Golgi

Innovación Tecnología

PROPUESTA ANTIVIRUS, CONSENTIMIENTO INFORMADO Y HARDWARE

HOSPITAL SANTA TERESITA PÁCORA

Agosto 3 de 2026



Pacora, 01 de agosto de 2026

Doctor

BRYAN SALDARRIAGA MOLINA

Gerente ESE HOSPITAL SANTA TERESITA

PACORA, CALDAS

CRA 2 # 2-49

Cordial saludo,

De antemano queremos agradecerle por su amable invitación a presentar nuestros servicios.

Esperamos que nuestra propuesta resulte de interés para ustedes y podamos acompañarlos en sus proyectos de presencia y evolución en medios digitales.

Atentamente,

Cordialmente,

Juan Pablo Suárez Martinez

Gerente General

Móvil: 317 432 72 14

gerencia@golgi.com.co

www.golgi.com.co

Golgi
Innovación Tecnología

Contenido

Perfil Empresarial 4

¿Quiénes Somos? 4

Oferta De Valor 4

Médula Tecnológica 4

Metodología 5

Características 5

Ventajas 6

Fase de Descubrimiento 6

Fase de Implementación 6

Entendimiento de la Necesidad 7

Objetivo General 8

Objetivos Específicos 8

Características Técnicas 8

Propuesta económica 13

Perfil Empresarial

¿Quiénes Somos?

Golgi se fundó por equipo multidisciplinario que quiere probar que las organizaciones y las personas que las habitan no necesitan hacer altas inversiones en tecnologías de última generación para contar con soluciones de valor; y que las experiencias en la gestión pueden ser mejores, más rápidas y eficientes.

Oferta De Valor

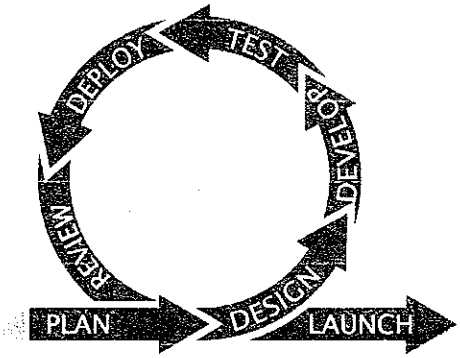
Soluciones para la gestión inteligente y eficaz de las organizaciones, con plataformas, servicios y herramientas tecnológicas de última generación.

- Consultoría para implementación de soluciones tecnológicas.
- Plataformas de gestión integral de procesos empresariales.
- Automatización de procesos críticos de negocio.
- Plataformas para la gestión del conocimiento (E-Learning + E-Training).
- Recursos virtuales de aprendizaje - Gamificación.
- Analítica.

Médula Tecnológica

- Movilidad
- Experiencia de usuario
- Infraestructura en la nube en alta disponibilidad
- Seguridad
- Analítica

Metodología



Nuestra visión de la transformación digital está fundamentada en las personas por encima de las tecnologías habilitadoras, sin embargo, no es viable dejar de lado los componentes tecnológicos como factores clave en el éxito del proyecto. Nuestra experiencia nos indica que los factores de éxito se enmarcan en:

- Elegir los habilitadores tecnológicos adecuados (Herramientas – Plataforma).
- Manejar un enfoque metodológico claro.
- Gestionar el proyecto incluso tras la salida en vivo.
- Incorporar mecanismos de QA.

La metodología utilizada por Golgi es una metodología con un enfoque simple al utilizar métodos ágiles, comenzando a entregar funcionalidades de manera incremental de la solución dentro de las primeras semanas de trabajo.

Características

Sus principales características son:

- Mezcla de metodologías de proyectos "Waterfall" y "Agile" tomando como punto de partida el diseño de proceso y la especificación detallada de requisitos.
- La implementación se realizará a través de "sprints" iterativos, cada uno considerando pruebas y puntos de control tempranos y frecuentes.
- Identifica y capitaliza numerosas funcionalidades out-of-the-box de las plataformas seleccionadas para la solución.
- Evita la re-ingeniería y minimiza la sobrecarga del proyecto.

Trabajaremos conjuntamente con Mandato S.A.S. mediante sesiones de trabajo (workshops) para entender el detalle de los requisitos del negocio, realizaremos propuestas al cliente en caso de diferentes alternativas, obtendremos feedback y promoveremos un entorno de trabajo colaborativo focalizado en proporcionar los mejores resultados posibles.

Ventajas

Algunas de las ventajas de este enfoque son:

- La configuración **iterativa** proporciona al cliente la posibilidad de identificar beneficios de forma temprana conforme se realizan entregas de funcionalidades específicas mientras el producto continúa su desarrollo.
- Incrementa la **visibilidad** hacia las partes interesadas al permitir la gestión efectiva de expectativas.
- Las pequeñas versiones **incrementales** ayudan a los owners de producto y de procesos a identificar problemas de forma temprana y facilitan la tarea de adaptarse a los cambios.
- Las pruebas están integradas en los sprints de configuración, permitiendo **la inspección recurrente** conforme la solución evoluciona.

Fase de Descubrimiento

El Proyecto se iniciaría con una reunión de kick-off, sesión en la que los equipos de trabajo se conocen y revisan conjuntamente el alcance, el plan de Proyecto y el enfoque, garantizando alineación de todos los miembros del equipo.

Después del kick-off, se realizarán sesiones de trabajo de descubrimiento y levantamiento de requerimientos, previos a los sprints de implementación, centrados en los módulos del alcance y las facilidades bridadas por la solución elegida.

Los requerimientos identificados en los workshops se registrarán como historias. Estas proporcionarán el detalle requerido para construir la funcionalidad durante los sprints y marcarán la cantidad de actividad requerida para cada entregable.

Fase de Implementación

La implementación de las funcionalidades se realizará a través de Sprints, cada uno de ellos con una duración variable que normalmente será de 2 o 3 semanas.

Se denomina sprint a cada ciclo o iteración de trabajo que produce una parte del producto terminada y funcionalmente operativa (incremento).

El número de sprints, la duración de cada uno de ellos y las historias de usuario que se abordarán en los mismos se decidirá durante una actividad de preparación previa al inicio de los despliegues en la que, en base a las necesidades de negocio del cliente y a sus prioridades se determinarán cuáles serán las funcionalidades que se incorporarán al producto final en cada sprint, en forma de "historias de usuario".

Tras la actividad de preparación se dará respuesta a los siguientes aspectos: qué se le entregará al cliente al término de cada sprint y cuál será el equipo de trabajo asignado a cada uno en función de la carga de trabajo necesaria para realizarlo.

Cada sprint comenzará con una reunión inicial de todo el equipo de proyecto. En esta reunión se partirá de las "historias de usuario" asignadas inicialmente al sprint, se analizarán sus prioridades y se asignarán a los miembros del equipo.

Durante la ejecución de cada sprint se podrá planificar una reunión diaria de revisión y sincronización de los trabajos, con el objetivo de analizar el trabajo completado el día anterior y revisar el trabajo planeado para el día actual, evaluando la velocidad del sprint (progreso del desarrollo) e identificando cualquier elemento bloqueante.

La funcionalidad se desarrolla de esta manera de forma iterativa, siendo realizadas para cada historia de usuario pruebas unitarias. Al final de cada sprint, habrá un incremento tangible en el desarrollo de cada aplicación que estará disponible para pruebas de usuario (UAT – User Acceptance Test).

Entendimiento de la Necesidad

Para la ESE Hospital Santa Teresita de Pácora Caldas se comprende la necesidad de implementar una solución de antivirus corporativo debido a los riesgos crecientes de ciberamenazas como malware, ransomware y ataques de phishing, los cuales pueden afectar la continuidad operativa, la confidencialidad de la información y la integridad de los sistemas institucionales. Contar con protección en los equipos y servidores, junto con una administración centralizada, permite prevenir infecciones, detectar comportamientos sospechosos oportunamente, reducir incidentes de seguridad y asegurar el cumplimiento de buenas prácticas y requisitos de control, garantizando un entorno tecnológico más confiable para los usuarios y los procesos misionales.

Objetivo General

Adquirir e implementar una solución de antivirus corporativo para 150 licencias, con administración centralizada, que permita fortalecer la seguridad de la información, prevenir y mitigar amenazas informáticas, y garantizar la continuidad operativa de los equipos y servicios tecnológicos de la ESE Hospital Santa Teresita de Pácora, Caldas.

Objetivos Específicos

- Proteger los equipos de cómputo y endpoints institucionales contra malware, ransomware, phishing y otras amenazas, mediante mecanismos de detección y prevención multicapa.
- Implementar una consola de administración centralizada que facilite el despliegue, la configuración de políticas, el monitoreo y la generación de alertas en tiempo real.
- Estandarizar políticas de seguridad (actualizaciones, análisis programados, control de dispositivos, exclusiones y cuarentena) para asegurar una protección homogénea en toda la organización.
- Reducir la probabilidad de incidentes de seguridad y la superficie de ataque, mejorando la capacidad de detección temprana y respuesta ante eventos.
- Garantizar la actualización permanente de firmas y motores de detección, asegurando la vigencia de la protección frente a nuevas amenazas.
- Generar reportes periódicos de estado, cumplimiento y eventos de seguridad que soporten auditorías, controles internos y toma de decisiones.
- Asegurar la compatibilidad y el adecuado desempeño de la solución en los sistemas operativos y aplicaciones institucionales, minimizando impactos sobre la operación.

Caracteristicas Técnicas

Kaspersky Next EDR Foundations ofrece una protección avanzada y simplificada para endpoints, brindando seguridad contra ransomware, *malware* sin archivos y amenazas emergentes. Su administración intuitiva permite una gestión eficiente de la ciberseguridad empresarial.

Características Principales

- Protección Avanzada de Endpoints: Supervisa todos los dispositivos de la red para una cobertura completa del sistema.
- Controles de Seguridad Esenciales: Acceso completo a herramientas de protección a través de una consola intuitiva.
- Análisis de Causa Raíz: Investigaciones exhaustivas de ciberataques para evaluación de vectores y respuesta efectiva.
- Seguridad con Aprendizaje Automático: Protección proactiva contra amenazas conocidas y desconocidas.
- Visibilidad Completa de Amenazas: Monitoreo constante de endpoints con detección en la nube y evaluación de vulnerabilidades.
- Control Web, de Aplicaciones y Dispositivos: Prevención de accesos no autorizados y riesgos externos.

Beneficios para su Empresa

- Implementación rápida y sencilla sin necesidad de conocimientos avanzados en ciberseguridad.
- Protección avanzada sin impacto en el rendimiento de los equipos.
- Cumplimiento con estándares de seguridad y mejores prácticas de protección de datos.
- Optimización de recursos de TI con una solución eficiente y confiable.
- Análisis forense de amenazas y respuesta efectiva ante incidentes.

Kaspersky Next EDR Optimum esencial para proporcionar una protección avanzada en endpoints, con capacidades de detección y respuesta frente a amenazas evasivas, administración centralizada, y soporte de seguridad en la nube. Esta solución está diseñada para proteger los activos digitales de **HOSPITAL SANTA TERESITA DE PÁCORA** ante amenazas actuales y futuras, optimizando la gestión de la seguridad y los recursos disponibles.

Componentes de la solución

Protección de Endpoints

- **Antivirus**: Protección avanzada para archivos, navegación web y correos electrónicos.
- **Protección de Red**: Monitoreo y control de tráfico malicioso con prevención de exploits y detección de comportamiento.
- **HIPS (Sistema de Prevención de Intrusiones en el Host)**: Monitoreo y control de actividades sospechosas a nivel de sistema.
- **Prevención y Corrección de Amenazas**: Medidas automatizadas de prevención y remediación para detener y mitigar ataques.

Gestión de la seguridad

- **Firewall**: Protección perimetral en dispositivos de endpoint.
- **Control de Aplicaciones, Dispositivos y Web**: Restricciones para limitar accesos no autorizados y garantizar el cumplimiento de políticas de uso.
- **Administración de Dispositivos Móviles (MDM)**: Gestión y protección de dispositivos móviles corporativos.

Escenarios de TI

- **Evaluación de Vulnerabilidades y Administración de Parches**: Identificación y aplicación de parches para mantener la seguridad actualizada.
- **Eliminación de Datos y Conexión Remota**: Borrado seguro de datos sensibles y acceso remoto controlado.
- **Inventario de Software y Hardware**: Gestión de activos y recursos.
- **Instalación de Sistemas Operativos y Aplicaciones**: Implementación y actualización de software en endpoints.

Cifrado

- **Cifrado de Datos**: Protección de la información mediante cifrado en dispositivos y administración centralizada del cifrado.

Seguridad en la nube

- **Descubrimiento y Bloqueo en la Nube**: Identificación de riesgos en entornos de nube y prevención de accesos no autorizados.
- **Seguridad Integral**: Protección de cargas de trabajo en la nube, adaptándose a entornos virtualizados y físicos.

Capacitación en ciberseguridad

- **Formación para Administradores de TI**: Capacitación en mejores prácticas de seguridad y uso de la solución.

Capacidades de EDR (Endpoint Detection and Response) Esencial

- **Análisis de Causas Raíz**: Evaluación de incidentes para identificar la fuente y prevenir recurrencias.
- **Análisis de Indicadores de Compromiso (IoC)**: Evaluación de riesgos de seguridad mediante IoCs.
- **Respuesta de Endpoint**: Acciones automáticas para proteger frente a amenazas detectadas.
- **Visibilidad y Análisis Visual**: Herramientas intuitivas para comprender el alcance de las amenazas y su mitigación.

Ventajas principales de la solución

- **Prevención de Amenazas Diversas**: Protección proactiva contra malware, ransomware, spyware y otras amenazas.
- **Detección y Respuesta Rápida**: Automatización de respuestas ante incidentes y análisis detallado de amenazas.
- **Ahorro de Recursos**: Simplificación de tareas de seguridad mediante una consola unificada en la nube o local.
- **Escalabilidad y Compatibilidad**: Adaptable a entornos virtuales, físicos y cargas de trabajo en la nube.
- **Verificación de Funcionalidad Completa en Endpoints**: Garantía de que todos los dispositivos están protegidos y gestionados correctamente.

- **Validación de Seguridad en Tiempo Real**: Monitoreo efectivo y remediación de incidentes.

- **Capacitación Completada**: Formación a los administradores de TI y entrega de la documentación correspondiente.

SOFTWARE DE CONSENTIMIENTO INFORMADO

El consentimiento informado es un pilar fundamental de la atención médica ética y legalmente adecuada. La transformación digital de los procesos hospitalarios permite optimizar esta práctica mediante el uso del **consentimiento informado digital (CID)**. Esta propuesta busca implementar una solución digital para garantizar un consentimiento informado ágil, seguro, trazable y centrado en el paciente en el Hospital Santa Teresita de Pacora.

OBJETIVOS

- Modernizar el proceso de consentimiento informado mediante plataformas digitales seguras.
- Asegurar la comprensión del paciente sobre su diagnóstico, tratamiento, riesgos, beneficios y alternativas.
- Cumplir con los requerimientos legales de la República de Colombia y normativas éticas internacionales.
- Facilitar la trazabilidad y archivo digital de los consentimientos otorgados.

ALCANCE

Este sistema se aplicará inicialmente en las siguientes áreas:

- Medicina General
- Odontología
- Procedimientos menores
- Urgencias
- Hospitalización
- Medicina Especializada

Posteriormente podrá extenderse al resto de los servicios hospitalarios.

CARACTERÍSTICAS DEL CONSENTIMIENTO INFORMADO DIGITAL

- **Formato electrónico** accesible desde tabletas o computadoras en todos los servicios.
- **Firma digital o biométrica** del paciente y del profesional de salud.
- **Lenguaje claro y comprensible**, con opción de audio o video explicativo.

- **Seguridad y confidencialidad**, conforme a la Ley 1581 de 2012 de Protección de Datos Personales de Colombia.
- **Almacenamiento en historia clínica electrónica (HCE)** del paciente.
- **Registro de fecha y hora** de aceptación, con copia digital entregada al paciente.

PROCESO DE CONSENTIMIENTO DIGITAL

1. **Ingreso al sistema** (por el profesional de salud autorizado).
2. **Revisión de la información por el paciente**, con posibilidad de aclarar dudas.
3. **Confirmación del entendimiento**, con casillas de verificación.
4. **Firma digital o biométrica** del paciente (y representante si aplica).
5. **Validación por el profesional de salud.**
6. **Generación automática del documento firmado**, con copia para el paciente y respaldo en la HCE.

ASPECTOS LEGALES Y ÉTICOS

- Cumplimiento con la **ley 1752 de 2015** sobre derechos y deberes de los pacientes.
- Adaptación a la **Ley 1581 de 2012** sobre protección de datos personales.
- Supervisión del proceso por el **Comité de Ética del Hospital**.

VENTAJAS ESPERADAS

- Ahorro de papel y espacio físico.
- Mejora en la comprensión y participación del paciente.
- Reducción de errores o pérdidas de documentación.

Propuesta económica

Ítem	Solución	Cantidad	Valor unitario	Subtotal
1,1	1Kaspersky Small Office Security 25-49 Mobile device; 25-49 Desktop; 3-5 FileServer; 25-49 User 1 year Base License	150	**$ 135.512**	**$ 20.326.800**
1,2	DISCO DURO SSD SATA 2.5 512 GB	12	**$ 503.333**	**$ 6.040.000**

1,3	DISCO DURO EXTERNO 2 TERAS ANTIGOLPES	2	**$ 535.000**	**$ 1.070.000**
1,4	TARJETA LOGICA EPSON L4260	1	**$ 290.000**	**$ 290.000**
1,5	KIT GOMAS DE ARRASTRE EPSON L3210	10	**$ 98.000**	**$ 980.000**
1,6	COMO TECLADO MOUSE ALÁMBRICO	5	**$ 105.000**	**$ 525.000**
1,7	SERVIDOR NAS DE RED SYNOLOGY DISKSTATION DS225+ DE 2 BAHÍAS CON 2 DISCOS SATA DE 10TB CADA UNO	1	**$ 12.000.000**	**$ 12.000.000**
1,8	SOFTWARE CONSENTIMIENTO INFORMADO	1	**$ 15.500.000**	**$ 15.500.000**

VALOR TOTAL: $ 56.731.000

VALORES EXENTOS DE IVA LICENCIAMIENTO ANTIVIRUS

HARDWARE Y SOFTWARE CONSENTIMIENTO INFORMADO IVA 19%.

FORMA DE PAGO

50% ANTICIPO, 50% CONTRA ENTREGA

VALORES AGREGADOS

✓ Incluye consola Web

✓ 300 licencias gratis para proteger dispositivos móviles (Celulares o Tabletas).

✓ 225 licencias gratis para proteger buzones de correo electrónico Microsoft 365. Solo aplica para Next Optimum.

✓ 24 usuarios para capacitación CITO (Cibersecurity for IT Online). Aplica para Optimum.

✓ Inducción vía teams al personal necesario para aprender las generalidades del funcionamiento de la consola.

✓ Soporte directo con el Fabricante durante el periodo que se encuentre activa la licencia.

✓ La licencia servidor se cobra al mismo costo que una licencia de PC y se puede instalar tanto en PCs como en servidores.

✓ Soporte directo con el Fabricante durante el periodo que se encuentre activa la licencia.

FORMA DE PAGO: 50% anticipo, 50% entrega a satisfacción.

JUAN PABLO SUÁREZ MARTÍNEZ

Gerente

CC 98667940

Cel: 317 432 7214