuera de las instalaciones del TRA.
9. Todo usuario debe asegurar que siempre se pueda identificar la localización física del dispositivo, así como conocer la sensibilidad de los datos en el equipo y el nivel de seguridad.
10. Se debe usar sin excepción candados de seguridad para las laptops en oficinas abiertas.
11. En caso de robo de la computadora portátil, se debe de reportar inmediatamente al encargado del inventario y a la autoridad policial respectiva.
12. No dejar el equipo portátil desatendido aunque este de viaje, hoteles, sitios de atención al cliente, vehículos.
13. Únicamente el usuario custodio del equipo debe de hacer uso del mismo, no se autoriza el uso por parte de amigos, miembros de la familia u otros para la manipulación del equipo.
14. Antes de apagar su computadora cierre todas las aplicaciones en uso para evitar fallas de funcionamiento al volver a encenderla.
15. Procure no tocar la superficie de la pantalla con los uñas o la punta de un lápiz o un bolígrafo.
16. Analizar los archivos antes de copiarlos a la portátil, independiente de la fuente de procedencia.
17. Cuando un funcionario termine su relación laboral con la institución o se le asigne un nuevo equipo o dispositivo deberá ser reportado por su jefe inmediato al Analista Programador con el fin de que sean ejecutadas las tareas informáticas como respaldo de datos del equipo, revisión del estado general del equipo, completar formulario de control de bienes.
18. La institución no se responsabiliza por los daños o desperfectos que puedan sufrir los equipos informáticos propiedad de los funcionarios del TRA o propiedad de terceros cuando ingresan a las instalaciones del TRA.
19. El Analista Programador deberá supervisar el equipo tecnológico que ingresa a la institución propiedad de funcionarios o propiedad de terceros y además deberá colocar una cinta o etiqueta de color para diferenciar el equipo ingresado de los equipos propiedad del TRA.
20. El Analista Programador debe realizar anualmente un avaluó de los bienes informáticos propiedad del TRA y dirigirlo a la comisión de bienes para su respectivo análisis y aprobación con el objetivo de dar de baja los bienes que así lo requieren.

Sobre los quemadores de CD o DVD

21. El uso de los grabadores de discos compactos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen y que la información sea estrictamente de carácter laboral.
22. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.
23. El Analista Programador debe controlar para que las nuevas compras de equipo de cómputo solo contengan quemadores de CD o DVD aquellos equipos de funcionarios que realmente lo necesiten para labores propias de su cargo.
24. El equipo debe de ser utilizado para labores institucionales; lo cual tiene implícito la no reproducción de películas, software, música ni datos personales.
25. En caso de presentar fallas técnicas, el usuario encargado del equipo deberá notificar de inmediato al Analista Programador.

Sobre el uso de dispositivos de almacenamiento como CD, DVD, Dispositivos USB o discos duros externos

26. Todos los dispositivos de almacenamiento deberán ser revisados previamente con el antivirus institucional instalado en el equipo del funcionario antes de abrir cualquier archivo.
27. Todos los usuarios deberán utilizar en los equipos del TRA solo los dispositivos de almacenamiento suministrados por la institución.
28. No deje los dispositivos de almacenamiento en el equipo cuando no esté en uso.
29. En caso de extraviar alguno de los dispositivos, el usuario deberá notificar la pérdida al Analista Programador y al encargado de bienes.
30. El usuario deberá tomar en cuenta condiciones ambientales tales como temperatura, humedad, entre otros; que pueden dañar los datos almacenados en los dispositivos de almacenamiento.
31. En el caso de tener que almacenar información sensible, realice al menos dos copias adicionales, debidamente protegidas como prevención.
32. Los usuarios deberán almacenar los dispositivos de almacenamiento en gabinetes bajo llave.
33. Cuando proceda, el analista de sistema implementará mecanismos para bloquear la conexión de dispositivos de almacenamiento externos a los equipos asignados a los funcionarios.

Política #2. Control de Acceso Lógico

Responsabilidades

- Auditoría Interna: Velar por el cumplimiento de lo estipulado en esta política.
- Funcionarios, terceros y usuarios: Conocer e implementar lo estipulado en esta política.
- Analista Programador: Autorizar los diferentes niveles de acceso a los sistemas de cada área.

Normas

1. El Analista Programador será el encargado de controlar el acceso de los usuarios de la institución a los sistemas de información, base de datos y servicios de información como carpetas compartidas en servidores de archivos.
2. El Analista Programador realizará el control de acceso lógico mediante la asignación de perfiles o roles de cada sistema de información con base en una solicitud expresa por medio de correo

electrónico del jefe inmediato del usuario que requiere el acceso a la aplicación. Además controlará la creación de usuarios, administración de privilegios, autenticación de usuarios incorporando en los procesos la firma digital.

3. El Analista Programador deberá documentar la lista de acceso de cada perfil de cada uno de los sistemas de información con que cuenta el TRA.
4. El Analista Programador en coordinación con las jefaturas de la institución deberá realizar las modificaciones o eliminaciones de privilegios en los sistemas de información a los que el usuario estaba autorizado, esto con base en una solicitud expresa de la jefatura.
5. Todas las aplicaciones de sistemas de información propiedad del TRA deben contar con una autenticación con base en un usuario y una contraseña o en su defecto poder ingresar con la firma digital.
6. Cada usuario debe controlar que al abandonar la estación de trabajo momentáneamente debe bloquear la sesión para posteriormente habilitarla con la su respectiva contraseña, esto con el fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.
7. Las sesiones inactivas deben cerrarse después de un período de inactividad definido por la institución.

Política #3. Sobre el uso y administración de contraseñas

Responsabilidades

- Auditoría Interna: Velar por el cumplimiento de lo estipulado en esta política.
- Analista Programador: Gestionar las claves que serán utilizadas por los usuarios en los Sistemas Informáticos del TRA.
- Funcionarios, terceros, usuarios de recursos tecnológicos: Conocer e implementar lo estipulado en esta política.

Normas

1. El jefe inmediato debe solicitar por medio de correo electrónico dirigido al Analista Programador la creación de una cuenta de usuario para los nuevos funcionarios así como la creación de la cuenta de correo electrónico
2. El nuevo usuario debe realizar el cambio de contraseña la primera vez que el usuario solicita su ingreso al a red.
3. Toda contraseña del usuario tendrá una duración máxima de 90 días, terminado dicho período el usuario de la cuenta deberá renovarlo, conforme las restricciones impuestas.
    a. La longitud de toda contraseña deberá ser igual o mayor a ocho caracteres.
    b. Ninguna contraseña podrá ser igual o similar a su respectivo nombre de usuario.
    c. Las contraseñas deben contener caracteres de al menos 3 de las siguientes 4 clases: Letras mayúsculas (A, B,…, Z), letras minúsculas (a, b,..., z), Números (0, 1, 2,… 9), Caracteres especiales (por ejemplo % & ¡@ ( )).
4. El usuario nunca debe dejar códigos de usuario o contraseñas escritas en medios o lugares donde puedan ser observados por terceros (por ejemplo, e n la carpeta del escritorio, en el monitor del equipo u otros).

5. Cuando un usuario olvide o extravíe su contraseña, deberá acudir al Analista Programador para que se le proporcione una nueva contraseña temporal, misma que deberá cambiar en forma inmediata cuando ingrese por primera vez, siguiente al cambio realizado por el personal de TI, esto con el fin de que la clave sea estrictamente personal.
6. Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con la misma.
7. Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona o se le haya olvidado, deberá cambiarla inmediatamente, sea por su propio conocimiento o solicitando la colaboración del Analista Programador.
8. El usuario estará enterado de que después de ejecutar tres intentos fallidos de logueo (acceso a la red) en su cuenta, la misma será bloqueada, esto para proteger sus datos e identidad. Si esto ocurre deberá comunicarse con el Analista Programador para que su contraseña le sea desbloqueada y de esta manera poderse validar nuevamente en la red.

Sobre la contraseña de administrador en las estaciones de trabajo

1. Cada estación de trabajo será configurada únicamente con dos usuarios, un usuario Administrador local del equipo y el usuario del funcionario restringido para que el usuario del mismo lo pueda utilizar y realizar sus labores diarias.
2. La contraseña administrador de los equipos de cómputo será conocido únicamente por el Analista Programador.
3. Ningún funcionario deberá bajo ninguna circunstancia cambiar contraseña de administrador local de la máquina.
4. No deberá modificar el acceso a los archivos, de modo que el usuario administrador local siempre tenga acceso total en la estación.

Política #4. Sobre el uso de la navegación de internet

Responsabilidades

- Jefaturas inmediatas y Auditoría Interna: Velar por el cumplimiento de esta política.
- Analista Programador: Facilitar el servicio, así como brindar los medios de control de acceso.
- Funcionarios, terceros: Conocer e implementar lo estipulado en esta política.

Normas

Usos Permitidos:

1. Navegación y comunicación electrónica estrictamente relacionadas con las labores desempeñadas para la institución.
2. Comunicación e intercambio de información con personas e instituciones con el fin de tener acceso a documentación y avances relacionados con la especialidad y/o trabajo del personal.

Usos Prohibidos relacionados con navegación:

3. Toda actividad que sea de carácter lucrativo o comercial en nombre individual, privado o negocio particular.
4. Acceso a lugares obscenos, que distribuyan material pornográfico, o bien materiales ofensivos en perjuicio de terceros.
5. La transmisión de materiales que violen cualquier regulación Costarricense como por ejemplo materiales con derechos de propiedad intelectual, materiales que legalmente se consideren amenazantes u obscenos.
6. No se deberá descargar de ningún sitio WEB software no licenciado en la Institución.
7. Acceso a sitios relacionados con: sexo, racismo, apuestas, actividades criminales, drogas, juegos, así como páginas similares, pudiendo restringirse en cualquier momento otro tipo de páginas por parte del Tribunal.
8. Se prohíbe a los funcionarios del TRA chatear durante la jornada laboral salvo casos que sean necesarios para asunto laboral.
9. El uso de las redes sociales personales y el uso de YouTube o cualquier otro sitio que sea para visualizar videos que no sean para uso estrictamente laboral están prohibidas y bloquedas salvo aquellos casos que sean aprobados por el Órgano Colegiado en que el uso de estas plataformas tecnológicas sea necesario para aquellos procesos o funcionarios que realmente sean de indispensable necesidad utilizarlos para la gestión de sus actividades laborales.

Régimen de responsabilidades:

10. El Analista Programador como administrador del servicio tiene la autoridad para controlar y negar el acceso a cualquiera que viole las políticas o interfiera con los derechos de otros usuarios.
11. El Analista Programador, podrá monitorear y controlar el acceso a internet desde la red interna y generar reportes de la actividad hacia internet por cuenta, por grupo de cuentas, departamento, estación de trabajo o subred.

Política #5. Sobre el uso del correo electrónico empresarial

Responsabilidades

- Auditoría Interna: Velar por el cumplimiento de lo estipulado en esta política.
- Jefaturas inmediatas: Velar por el cumplimiento de lo estipulado en esta política.
- Analista Programador:
    - Crear y configurar las Listas de Distribución de Correo y de configurar a los funcionarios que sean autorizados por cada jefatura de área funcional para hacer envío de correos masivos, con fines laborales y de interés institucional
    - Mantenerse informado con respecto a la seguridad del sistema, evaluando e implementando los productos de seguridad informática necesarios que permitan garantizar un ambiente seguro.
    - Supervisar el buen funcionamiento del Servicio de Correo Electrónico Institucional.

    - Brindar el soporte necesario del Servicio de Correo Electrónico Institucional cuando algún funcionario lo requiera.
    - Mantener un respaldo diario de todos los correos almacenados en el servidor del Correo del Servicio de Correo Electrónico Institucional.
- Funcionarios, terceros y usuarios: Conocer e implementar lo estipulado en esta política.

Normas

1. El tamaño máximo definido para la recepción o envío de mensajes a través del sistema de correo electrónico es de 50 MB, considerando el cuerpo del mensaje como los archivos adjuntos que se añadan.
2. Los mensajes que tengan más de 12 meses de antigüedad en el servidor de correo electrónico podrán ser eliminados por el administrador del servicio, previa notificación formal al usuario dueño de dichos mensajes.
3. Solamente está autorizado el uso del correo oficial institucional, excluyendo servicios comerciales como Hotmail, Yahoo, Gmail, entre otros.
4. El funcionario debe revisar su cuenta de correo electrónico diariamente, de tal forma que descargue todos aquellos mensajes almacenados en el servidora su computador.
5. El funcionario es responsable de dar respuesta por medio del Servicio de Correo Electrónico de confirmación de recibido y lectura a cada uno de los correos enviados y utilizados como medio de comunicación oficial del Servicio de Correo Electrónico Institucional.
6. El funcionario debe llevar a cabo cambios periódicos de la clave de acceso de su cuenta de correo electrónico, cumpliendo con lo estipulado en la Política de Uso de Contraseñas.
7. El fondo autorizado para el envío de correos electrónicos debe ser de color blanco y no se deben utilizar imágenes de fondo de ningún tipo, para lo cual se procederá a estandarizar con el logotipo de la institución.
8. Todo correo electrónico que sea enviado desde el Sistema de Correo Electrónico del Tribunal Registral Administrativo debe incluir una firma automatizada, configurada en cada cliente de correo electrónico, en la cual se destaquen los datos del remitente.
9. Todo correo electrónico que sea enviado desde el Sistema de Correo Electrónico del Tribunal Registral Administrativo debe incluir un aviso de confidencialidad.
10. Ningún usuario puede ver, copiar, alterar o destruir el contenido del correo o directorio de trabajo de otra persona sin el consentimiento explícito del dueño de la cuenta de correo.
11. Cada vez que utiliza una comunicación con varias personas (uno a muchos), cerciórese que el mensaje esté dirigido a las personas que realmente deben de recibir el mensaje, si encuentra que un mensaje fue enviado a una persona que no corresponde, deberá enviar una disculpa de inmediato.
12. Se prohíbe utilizar el Servicio de Correo Electrónico para divulgar información propiedad del Tribunal Registral Administrativo considerada como confidencial, a terceras personas u organizaciones no autorizadas para recibirla.
13. El usuario no debe abrir correos de dudosa procedencia, que no han sido solicitados explícitamente, o que provengan de un remitente desconocido. Tampoco aquellos que no tengan un asunto, tema o

"Subject" específico, o que en su interior contengan un archivo adjunto no solicitado con una extensión considerada como peligrosa, por ejemplo: .com, .exe, .src, .bat, .cpl, .hta, .vbs,.cmd, .pif, .bmp, .gif; .scr o .hlp. El correo debe ser eliminado en caso de existir duda.

14. Se prohíbe utilizar los recursos del Servicio de Correo Electrónico del Tribunal Registral Administrativo para actividades con fines de lucro; manejo de material pornográfico; actividades con fines publicitarios o comerciales de bienes y servicios en beneficio propio, entre otros.
15. Se prohíbe el envío de correos tipo "SPAM", es decir "correo basura no solicitado".
16. Los usuarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del TRA. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.
17. Se prohíbe utilizar el correo electrónico para recibir o enviar mensajes que no sean de índole laboral.
18. Los usuarios deben reportar inmediatamente, a su superior inmediato, cualquier situación que pueda comprometer la seguridad y buen funcionamiento del sistema, ya sea virus, modificación o pérdida de datos, sospecha de robo de claves y otras actividades poco usuales, a efectos de canalizarlo ante el Analista Programador de la institución.
19. El Analista Programador del TRA no podrá monitorear los correos electrónicos de los funcionarios del Tribunal.

Política #6. Sobre la Seguridad Física y Ambiental

Responsabilidades

- Auditoría Interna: Velar por el cumplimiento de lo estipulado en esta política.
- Funcionarios, personas y empresas que prestan servicios profesionales y técnicos, usuarios de recursos tecnológicos: Conocer e implementar lo estipulado en esta política.

Normas

1. Los perímetros de seguridad de todo el edificio del TRA deben estar delimitados por una barrera, por ejemplo: una pared, una puerta de acceso con cerradura, controlado por dispositivo de autenticación, cámaras de seguridad, alarmas de seguridad o un escritorio u oficina de recepción atendidos por personas para controles de acceso físico.
2. Todas las áreas destinadas al procesamiento o almacenamiento de información así como aquellas en las que se encuentren los equipos y demás infraestructura que soporte a los sistemas de información y comunicaciones deben ser protegidas con medidas de control de acceso físico.
3. El acceso al cuarto de comunicaciones está autorizado solo al Analista Programador.
4. Por efectos de seguridad, no se debe colocar rótulos que identifiquen los sitios donde se ubican los servidores, el equipo de comunicaciones y otros equipos de cómputo dentro de las instalaciones del TRA.
5. Las puertas de acceso al cuarto de servidores deben permanecer siempre cerradas con cerradura.

6. Los recursos de TI que por su valor o exposición pueden estar sujetos a pérdidas o sustracción, deben ser protegidos con medios físicos.
7. Las instalaciones que alberguen equipos de cómputo se deben proteger de amenazas ambientales tales como: incendio, explosivos, inundaciones o filtraciones de agua, polvo, vibraciones, efectos químicos, derrumbes que puedan ocasionar daños físicos y lógicos a los equipos.
8. El Analista Programador es el responsable de revisar regularmente las condiciones ambientales para verificar que las mismas no afecten el funcionamiento de los equipos.
9. Todos los equipos deben ser objeto de mantenimiento preventivo cada 2 meses, de conformidad con un cronograma preestablecido por el Analista Programador.

Acceso físico a las instalaciones

10. Se deben definir niveles de seguridad según la información administrada en cada área de la Institución.
11. Es responsabilidad de todos los funcionarios el uso adecuado de los dispositivos de seguridad que se han implementado en las distintas áreas de ingreso a la Institución.
12. Todo funcionario, personas y empresas que prestan servicios profesionales y técnicos al TRA deben portar el carné asignado en un lugar visible.
13. Todo funcionario es responsable por las personas que lo visitan en función de sus labores asignadas. Es obligación de cada uno escoltar a la visita, desde el ingreso a la salida de la Institución correspondiente.

Política #7. Sobre el control contra código malicioso o virus

Responsabilidades

- Análisis de Sistemas: Instalar, actualizar y adquirir paquetes de software de antivirus y realizar un monitoreo a través de software centralizado.
- Jefatura de cada área: Velar por el cumplimiento de lo estipulado en esta política.
- Funcionarios, terceros y usuarios: Conocer e implementar lo estipulado en esta política.

Normas

1. Para prevenir infecciones por virus informático, los usuarios no deben hacer uso de software que no haya sido proporcionado y validado por el Analista Programador.
2. Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el usuario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.
3. Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá llamar al Analista Programador para la detección y erradicación del virus.

4. Debido a que algunos virus son extremadamente complejos, ningún usuario debe intentar erradicarlos de las computadoras sin la ayuda del Analista Programador.
    - En caso de funcionarios externos, que por sus labores necesiten hacer uso de la red de la institución con equipos de su propiedad, deberán contar con un software de antivirus debidamente licenciado.
    - El software de antivirus no puede ser deshabilitado, y la configuración del mismo no debe de ser alterada. Igualmente, la frecuencia del escaneo automático del software no debe ser modificada.
    - El Analista Programador deberá alertar e informar de forma periódica a todos los usuarios sobre posibles amenazas de virus, así como los riesgos asociados al uso de software malicioso en sus equipos.

Política #8: Sobre el desarrollo, mantenimiento y actualización de software y hardware

Responsabilidades

- Análisis de Sistemas: Gestionar toda la infraestructura tanto de software como de hardware del Tribunal Registral Administrativo.
- Jefatura de cada área: Velar por el cumplimiento de lo estipulado en esta política.
- Funcionarios, terceros y usuarios: Conocer e implementar lo estipulado en esta política.

Normas

Sobre el software

1. El Analista Programador debe asegurar el funcionamiento correcto y adecuado de la infraestructura de software del TRA.
2. El Analista Programador debe procurar mantener software actualizado, con su respectiva instalación de parches y actualizaciones de versiones.
3. El TRA proveerá el software necesario para que los funcionarios puedan realizar sus labores, bajo los lineamientos establecidos para la adquisición de software. Todas las copias de software que se instalen en las computadoras del TRA tendrán una licencia vigente.
4. La infraestructura de software del TRA, incluyendo aplicaciones, sistemas de Información y los datos que éstos generen son propiedad del TRA y sólo pueden utilizarse para fines estrictamente oficiales y legales.
5. Está prohibido el uso de la infraestructura de software del TRA para fines ajenos a las actividades de la Institución.
6. En caso de que el usuario descubra software sin licencia en su computadora del TRA, deberá tomar medidas inmediatas para rectificar la situación, ya sea borrándolo de la computadora o reportándolo al Analista Programador.
7. En caso de que un usuario necesite instalar un software especial en su computadora, deberá realizar la solicitud al Analista Programador, contando con el visto bueno de la jefatura inmediata. Todas

las solicitudes para instalar software deben incluir los detalles del uso que se planea darle al software, justificaciones para la instalación, detalles acerca de la duración del uso, el número de licencias a instalar e información relevante respecto a la licencia.

8. Se debe contar con un registro detallado de las licencia de software adquiridas, con sus respectivas fechas de compra, vigencia y ubicación de la licencia. Este registro debe de ser consistente para facilitar la auditoría y creación de reportes.
9. Se debe mantener un respaldo de todos los programas de software antes de que éstos sean utilizados. Se deben guardar en un lugar seguro todas las copias originales, licencias y manuales de los programas adquiridos, y se deben utilizar las copias para instalar el software en los equipos.
10. Para que un proceso de adquisición sea válido deberá cumplir con los requerimientos internos definidos por el Analista Programador y el área de Proveeduría.
11. El Analista Programador debe contar con un documento de requerimientos y controles de seguridad que debe ser considerado para la implementación y mantenimiento del software para el TRA.
12. Se debe establecer y aplicar un procedimiento formal para la solicitud de cambios y nuevos requerimientos hacia la infraestructura de software del TRA.
13. Se debe establecer un procedimiento para el control de versiones y cambios en la infraestructura de software del TRA.
14. Se debe mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, pruebas y producción.
15. Todo proceso de implementación de sistemas de información o adquisición de software debe considerar la capacitación o transferencia del conocimiento requerido para todos sus usuarios.
16. El acceso a archivos ejecutables, código fuente, librerías y otra documentación o recursos asociados al diseño de una aplicación, debe ser estrictamente controlado y manejado por el Analista Programador.
17. Los roles de usuario asociados a los sistemas de información y/o aplicativos del TRA serán definidos, otorgados y documentados por el administrador asignado en cada Unidad Administrativa para tal fin.
18. Los usuarios de la infraestructura de software del TRA deben respetar los derechos de propiedad intelectual de los autores de las obras, programas y aplicaciones, manejadas o accedidas a través de dichos sistemas.
19. Los programas o recursos utilizados en los sistemas de información del TRA deben tener su correspondiente licencia vigente o autorización de uso para poder ser utilizadas. Dichos programas solo podrán ser instalados por el personal autorizado para tales efectos. Además, no podrán instalarse programas sin la previa autorización del Analista Programador, aunque sean programas libres de costo.
20. Los programas y aplicaciones contenidos en los sistemas de información no podrán reproducirse sin autorización de la Unidad Administrativa responsable o ser utilizados para fines ajenos a las funciones o poderes del TRA.
21. El acceso a información o a una cuenta ajena sin autorización, obtenido mediante la modificación de privilegios de acceso o la interceptación de información en cualquier otra manera está prohibido, por lo que tal conducta se castigará conforme a la legislación local y vigente y a las normas aplicables que rigen la conducta de los empleados.
22. Los relojes de todos los sistemas y terminales deberán ser sincronizados para corregir cualquier diferencia entre los mismos y que todos cuenten con la hora oficial de la Institución.

23. El Analista Programador debe utilizar técnicas de seguridad y procedimientos de administración asociados (por ejemplo firewalls, dispositivos de seguridad, segmentación de redes y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia las redes.
24. Con respecto a la instalación de software, debe acatarse lo dispuesto en el documento propiedad del TRA denominado “Manual de Uso y Instalación de Programas de Cómputo”.

Sobre el hardware

25. Ningún usuario debe realizar reparaciones o hacer alteraciones al equipo de hardware. Únicamente el personal autorizado por el Analista Programador puede realizar éstas acciones.
26. El Analista Programador debe asegurar el funcionamiento correcto y adecuado de la infraestructura de hardware. Además deberá asegurar que todos los recursos cuenten con un suministro de energía eléctrica adecuado con el propósito de prevenir daños a los equipos y a la instalación eléctrica de la institución.
27. El Analista Programador debe contar con una lista actualizada de los proveedores de hardware, sus teléfonos, direcciones y contacto.
28. El Analista Programador es responsable de almacenar en un lugar seguro las garantías, acuerdos de servicio y copias de las facturas de todos los componentes de hardware adquiridos.
29. El Analista Programador debe dar mantenimiento preventivo al equipo de hardware para maximizar su desempeño y vida del mismo. Se debe inspeccionar y dar mantenimiento al equipo según las especificaciones de fábrica.
30. Se mantendrá un registro de las reparaciones y servicios prestados a cada componente de hardware, a través de reportes automatizados o del Analista Programador.
31. Los componentes de hardware deberán permanecer en temperaturas adecuadas. Se instalarán sistemas de ventilación o aire acondicionado cuando sea necesario.
32. Los equipos deberán limpiarse periódicamente según las especificaciones de los fabricantes de la empresa. Se deberá instruir a los encargados de limpieza acerca de la vulnerabilidad de los equipos, y de los materiales adecuados para el aseo de éstos. En esta pauta se incluye la limpieza del centro de datos.
33. Los dispositivos de respaldo eléctrico deben ser revisados periódicamente para cerciorarse de que pueda proveer suficiente tiempo de respaldo. También se deben realizar las pruebas que recomiendan sus fabricantes.
34. Cuando una Unidad Administrativa presente la necesidad de adquirir nuevos componentes de hardware, ésta deberá presentar la justificación escrita al área de Proveeduría y solicitar al Analista Programador los requerimientos técnicos del equipo.
35. El Analista Programador debe presentar anualmente al Órgano Colegiado el plan de renovación de hardware institucional con el respectivo presupuesto.
36. Los nuevos activos deben rotularse con la respectiva placa y número de activo, esto es responsabilidad del encargado de bienes.

Política #9: Sobre el control de respaldos, resguardo y recuperación de información

Responsabilidades

- Analista Programador: Proveer los medios y mecanismos seguros que garanticen el respaldo y restauración de la información crítica del TRA. Además de gestionar de forma adecuada y segura los respaldos de información.
- TRA: Proveer los recursos para adquisición de mecanismos de respaldos.

Normas

1. El Analista Programador es el responsable de definir los procedimientos y técnicas para administrar, proteger, respaldar, conservar y eliminar la información digital, contenida en los diferentes medios de almacenamiento (cintas, discos y otros medios).
2. Los respaldos de las bases de datos deben ser realizados diariamente de lunes a viernes por el Analista Programador al igual que los respaldos de los sistemas de Información y toda la información almacenada en los servidores propiedad del TRA. Dicho respaldos serán están custodiados en el cuarto de servidores del TRA.
3. El Analista Programador será el encargado de supervisar que el contrato con terceros de almacenamiento de respaldos en servidores fuera del TRA sean ejecutados diariamente de lunes a viernes.
4. El Analista Programador debe velar por el correcto y seguro almacenamiento de los dispositivos que contienen los datos generados en los respaldos.
5. El analista de sistema es el responsable de realizar pruebas periódicas, para verificar que los respaldos almacenados se están ejecutando correctamente.
6. El Analista Programador no se hará responsable de respaldar la información personal de cada usuario. Solo se respaldara la información pública que es del trabajo diario del funcionario y que se encuentre almacenada debidamente en las carpetas compartidas indicadas.

Política #10. Sobre la Clasificación de la Información

Responsabilidades

- Auditoría Interna: Velar por el cumplimiento de esta política.
- Analista Programador: Desarrollar los procedimientos necesarios para el seguimiento de las pautas descritas en esta política.
- Dueños de los datos: Identificar la información y clasificarla con el fin de asegurar que reciba un apropiado nivel de protección según su sensibilidad y criticidad.
- Funcionarios y terceros: Aplicar las pautas y procedimientos definidos en relación con esta política.

Normas

1. La información debe ser clasificada en función de su valor, sensibilidad y criticidad para la Institución, con el fin de determinar el grado de protección requerida al ser manipulada.
2. El Analista Programador debe definir un método para la clasificación de la información administrada, donde se definan las categorías a utilizar.
3. El método de clasificación de la información debe considerar información impresa o digital, independientemente del tipo de almacenamiento o medio de transferencia.
4. Se deben definir revisiones periódicas del método de clasificación de la información.

5. El Analista Programador debe desarrollar los procedimientos establecidos para la revisión del método de clasificación de la información, los cuales deben incluir la valoración de las necesidades del negocio para compartir y restringir la información, las obligaciones legales en caso de que existan y el nivel de impacto asociado.
6. Toda información clasificada debe ser rotulada. La etiqueta debe reflejar la clasificación. Esto aplica para reportes impresos y en pantalla, medio de almacenamiento (cintas, discos, entre otros), mensajes electrónicos y archivos transferidos.
7. Los dueños de los documentos impresos, digitalizados y electrónicos, y las personas que los manipulen, son responsables de mantenerlos seguros de acuerdo al método de clasificación definido.
8. Los acuerdos con otras organizaciones que compartan información deben incluir procedimientos para identificar la clasificación de dicha información e interpretar la marca de clasificación de otras organizaciones.

Política #11. Sobre los Servicios de Red

Responsabilidades

- Auditoría Interna: Velar por el cumplimiento de lo estipulado en esta política.
- Analista Programador: Gestionar los cambios relacionados con la infraestructura de red del TRA.

Normas

1. Se deben mantener acuerdos de nivel de servicio con los proveedores de equipos de comunicación y demás equipos críticos que brindan los servicios de red del TRA.
2. El Analista Programador debe proveer adecuados mecanismos de seguridad que brinden la protección necesaria a los servicios de red establecidos en el TRA.
3. Se deben establecer y seguir procedimientos y guías que dicten los requerimientos y parámetros para garantizar la seguridad en la activación de cualquier servicio de red.
4. Deben existir mecanismos de autenticación y control de acceso en los servicios de red.
5. Cualquier cambio en las reglas de enrutamiento, establecimiento de nuevos enlaces, habilitación de un servicio, puerto, exclusión de alguna restricción establecida o cualquier tipo de solicitud relacionada con los servicios de red, se debe justificar adecuadamente y guardar evidencia de dicha justificación.
6. Todas las conexiones a Internet deberán ser protegidos por un firewall para prevenir el acceso no autorizado desde y hacia la red del TRA.
7. Todos los servicios de red deben ser monitoreados en intervalos regulares y cumplir con una revisión periódica.
8. Debe existir una adecuada auditoría y gestión de bitácoras de los servicios de red.
9. Debe existir un adecuado control, administración y seguridad de los puertos de red.
10. Los servicios de red que no sean requeridos serán deshabilitados.
11. Los equipos y dispositivos que brinden servicios de red deben ubicarse en áreas seguras y restringidas.
12. Se deben utilizar protocolos seguros para administración remota de equipos de red y servidores tales como SSH y TFTP.

Política #12. Sobre la Concientización y Capacitación

Responsabilidades

- Auditoría Interna: Velar por el cumplimiento de lo estipulado en esta política.
- Consejo Académico en coordinación con la Jefatura de cada área: aplicar un proceso de inducción en temas de políticas para todos los funcionarios de la Institución.
- Funcionarios, terceros y usuarios: Conocer e implementar lo estipulado en esta política.
- Consejo Académico: Gestionar la logística de los cursos de capacitación en temas de seguridad y políticas.
- Analista Programador: solicitar en los planes operativos anuales capacitación para la totalidad de funcionarios.

Normas

1. Se debe establecer un programa de capacitación formal y periódica sobre temas de Seguridad de la Información para todos los usuarios de los sistemas de información del TRA.
2. Todos los funcionarios de la organización y terceros, en caso de ser requerido, deben recibir apropiados entrenamientos de concienciación y actualizaciones regulares en políticas y procedimientos en relación a sus funciones laborales.
3. Se debe definir un proceso de inducción formal, para dar a conocer las Políticas de Seguridad y las expectativas de la Institución en esta materia. Es responsabilidad del Consejo Académico, en coordinación con el Analista Programador, gestionar este proceso de inducción.
4. Todo cambio en las políticas debe ser comunicado inmediatamente a todos los funcionarios, y al mismo tiempo reforzar el cumplimiento de las mismas.
5. Debe existir un sitio centralizado donde los funcionarios tengan acceso al Marco de Políticas y a información relacionada en temas de Seguridad de la Información.
6. El Analista Programador es el encargado de gestionar periódicamente encuestas para evaluar las debilidades presentadas por los funcionarios de la Institución, en temas relacionados con las políticas.
7. Se deberán definir o fomentar campañas masivas de concienciación necesarias para divulgar las políticas, utilizando por ejemplo afiches, pancartas, boletines, entre otros.

Política # 13. Sobre la Administración de Terceros

Responsabilidades

- Analista Programador: Aplicar las pautas y procedimientos definidos en relación con esta política.
- Órganos Fiscalizadores y terceros: Conocer y cumplir con lo estipulado en esta política.
- Auditoría Interna: Velar por el cumplimiento de lo estipulado en esta política.

Normas

1. Debe existir un Órgano Fiscalizador responsable de valorar y recomendar la aprobación técnica de la contratación de un tercero.
2. El Órgano Fiscalizador debe velar por el cumplimiento y ejecución de lo pactado entre las partes.

3. Toda documentación que establezca las responsabilidades de las partes debe ser almacenada en un lugar que garantice su integridad y disponibilidad.
4. En toda contratación se deben especificar los requerimientos de seguridad de la información que deben cumplirse, así como las acciones a tomar en caso de violaciones a estas cláusulas definidas.
5. Para la implementación de cualquier servicio contratado, el Analista Programador brindará acceso supervisado a los recursos tecnológicos estrictamente necesarios, de acuerdo a los lineamientos estratégicos definidos.
6. Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.
7. Toda contratación en la que se requiera interactuar con información perteneciente al TRA, debe incluir el respectivo acuerdo de confidencialidad y/o no divulgación de información debidamente firmada. Se debe definir un responsable por parte del personal externo para las acciones realizadas por los terceros.
8. Si la contratación está sujeta a un Acuerdo de Nivel de Servicio, en dicho acuerdo se debe incluir una cláusula en la cual se especifique que el bien o servicio proporcionado por la contraparte podría ser sujeta a una revisión por parte del TRA.
9. En toda contratación se deben cumplir las políticas institucionales, y es responsabilidad del Órgano Fiscalizador dar a conocerlas.