GUÍA DE BUENAS PRÁCTICAS PARA UN TRATAMIENTO ADECUADO DE LOS DATOS PERSONALES Y SEGURIDAD DE LA INFORMACIÓN

COOPERATIVA DE AHORRO Y CRÉDITO COOPROGRESO LIMITADA

Contenido

1. Objetivo

El objetivo de esta guía es orientar a los colaboradores de la **Cooperativa de Ahorro y Crédito COOPROGRESO Limitada (COOPROGRESO)** en el tratamiento adecuado de los datos personales para garantizar el cumplimiento de la normativa de protección de datos personales y la protección de la información sensible

2. Alcance

El ámbito de aplicación abarca todas las actividades de colaboradores de la **COOPROGRESO** en las que, en virtud de sus tareas y funciones, se realice un tratamiento de datos personales. Mediante la adopción de las medidas descritas en este Manual, los colaboradores de la cooperativa contribuirán a proteger la privacidad y seguridad de los datos personales de manera efectiva.

3. Consideraciones generales

La protección de los datos personales y la seguridad de la información son aspectos fundamentales en el contexto de tratamiento de datos económicos y financieros, particularmente con relación al deber de sigilo bancario.

4. Documentos de referencia

Además de las disposiciones de carácter obligatorio contenidas en la Ley Orgánica de Protección de Datos Personales y su Reglamento, la COOPROGRESO ha diseñado los siguientes documentos para orientar el tratamiento de los datos personales:

4.1 Política de Privacidad: documento en el que se informa sobre cómo la Cooperativa recopila, utiliza y protege el conjunto de datos personales que tiene en su poder.

4.2 Política Corporativa de Protección de datos Personales: establece directrices y mecanismos para el tratamiento y protección de datos personales a fin de garantizar los derechos de las personas que tengan relación con la COOPROGRESO.

4.3 Procedimiento para requerimientos de protección de datos personales: regula la forma en la que tienen que atenderse las solicitudes de ejercicio de derechos en lo referente a sus datos personales de parte de los titulares.

4.4 Política para eliminación de documentos: establece directrices operativas para el almacenamiento seguro y la destrucción de los datos personales en poder de la COOPROGRESO, para cumplir con el principio de limitación del período de almacenamiento de datos.

4.5 Manual de Seguridad de la Información: establece las políticas que norman el uso adecuado de la información y los recursos informáticos, este documento sirve de consulta y será acatado por todos los colaboradores, directores y gerencias de Cooprogreso para el desarrollo de sus actividades.

5. Descripción de Buenas prácticas para tratamiento de datos personales de la COOPROGRESO

5.1. Obligaciones generales

a) Verificar que en todos los formularios (en papel o electrónicos) en que se recaben datos personales se incluye la cláusula de información relativa a la protección de datos.

b) Recabar datos estrictamente pertinentes, necesarios e imprescindibles para el uso o finalidad del tratamiento.

c) Desestimar los datos para otros usos o fines diferentes e incompatibles con el inicial para el que se recabaron o solicitaron del titular.

d) Acceder exclusivamente a aquella información personal o recursos técnicos que se precise y esté autorizado para el desarrollo de las funciones propias de la actividad profesional y no a otros datos o recursos, aunque estén disponibles y sean accesibles.

e) Guardar secreto profesional y confidencialidad de la información a la que se tiene acceso; nunca divulgues, publiques ni reveles datos de carácter personal a terceras personas.

f) Restringir comunicación de datos personales a terceros salvo que sea necesario para el tratamiento, por obligación legal o por consentimiento expreso del titular.

g) Impedir publicar listados en la página web o tablones de anuncios con nombres y apellidos y documentos de identificación/identidad completos sin anonimizar.

h) Impedir grabar ni difundir imágenes sin el previo y expreso consentimiento de los titulares.

i) Restringir enviar por emails archivos o ficheros con datos personales fuera del ámbito de la Cooperativa sin las medidas de seguridad que garanticen que dicha información solo sea accesible por su destinatario (p.ej. contraseña de acceso, cifrado de datos, etc.).

j) Borrar los datos personales, o bloquea su acceso, cuando ya no sea necesario su tratamiento o conservación para la finalidad para la cual se recabaron.

k) Cumplir todas las medidas de seguridad establecidas por la normativa en protección de datos, y demás requisitos aplicables conforme a las normas y procedimientos establecidos por la Cooperativa en el acceso y tratamiento de la información los usuarios.

l) Facilitar el ejercicio de los derechos a los titulares de los datos personales que lo soliciten, informando al Delegado de Protección de Datos Personales al correo: datospersonales@cooprogreso.fin.ec

m) Comunicar cualquier incidencia, vulneración o quiebra de seguridad en el tratamiento de los datos personales al correo: datospersonales@cooprogreso.fin.ec y a Seguridad de la Información reqseguridadinfo@cooprogreso.fin.ec

n) Asistir a la capacitación anual sobre protección de datos personales, impartida por el Delegado de Protección de Datos Personales.

5.2. Tratamiento de imágenes de titulares

a) Evitar la captura de rasgos físicos de menores de edad, personas incapaces o de grupos vulnerables durante cualquier evento organizado por la COOPROGRESO.

b) Solicitar el consentimiento informado de los socios (o de los padres/tutores en el caso de menores de edad invitados) antes de capturar, almacenar o utilizar su imagen o datos personales. Se debe tener constancia del consentimiento entregado, por lo que es importante almacenar los documentos en los que se haya proporcionado, sea este físico o digital.

c) Utilizar la imagen o los datos personales solo para el propósito específico para el cual se obtuvo el consentimiento. Evita usar esta información para otros fines sin autorización adicional, especialmente evita utilizar las imágenes para promoción de actividades de la institución si no se cuenta con el consentimiento de los titulares para ello.

d) Informar a la entrada de cualquier evento sobre la finalidad de grabar imágenes de los asistentes mediante carteles, paneles informativos, folletos u otros medios adecuados. Además, se debe facilitar la posibilidad de que el personal del evento pueda ser informado si algún asistente no desea ser fotografiado.

e) Advertir de que la Cooperativa tomará fotografías y/o grabará vídeos.

f) Repartir algún tipo de distintivo de color entre los asistentes que permita a los fotógrafos evitar a aquellos que no desean ser retratados.

5.3. Seguridad de la información: uso y configuración de los equipos

g) Comunicar que los equipos informáticos que la Cooperativa pone a disposición de sus empleados no deben ser utilizados para fines particulares o privados, tan solo se permite su uso para el desarrollo de tareas académicas, investigadoras o profesionales debiendo observarse en todo momento el deber de diligencia en la utilización del mismo.

h) Impedir modificar la configuración de los equipos informáticos ni el software instalados a nivel corporativo, ni conectar los puestos de trabajo a redes o sistemas exteriores ajenos a la Cooperativa, que no estén autorizados por los administradores del sistema.

i) Todos los equipos deberán mantener siempre actualizadas las aplicaciones informáticas y el antivirus correspondiente. No está permitida la desactivación de dichos mecanismos.

j) Activar el bloqueo automático de sesión de nuestros equipos cuando no se utilicen durante un tiempo determinado (p.ej. 5-10 minutos de inactividad)

k) Restringir la instalación de programas o software sin licencia o no corporativos en los ordenadores dado el peligro de que puedan contener programas malignos, como virus, troyanos o malware, conforme política establecida en el Manual de Seguridad de la Información.

l) Optar por almacenar en el disco duro o memoria de los ordenadores documentos que contengan datos de carácter personal utilizando preferentemente las carpetas de las unidades de red o el almacenamiento en la nube a través de OneDrive o Microsoft Teams. En caso contrario, los usuarios serán responsables de la custodia y respaldo de toda la información que almacenen en los mismos y deberán realizar periódicamente copias de seguridad, respaldo o *backups* de los ficheros. Conforme política establecida en el Manual de Seguridad de la Información.

m) Gestionar archivos temporales o las descargas de archivos que contengan datos personales se realizarán en un mismo directorio de forma que no queden dispersos por

todo el disco duro del ordenador para proceder periódicamente a su borrado cuando ya no sean necesarios.

n) Restringir salida equipos fuera de las instalaciones de la Cooperativa, excepto que estuviera previamente autorizado para ello y se apliquen las debidas medidas de seguridad para proteger su contenido y archivos. Conforme política establecida en el Manual de Seguridad de la Información.

o) Comunicar cualquier incidencia de funcionamiento o deficiencia de las aplicaciones informáticas que hubieran podido observar al responsable informático del centro, y/o al centro de atención a usuarios requser@cooprogreso.fin.ec

p) Notificar incidencia y/o deficiencia pudiera suponer una vulneración o quiebra de seguridad en el tratamiento de los datos personales, al correo datospersonale@cooprogreso.fin.ec y a Seguridad de la Información al correo reqseguridadinfo@cooprogreso.fin.ec a fin de que se adopten las medidas oportunas.

5.4. Control de cuentas de usuarios y contraseñas

a) Tanto las cuentas de usuario como los certificados digitales son personales e intransferibles y los usuarios deben ser conscientes de que son responsables de las acciones que se realicen con su identidad en los sistemas de información. En ningún caso, se deberán facilitar ni revelar a terceros u otros usuarios las claves, *password* o códigos (PIN, contraseña, etc.) que puedan ser necesarios para su acceso o activación debiendo mantenerlas en todo momento en secreto. Conforme política establecida en el Manual de Seguridad de la Información.

b) Salvaguarda claves privadas y contraseñas, debiendo informar a la mayor brevedad al centro de atención a usuarios reqseguridadinfo@cooprogreso.fin.ec cuando haya razones para creer que una contraseña ha sido robada, comprometida o compartida.

c) Evitar reutilizar las contraseñas utilizadas en las distintas aplicaciones de la COOPROGRESO en servicios proveedores de terceros o para usos privados y personales.

Cada usuario es responsable del control, confidencialidad y cambio de la contraseña de acceso a los equipos informáticos. Por tanto, se recomienda considerar el ANEXO 1 CARACTERISTICAS DE CONTRASEÑAS del Manual de Seguridad de la Información donde el cambio es cada 30 días.

- La contraseña deberá cambiarse cada 30 días y ser lo suficientemente larga y compleja para no ser predecible por terceros. Preferiblemente deberá contener al menos 10 caracteres, al menos una mayúscula, un signo especial y un número, de conformidad con el ANEXO 1 CARACTERISTICAS DE CONTRASEÑAS del Manual de Seguridad de la Información.
- Activar la autenticación de doble factor o multifactor (MFA) siempre que sea posible.
- Use un programa de gestión de contraseñas (p.ej. LastPass, Dashlane) para poder recordarlas y nunca las anote en una libreta o cuaderno.

5.5. Internet y cuentas de correo electrónico

a) Promover la utilización de Internet y el correo electrónico corporativo debe responder exclusivamente a fines profesionales, debiendo observarse el deber de diligencia en la utilización del mismo. Conforme política establecida en el Manual de Seguridad de la Información.

b) Restringir el acceso a páginas de intercambio y descarga de archivos P2P, redes sociales, correo electrónico personal, páginas web inseguras, así como otros sitios susceptibles de contener virus o favorecer la ejecución de código dañino. Conforme política establecida en el Manual de Seguridad de la Información.

c) Prohibir divulgación en internet, redes sociales, foros, etc. imágenes, videos o listados con nombres y apellidos y número de documento de identificación completos sin anonimizar (sin consentimiento expreso de los titulares o lo habilite una ley). Conforme política establecida en el Manual de Seguridad de la Información.

d) Restringir el envió por emails archivos o ficheros con datos personales sin las medidas de seguridad que garanticen que dicha información no sea inteligible ni manipulada por terceros durante la transmisión o que tan solo sea accesible por su destinatario (p.ej. contraseña de acceso, cifrado de datos, etc.)

e) Evitar el correo masivo no solicitado, también denominado "spam", como regla general, solo se debe dar nuestra dirección de correo electrónico a personas y/o entidades conocidas. Nunca se facilitará nuestra cuenta de correo electrónico en foros, redes sociales o páginas web no institucionales. Conforme política establecida en el Manual de Seguridad de la Información.

f) Comunicarse con el centro de atención de usuarios reqserguridadinfo@cooprogreso.fin.ec, en el caso de recibir correos electrónicos cuyo remitente y/o contenido sea dudoso.

5.6. La seguridad en los dispositivos móviles y smartphones proporcionados

a) Activar el desbloqueo del teléfono con contraseña o datos biométricos mejor que un patrón. Conforme política establecida en el Manual de Seguridad de la Información.

b) Mantener siempre el dispositivo, aplicaciones y los antivirus actualizados. Conforme política establecida en el Manual de Seguridad de la Información.

c) Desactivar la Wifi y el Bluetooth cuando no sean necesarios. No conectarse a redes Wifi-públicas y abiertas. Conforme política establecida en el Manual de Seguridad de la Información.

d) Modificar tu configuración de privacidad para limitar el acceso de las diferentes aplicaciones a tus datos. Esto se puede realizar al controlar los permisos que habilitas en la descarga de aplicaciones o apps.

e) Evitar descargar y guardar en el dispositivo archivos con datos personales o confidenciales. Si es necesario conservarlos, almacénalos en la nube en carpetas de OneDrive o protégelos con una contraseña de acceso. Conforme política establecida en el Manual de Seguridad de la Información.

f) Instalar o activar un servicio de localización para poder recuperar los dispositivos en caso de pérdida, extravío o sustracción. Conforme política establecida en el Manual de Seguridad de la Información.

5.7. Uso de dispositivos móviles o smartphones personales

a) Restringir que el personal administrativo guarde datos personales de socios, colaboradores o proveedores en dispositivos personales. Conforme política establecida en el Manual de Seguridad de la Información.

b) Mantener comunicaciones entre los colaboradores y socios deben realizarse exclusivamente a través de los medios proporcionados por la Cooperativa, como el correo electrónico institucional.

c) Evitar conectar tus dispositivos personales en los ordenadores corporativos. Solo el personal autorizado puede conectar dispositivos de acuerdo a la Política Institucional.

d) Evitar traslado información de ordenadores o dispositivos de la COOPROGRESO a tus dispositivos personales en ninguna circunstancia.

e) Utilizar exclusivamente el equipo proporcionado por la Cooperativa en caso de trabajo remoto, aprobado previamente por COOPROGRES, ya que cuenta con las configuraciones de seguridad requeridas. No está permitido el uso de equipos personales bajo ninguna circunstancia. Al finalizar la jornada, debe cerrarse la sesión de acceso remoto y bloquear o apagar el equipo.

5.7. Accesibilidad a los datos por personas no autorizadas

a) Custodiar la documentación y garantizar que los datos e información tratada desde su puesto de trabajo no pueda ser visible ni accesible por personas no autorizadas. Por tanto, considerar:
   - La pantalla del ordenador estará orientada para que la información sólo pueda ser visible por el usuario y no por terceras personas.
   - No deje a la vista documentos con datos personales sobre la mesa, fotocopiadoras o impresoras, etc.
   - Una vez que haya finalizado el trabajo, los documentos en papel no deben quedarse en la mesa y deberán guardarse bajo llave en su archivador correspondiente o se destruirán.
   - Cuando los usuarios dejen desatendido el ordenador deberán activar el sistema de bloqueo del que disponga su equipo (salvapantalla protegido por contraseña, bloqueo del terminal, etc.) con el fin de que se no visualicen datos en la pantalla, así como evitar que se acceda al equipo o aplicaciones por terceros no autorizados.

b) Verificar que el despacho quede cerrado con llave, el ordenador queda apagado cuando finalice sus actividades laborales para evitar que se acceda al equipo y no quedan sobre la mesa documentos que contengan datos de carácter personal.

5.8. Recomendaciones de seguridad para trabajo fuera de las oficinas o teletrabajo

a) Conectarse únicamente a redes seguras que requieren usuario y contraseña. Además, se debe utilizar la conexión VPN.

Existen restricciones de acceso mediante etiquetas y sitios configurados por el DLP, para garantizar la integridad y confidencialidad de los datos personales.

b) Restringir el transportar expedientes ni documentación en papel sin las correspondientes medidas de seguridad que garanticen su custodia y confidencialidad (p.ej. archivadores con llave). Siempre que sea posible y los medios lo permitan, se recomienda escanear la documentación para convertir los documentos en papel a soporte electrónico.

c) Restringir copiar y transportar información en ordenadores portátiles, smartphone, tabletas, discos externos, pendrive, etc. sin las correspondientes medidas de seguridad (contraseña de acceso, cifrado de datos, etc.).

d) Evitar que se puedan escuchar conversaciones por parte de terceros ajenos utilizando, por ejemplo, auriculares y micrófono o retirándose a un espacio en el que la persona empleada no esté acompañada.

e) Desconectar la sesión de acceso remoto y bloquear o apagar el uso del dispositivo en las pausas o concluida la jornada de trabajo, para evitar accesos no autorizados por parte de terceros y guardar los documentos que contengan datos de carácter personal.

5.9. Recomendaciones para la destrucción de información y soportes que contiene datos personales

a) Robustecer las precauciones para evitar arrojar hojas enteras o en trozos en papeleras a los que alguien podría acceder y recuperar la información de carácter personal.

b) Destruir la información que contenga datos de carácter personal, cualquiera que sea su soporte (ordenadores, CDs, USB portable o en papel) deberá ser de tal forma que no pueda ser recuperada ni manipulada por terceras personas utilizando preferentemente las máquinas destructoras.