Modelos de Protocolos

Ejemplos y guías que pueden ser adaptados a un Proyecto según sus necesidades o condiciones particulares

Guía y Comentarios:

- Estos modelos de protocolos son una guía, no es necesario que su proyecto siga exactamente este formato, pero sí deben cubrir el mismo *tipo* de contenido. El nivel de detalle o extensión de los protocolos lo determina el Proyecto.
- Los protocolos en cada proyecto deben reflejar las particularidades de este, pero si estos modelos se ajustaran a su programa, pueden utilizarlos de base editando la información pertinente.
- Aquí se presentan los modelos de protocolos separados por tema según se evalúan en la monitoría, pero en la práctica se pueden integrar si su proyecto entiende que es más clara su redacción o si un mismo protocolo escrito puede cubrir varios requerimientos.
- Algunos programas son parte de organizaciones más complejas, como Municipios, que ya tienen reglamentaciones o protocolos que pueden usarse como guía para que estén en cumplimiento con estos. En esos casos podría tener copia de dichas ordenanzas o reglamentaciones, o referirse a ellas en su protocolo.

Respecto a los Modelos a continuación:

- En los modelos a continuación la información que varía según su programa aparece [*subrayados en paréntesis*]. Si los utiliza de modelo se tiene que sustituir por la información correspondiente. *

Las sugerencias o comentarios adicionales estarán en burbujas de comentario como esta.

** Las burbujas de comentario se pueden referir a un segmento marcado, como aquí con el asterisco *.*

Protocolo De Colección De Datos De Los Participantes HMIS

- Objetivos:
  - Describe cómo se colecta la información de los participantes, dónde y cómo se guarda (sea física y/o digital).
  - Es un protocolo descriptivo del procedimiento, que deben conocer los empleados del proyecto para cumplir sus funciones.
  - Provee la guía que describe como se prepara un expediente de caso de los participantes.
  - **Nota**: *Este protocolo sería el más individualizado y diferente de proyecto en proyecto, debido a la variación en cantidad de personal, frecuencia de entrevistas, documentación requerida, estilos diferentes de preparar los expedientes, etc.*

Ejemplo:

La recolección inicial de datos estará a cargo de [*persona encargada*] mediante la entrevista inicial al participante. Esta información será recopilada en [*la hoja de entrevista*] y será guardada [*cómo/dónde/cuando los guarda*] posteriormente[1].

1- Aquí puede incluir si esta información pasa a alguna otra persona en la organización o cuán pronto la va a archivar.

La entrevista se realizará en [*lugar*] bajo las siguientes condiciones: [*con o sin acompañantes, si es durante una o más sesiones, etc.*]

El proceso de entrevista debe proveer un ambiente de privacidad para la información a discutirse con los participantes.

Se le solicitará al participante presentar los siguientes documentos durante la entrevista: [*listado de documentos personales que debe presentar participante para entrevistarse*] y se guardará copia de los siguientes solamente: [*listado de documentos de los que se guarda copia en expediente*]

Se le entregará al participante los siguientes documentos, [*listado de documentos a entregar*] y se le solicitará la firma al participante de los siguientes documentos: [*listado de documentos que debe firmar participante*][2]

2- Aquí puede especificar cuales documentos se lleva el/la participante y cuales se dejan en expediente físico.

Una vez realizada la entrevista, [*persona encargada*] creará o actualizará un expediente (si ya existe) para dicho participante no más tarde de [*en cuanto tiempo debe completarlo*]. El

expediente constará de las siguientes secciones (si alguna) [*Secciones*] y estas se compondrán de los siguientes documentos: [*documentos que lleva cada sección del expediente*]

La entrada de datos al sistema HMIS estará a cargo de [*persona encargada*] y se debe realizar dentro de [*período de tiempo*] luego de la entrevista inicial, y esta información deberá ser fiel y correspondiente a la recolectada en el proceso de entrevista.

Adicionalmente puede describir qué sucede con el expediente una vez creado y cualquier otra actividad que conlleve recolectar y almacenar datos, como si hay que realizar llamadas, seguimientos, etc.

Procedimiento De Monitoreo De Calidad De Datos de HMIS

Objetivos:

- Asegurar que los datos entrados en HMIS y los expedientes sean correctos y de buena calidad
- Fomentar que los datos cumplan con ciertas dimensiones para ser de buena calidad, como entrados a tiempo y estar vigentes, estar completos, ser precisos (sin errores), ser consistentes (utilizarse de la misma manera por diferentes empleados y para diferentes participantes)

Los detalles de implementación de este procedimiento varían según el tipo de proyecto: volumen de participantes, cantidad de personal disponible, tipo de expedientes creados, y otros factores.

Pueden usar como referencia el documento "Plan de Calidad de Datos" de la Coalición de San Juan y el CoC como guía para definir la calidad de los datos y para evitar errores.

Este procedimiento debe ser uno preventivo del Proyecto, y no puede ser únicamente esperar a los reportes de calidad de la Coalición, se refiere a esfuerzos adicionales.

Se puede guiar por el documento Plan de Calidad de Datos disponible en la página de la Coalición, sección de Documentos de HMIS.

***Nota**: En la Monitoria actual se pregunta acerca de este procedimiento pero no se pide ver una copia por escrito como los Protocolos. Aún así es más eficaz y beneficioso para la organización si desarrollan un procedimiento formal y documentarlo por escrito.*

Protocolo Para Velar Por La Información Protegida A Nivel Organizacional

Objetivos:

- Cumplir con principios de protección de información protegida en el transcurso de la operación normal del proyecto.
- Dejar claro qué tipo de información es la protegida de los participantes
- Establecer responsabilidades de personal al acceder esta información
- Enfatizar en que solamente las personas autorizadas pueden acceder expedientes

Ejemplo:

La información de los participantes de [*nombre del proyecto*] debe ser siempre protegida en todas las prácticas de la organización; sea esta información física (copias, fotos, documentos), escrita (formularios llenos), o digital.

Para lograr este propósito, se seguirán las siguientes prácticas:

Los expedientes de casos de los participantes siempre deben estar guardados en [*lugar seguro como archivo o cuarto designado*], y bajo llave. Las llaves para acceder los expedientes estarán custodiadas por [personas designadas] y no serán transferibles a otro personal no autorizado.

Los expedientes sólo se removerán de [*lugar seguro como archivo o cuarto designado*] para funciones de trabajo o atención al cliente por [*personal autorizado*], y serán devueltos a la mayor brevedad posible.[3]

3- Aquí puede abundar o especificar si hay reglas o procedimientos para mover o utilizar expedientes fuera del archivo; si se mueven a otra oficina, etc.

Preferible si puede incluir disposiciones claras respecto a quién puede acceder la información de los expedientes y para cuáles propósitos de trabajo.

El lugar de trabajo ofrecerá una posibilidad de privacidad razonable respecto a otras personas ver o escuchar la información manejada por [*personal designado]*, y serán responsables de observar prácticas de manejo responsable de la información para fomentar la privacidad durante el trabajo. Además, deberán cuidar el acceder la información de participantes en la computadora y no dejar la información a simple vista de otro personal. Evitar dejar documentos

o expedientes expuestos o no custodiados, y no comentar con terceras personas el contenido de los expedientes.

Prácticas de protección de información en formato digital (aparte de la información en HMIS): [4]

4- Pueden haber guías respecto a cual información (si alguna) se permite compartir por correo electrónico u otros medios electrónicos.

Nota: Para este Protocolo se puede usar de guía las responsabilidades descritas en los Avisos de Prácticas de Privacidad y en la Hoja de Consentimiento.

Protocolo Para Disponer De La Información Protegida (Datos Inactivos)

Objetivos:

- Proteger la privacidad de la información de los participantes aún cuando sus casos estén inactivos o cualquier información recopilada que no esté en uso activo (ejemplo copias o scans de documentos, fotos, etc.)
- Velar por la seguridad física de los documentos en expediente y cualquier otra información que haya sido recopilada.
- Establecer que la información de un caso cerrado o inactivo merece el mismo nivel de protección que uno abierto.

Ejemplo:

Una vez un caso es cerrado o pasa a ser inactivo, su expediente será guardado en [*lugar designado*][5] y debe protegerse de igual manera.

5- Este puede ser un archivo diferente, el mismo archivo, pero otra sección, etc.

Según la política de retención y decomisar expedientes, los expedientes serán retenidos por un período de [*tiempo que se retienen dichos expedientes*] para luego disponer de ellos [*en fecha o periodo indicado*]. Dicha disposición estará a cargo de [*persona, departamento, oficina designada*] mediante el siguiente proceso: [*especificar cómo realiza la disposición*][6]

6- Aquí puede mencionar si se trituran los expedientes, si lo hace personal interno o una compañía contratada, etc.

Cualquier información recopilada durante la entrevista de participante que no se incluya dentro del expediente físico será decomisada por [*persona indicada*] mediante [*método a usarse, borrando información en computadoras, triturando documentos físicos, etc.*]

***Nota**: Debe mencionar, si aplica, cómo se protege o elimina cualquier información física o digital adicional (fotos, scans, información que esté fuera del HMIS, si alguna) generada durante el proceso de crear el expediente o posteriormente.*

Nota: En proyectos pertenecientes a organizaciones más complejas como Municipios o Agencias de Gobierno se puede preparar este protocolo a tono con las políticas existentes

Protocolo Para Velar Por La Información Protegida En El Uso De HMIS

Objetivos:
• Cumplir con principios de protección de información protegida de los Participantes, en el contexto del Sistema HMIS: • Proteger la información entrada por los usuarios al sistema HMIS • Proteger la información generada por el HMIS en reportes generados por el mismo, impresos, capturas de pantalla, etc.

Ejemplo:

Para proteger la información de los participantes manejada en el sistema de HMIS, [nombre del proyecto] establece protocolos asociados al uso de los equipos, la protección de estos, y el manejo de los reportes producidos por el sistema. En adelante la frase "el sistema" se refiere específicamente a la plataforma de HMIS.

Protocolos para los usuarios de HMIS:

El sistema HMIS será utilizado únicamente por [*personal autorizado*], quienes habrán participado de los entrenamientos pertinentes y firmado los documentos de usuario correspondientes: Hoja Cuenta de Usuarios, Declaración de Usuario, Acuerdo de Confidencialidad y No Divulgación, Plan de Calidad de Datos.

El sistema HMIS será accedido mediante un navegador de web en la dirección indicada en los entrenamientos de HMIS.

Los usuarios de HMIS siempre protegerán la información de los participantes en el sistema observando las disposiciones del Protocolo [*nombre del protocolo para velar por la información en la Organización*] y adicionalmente tomarán las siguientes medidas de protección respecto al uso del HMIS:

Observarán siempre buenas prácticas de privacidad del equipo, credenciales, y accesos:

- Utilizarán el sistema de HMIS y accederán a información de expedientes o reportes únicamente para propósitos oficiales de trabajo[7]
- Su nombre de Usuario es su dirección de email registrada con HMIS/Coalición de SJ
- Su contraseña de HMIS será siempre privada:
    - Nunca se comparte, con nadie, incluyendo supervisores o compañeros.
    - No se escribe en notas o lugares visibles.
    - No se deja grabada en el navegador de web.
    - Si se le olvida o entiende que alguien puede haberla visto, se debe cambiar de inmediato.

- Protegerá siempre las pantallas de las computadoras cuando sea visible el HMIS, ya sea en uso o en inactividad, para evitar que personas no autorizadas vean la información contenida en las bases de datos o reportes.
- Utilizará en su computadora un "Lock Screen" activado automáticamente a [*cuantos minutos*] o menos que requiera contraseña para desactivarlo[8].

8- El "Lock Screen" es algo que podría estar manejado por IT de la oficina en lugar del usuario en algunos casos.

- Observar buenas prácticas de manejo de credenciales de las computadoras[9]
    - Nunca revelar o compartir su contraseña
    - No dejarla escrita en notas o papeles en el escritorio o cerca
    - Si se le olvida o entiende que alguien puede haberla visto, se debe cambiar de inmediato.

9- *Estos credenciales los establece el administrador de la computadora. Las prácticas deben ser reglas parecidas las de protección de la contraseña de HMIS, con la excepción de que en ciertos casos la contraseña de la computadora se comparte entre más de un usuario con autorización de la administración del proyecto.*

Protocolos de Manejo de los Reportes Generados por HMIS (*cómo y a quien se puede compartir información*)

El Proyecto debe establecer reglas respecto a imprimir contenido de HMIS, hacer capturas de pantalla, o de cualquier otra manera extraer información de los expedientes electrónicos.

Puede especificar otras disposiciones relevantes respecto a manejo de esa información, si se puede compartir y con quien, bajo cuales condiciones, en acorde con el Protocolo de Protección de Información a Nivel Organizacional.

Ejemplos: el uso de listados o bitácoras de personas que han accedido los expedientes

Protocolos de Protección de los Equipos usados para acceder HMIS de HMIS:

Se observarán buenas prácticas de protección de los equipos de computadora, como:

- Usar siempre Firewall, Antivirus, y Antispyware en modo activos (en modo automático) en computadoras[10]
- Mantener siempre Firewall, Antivirus, y Antispyware actualizados en computadoras[11]
- Contar con navegador de internet actualizado y evitar extensiones de navegador peligrosas.
- Los equipos de computadora se utilizarán y guardarán siempre en lugar seguro, bajo llave.

10- Cuando la PC es de la Coalición, tiene asistencia en este renglón.

11- El Firewall podría estar a nivel del servidor de la oficina y ser manejado por departamento de IT de su Proyecto

Protocolo Para Uso De HMIS Fuera Del Área De Trabajo

Objetivos:

- Establecer los pasos a seguir para un uso responsable y seguro del HMIS cuando los equipos no estén dentro de la oficina del proyecto.
- Cubrir todo tipo de dispositivos que se usen fuera de la red del trabajo, sean móviles (laptops o tabletas) o fijos (computadoras de escritorio).
- Cumplir con todas las mismas disposiciones del protocolo de HMIS añadiendo precauciones o aspectos relativos a uso remoto o móvil.

Ejemplo:

Los usuarios del sistema HMIS deberán seguir las mismas medidas de uso de equipos y seguridad cuando utilicen el sistema fuera del área de trabajo que las especificadas en el Protocolo [*nombre del protocolo para velar por la información en HMIS*] y en adición, cumplir con las siguientes disposiciones:

Los usuarios están autorizados a utilizar los siguientes dispositivos para acceder HMIS: [*establecer si el proyecto autorizará usar computadoras/tabletas personales o va a proveer equipo específico*], los cuales deben contar con las mismas protecciones de seguridad especificadas en el Protocolo [*nombre del protocolo para velar por la información en HMIS*].

Debe siempre utilizar una red de internet con seguridad (con contraseña) y evitar siempre el uso de redes abiertas públicas[12].

12- Aquí puede especificar si adicionalmente sólo se autoriza el uso de ciertas redes, cómo Wi-Fi hotspots provistos por la organización.

Los usuarios serán responsables de proteger físicamente dichos equipos para evitar robos (en un lugar público, de un auto, etc.) y deben observar prácticas de uso responsable para fomentar la privacidad durante el trabajo, como evitar acceder información de participantes a simple vista del público, o comentar con terceras personas el contenido de los expedientes.

Nota:** Si el proyecto no autoriza el uso de HMIS fuera del área de trabajo, esto debe estar mencionado por escrito en este protocolo o en el protocolo de protección de información en el HMIS**, pero no se puede dejar abierto a interpretación si está autorizado o no.