COLEGIO DE PROFESIONALES EN PSICOLOGÍA DE COSTA RICA

POLITICAS Y ESTANDARES DE CONTROLES DE ACCESO LOGICO

COLEGIO DE PROFESIONALES EN PSICOLOGÍA DE COSTA RICA		
Elaborado por:	**Revisado por:**	**Aprobado por:**
Jefatura TI	Dirección Ejecutiva	Junta Directiva
Código: Código: PO-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			

Contenido

POLÍTICA

Cada persona usuaria es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario (userID) y contraseña (password) necesarios para acceder a la información y a la infraestructura tecnológica del Colegio de Profesionales en Psicología de Costa Rica, por lo cual deberá mantenerlo de forma confidencial.

1. Controles de acceso lógico

1.1 Todos las personas usuarias de servicios de información son responsables de su identificador de usuario y contraseña que recibe para el uso y acceso de los recursos.

1.2 Las personas usuarias no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica del Colegio, a menos que se tenga autorización del Departamento de Tecnologías de Información.

1.3 Cada usuario que accede a la infraestructura tecnológica del Colegio debe contar con un identificador de usuario único y personalizado, por lo cual no está permitido el uso de un mismo identificador de Usuario por varios usuarios.

1.4 Las personas usuarias tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

1.5 Las personas usuarias tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

1.6 Está prohibido que las personas usuarias utilicen la infraestructura tecnológica del Colegio de Profesionales en Psicología de Costa Rica para obtener acceso no autorizado a la información administrada en sus bases de datos o a los otros sistemas de información del Colegio.

1.7 Todas las personas profesionales consultoras externas que realicen actividades de manera conjunta con el personal el Colegio de Profesionales en Psicología de Costa Rica en lo que respecta la infraestructura tecnológica, requieren previamente obtener un permiso de la jefatura del área del Colegio donde estarán brindando la asesoría especializada o desempeñando la actividad por la cual fueron contratados, posteriormente, la jefatura del área, enviará un correo al Departamento de Tecnología de información justificando el motivo por el cual se les debe dar acceso a la infraestructura Tecnológica y el tiempo que requiere el acceso lógico.

2. Administración de privilegios

2.1 Cambio de roles o responsabilidades de un empleado

Cualquier cambio que requiera hacerse a los roles y responsabilidades de algún empleado en la temática de privilegios y accesos a la infraestructura tecnológica del Colegio de Profesionales en Psicología de Costa Rica, se debe ser solicitado vía correo electrónico dirigido a la Jefatura de Tecnologías de Información y enviando desde el correo oficial de la Jefatura o Coordinación del Área en la que esté adscrito el empleado

2.2 Equipo desatendido

- Activar protector de pantalla

La Oficina de Tecnologías de Información establecerá en cada equipo de cómputo una configuración de energía y suspensión con un tiempo de 10 minutos, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

- Apagar computadoras y recursos tecnológicos cuando termina la jornada laboral

Las personas usuarias deben apagar sus computadoras u otros recursos tecnológicos cuando hayan terminado su jornada laboral diaria con la finalidad de proteger los equipos ante eventuales cortes de energía eléctrica. (Computadora, Monitor, Mouse inalámbricos, Teclados inalámbricos, entre otros.)

2.3 Administración y uso de Passwords

- La asignación de la contraseña para acceso a la red y la contraseña para acceso a sistemas, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

- Cuando una persona usuaria olvide, bloquee o extravíe su contraseña deberá reportarlo por escrito o enviar un correo a la Oficina de Tecnologías de Información, indicando si es de acceso a la red o a los diferentes sistemas del Colegio, para que se le proporcione una nueva contraseña.

- Está prohibido que los identificadores de usuarios y contraseñas se encuentren en forma visible en cualquier medio impreso o escrito en el área de trabajo de la persona usuaria, de manera que se permita a personas no autorizadas su conocimiento.

- Todos los usuarios deberán observar los siguientes lineamientos para la construcción de sus contraseñas:

  - ❖ No deben ser números consecutivos
  - ❖ Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10), estos caracteres deben ser alfanuméricos, o sea, números y letras.
  - ❖ Deben ser diferentes a las contraseñas (passwords) que se hayan usado previamente.

- La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

- Toda persona usuaria que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarlo inmediatamente.

- Los cambios o desbloqueo de contraseñas solicitados por el usuario a Departamento de Tecnologías de Información serán solicitados mediante aprobación del jefe inmediato del usuario que lo requiere, enviando un correo electrónico Departamento de TI.

2.4 Control de accesos remotos

- Está prohibido el acceso a redes externas por vía de cualquier dispositivo, cualquier excepción deberá ser documentada y contar con el visto bueno de la Oficina de Tecnologías de Información.

- La administración remota de equipos conectados a internet no está permitida, salvo que se cuente con la autorización y con un mecanismo de control de

- Toda vez que se requiera realizar teletrabajo, el Departamento de Tecnologías de Información proveerá las herramientas y claves necesarias para que las y los trabajadores puedan tener la seguridad en sus equipos y respaldo de información de la organización.