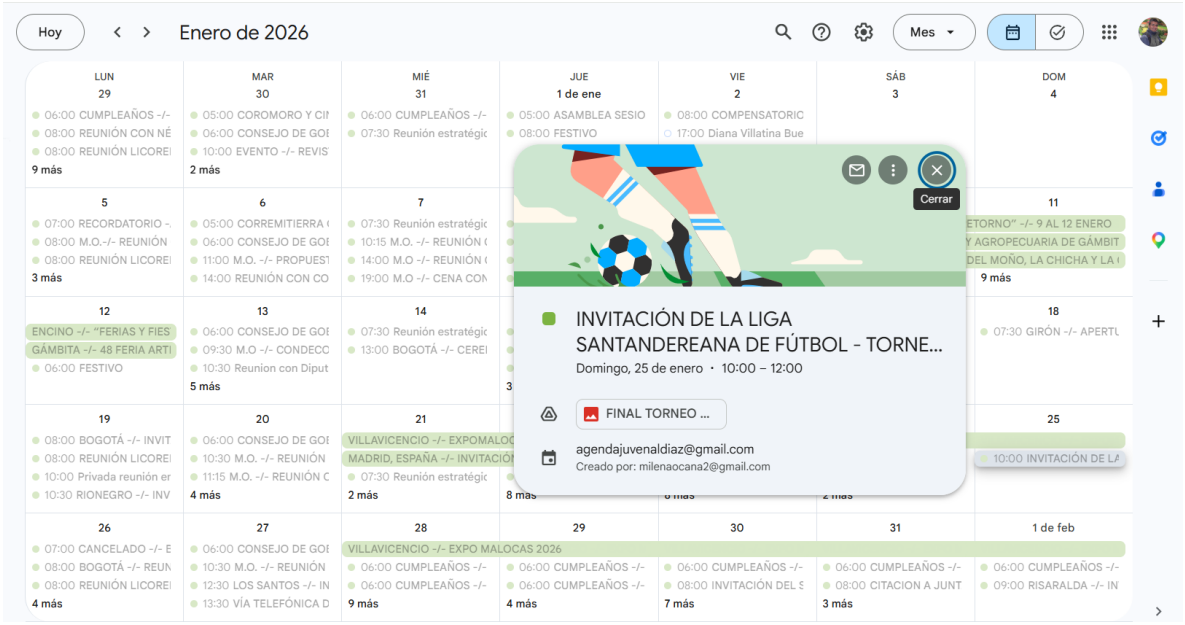
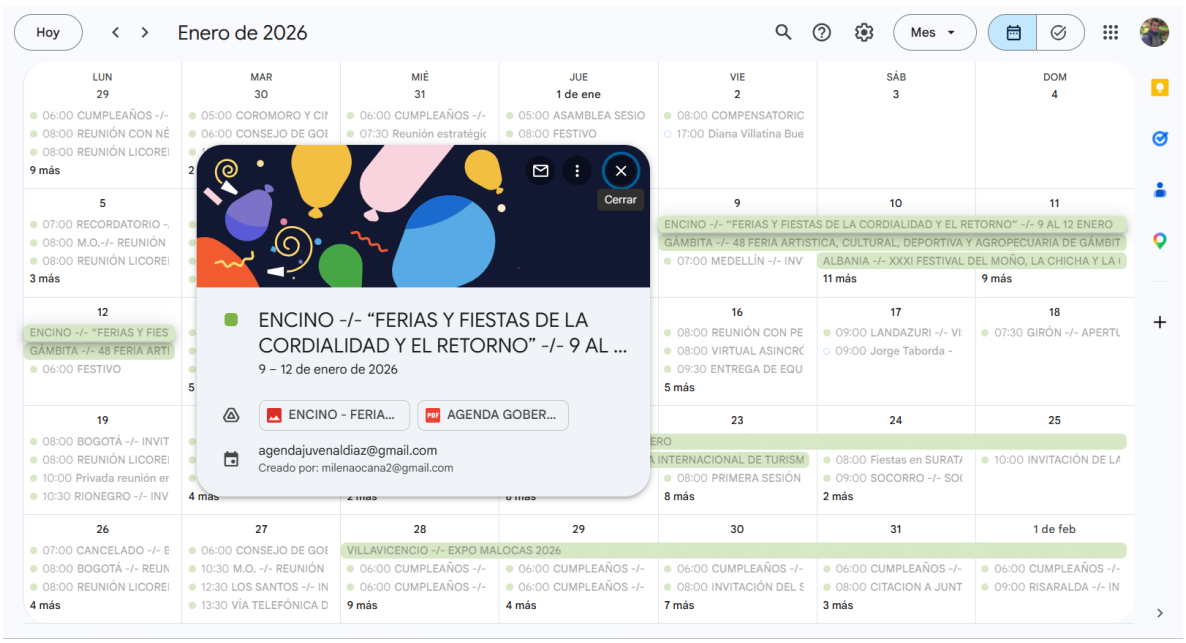
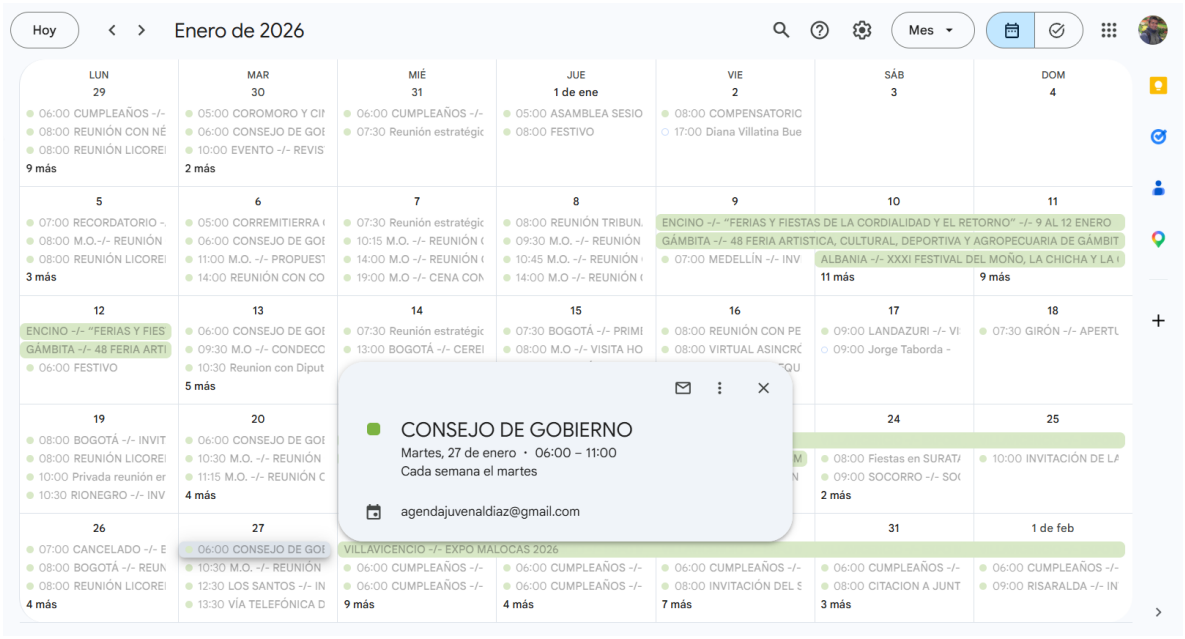
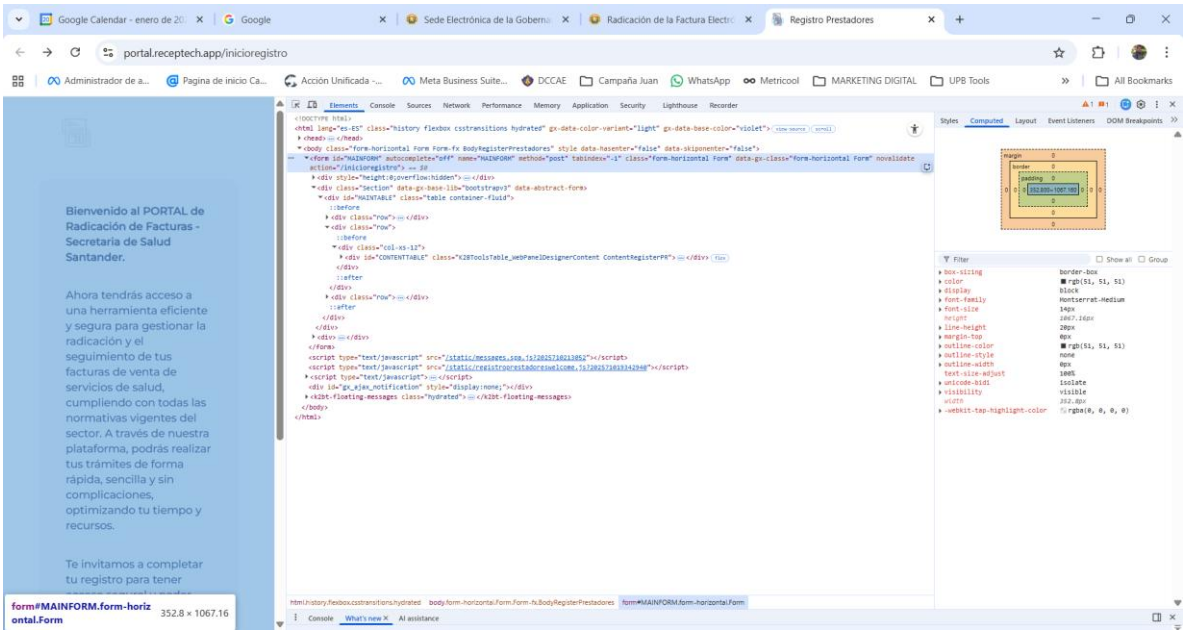
EVIDENCIAS DEL CONTRATISTA 2

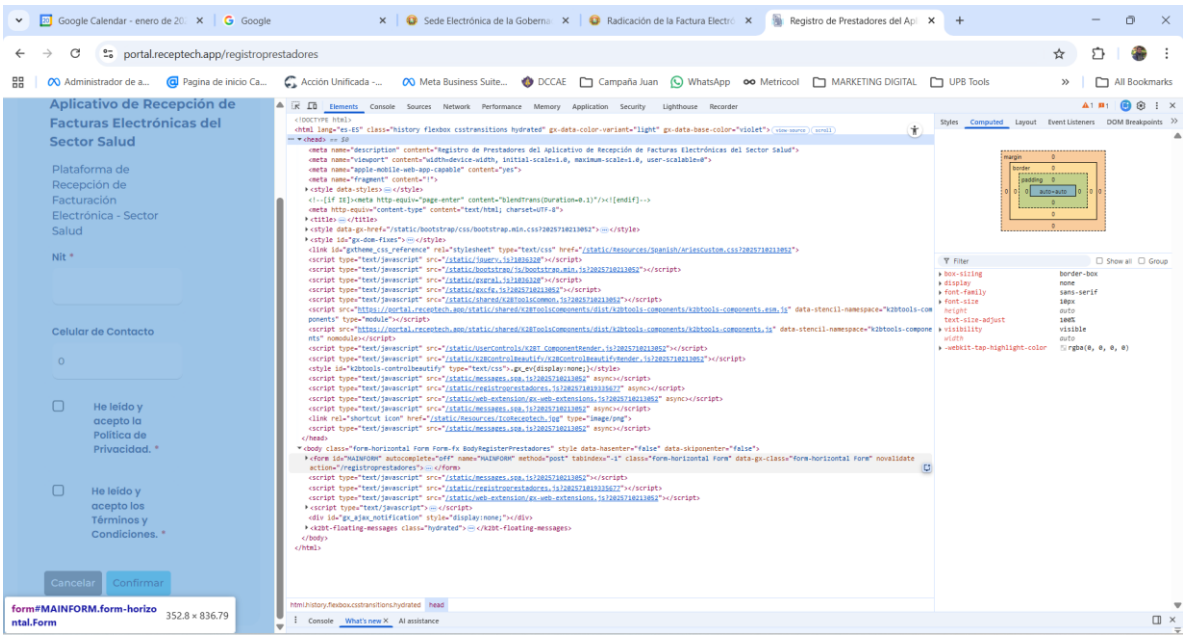
Anexo 1.



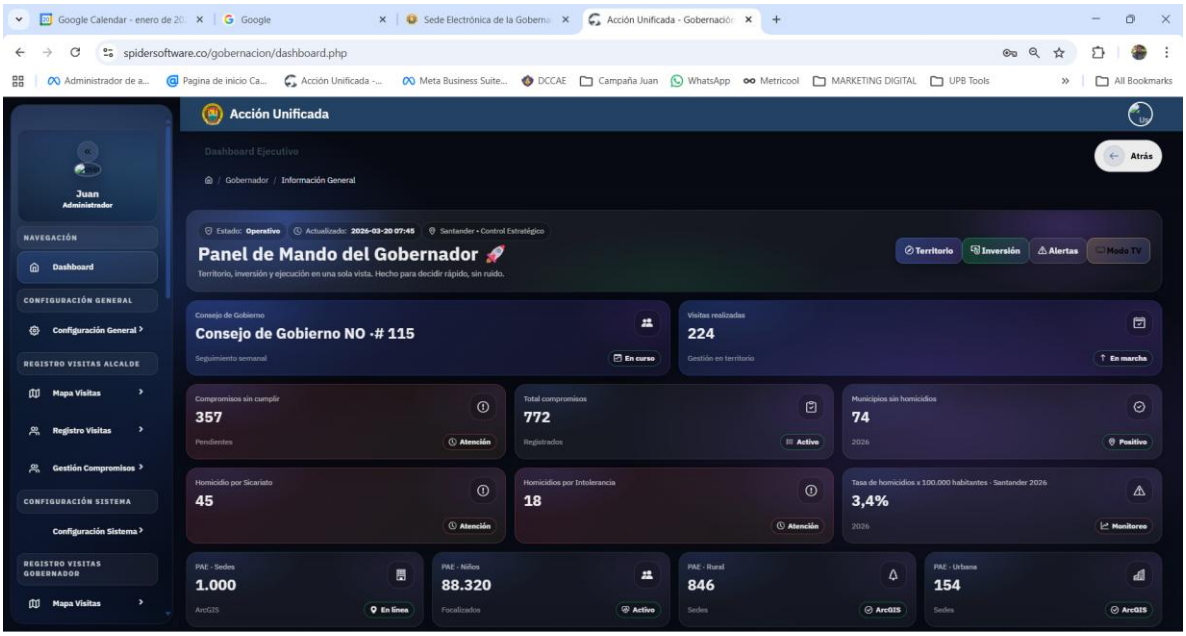


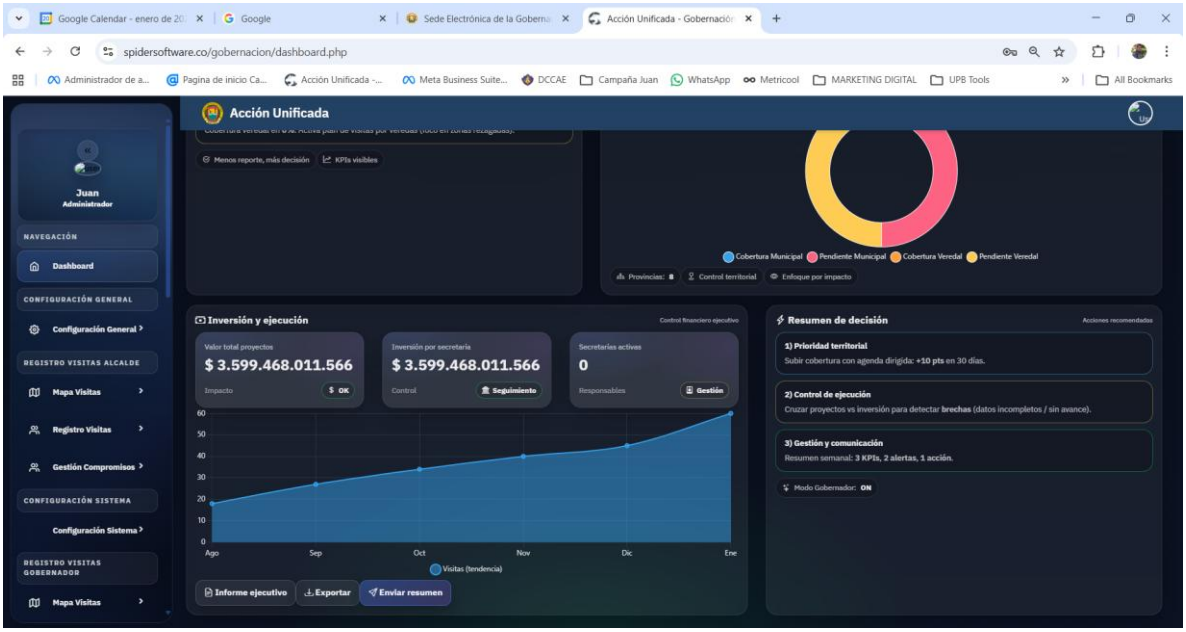

Hoy
Enero de 2026
Mes
LUN
MAR
MIÉ
JUE
VIE
SÁB
DOM
CONSEJO DE GOBIERNO
Martes, 27 de enero · 06:00 – 11:00
Cada semana el martes
agendajuvenaldiaz@gmail.com

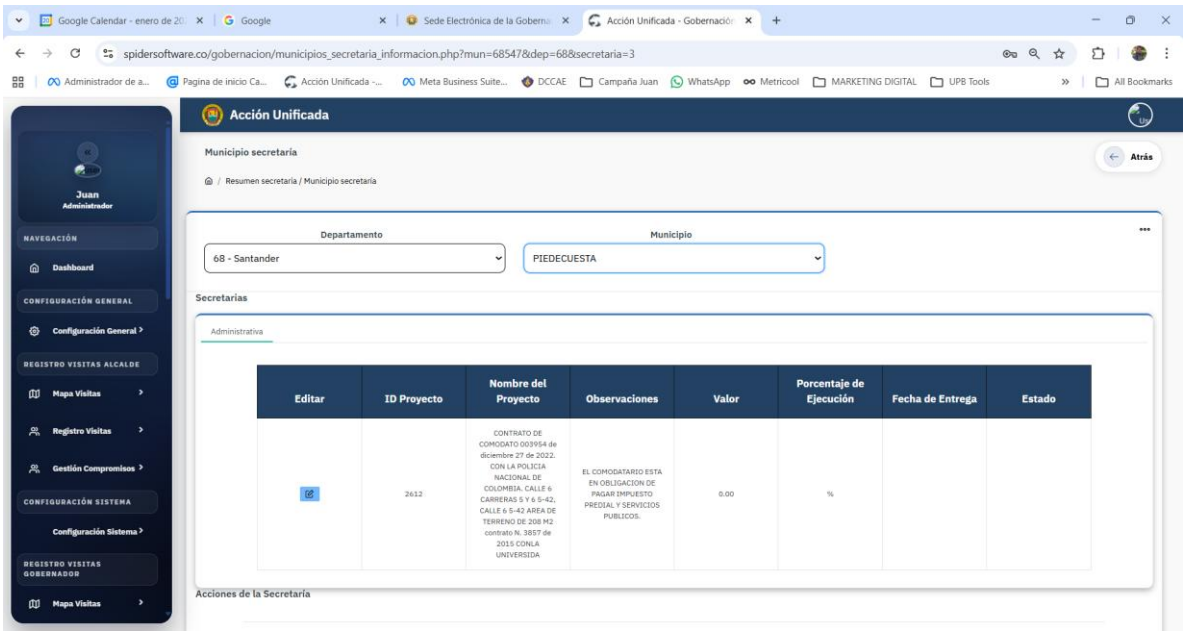

Registro Prestadores
portal.receptech.app/inicioregistro
Bienvenido al PORTAL de Radicación de Facturas - Secretaría de Salud Santander.
Ahora tendrás acceso a una herramienta eficiente y segura para gestionar la radicación y el seguimiento de tus facturas de venta de servicios de salud, cumpliendo con todas las normativas vigentes del sector. A través de nuestra plataforma, podrás realizar tus trámites de forma rápida, sencilla y sin complicaciones, optimizando tu tiempo y recursos.
Te invitamos a completar tu registro para tener
form#MAINFORM.form-horiz
ontal.Form
352.8 × 1067.16

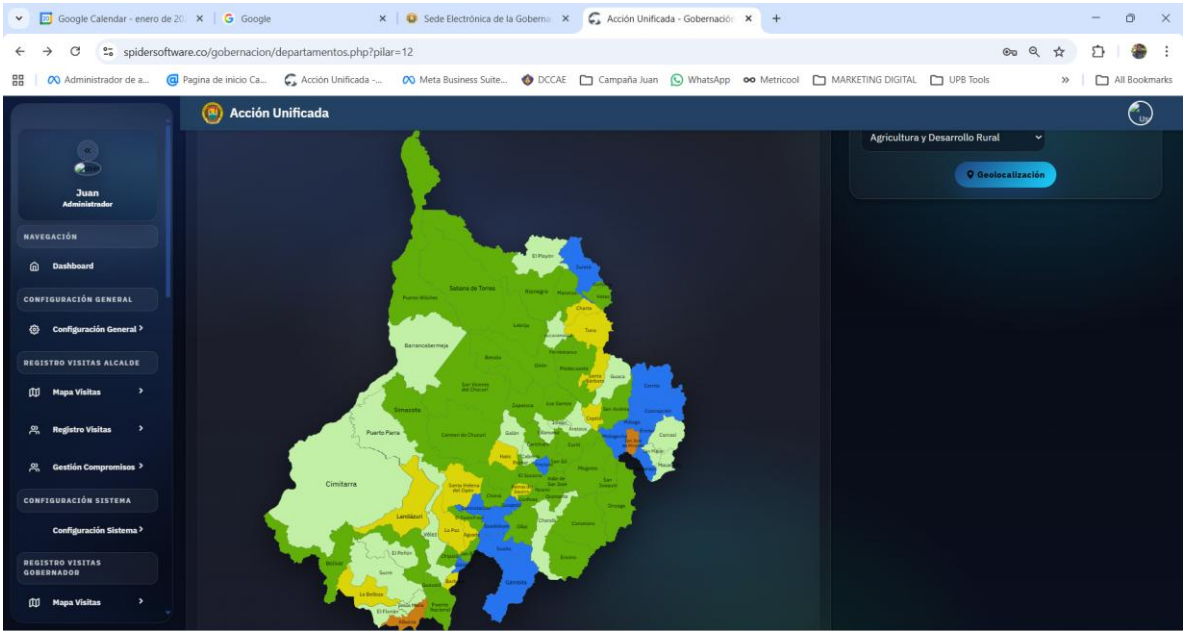

Registro de Prestadores del Ap
portal.receptech.app/registroprestadores
Aplicativo de Recepción de Facturas Electrónicas del Sector Salud
Plataforma de Recepción de Facturación Electrónica - Sector Salud
Nit *
Celular de Contacto
He leído y acepto la Política de Privacidad. *
He leído y acepto los Términos y Condiciones. *
Cancelar
Confirmar
form#MAINFORM.form-horizontal.Form
352.8 × 836.79

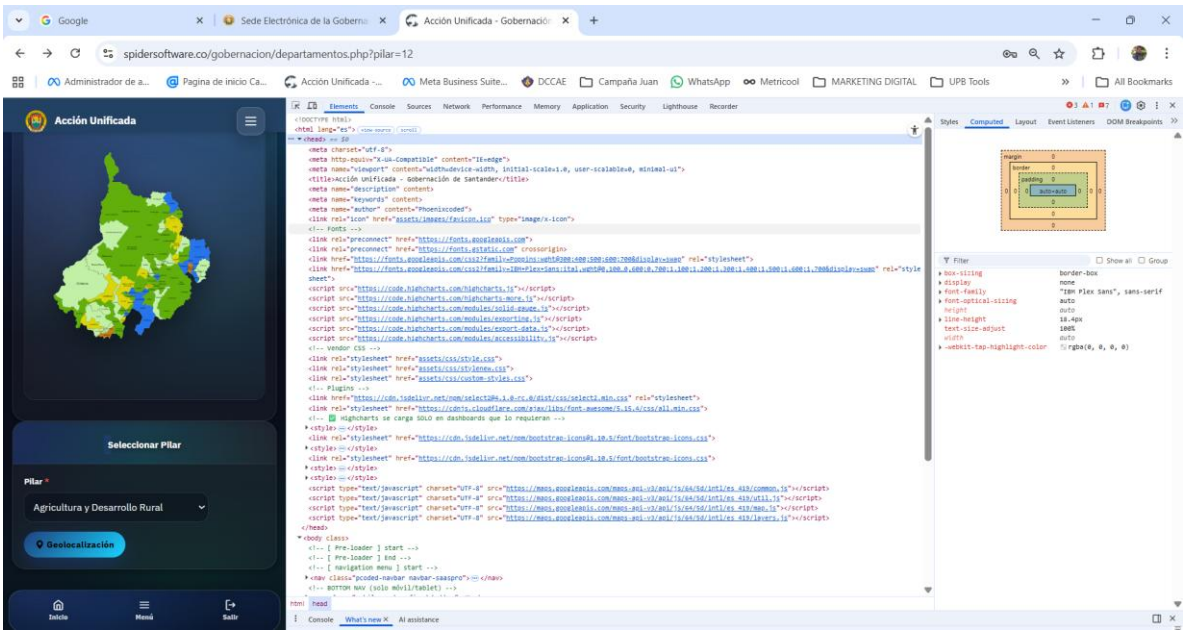
Anexo 2


spidersoftware.co/gobernacion/dashboard.php
Acción Unificada
Juan
Administrador
NAVEGACIÓN
Dashboard
CONFIGURACIÓN GENERAL
Configuración General
REGISTRO VISITAS ALCALDE
Mapa Visitas
Registro Visitas
Gestión Compromisos
CONFIGURACIÓN SISTEMA
Configuración Sistema
REGISTRO VISITAS GOBERNADOR
Mapa Visitas
Dashboard Ejecutivo
Gobernador / Información General
Atrás
Panel de Mando del Gobernador
Territorio, inversión y ejecución en una sola vista. Hecho para decidir rápido, sin ruido.
Territorio
Inversión
Alertas
Modo TV
Consejo de Gobierno NO -# 115
Seguimiento semanal
En curso
Visitas realizadas
224
Gestión en territorio
En marcha
Compromisos sin cumplir
357
Pendientes
Atención
Total compromisos
772
Registrados
Activo
Municipios sin homicidios
74
2026
Positivo
Homicidio por Sicariato
45
Atención
Homicidios por Intolerancia
18
Atención
Tasa de homicidios x 100.000 habitantes - Santander 2026
3,4%
2026
Monitoreo
PAE - Sedes
1.000
ArcGIS
En línea
PAE - Niños
88.320
Focalizados
Activo
PAE - Rural
846
Sedes
ArcGIS
PAE - Urbana
154
Sedes
ArcGIS


Acción Unificada - Gobernación
spidersoftware.co/gobernacion/dashboard.php
Acción Unificada
Juan
Administrador
NAVEGACIÓN
Dashboard
CONFIGURACIÓN GENERAL
Configuración General
REGISTRO VISITAS ALCALDE
Mapa Visitas
Registro Visitas
Gestión Compromisos
CONFIGURACIÓN SISTEMA
Configuración Sistema
REGISTRO VISITAS GOBERNADOR
Mapa Visitas
Menos reporte, más decisión
KPIs visibles
Cobertura Municipal
Pendiente Municipal
Cobertura Veredal
Pendiente Veredal
Provincias:
Control territorial
Enfoque por impacto
Inversión y ejecución
Control financiero ejecutivo
Valor total proyectos
$ 3.599.468.011.566
Impacto
$ OK
Inversión por secretaría
$ 3.599.468.011.566
Control
Seguimiento
Secretarías activas
0
Responsables
Gestión
Ago
Sep
Oct
Nov
Dic
Ene
Visitas (tendencia)
Informe ejecutivo
Exportar
Enviar resumen
Resumen de decisión
Acciones recomendadas
1) Prioridad territorial
Subir cobertura con agenda dirigida: +10 pts en 30 días.
2) Control de ejecución
Cruzar proyectos vs inversión para detectar brechas (datos incompletos / sin avance).
3) Gestión y comunicación
Resumen semanal: 3 KPIs, 2 alertas, 1 acción.
Modo Gobernador: ON


Acción Unificada - Gobernación
spidersoftware.co/gobernacion/municipios_secretaria_informacion.php?mun=68547&dep=68&secretaria=3
Acción Unificada
Juan
Administrador
NAVEGACIÓN
Dashboard
CONFIGURACIÓN GENERAL
Configuración General
REGISTRO VISITAS ALCALDE
Mapa Visitas
Registro Visitas
Gestión Compromisos
CONFIGURACIÓN SISTEMA
Configuración Sistema
REGISTRO VISITAS GOBERNADOR
Mapa Visitas
Municipio secretaría
Atrás
Resumen secretaría / Municipio secretaría
Departamento
68 - Santander
Municipio
PIEDECUESTA
Secretarías
Administrativa
Editar
ID Proyecto
Nombre del Proyecto
Observaciones
Valor
Porcentaje de Ejecución
Fecha de Entrega
Estado
2612
CONTRATO DE COMODATO 003954 de diciembre 27 de 2022. CON LA POLICIA NACIONAL DE COLOMBIA. CALLE 6 CARRERAS 5 Y 6 5-42, CALLE 6 5-42 AREA DE TERRENO DE 208 M2 contrato N. 3857 de 2015 CONLA UNIVERSIDA
EL COMODATARIO ESTA EN OBLIGACION DE PAGAR IMPUESTO PREDIAL Y SERVICIOS PUBLICOS.
0.00
%
Acciones de la Secretaría


Acción Unificada - Gobernación
spidersoftware.co/gobernacion/departamentos.php?pilar=12
Acción Unificada
Juan
Administrador
NAVEGACIÓN
Dashboard
CONFIGURACIÓN GENERAL
Configuración General
REGISTRO VISITAS ALCALDE
Mapa Visitas
Registro Visitas
Gestión Compromisos
CONFIGURACIÓN SISTEMA
Configuración Sistema
REGISTRO VISITAS GOBERNADOR
Mapa Visitas
Agricultura y Desarrollo Rural
Geolocalización
Cimitarra
Puerto Parra


Acción Unificada - Gobernación
spidersoftware.co/gobernacion/departamentos.php?pilar=12
Acción Unificada
Seleccionar Pilar
Pilar *
Agricultura y Desarrollo Rural
Geolocalización
Inicio
Menú
Salir
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Styles
Computed
Layout
Event Listeners
DOM Breakpoints

Anexo 3

GOBERNACION DE SANTANDER
SECRETARÍA PRIVADA

Documento técnico
Recomendaciones en seguridad informática y medios tecnológicos

Fecha: 20 de enero de 2026

Dirigido a: Secretaría Privada – Gobernación de Santander

1. Objeto del documento

En cumplimiento de la función contractual consistente en apoyar asesorando integralmente la gestión tecnológica y operativa de la Secretaría Privada, mediante la optimización de procesos, la elaboración de informes técnicos, la asistencia a reuniones y el seguimiento de las actividades asignadas por el supervisor del contrato, se presenta el siguiente documento técnico con recomendaciones en materia de seguridad informática y medios tecnológicos.

El propósito de este informe es brindar lineamientos concretos para fortalecer la protección de la información institucional, reducir riesgos asociados al uso de herramientas tecnológicas, mejorar la trazabilidad de los procesos y promover buenas prácticas en el manejo de medios digitales al interior de la Secretaría Privada. Aunque el documento tiene una base técnica, su redacción busca ser comprensible para los servidores, contratistas y usuarios finales que intervienen en la operación diaria de la dependencia.

Estas recomendaciones se alinean con buenas prácticas reconocidas en seguridad de la información, continuidad operativa, gestión del riesgo tecnológico y protección de datos, y pueden ser adoptadas de manera progresiva conforme a las capacidades institucionales de la Gobernación de Santander.

2. Contexto operativo de la Secretaría Privada

La Secretaría Privada, por la naturaleza de sus funciones, administra, recibe, tramita y comparte información de alta sensibilidad institucional. Dentro de esa información pueden encontrarse agendas oficiales, convocatorias reservadas, comunicaciones estratégicas, documentos previos a la toma de decisiones, archivos de seguimiento, autorizaciones, respuestas interinstitucionales y datos de contacto de actores clave del nivel departamental y nacional.

Desde una perspectiva de seguridad informática, esto convierte a la Secretaría Privada en un punto crítico de la operación institucional. Un incidente en esta dependencia no solo puede afectar la disponibilidad de los sistemas o el acceso a documentos, sino que también puede tener consecuencias administrativas, reputacionales, jurídicas y operativas. Por ejemplo, el acceso indebido a una agenda oficial, la filtración de un documento sensible o la pérdida de un archivo de seguimiento podrían impactar directamente la coordinación del despacho y la confianza en la gestión pública.

Adicionalmente, el trabajo de la Secretaría Privada suele desarrollarse bajo condiciones de alta inmediatez, múltiples canales de comunicación, interacción con distintos niveles jerárquicos y presión por respuesta oportuna. Ese entorno, aunque operativo y necesario, aumenta el riesgo de errores humanos, envío de información a destinatarios equivocados, uso de canales no autorizados, apertura de archivos maliciosos o exposición innecesaria de datos institucionales.

3. Diagnóstico general de riesgos observables

Con base en la dinámica operativa que normalmente enfrenta una dependencia de esta naturaleza, se identifican riesgos frecuentes que deben ser gestionados con prioridad:

Primero, el uso de cuentas, dispositivos o medios personales para el desarrollo de actividades institucionales. Aunque en ocasiones esto ocurre por rapidez o necesidad operativa, implica pérdida de control sobre la información, dificultad para auditar accesos y exposición a entornos que no siempre cumplen condiciones de seguridad.

Segundo, el intercambio de archivos y mensajes por canales no institucionales o sin controles de protección suficientes. Esto incluye documentos enviados por aplicaciones de mensajería instantánea, correos reenviados a cuentas personales o archivos almacenados fuera de plataformas autorizadas.

Tercero, la ausencia de una administración estricta de permisos sobre documentos sensibles. En muchos casos, varias personas conservan acceso a carpetas, correos o repositorios aun cuando ya no requieren dicho nivel de consulta o edición.

Cuarto, la falta de monitoreo centralizado. Si la entidad no registra de manera adecuada los eventos de acceso, descarga, modificación o intento de ingreso no autorizado, se dificulta detectar incidentes a tiempo y reaccionar con evidencia técnica.

Quinto, la inexistencia o debilidad de protocolos claros para atender incidentes tecnológicos. Cuando no hay una ruta definida, cada evento termina manejándose de forma improvisada, lo que incrementa el impacto y retrasa la recuperación.

Sexto, la dependencia de múltiples herramientas digitales sin criterios unificados de seguridad, almacenamiento, respaldo y trazabilidad. Esto genera dispersión de la información, duplicidad de versiones y baja capacidad de control institucional.

4. Recomendaciones técnicas detalladas

4.1 Gestión de identidades y accesos (IAM)

La gestión de identidades y accesos es el conjunto de controles que permite definir quién puede ingresar a los sistemas, a qué información puede acceder, qué acciones puede realizar y bajo qué condiciones se autoriza dicho acceso. En términos simples, este componente busca asegurar que únicamente las personas correctas tengan acceso a los recursos correctos, durante el tiempo estrictamente necesario.

En la Secretaría Privada este punto es especialmente importante, porque no toda la información debe estar disponible para todos los usuarios. Existen documentos de consulta general, pero también archivos, carpetas, correos o aplicaciones cuyo acceso debe limitarse a determinados perfiles por su carácter sensible o estratégico.

Por ello, se recomienda implementar autenticación multifactor, conocida como MFA, en todos los sistemas críticos. Esto significa que además de la contraseña, el usuario deba validar su acceso mediante un segundo mecanismo, como un código temporal, una aplicación autenticadora o una confirmación en su dispositivo. La finalidad es evitar que una credencial robada sea suficiente para entrar al sistema.

También se recomienda fortalecer la política de contraseñas institucionales. Las claves deben ser robustas, difíciles de adivinar, distintas entre sistemas y no reutilizadas. Técnicamente, deben tener una longitud mínima adecuada, combinar caracteres y estar asociadas a políticas de bloqueo tras múltiples intentos fallidos. Desde el punto de vista práctico, esto reduce el riesgo de acceso por fuerza bruta, suplantación o uso indebido de claves expuestas.

Otra medida importante es la implementación de un esquema de acceso basado en roles. Esto quiere decir que los permisos no deben entregarse de forma general o informal, sino según la función que cumple cada servidor o contratista. Por ejemplo, un usuario puede requerir lectura, otro lectura y edición, y otro acceso administrativo. Esta diferenciación reduce el riesgo de modificaciones accidentales, consulta innecesaria de datos y elevación injustificada de privilegios.

De igual manera, se recomienda revisar periódicamente las cuentas activas, las cuentas inactivas y los privilegios especiales. Es frecuente que usuarios que cambian de dependencia, terminan contrato o modifican funciones mantengan accesos que ya no corresponden. Esa situación constituye una vulnerabilidad, ya que deja abiertas puertas innecesarias dentro del entorno institucional.

Finalmente, conviene centralizar la autenticación en una única plataforma institucional, cuando la arquitectura tecnológica lo permita. Esto facilita el control, mejora la trazabilidad y permite aplicar políticas uniformes sobre todos los accesos. En resumen, la gestión de identidades y accesos debe entenderse como la primera barrera de protección de la información institucional.

4.2 Seguridad en comunicaciones digitales

La seguridad en las comunicaciones digitales busca proteger la información que se transmite por correo electrónico, plataformas colaborativas, mensajería, reuniones virtuales y otros medios electrónicos. En un entorno como el de la Secretaría Privada, donde circulan instrucciones, archivos, datos de contacto, enlaces de reunión y decisiones de coordinación, este frente resulta fundamental.

El primer aspecto que debe garantizarse es que la información viaje protegida. Para ello, los servicios institucionales deben operar bajo protocolos de comunicación seguros, con cifrado activo, de manera que terceros no puedan interceptar, leer o alterar los datos durante la transmisión. Aunque este es un tema técnico, su efecto práctico es sencillo: evitar que la información sea vista o manipulada mientras pasa de un punto a otro.

En materia de correo electrónico, es indispensable configurar y mantener mecanismos de protección contra suplantación de dominio. Esto ayuda a impedir que terceros envíen mensajes haciéndose pasar por funcionarios o cuentas oficiales de la Gobernación. Este tipo de ataque es común en campañas de phishing y suele utilizarse para engañar usuarios, robar credenciales o lograr que se abran enlaces o archivos maliciosos.

Asimismo, se recomienda establecer criterios claros sobre qué tipo de información puede enviarse por cada canal. No toda comunicación debe circular por aplicaciones de mensajería instantánea o medios personales. Los documentos sensibles, listados estratégicos, archivos internos o enlaces de reunión con carácter reservado deben gestionarse por canales institucionales, con usuarios identificados y con posibilidad de trazabilidad.

También es importante controlar las reuniones virtuales. Los enlaces deben compartirse solo con los participantes requeridos, preferiblemente con acceso restringido, salas de espera o autenticación previa. Cuando no se controla este aspecto, se corre el riesgo de ingreso de terceros no autorizados, grabaciones no aprobadas o exposición de información que se asume reservada.

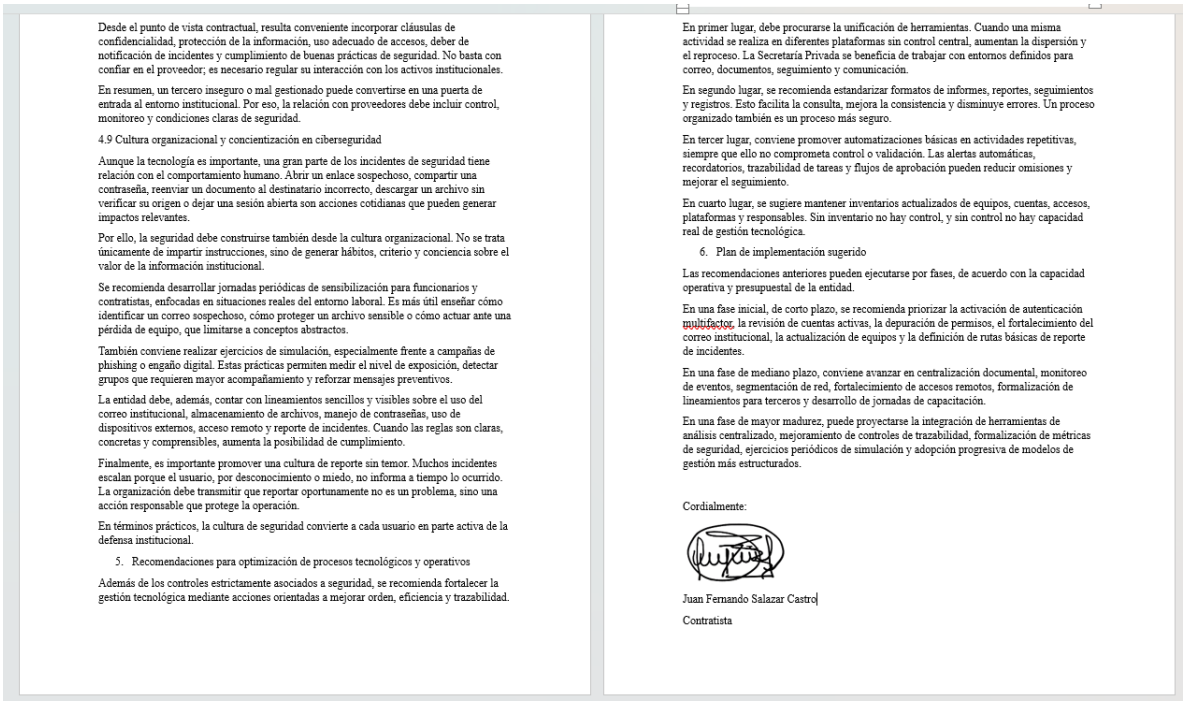
Por último, debe promoverse una cultura de verificación en todas las comunicaciones. Antes de abrir un archivo, responder un correo sospechoso o reenviar un documento, el usuario debe revisar remitente, asunto, contexto y destinatarios. En la práctica, muchas filtraciones o incidentes no ocurren por fallas avanzadas del sistema, sino por errores cotidianos en el manejo de la comunicación digital.

4.3 Gestión documental segura

La gestión documental segura consiste en administrar los documentos institucionales bajo criterios de organización, control, acceso autorizado, conservación, trazabilidad y protección. No se trata solo de almacenar archivos, sino de garantizar que cada documento tenga un ciclo de vida controlado desde su creación hasta su archivo o eliminación.

En la Secretaría Privada, donde la documentación puede incluir oficios, borradores, respuestas, agendas, soportes, reportes y archivos de coordinación, resulta indispensable trabajar sobre plataformas institucionales centralizadas. Esto significa evitar, en la medida de lo posible, que los documentos reposen únicamente en discos locales, memorias USB, equipos personales o cadenas informales de mensajería.

La centralización permite que la entidad conserve control sobre la ubicación del archivo, sus versiones y los usuarios que lo consultan o modifican. Además, facilita la recuperación de la información en caso de pérdida del equipo, daño del dispositivo o cambio de personal.



Desde el punto de vista contractual, resulta conveniente incorporar cláusulas de confidencialidad, protección de la información, uso adecuado de accesos, deber de notificación de incidentes y cumplimiento de buenas prácticas de seguridad. No basta con confiar en el proveedor; es necesario regular su interacción con los activos institucionales.

En resumen, un tercero inseguro o mal gestionado puede convertirse en una puerta de entrada al entorno institucional. Por eso, la relación con proveedores debe incluir control, monitoreo y condiciones claras de seguridad.

4.9 Cultura organizacional y concientización en ciberseguridad

Aunque la tecnología es importante, una gran parte de los incidentes de seguridad tiene relación con el comportamiento humano. Abrir un enlace sospechoso, compartir una contraseña, reenviar un documento al destinatario incorrecto, descargar un archivo sin verificar su origen o dejar una sesión abierta son acciones cotidianas que pueden generar impactos relevantes.

Por ello, la seguridad debe construirse también desde la cultura organizacional. No se trata únicamente de impartir instrucciones, sino de generar hábitos, criterio y conciencia sobre el valor de la información institucional.

Se recomienda desarrollar jornadas periódicas de sensibilización para funcionarios y contratistas, enfocadas en situaciones reales del entorno laboral. Es más útil enseñar cómo identificar un correo sospechoso, cómo proteger un archivo sensible o cómo actuar ante una pérdida de equipo, que limitarse a conceptos abstractos.

También conviene realizar ejercicios de simulación, especialmente frente a campañas de phishing o engaño digital. Estas prácticas permiten medir el nivel de exposición, detectar grupos que requieren mayor acompañamiento y reforzar mensajes preventivos.

La entidad debe, además, contar con lineamientos sencillos y visibles sobre el uso del correo institucional, almacenamiento de archivos, manejo de contraseñas, uso de dispositivos externos, acceso remoto y reporte de incidentes. Cuando las reglas son claras, concretas y comprensibles, aumenta la posibilidad de cumplimiento.

Finalmente, es importante promover una cultura de reporte sin temor. Muchos incidentes escalan porque el usuario, por desconocimiento o miedo, no informa a tiempo lo ocurrido. La organización debe transmitir que reportar oportunamente no es un problema, sino una acción responsable que protege la operación.

En términos prácticos, la cultura de seguridad convierte a cada usuario en parte activa de la defensa institucional.

5. Recomendaciones para optimización de procesos tecnológicos y operativos

Además de los controles estrictamente asociados a seguridad, se recomienda fortalecer la gestión tecnológica mediante acciones orientadas a mejorar orden, eficiencia y trazabilidad.

En primer lugar, debe procurarse la unificación de herramientas. Cuando una misma actividad se realiza en diferentes plataformas sin control central, aumentan la dispersión y el reproceso. La Secretaría Privada se beneficia de trabajar con entornos definidos para correo, documentos, seguimiento y comunicación.

En segundo lugar, se recomienda estandarizar formatos de informes, reportes, seguimientos y registros. Esto facilita la consulta, mejora la consistencia y disminuye errores. Un proceso organizado también es un proceso más seguro.

En tercer lugar, conviene promover automatizaciones básicas en actividades repetitivas, siempre que ello no comprometa control o validación. Las alertas automáticas, recordatorios, trazabilidad de tareas y flujos de aprobación pueden reducir omisiones y mejorar el seguimiento.

En cuarto lugar, se sugiere mantener inventarios actualizados de equipos, cuentas, accesos, plataformas y responsables. Sin inventario no hay control, y sin control no hay capacidad real de gestión tecnológica.

6. Plan de implementación sugerido

Las recomendaciones anteriores pueden ejecutarse por fases, de acuerdo con la capacidad operativa y presupuestal de la entidad.

En una fase inicial, de corto plazo, se recomienda priorizar la activación de autenticación multifactor, la revisión de cuentas activas, la depuración de permisos, el fortalecimiento del correo institucional, la actualización de equipos y la definición de rutas básicas de reporte de incidentes.

En una fase de mediano plazo, conviene avanzar en centralización documental, monitoreo de eventos, segmentación de red, fortalecimiento de accesos remotos, formalización de lineamientos para terceros y desarrollo de jornadas de capacitación.

En una fase de mayor madurez, puede proyectarse la integración de herramientas de análisis centralizado, mejoramiento de controles de trazabilidad, formalización de métricas de seguridad, ejercicios periódicos de simulación y adopción progresiva de modelos de gestión más estructurados.

Cordialmente:

Juan Fernando Salazar Castro

Contratista

Aneo 4

