Como se actualizará la información para la gestión de conocimiento

Para esto se utilizarán algunas estrategias para que se pueda realizar la autoevaluación de la información, estas estrategias serían:

**-Integración con Fuentes de Datos en Tiempo Real:**

Conecta el sistema de telemedicina con fuentes de datos en tiempo real, como dispositivos médicos conectados, registros médicos electrónicos y bases de datos de salud. Esto permite que los datos se actualicen automáticamente a medida que cambian, sin necesidad de intervención manual.

**-Alertas y Recordatorios de Actualización:**

Implementa alertas y recordatorios automáticos para el personal médico y los administradores del sistema, indicando cuándo es necesario actualizar información crítica. Por ejemplo, se pueden programar alertas para revisar y actualizar registros médicos de pacientes de manera regular.

**-Actualización de Guías Clínicas:**

Si el programa de telemedicina utiliza guías clínicas, establece un proceso para revisar y actualizar regularmente estas guías con las últimas recomendaciones médicas y evidencia científica.

**-Feedback de Usuarios y Profesionales de la Salud:**

 Permite a los usuarios, médicos y otros profesionales de la salud proporcionar retroalimentación sobre la calidad de los datos y la información.

**-Capacitación Continua:**

Dar una capacitación continua al personal médico y los usuarios finales sobre cómo utilizar el sistema y cómo acceder a la información más actualizada y cada cambio que se haga.

**-Auditorías y Revisiones Periódica:**

 Realiza revisiones periódicas de la información almacenada en el sistema para garantizar su precisión y actualización.

Niveles de protección de seguridad

**-Auditoría y Registro de Actividades:**

Lleva un registro de todas las actividades en el sistema para rastrear el acceso y las acciones realizadas por los usuarios. Esto permite la detección temprana de posibles amenazas.

**-Actualizaciones de Software y Parches:**

Mantén el software y los sistemas operativos actualizados con los últimos parches de seguridad para abordar vulnerabilidades conocidas.

**-Entrenamiento de Usuarios:**

Proporciona capacitación a los usuarios para concientizarlos sobre las prácticas de seguridad y fomentar la responsabilidad en la protección de datos.

**-Gestión de Contraseñas:**

Establece políticas de contraseñas sólidas que requieran contraseñas seguras y cambios regulares de contraseñas.

**-Evaluación de Riesgos y Pruebas de Vulnerabilidad:**

Realiza evaluaciones de riesgos y pruebas de vulnerabilidad periódicas para identificar y abordar posibles debilidades en el sistema.

**-Autenticación y Autorización de Usuarios:**

Implementa un sólido sistema de autenticación, como la autenticación de dos factores, para garantizar que solo usuarios autorizados tengan acceso al sistema.

Asigna roles y permisos específicos a los usuarios para limitar su acceso a la información.

**-Seguridad en el Almacenamiento de Datos:**

Almacena los datos médicos de manera segura en servidores con medidas de seguridad física y lógica, como firewalls y sistemas de detección de intrusiones.