COLEGIO
DE PROFESIONALES
EN PSICOLOGÍA
DE COSTA RICA

MANUAL DE POLITICAS DE SEGURIDAD INFORMATICA

COLEGIO DE PROFESIONALES EN PSICOLOGÍA DE COSTA RICA		
Elaborado por:	**Revisado por:**	**Aprobado por:**
Jefatura TI	Dirección Ejecutiva	Junta Directiva
Código: MA-TI-001	Versión: 1	Junio 2020

	SECCIÓN / PÁRRAFO MODIFICADO	CAMBIO REALIZADO	FECHA MES / AÑO
1	Creación inicial del documento	Creación del documento	Junio 2020
2			
3			
4			
5			
6			

1. ALCANCES

Los lineamientos contenidos en el presente Manual son de observancia y cumplimiento obligatorio para todas los Oficinas y áreas del Colegio de Profesionales en Psicología de Costa Rica, así como para todo el personal, 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 sistemas de Tecnología de Información de la Dependencia.

2. 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.

3. OBJETIVOS ESPECIFICOS

- Colaborar en el cumplimiento de las regulaciones legales o técnicas emitidas por el ente regulador.
- 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.
- Servir de guía para el comportamiento profesional y personal de los colaboradores.
- Promover el uso de las mejores prácticas de seguridad informática en el trabajo.
- Garantizar que los procedimientos de seguridad sean uniformes y coherentes en toda la Institución.
- Poner por escrito la obligación del CPPCR con respecto a la seguridad de la Información, previniendo posibles negligencias.

4.4 MARCO LEGAL Y REGULATORIO

- Normas técnicas para la gestión y el control de las Tecnologías de Información. (N-2-2007-CO-DFOE)

CONTENIDO

PSI-001 POLÍTICA PARA EL USO DE QUEMADORES DE CD Ó DVD

1. **Política:**

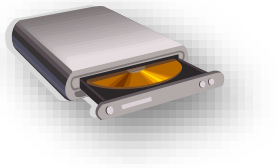
Dada la importancia de la información que maneja la institución y la necesidad de resguardar algunos de los datos, así como emitir información a otras entidades, surge la necesidad de establecer la normativa para regular el uso de los quemadores de discos compactos o DVD, con el objeto de que su uso sea para labores propias de la institución.

2. **Responsabilidad:**

Será responsabilidad de las personas funcionarias del Colegio de Profesionales en Psicología de Costa Rica que cuentan con dispositivos electrónicos en los cuales se cuentan con dispositivos grabadores de discos compactos o DVD, acatar lo dispuesto en esta política y velar por el uso óptimo de los equipos.
Dado que los quemadores pueden ser internos o externos, esa política aplica para cualquiera de los casos.

3. **Normas**

a. 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.
b. El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.
c. Utilizarlo para labores institucionales; lo cual tiene implícito la no reproducción de películas, software, música ni datos personales.
d. En caso de fallas técnicas notificar de inmediato al personal de Soporte Técnico.
e. En caso de robo o extravío notificar a la instancia respectiva para iniciar el proceso administrativo respectivo.



PSI-002 POLÍTICA PARA EL USO, CD, DVD, LLAVES MAYAS

1. **Política:**

La información constituye uno de los principales activos para la institución, por tanto el manejo adecuado de la misma es responsabilidad de todos los funcionarios así como la correcta utilización de los dispositivos que el mercado ofrece para la manipulación de la misma.

2. **Responsabilidad:**

Es responsabilidad de todas las personas funcionarias del Colegio de Profesionales en Psicología de Costa Rica que entren en contacto con un equipo de cómputo, velar por el cumplimiento de las normas con relación al manejo de la información y la utilización de los dispositivos tecnológicos en el tema.

3. **Normas :**

a. Mantenga sus discos rotulados y en un lugar seguro, de forma tal que en caso de requerir alguno de estos, sea de fácil acceso.
b. No deje discos en el equipo cuando no esté en uso.
c. No deje la llave maya en el equipo cuando usted no esté utilizando el equipo.
d. Maneje en los dispositivos la información que requiere únicamente.
e. En caso de requerir el almacenamiento de volúmenes grandes de información notificarlo a su jefatura, justificando la necesidad de la misma.
f. Escanee los archivos antes de copiarlos ya sea del dispositivo a la máquina o viceversa.
g. En caso de extraviar alguno de los dispositivos, notificar la pérdida.
h. Siga las recomendaciones del fabricante sobre el uso y cuidados de los dispositivos.
i. Tome en cuenta condiciones ambientales tales como temperatura, humedad, entre otros; que pueden dañar los datos.
j. En el caso de tener que almacenar información sensible, realice al menos dos copias adicionales, debidamente protegidas como prevención.

PSI-003 POLÍTICA PARA LA MANIPULACIÓN Y CAMBIO DE CONTRASEÑAS PARA LOS USUARIOS FINALES.

1. **Política:**

La manipulación responsable de las contraseñas generadas para los usuarios de la red es de vital importancia en la seguridad de toda la información institucional, por lo tanto deben considerarse aspectos básicos de seguridad que serán de acatamiento obligatorio por parte de todos los usuarios de la red.

2. **Responsabilidad:**

Será responsabilidad de todas las personas usuarias de la red acatar las normas más adelante incluidas.

3. **Normas:**

a. Toda persona funcionaria de la red institucional que posea una o varias cuentas creadas a su nombre, deberá cumplir con las siguientes normas, que constituyen las mejores prácticas para la manipulación de las contraseñas personales y lo protegerán del robo y manipulación de la información que administra o de la información institucional.
b. Queda estrictamente prohibido al funcionariado de la institución que posee una cuenta de usuario y contraseña, utilizarlos en los sistemas a los cuales se ha dado acceso para obtener cualquier clase de beneficio propio y /o para terceros.
c. La persona usuaria nunca debe dejar códigos de usuario o contraseñas escritas en medios o lugares donde puedan ser accesados por terceros (por ejemplo, en la carpeta del escritorio, en el monitor del equipo u otros).
d. Cuando una persona usuaria olvide o extravíe su contraseña, deberá acudir al Área de soporte 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 sea personal
e. 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.
f. La persona usuaria 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 al área de soporte técnico para que su contraseña le sea desbloqueada y de esta manera poderse validar nuevamente en la red.

g. Toda persona usuaria deberá hacer el cambio periódico de su contraseña cuando el sistema se lo solicite (El cual no podrá ser mayor a 45 días).

h. Las contraseñas generadas por las personas usuarias para su uso en la red, deben contener caracteres de al menos 3 de las siguientes 4 clases:

Letras mayúsculas	A,B,C,……Z
Letras minúsculas	a,b,c,…….z
Números	0,1,2,…….9
Caracteres especiales	Por ejemplo: Símbolos puntuación u otros como % & ¡ @()

i. Toda persona usuaria deberá tomar en cuenta las siguientes restricciones, que han sido configuradas para que las contraseñas sean más seguras:

- La longitud de toda contraseña a utilizar deberá ser igual o mayor a ocho caracteres.
- La contraseña a adoptar no podrá ser igual o similar a su respectivo nombre de usuario.
- No podrá repetir ninguna de las últimas tres contraseñas utilizadas.
- No se podrá dejar contraseñas en blanco.

PSI-004 POLÍTICA PARA LA GESTIÓN DE CONTRASEÑAS SEGURAS PARA USO DE LAS APLICACIONES EN RED

1. **Política:**

La correcta administración de las contraseñas generadas para las personas usuarias de la red del CPPCR, es de vital importancia en la seguridad de toda la información institucional, por lo tanto deben considerarse aspectos básicos de seguridad que serán de acatamiento obligatorio por parte de todas las personas usuarias de la red, y deberán ser configuradas por los administradores de red.

2. **Responsabilidad:**

Será responsabilidad del administrador de la Red, con permisos para administrar dominios, implementar las normas más adelante incluidas.

3. **Normas**

- El administrador de las cuentas de usuario, deberá configurar las siguientes normas, aplicables a todas las cuentas y contraseñas de red.
- Sobre la duración de la contraseña: Toda contraseña tendrá una duración máxima de **45 días,** terminado dicho período la persona usuaria de la cuenta deberá renovarlo, conforme las restricciones impuestas.
- Sobre la longitud de la contraseña: La longitud de toda contraseña deberá ser igual o mayor a ocho caracteres.
- Sobre la robustez de la contraseña: Ninguna contraseña podrá ser igual o similar a su respectivo nombre de usuario.
- Las contraseñas generadas por las personas usuarias para su uso en la red, deben contener caracteres de al menos 3 de las siguientes 4 clases:

Letras mayúsculas	A,B,C,……Z
Letras minúsculas	a,b,c,……z
Números	0,1,2,……9
Caracteres especiales	Por ejemplo: Símbolos puntuación u otros como % & ¡ @()

- Sobre los requerimientos de logueo: Requerir automáticamente el cambio de contraseña la primera vez que el usuario solicita su ingreso al a red.
- Sobre los requerimientos de logueo: Se debe incluir la respectiva configuración para que después de 3 intentos fallidos de logueo la cuenta sea bloqueada.
- Sobre la seguridad de las contraseñas: Se debe incluir la respectiva configuración para que se guarde un histórico de al menos las últimas tres contraseñas usadas por el usuario, para prevenir su reutilización.
- Sobre la seguridad de las contraseñas: El personal de TI no realizará cambios a las cuentas o contraseñas que sean solicitados vía telefónica a menos que esté completamente seguro de que no se trata de un engaño (por ejemplo cuando reconoce 100% la voz del solicitante). Los cambios debe solicitarlos el usuario personalmente, siempre que sea posible, de lo contrario debe pedir al solicitante información que ratifique su identidad.

PSI-005 POLITICA PARA LA ADMINISTRACION Y CONTOL DE EQUIPOS DE CÓMPUTO

1. **Política:**

La Oficina de Tecnologías de Información en coordinación con la Sección de Bienes de la Unidad Administrativa, deberá tener un registro o inventario actualizado de todos los equipos de cómputo propiedad del Colegio de Profesionales en Psicología de Costa Rica

2. **Responsabilidad:**

La Oficina de Tecnologías de Información deberá tener un registro actualizado de todos los equipos de cómputo propiedad del Colegio de Profesionales en Psicología de Costa Rica

3. **Norma**

Se debe tener un registro actualizado periódicamente de todos los equipos de cómputo propiedad de Colegio de Profesionales en Psicología de Costa Rica que contenga el siguiente detalle:

- Usuario
- Funcionario Responsable
- Oficina
- Sistema Operativo
- Tipo de licencia
- Monitor
- Batería o UPS
- Placa de Activo
- Fecha de ingreso
- Proveedor
- Valor inicial

PSI-006 POLÍTICA PARA LA MANIPULACIÓN DE CONTRASEÑA DE ADMINISTRADOR EN LAS ESTACIONES DE TRABAJO

1. **Política:**

La manipulación responsable de las contraseñas generadas para administrar las estaciones de trabajo propiedad de la red del Colegio Profesional de Psicología de Costa Rica, es de vital importancia en la seguridad de la información institucional que cada usuario manipula en su estación de trabajo, por lo tanto, deben considerarse aspectos básicos de seguridad y administración que serán de acatamiento obligatorio por parte de todos los usuarios de la red, su jefatura inmediata y administradores de red.

2. **Justificación de la política:**

Prevenir el acceso restringido a los datos de una estación de trabajo en caso de accidente u otro inconveniente del usuario o en caso que nadie conozca la contraseña de administrador excepto el mismo usuario.

3. **Responsabilidad:**

Será responsabilidad de los administradores de red, el acatamiento de las normas aquí estipuladas.

4. **Normas**

- De cumplimiento por parte del encargado de soporte de las estaciones de trabajo:
  - Cada estación de trabajo será configurada únicamente con dos usuarios, un usuario Administrador local del equipo y un usuario restringido para que el usuario del mismo lo pueda accesar y realizar sus labores diarias.
  - La contraseña Administrador de los equipos de cómputo será conocido únicamente por el personal autorizado del Oficina de Tecnologías de Información. Dicho contraseña será estándar para todas las estaciones de trabajo y deberá cumplir con lo establecido en la norma **PSI-003** sobre la complejidad de los mismos.

- De cumplimiento por parte del usuario de la estación de trabajo:
  - No deberá bajo ninguna circunstancia cambiar contraseña de administrador local de la máquina en caso de que por motivos de fuerza mayor haya sido necesario asignar le un perfil avanzado. Lo anterior por ejemplo en caso de que alguna aplicación específica no funcione con permisos restringidos.
  - No deberá modificar el acceso a los archivos, de modo que el usuario administrador local siempre tenga acceso total en la estación.

PSI-007 POLÍTICA PARA LA REALIZACIÓN DE RESPALDOS DE APLICACIONES.

1. Política:

La realización periódica de respaldos tanto en los sistemas de información como en las bases de datos y toda la información almacenada en los servidores propiedad del Colegio Profesional de Psicología de Costa Rica, es de gran importancia para brindar continuidad de los servicios. Por lo tanto la elaboración de los mismos deberá realizarse periódicamente conforme las características de las aplicaciones y los datos asociados.

2. Responsabilidad:

Será responsabilidad de cada área u Oficina definir los datos críticos que se deben respaldar e informar por escrito al responsable de realizar los respaldos para que los incluya en la programación de los respaldos periódicos, (bases de datos, sistemas de información, información almacenada en todos los servidores, configuraciones de los equipos de telecomunicaciones como los router, switch, entre otros, respaldo de las configuraciones de los software, en general toda la información generada en la institución.) Los respaldos de las bases de datos deben ser realizados por la Oficina de Tecnologías de Información.

3. Normas

- Elaboración de un plan de recuperación y respaldo de información, basados en las características de la aplicación y los datos asociados a él.
- Ejecución del plan de recuperación y respaldo de información y atención de eventualidades.
- Velar por el correcto y seguro almacenamiento de los dispositivos que contienen los datos generados en los respaldos. Llevar un buen control de la existencia de dichos dispositivos, conforme se vayan necesitando.
- Realizar pruebas periódicas, para verificar que los respaldos se están ejecutando correctamente.

PSI-008 POLÍTICA PARA LA NAVEGACIÓN EN INTERNET, MEDIANTE EL SERVICIO BRINDADO POR EL CPPCR

1. Política:

El uso de Internet se otorga a los funcionarios como una herramienta que colabora y apoya en la realización de las tareas, cada usuario debe darle un uso apropiado a este servicio estrictamente relacionado con las labores que se desempeñan en la institución, los usos para otros propósitos no son aceptables, el uso de este servicio deberá tomar en cuenta que se guarden las medidas de racionalidad y seguridad que garanticen la integridad y disponibilidad necesaria con el fin de llevar a cabo un trabajo eficiente y productivo.

2. Responsabilidad:

Será responsabilidad de todas las personas usuarias a las cuales se les haya otorgado cuenta para navegación en Internet, de acatar las normas más adelante incluidas.

La Oficina de Tecnologías de Información cuenta con herramientas automatizadas para monitorear y filtrar todas las actividades que al respecto del uso de Internet realicen los usuarios. Los informes y reportes que se generen con estas herramientas podrán ser utilizadas como evidencia del mal uso o abuso del servicio.

En caso del mal uso, la Oficina de Tecnologías de Información comunicará a la jefatura respectiva para que se tomen las medidas correspondientes.

3. Normas

- Al respecto del uso de navegación en Internet se establece lo siguiente:
    - Usos Permitidos:
        - Navegación y comunicación electrónica estrictamente relacionadas con las labores desempeñadas para la Institución.
        - 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:

  - Toda actividad que sea de carácter lucrativo o comercial en nombre individual, privado o negocio particular.
  - Acceso a lugares obscenos, que distribuyan material pornográfico, o bien materiales ofensivos en perjuicio de terceros.
  - 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.
  - No se deberá descargar de ningún sitio WEB software no licenciado en la Institución.

- Régimen de responsabilidades.

  - La Oficina de Tecnologías de Información como administradora 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.
  - Ante la infracción de alguna(s) de las disposiciones de este Instructivo, el Oficina de Tecnologías de Información lo reportara a la jefatura inmediata, quien procederá con la investigación administrativa correspondiente.
  - Corre por cuenta y riesgo del usuario cualquier información obtenida y/o difundida por medio del servicio de comunicaciones del nodo de Internet.
  - Respetar los derechos de todas las personas, tanto dentro de la red Institucional como fuera de ella.
  - Se recomienda dar el mejor uso posible a esta herramienta, por ejemplo, no abusando del tiempo de utilización, lo que contribuirá a un mejor aprovechamiento y rendimiento del recurso.
  - La Oficina de Tecnologías de Información, 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.

PSI-009 POLÍTICA PARA EL USO DEL CORREO ELECTRÓNICO INSTITUCIONAL.

1. **Política:**

El uso del correo electrónico se otorga a los funcionarios como una herramienta que colabora y apoya en la realización de las tareas, cada usuario debe darle un uso apropiado a este servicio estrictamente relacionado con las labores que se desempeña en la institución, los usos para otros propósitos no son aceptables, el uso de este servicio deberá tomar en cuenta que se guarden las medidas de racionalidad y seguridad que garanticen la integridad y disponibilidad necesaria con el fin de llevar a cabo un trabajo eficiente y productivo.

2. **Responsabilidad:**

- Será responsabilidad de todas las personas usuarias a las cuales se les haya otorgado cuenta para correo electrónico, de acatar las normas más adelante incluidas.
- La Oficina de Tecnologías de Información cuenta con herramientas automatizadas para monitorear y filtrar todas las actividades que al respecto del uso del correo electrónico realicen los usuarios.
- Los informes y reportes que se generan con dicha herramienta podrán ser utilizados como evidencia del mal uso o abuso del servicio.
- Es importante hacer notar acá, que en estas revisiones no hay intervención manual, donde se asegura a los usuarios que no hay ningún funcionario del Oficina de Tecnologías de Información, leyendo o analizando el contenido de los correos para eliminarlos, dicho proceso se hace de manera completamente automática, mediante la configuración de reglas de filtrado en los sistemas de protección para el correo electrónico institucional. La Oficina de Tecnologías de Información lo reportara a la jefatura inmediata, quien procederá con la investigación administrativa correspondiente.
- La Oficina de Tecnologías de Información como administradora 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.

3. Normas

- Usos Permitidos:

  - Navegación y comunicación electrónica estrictamente relacionadas con las labores desempeñadas para la Institución.
  - 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:

  - Las personas usuarias no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe re direccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al Colegio de Profesionales en Psicología de Costa Rica, a menos que cuente con la autorización de la de la jefatura correspondiente.
  - Las personas usuarias deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del CPPCR. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor
  - Toda actividad que sea de carácter lucrativa o comercial en nombre individual, privado o negocio particular.
  - 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.
  - El envío de mensajes en forma masiva a todos y/o varios grupos de usuarios tanto internos como externos solo se pueden enviar a través de la plataforma de envíos masivos de la Oficina de Comunicaciones.

- Régimen de responsabilidades.

- La persona usuaria emisora, cuando envíe a través de la red archivos y/o mensajes electrónicos con archivos adjuntos, debe verificar antes de su envío que los archivos a transmitir estén libres de cualquier virus informático.
- Cada vez que reciba un correo de una persona que no conoce, o correos con asuntos potencialmente inseguros, proceda a borrarlos y eliminarlos incluso de la carpeta de elementos eliminados.

PSI-010 POLÍTICA PARA EL USO ADECUADO DE ESTACIONES DE TRABAJO.

1. **Política:**

El CPPCR aporta a cada persona funcionaria, en apoyo al cumplimiento de sus labores, cuando así se requiere, una estación de trabajo. Dichos equipos son parte del patrimonio institucional y por lo tanto, el CPPCR debe buscar la mejor forma de administrarlos.

2. **Responsabilidad:**

- Será responsabilidad de todas las personas usuarias a los cuales se les haya asignado una estación de trabajo, acatar las normas más adelante incluidas. La Oficina de Tecnologías de Información realizará dos mantenimientos preventivos anuales a los equipos de la institución.

- Cada persona usuaria debe conocer y tener un listado de las características técnicas del hardware del equipo que se le ha asignado, donde al menos conozca:

  - ✓ Darle un uso adecuado donde el mismo no deberá recibir más que el deterioro normal, derivado de su uso. Se recomienda como buenas prácticas:
    - No ingerir alimentos cerca del equipo de cómputo, de modo que no se vea dañado por regarle líquidos o residuos de comida.
    - En la medida de lo posible velar porque no esté ubicado debajo de goteras, y movilizarlo cuanto antes si se detecta dicho problema.
    - No utilizarlo sobre ningún tipo de base inestable, como cajas, o mesas en mal estado, de modo que la probabilidad de que el mismo caiga al suelo sea alta.
    - Reportar al encargado de soporte cualquier anomalía que se esté presentando durante su uso.
    - Cuando el equipo presente problemas de funcionamiento, si no cuenta con experiencia suficiente en mantenimiento de equipos no tratar usted de arreglarlo, preferiblemente contactar al responsable de soporte técnico

- Acatar las instrucciones sobre el adecuado uso que le dé el encargado de soporte técnico.
- En caso de tener que movilizar el equipo, contactar al responsable de soporte técnico.
- No colocarle adornos, adhesivos, plantas o imanes que podrían afectar el desempeño del equipo.
- 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 con el personal de Tecnologías de la Información
- Queda totalmente prohibido que el usuario abra o desarme los equipos de cómputo.

✓ En cuanto a la información almacenada en la estación de trabajo, se tiene que:

- Los equipos facilitados por la institución para que el funcionariado desarrolle sus labores son propiedad del CPPCR, por lo que para efectos del CPPCR toda la información contenida en las mismas es de carácter público. En caso de requerirse por cualquier motivo acceder al equipo de una persona funcionaria, esta última no podrá alegar que la institución está violando su privacidad, por cuanto toda la información almacenada en los equipos es propiedad del CPPCR. De tener información personal, que no está directamente relacionada con el trabajo, es recomendable que la misma sea identificada mediante una carpeta llamada “Información Personal”.
- 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.
- Es responsabilidad de las personas usuarias mantener la información almacenada en las carpetas de respaldo establecidas por parte de la Oficina de Tecnologías de Información.

PSI-011 POLÍTICA PARA EL USO ADECUADO DE LA RED DE DATOS INSTITUCIONAL.

1. **Política:**

El CPPCR asigna a cada persona funcionaria en apoyo al cumplimiento de sus labores, una cuenta de acceso a la red de datos institucional, con la cual el dueño puede accesar diferentes elementos que la componen: Servidores de Archivos, Servidores de Bases de Datos, Impresoras, Archivos compartidos en otras estaciones de trabajo, Sistemas y Aplicaciones Institucionales. Dicha cuenta es otorgada para facilitar las labores del funcionariado mediante el uso de tecnología informática. Por lo anterior, esta política busca regular el uso de las cuentas, de modo que sean utilizadas estrictamente en cumplimiento de las labores institucionales.

2. **Responsabilidad:**

Será responsabilidad de todas las personas usuarias a los cuales se les haya asignado una cuenta de acceso a la red, acatar las normas más adelante incluidas.

3. **Normas**

La persona usuaria con una cuenta de red tendrá las siguientes responsabilidades:

- Cambio periódico de la contraseña de la cuenta de red, para lo cual debe acatar lo estipulado en la política **PSI-0003** “Manipulación y cambio de contraseñas para usuarios finales”.
- No compartir archivos o carpetas en su estación de trabajo, sin restricción de usuarios o atributos. Esta situación puede poner en peligro la información que está almacenada en su estación de trabajo y que es propiedad de la institución. De tener la necesidad de compartir archivos, hacer la consulta con el responsable del soporte técnico.
- No saturar el ancho de banda de la red, copiando archivos utilizando infraestructura de la red, descargando imágenes, archivos de música o cuando se trate de archivos muy grandes, no importa cuál sea su formato.

.

PSI-012 POLÍTICA PARA EL USO DE EQUIPOS PORTÁTILES

1. **Política:**

La institución asigna equipos tipo portátil a su funcionariado para facilitarles el cumplimiento de sus labores.

Esta política describe una serie de lineamientos relacionados con el uso correcto de este tipo de tecnología y de la información que contienen, esto porque dadas las características de este tipo de dispositivos, se presenta mayor probabilidad de vulnerabilidades dado que puede ser conectado en diferentes ambientes informáticos, en los cuales la institución no tiene control.

2. **Responsabilidad:**

Será responsabilidad de toda persona funcionaria del CPPCR, a la que se le haya autorizado o asignado la utilización de un computador portátil, u otro tipo de equipo portátil, velar por la protección, uso adecuado y buen funcionamiento del mismo tal y cual lo establecen las normas asociadas a la política.

3. **Normas**

Esta política es una extensión de la “PSI-010 Política para el uso adecuado de estaciones de trabajo”, constituye el complemento necesario para la manipulación de equipos portátiles.

A cada persona funcionaria a la quen se le asigna el equipo, debe:

- Asegurarse tener la autorización respectiva para el uso del equipo, para portarlo fuera de las instalaciones del CPPCR. Procedimiento de Control de Salida y Entrada del Equipo utilizado por funcionarios del CPPCR.
- Mantener el equipo en el estuche de protección adecuado.
- En caso de robo de la computadora portátil, reportar inmediatamente a la persona encargada del inventario y a la autoridad policial respectiva, según procedimiento administrativo establecido.
- No dejar el equipo portátil desatendido aunque este de viaje, hoteles, sitios de atención al cliente, vehículos.

- Asegurar que estén disponibles las facilidades de protección física del equipo, las cuales deben de aplicarse mientras el equipo no esté en uso.
- Asegurar que exista la protección física adecuada para aplicarse si el equipo es custodiado en el hogar del usuario. .
- Uso apropiado de las aplicaciones del correo electrónico.
- 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.
- Antes de apagar su computadora cierre todas las aplicaciones en uso para evitar fallas de funcionamiento al volver a encenderla.
- No colocar una computadora portátil en posiciones que obstruyan la entrada de aire del ventilador y salida de calor del sistema.
- Procurar no tocar la superficie de la pantalla con los uñas o la punta de un lápiz o un bolígrafo. Al limpiarla, usar telas antiestáticas secas y líquidos especiales para este tipo de pantallas (sin alcohol, sin jabón y sin agentes abrasivos), y hágalo sólo cuando la computadora esté apagada.
- Hacer respaldos de la información contenida en el equipo portátil regularmente. La persona usuaria es responsable de la información que se encuentre almacenada en el equipo.
- Utilizar siempre una contraseña al encender el equipo como un simple bloqueo para usos oportunistas.
- Analizar los archivos antes de copiarlos a la portátil, independiente de la fuente de procedencia.

PSI-013 POLITICA DE INSTALACION DE SOFTWARE

1. **Política:**

En los equipos de cómputo, de telecomunicaciones y en dispositivos basados en sistemas de cómputo propiedad del CPPCR, únicamente se permitirá la instalación de software con licenciamiento apropiado en respeto a la propiedad intelectual.

2. **Responsabilidad:**

La instalación asesoría y supervisión del software en cualquier equipo propiedad del CPPCR corresponde únicamente al Oficina de Tecnologías de Información específicamente al área de Soporte.

3. **Normas:**

- No está permitido la instalación de software de ningún tipo en los equipos de cómputo propiedad del CPPCR por parte de los usuarios sin la respectiva autorización por parte de la Oficina de Tecnologías de Información.
- No está permitida la instalación de software que desde el punto de vista de la Oficina de Tecnologías de Información pudiera poner en riesgo los recursos de la institución.
- Con el propósito de proteger la integridad de los sistemas informáticos y de telecomunicaciones, es imprescindible que todos y cada uno de los equipos involucrados dispongan de software de seguridad (antivirus, vacunas, privilegios de acceso, actualizaciones y otros que se apliquen)
- La Oficina de Tecnologías de Información es el responsable de realizar revisiones periódicas para asegurar que sólo programas autorizados esté instalada en las computadoras de la institución.

PSI-0014 POLITICA DE MANTENIMIENTO AL EQUIPO DE CÓMPUTO.

1. **Política:**

Únicamente el personal autorizado por la Oficina de Tecnologías de Información podrá llevar a cabo los servicios de mantenimiento correctivo y preventivo al equipo informático.

2. **Responsabilidad:**

Es responsabilidad del área de soporte velar por un adecuado mantenimiento preventivo y correctivo del equipo informático. Se deben realizar mantenimientos semestrales tanto al equipo de cómputo de las oficinas centrales como al de las regionales.

3. **Normas:**

- El área de soporte deberá cumplir un programa regular para dar el mantenimiento preventivo a todo el equipo de cómputo propiedad del CPPCR.
- La persona técnica de soporte deberá evaluar, según sea el caso, si el equipo puede ser reparado en el área de trabajo o enviarlo a un taller autorizado para tal fin.
- Las personas usuarias deberán asegurarse de respaldar la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación.

PSI-0015 POLITICA DE CONTROL CONTRA CODIGO MALICIOSO.

1. **Política:**

Tanto el equipo de cómputo (hardware) como sus programas instalados (Software) y los datos, representan un valioso activo para la institución, por lo tanto se debe actuar con gran responsabilidad ante cualquier evento que ponga en riesgo estos activos.

2. **Responsabilidad:**

Es responsabilidad de todos las personas funcionarias del CPPCR que entren en contacto con un equipo de cómputo, evitar el ingreso de virus, malware, ad Ware o cualquier tipo de código malicioso que ponga en peligro el equipo y la información.

3. **Normas:**

- Para prevenir infecciones por virus informático, las personas usuarias no deben hacer uso de software que no haya sido proporcionado y validado por la Oficina de Tecnologías de Información.
- Las personas usuarias deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por la Oficina de Tecnologías de Información.
- 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.
- Ninguna perona usuaria, empleada o personal externo, podrá bajar o descargar software de sistemas, boletines electrónicos, sistemas de correo electrónico, de mensajería instantánea y redes de comunicaciones externas, sin la debida autorización de la Oficina de Tecnologías de Información.
- Cualquier persona usuaria que sospeche de alguna infección por virus de computadora, deberá llamar a la Oficina de Tecnologías de Información para la detección y erradicación del virus.
- Debido a que algunos virus son extremadamente complejos, ninguna persona usuaria debe intentar erradicarlos de las computadoras.

PSI-0016 POLITICA DE PRESTAMOS DE EQUIPOS EVENTOS INTERNOS DEL COLEGIO

1. **Política:**

El departamento cuenta con un presupuesto para brindar el soporte y prestamos de equipo para el uso de las actividades del Colegio de Profesionales en Psicología de Costa Rica.

2. **Responsabilidad:**

Es responsabilidad de la Oficina de Tecnologías de Información brindar la información y el cuido del equipo en préstamo lo cual será entregado a la persona que solicito dicho equipo de cómputo. Dando las indicaciones y asegurándose que el equipo va en excelente estado, la persona usuaria tendrá el cuidado y la responsabilidad del equipo una vez firmado la boleta de Salida.

3. **Normas:**

- Toda solicitud de reservación de equipo se efectuará a través del acceso web provisto por la Oficina de Tecnologías de Información.
- En encargado Soporte Técnico colocará los equipos en el espacio físico y en la hora indicados según solicitud de reservación.
- El usuario firmará la hora de entrega y préstamo del equipo.
- No está permitido la salida de los equipos de cómputo sin el llenado de la boleta de correspondiente y con la autorización de la Jefatura del área solicitante.
- Si el usuario durante el periodo de préstamo ocasionó algún daño sobre el equipo prestado será responsabilidad notificar a su jefatura lo cual informará a la Oficina de Tecnologías de Tecnologías, si el daño fue ocasionado por mal uso del equipo el costo de la reparación la asumirá el usuario.

PSI-0017 POLITICA SALIDA DE EQUIPOS DE LAS INSTALACIONES DEL COLEGIO

1. **Política:**

El departamento cuenta con un presupuesto para brindar el soporte y prestamos de equipo para el uso de las actividades del Colegio de Profesionales en Psicología de Costa Rica.

2. **Responsabilidad:**

Es responsabilidad de la Oficina de Tecnologías de Información brindar la información y el cuido del equipo en préstamo lo cual será entregado a la persona que solicitó dicho equipo de cómputo. Dando las indicaciones y asegurándose que el equipo va en excelente estado, la persona usuaria tendrá el cuidado y la responsabilidad del equipo una vez firmado la boleta de Salida.

3. **Normas:**
    - La persona usuaria solicitará la salida del equipo por medio del correo electrónico a la Oficina de Tecnologías de Información.
    - En la Oficina de Tecnologías de Información se les entregara la Boleta ya sea por el correo electrónico vía digital o en físico.
    - Con la entregada la boleta “FO-TI-010-PretamoEquipo” la persona usuaria tendrá que firmar la salida y después la entrega del equipo.
    - Si el equipo ocasionó algún daño sobre el equipo prestado será responsabilidad de notificar a su jefatura lo cual informara a la Oficina de Tecnologías de Tecnologías, si el daño fue ocasionado por mal uso del equipo el costo de la reparación la asumirá la persona usuaria.

PSI-0018 POLITICA DE CONTROL DE CÁMARA DE SEGURIDAD.

1. **Política:**

   El Colegio de Profesionales en Psicología de Costa Rica se cuenta con la seguridad y el sistema de Cámara de Seguridad Digitales que protege la vigilancia de los Colegiados y la persona que laboran en el CPPCR.

2. **Responsabilidad:**

Es responsabilidad de la Oficina de Tecnologías de Información tener y acatar la seguridad del monitoreo, grabación, respaldos, vigilancia que dicho Software y Hardware en excelente estado y funcionamiento.

3. **Normas:**

- El monitoreo se llevará en la caseta del guarda ubicada en la entrada principal del CPPCR al igual en las Oficina de Tecnologías de Información.

- Si un usuario desea ver una grabación de alguna cámara de seguridad tendrá que solicitar dicho permiso a la jefatura de la unidad solicitante el cual lo notificará a la Coordinadora de la Oficina de Tecnologías de Información.

- En caso que no se encuentre la jefatura, la persona usuaria se tendrá que comunicar con la Dirección Ejecutiva para dicho permiso.

- Se entregará el video y se instalara el Software para que el mismo puede ser reproducido, ya que se encuentra encriptado por seguridad y confiabilidad.

PSI-0019 POLITICA DE ACCESO REMOTO POR VPN.

1. **Política:**

   La política de uso de Red Privada Virtual (VPN por sus siglas en inglés), tiene como objetivo principal, ofrecer al funcionariado una guía sobre las características y requerimientos mínimos que deben ser cumplidos respecto del uso del servicio VPN institucional que provee el Colegio de Profesionales en Psicología de Costa Rica, como también las implicancias del mal uso.

   Es importante mencionar que el uso inapropiado de los recursos dispuestos para los usuarios autorizados, expone al Colegio a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas.

2. **Responsabilidad:**

   Sólo los usuarios previamente autorizados podrán utilizar los beneficios del Sistema VPN, los que además, serán los responsables del correcto uso del servicio de acceso remoto.

3. **Normas:**

- Es de responsabilidad del usuario con privilegios VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.
- La conexión remota mediante VPN no será configurados en equipos personales.
- Para la solicitud de acceso remoto por medio de VPN, el usuario llenará la boleta de solicitud con autorización de la jefatura correspondiente, en donde se especificar las fechas en las que requerirá el servicio.
- La Oficina de Tecnologías de Información configurará el equipo que utilizará el usuario, y efectuará las pruebas correspondientes para confirmar correcto funcionamiento del software dando una buena aprobación del uso.
- Una vez firmada la entrega de la boleta el Departamento se desactivaran los permiso en el servidor para dicha seguridad de la información.