

	ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS	Código: GTIGP01-F004
	MACROPROCESO: GESTIÓN TECNOLOGIA E INFORMATICA	Versión: 1.0
	PROCESO/ SUBPROCESO: GESTION DE PROYECTOS DE TECNOLOGIAS DE LA INFORMACION / GESTION DE PROYECTOS TI	Fecha: 20/05/2021
	FORMATO INFORME DE EJECUCION DE PROYECTOS TI	Páginas: 1 de 30

Tabla de contenido

1. Introducción al proyecto	3
1.1. Objetivos del proyecto	3
1.2. Productos	4
1.2.1. P02 - Estrategia de Cultura y Apropiación – OAI Avanza	4
1.3. Entidades Participantes	4
1.4. Equipo de trabajo.....	5
2. Avance en la planificación de la Avanzada	6
3. Problemas en la ejecución, riesgos, imprevistos a atender.....	6
3.1. Problemas encontrados.....	6
3.2. Problemas resueltos	6
3.3. Compromisos	7
3.4. Imprevistos.....	7
4. Población impactada - Datos Estadísticos	7
4.1. Cantidad de personas.....	7
4.1. Datos Estadísticos	11
4.2 Encuesta de Satisfacción Final	21
4.2.1 Percepción de conectividad	21

4.2.2 Compromisos Resueltos	21
4.2.3 Comentarios	21
5. Otros.....	22

1. Introducción al proyecto

La política de Gobierno Digital establecida mediante el Decreto 1008 de 2018 (cuyas disposiciones se compilan en el Decreto 1078 de 2015, “Decreto Único Reglamentario del sector TIC”, específicamente en el capítulo 1, título 9, parte 2, libro 2), forma parte del Modelo Integrado de planeación y Gestión (MIPG), que busca promover una adecuada gestión interna de las entidades y un buen relacionamiento con el ciudadano, a través de la participación y la prestación de servicios de calidad. También nos menciona que la Política de Gobierno Digital tiene como objetivo *“Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”*.

A partir de ello, uno de sus retos es:

...”se requiere contar con ciudadanos y actores sociales que *conozcan, entiendan y apropién el uso de las TIC*, para dar solución a sus necesidades. Estos actores no solo consumen lo que le ofrece el Estado, sino que ellos mismos son un gestor del cambio que produce soluciones”.

La nueva visión de la política incluye aspectos que buscan desarrollar una mirada más integral sobre las necesidades y problemáticas de la sociedad y cómo el uso de las TIC, son una herramienta para generar soluciones.¹

A continuación, se presenta el informe de avance del habilitador de Uso y Apropiación de la Política de Gobierno Digital a la cual incluye la caracterización de los grupos de valor, estrategia de uso y apropiación, conceptos claves.

Texto Normal del menú de estilos.

1.1. Objetivos del proyecto

Realización de tomas o brigadas a las dependencias del distrito con el fin de identificar de primera mano cómo los funcionarios y contratistas utilizan las herramientas tecnológicas disponibles con el fin de validar los conocimientos adquiridos en los procesos de capacitación e inducción en el uso de las herramientas; validar que los funcionarios y contratistas pongan

¹ Manual de Gobierno Digital. Ministerio de Tecnologías de la información y Comunicaciones

en práctica todos los lineamientos establecidos en las Políticas de Gobierno Digital y Seguridad Digital; constatar el cumplimiento de todos los controles de seguridad establecidos en el mapa riesgos además de realizar un seguimiento como segunda línea de defensa de acuerdo con la política de administración de riesgos de la Alcaldía Mayor de Cartagena; levantamientos de actas de compromiso y seguimiento en caso de riesgos detectados.

1.2. Productos

ID del producto	Nombre del producto
P02	Estrategia OAI Avanza

1.2.1. P02 - Estrategia de Cultura y Apropiación – OAI Avanza

Se tiene la versión 001 de la Estrategia de Cultura y Apropiación de la Oficina Asesora de Informática denominada **OAI Avanza**, con sus tres componentes que son:

- Guardianes Digitales
- Inspectores TIC
- Agentes Digitales

1.3. Entidades Participantes

Entidades	Rol
Oficina asesora de Informática	Desarrolladora y Ejecutora de la estrategia
Secretaría de Educación	Entidad donde se realizó la brigada de la estrategia OAI Avanza

1.4. Equipo de trabajo

Nombre	Rol del Grupo	Nombres y apellidos	Dependencia
Guardianes Digitales	Enfatizar y validar por parte del equipo de la OAI, la importancia del tratamiento de los datos, seguridad digital y los controles que se deben tener, además de mitigar los riesgos asociados al uso de la tecnología desde el usuario final garantizando que se cumplan las Políticas Institucionales y sus riesgos asociados.	Sebastián Hernández Lucas Pedrozo	Oficina Asesora de Informática
Inspectores TIC	Garantizar y afianzar el correcto uso de las herramientas tecnológicas institucionales utilizadas por los contratistas y funcionarios en sus actividades diarias.	Claudia Leottau Jair José Sánchez Pérez	Oficina Asesora de Informática
Agentes de soporte	Garantizar el óptimo funcionamiento de los equipos tecnológicos dispuestos para los usuarios finales tales como equipos de cómputo, impresoras, teléfonos IP, conectividad alámbrica e inalámbrica, credenciales de acceso, validando el estado de los recursos tecnológicos y problemas presentados con el uso de estos, con la finalidad de que sean solucionados en el momento de la intervención y de manera oportuna en el tiempo.	Silfredo Godoy Chávez Alan Flórez	Oficina Asesora de Informática

2. Avance en la planificación de la Avanzada

El avance fue de acuerdo a los objetivos pactados para la brigada en la fecha estipulada hasta el momento, teniendo un diagnóstico inicial del entorno en cuanto a seguridad digital, soportes y conocimientos en las herramientas tecnológicas.

De esta forma podemos identificar fortalezas y debilidades para así desarrollar estrategias, gestionar y ejecutar el día de la avanzada.

3. Problemas en la ejecución, riesgos, imprevistos a atender

3.1. Problemas encontrados

- Necesidad para capacitaciones presenciales de Sigob versión escritorio y web
- Revisión para el funcionamiento de GLPI Saus
- Oficina 1401 – Planta. Presenta dos (02) computadores lentos
- Oficina 1403 – Talento Humano. Asesoría para el desarrollo Software de Horas Extras en Nómina.
- Revisión de dos (02) computadores para repotenciar Piso 14
- Solicitan capacitación Políticas de Seguridad
- Cambiar cable de red computador Sr Rafael Galvis Jimenes oficina 1704 inspección y vigilancia
- Solicitud punto de red en la Oficina Asesora Jurídica - 1707
- Solicitud de cruzar Sigob con SAC
- Señor Guillermo Peña Solicitud licencia de Autocad para cumplir funciones.
- Solicitud Equipos de Computo
- Sra. Diana Gómez solicita caracterización para colegios

3.2. Problemas resueltos

- Se da instrucciones para empezar caracterización para los colegios y validando una reunión para el tema.
- Se programa capacitación de Sigo para el jueves 27 de marzo. Esperando confirmación de horario.

- Se programa reunión para dar solución al GLPI Saus
- Se aclaran dudas existentes en cuanto a Sigob de escritorio y web
- Se hace cambio cable de red a computador del funcionario Rafael Galvis Jiménez en la oficina 1704 Inspección y Vigilancia.

3.3. Compromisos

- Cursos presenciales de Sigob Escritorio y Web
- Capacitación en el Manual Políticas de Seguridad
- Habilitar punto de red en la Oficina Asesora Jurídica – 1707
- Asesorar para el desarrollo Software de Horas Extras en la nómina de Talento Humano.

3.4. Imprevistos

- Demora asistencia de contratistas y funcionarios a la hora informada sobre la avanzada, lo que dificultó la hora de inicio.

4. Población impactada - Datos Estadísticos

4.1. Cantidad de personas

La cantidad total de funcionarios y contratistas la cual se les hizo Encuesta de Diagnóstico y Apropiación de las Tics fueron cuarenta y nueve (49), detalladas a continuación.

ITEM	NOMBRES	CARGO
1	JOSE DEL RIO NOGUERO	FUNCIONARIO
2	VICTORIA DE LA ROSA PAJARO	CONTRATISTA
3	OLGA MALDONADO	FUNCIONARIO
4	LUIS RODRIGUEZ HERNANDEZ	FUNCIONARIO

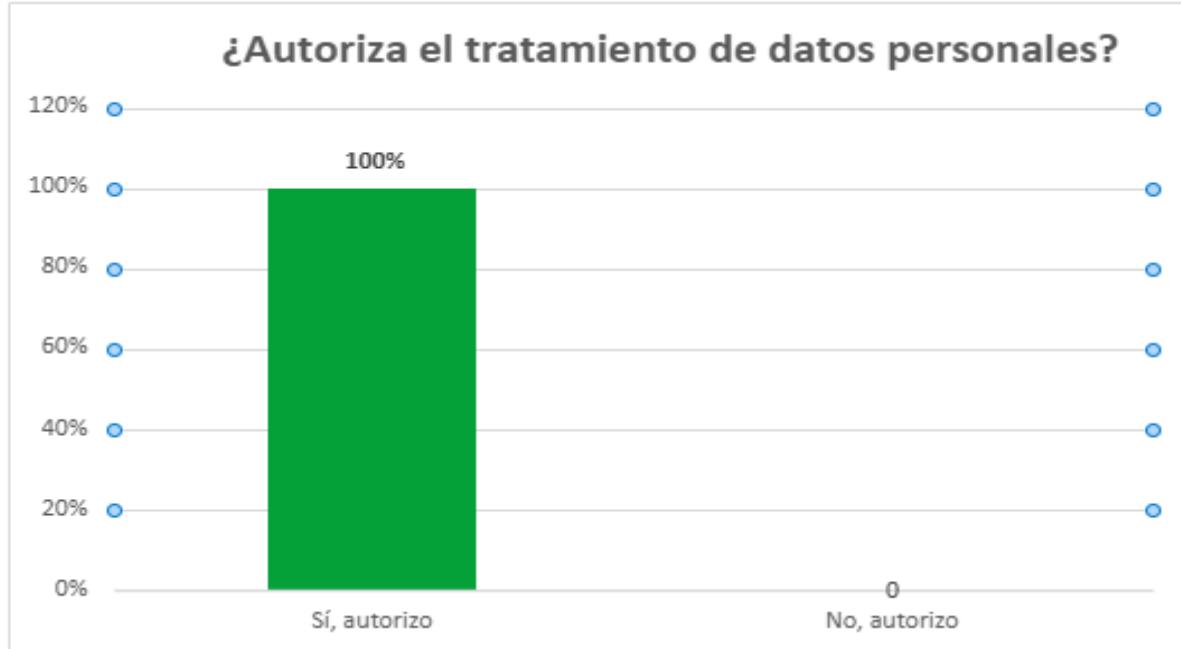
ITEM	NOMBRES	CARGO
5	DIANA ULLOQUE CUADROS	FUNCIONARIO
6	DIANA GOMEZ GARCES	FUNCIONARIO
7	MAYGRET ANAYA RODRIGUEZ	FUNCIONARIO
8	MARTA CAMPO GAIBAO	FUNCIONARIO
9	CLAUDIA AGUDELO PEREZ	FUNCIONARIO
10	LISBETH OLEA BONFANTE	CONTRATISTA
11	ELIZABETH MADERO FAJARDO	FUNCIONARIO
12	MARCELA MEZA ALMEIDA	CONTRATISTA
13	LUIS ROMERO	CONTRATISTA
14	MARCEL MENDOZA CEDEÑO	FUNCIONARIO
15	ORLANDO BACCI BOBILLA	FUNCIONARIO
16	HILDA CARREÑO SUAREZ	FUNCIONARIO
17	ANGEL OSPINO CANTILLO	CONTRATISTA
18	GENERA NEGRETTE POLO	FUNCIONARIO
19	RAFAEL GALVIS JIMENEZ	FUNCIONARIO
20	MARLENE RUIZ DE AVILA	FUNCIONARIO
21	BERLINEZ MARTINEZ GUTIERREZ	CONTRATISTA

ITEM	NOMBRES	CARGO
22	DENNY GAMBOA ARBOLEDA	FUNCIONARIO
23	DAVID HERNANDEZ FERNANDEZ	CONTRATISTA
24	JUSTINA YANCES AYOLA	FUNCIONARIO
25	LAUDINA SANCHEZ DE SILVA	FUNCIONARIO
26	JOSE HERAZO BUELVAS	FUNCIONARIO
27	FREDY TORRES ARROYO	FUNCIONARIO
28	CAMILO TORRES VERGEL	FUNCIONARIO
29	ILCE RUIZ HERNANDEZ	FUNCIONARIO
30	JOSEFINA PEDROZO PALOMINO	FUNCIONARIO
31	KATIA MONTIEL LEDESMA	FUNCIONARIO
32	NAZLY PUELLO ESTRADA	FUNCIONARIO
33	CARLOS CONEO YANCES	FUNCIONARIO
34	MARTHA VARGAS MENDOZA	CONTRATISTA
35	NADINA MANJARREZ	FUNCIONARIO
36	ELIS CASTELLANO ARROYO	CONTRATISTA
37	LEYDI MADRID ANAYA	CONTRATISTA
38	EILEEN GUTIERREZ MARRUGO	CONTRATISTA

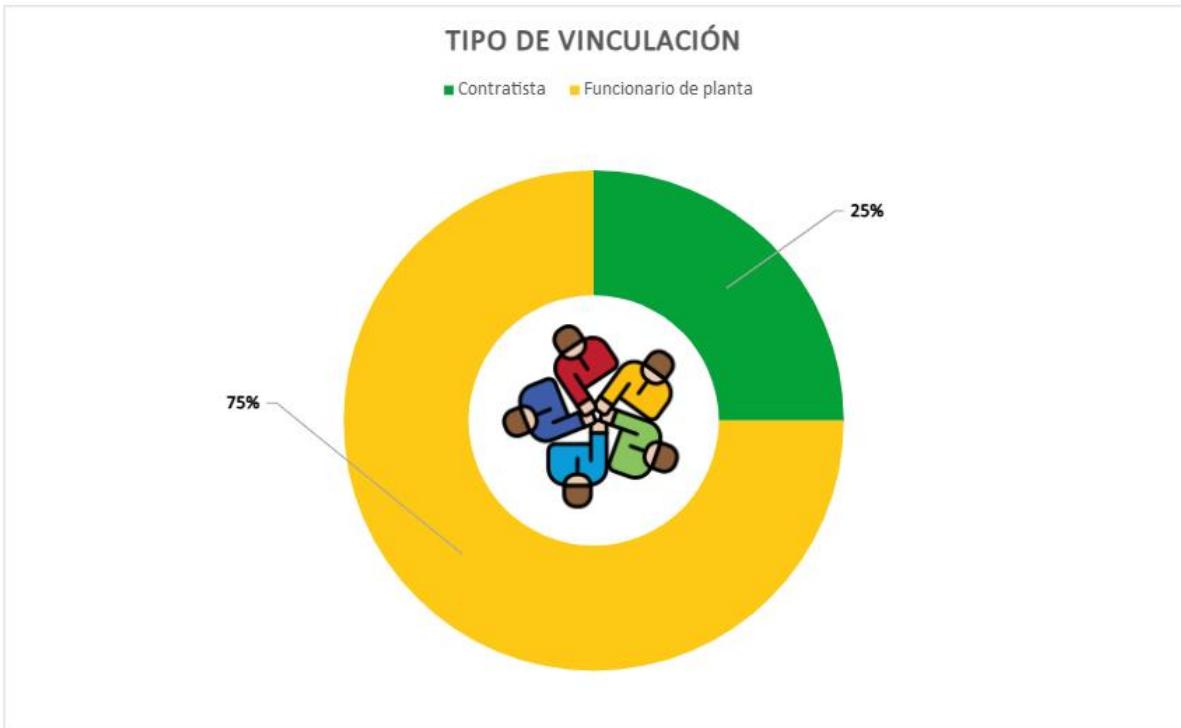
ITEM	NOMBRES	CARGO
39	SHIRLYS BERDUGO PEREZ	CONTRATISTA
40	SERGIO MENDEZ VERGARA	FUNCIONARIO
41	STEPHANI CARRASCAL LLAMAS	FUNCIONARIO
42	BLANCA BARON RIVERA	FUNCIONARIO
43	JENNIFER MENDEZ	FUNCIONARIO
44	DARLING RODRIGUEZ OSORIO	FUNCIONARIO
45	HEIDY BUELVAS MESTRE	FUNCIONARIO
46	ARELIS HERNANDEZ	FUNCIONARIO
47	MARIA DEL VILLAR CARRILLO	FUNCIONARIO
48	RAFAEL PEREIRA EVILS	FUNCIONARIO
49	KELLY ORTEGA NIEVES	CONTRATISTA

4.1. Datos Estadísticos

Número de Encuestas: **52**

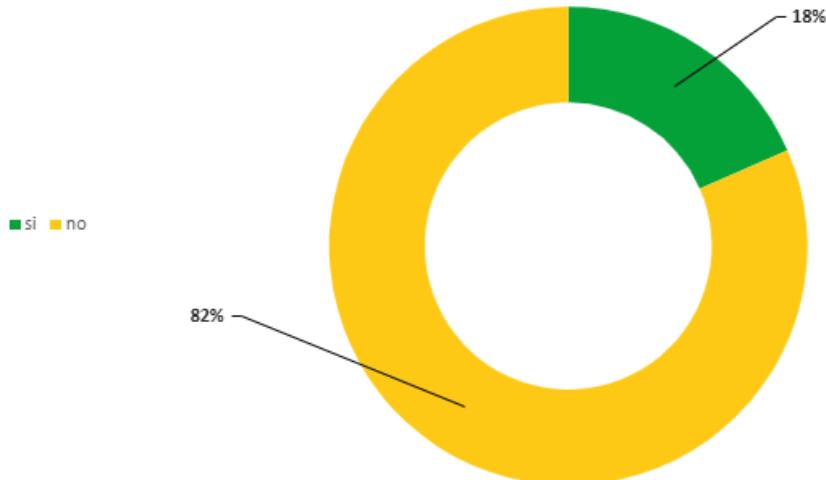


Interpretación: Se evidencia aceptación del 100% para el tratamiento de datos personales



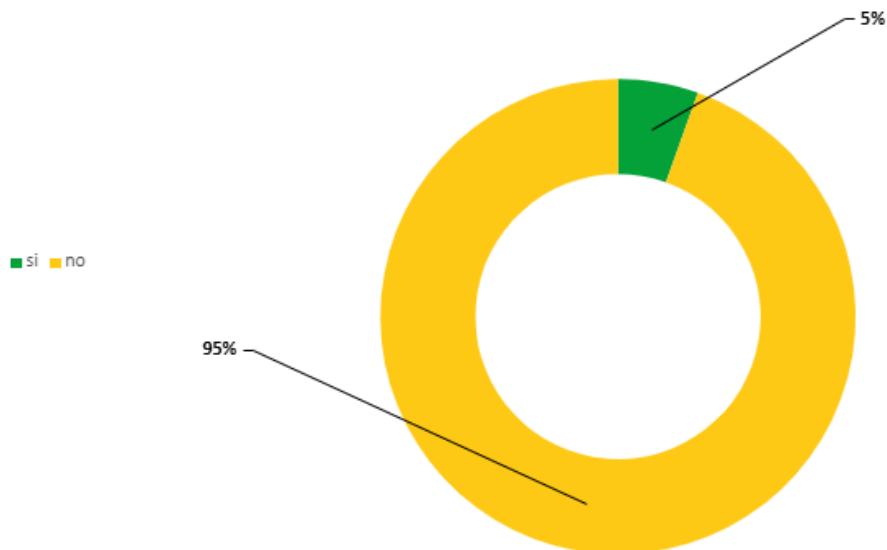
Interpretación: La gráfica arroja un resultado del 13% donde el personal encuestado son contratistas y el 39% son funcionarios de planta.

¿CONOCE EL MANUAL DE SEGURIDAD DIGITAL DE LA ALCALDÍA DE CARTAGENA?

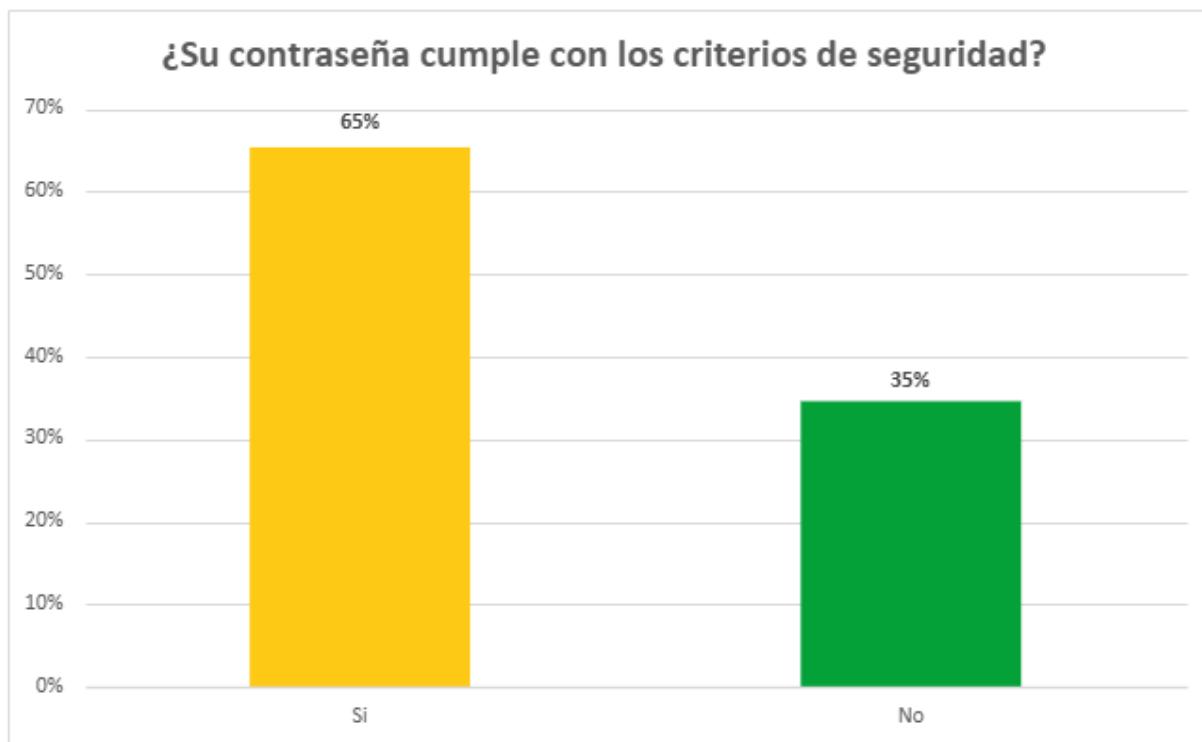


Interpretación: El 82% de los encuestados desconocen la existencia y conocimiento del manual de políticas de seguridad, el cual indica que el manual no es lo suficientemente accesible o que no se ha comunicado de manera efectiva. La falta de conocimiento puede significar que muchas personas no están preparadas para enfrentar amenazas digitales, lo que podría poner en riesgo tanto a contratistas / funcionarios como a la entidad.

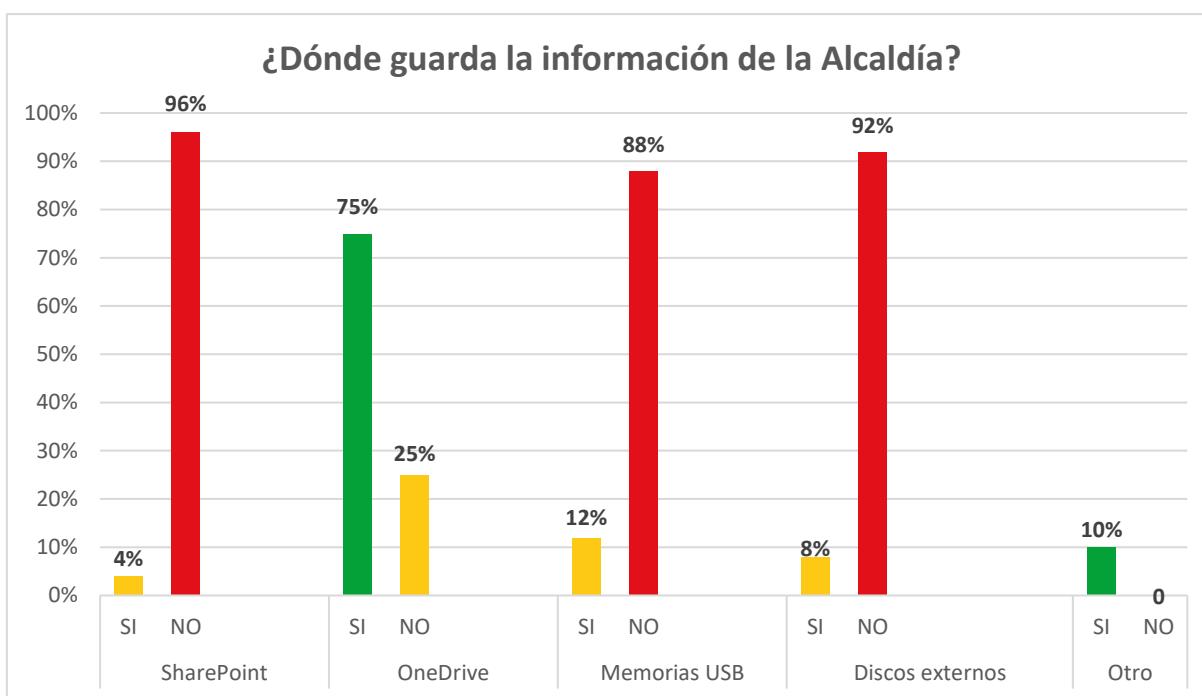
¿EN LA VIGENCIA 2025 HA RECIBIDO UNA CAPACITACIÓN SOBRE SEGURIDAD DIGITAL?



El hecho de que solo el 5% haya recibido capacitación sobre seguridad digital en la vigencia 2025 indica que es urgente la implementación en programas de capacitación en seguridad digital. Esto no solo ayudaría a prevenir riesgos, sino también a fortalecer la confianza de los ciudadanos en la gestión digital.

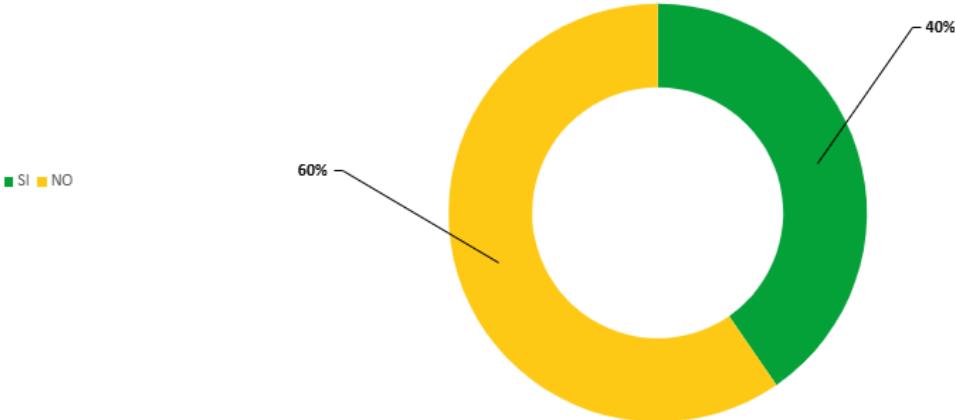


El 65% es un porcentaje relativamente positivo, ya que más de la mitad está utilizando contraseñas seguras, cumplen con los criterios de seguridad y están al tanto de las buenas prácticas, sin embargo, el 35% podría estar utilizando contraseñas débiles que representan un riesgo mayor de ciberataques la cual debe entrenarse para cumplir con los criterios.



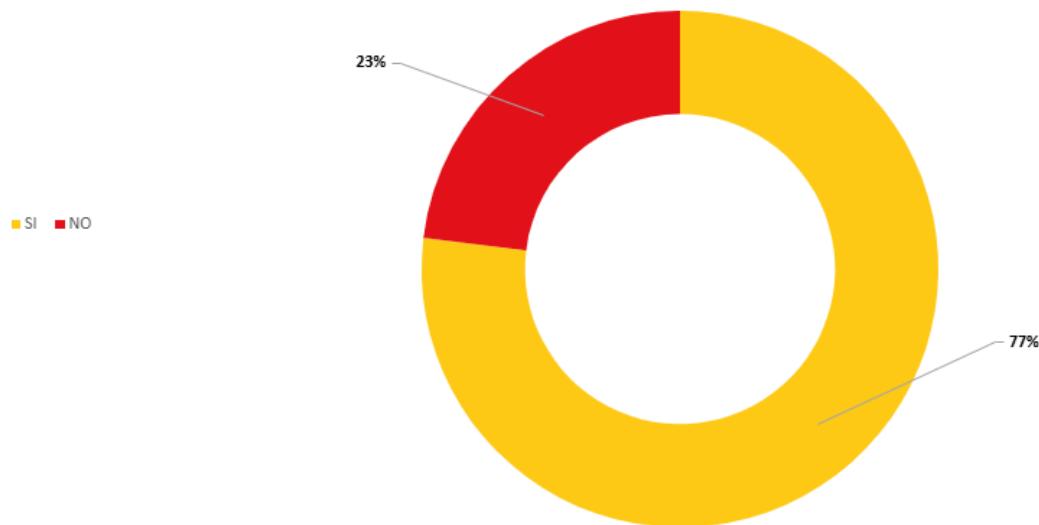
Solo un 4% guarda información en SharePoint, la cual puede indicar que los contratistas / funcionarios no están completamente familiarizados con esta plataforma o no han sido entrenados para utilizarla de manera efectiva; El 75% de la información se guarda en OneDrive y es un dato positivo, ya que ofrece ventajas como seguridad avanzada, acceso remoto y colaboración eficiente entre contratista / funcionarios; El almacenamiento en memorias USB (12%) y discos externos (8%) es preocupante desde una perspectiva de seguridad. Estos dispositivos físicos son más vulnerables a la pérdida o robo de datos, y, en muchos casos, no ofrecen las mismas medidas de protección que los servicios en la nube..

¿UTILIZA CORREO PERSONAL PARA ADELANTAR ACTIVIDADES LABORALES?

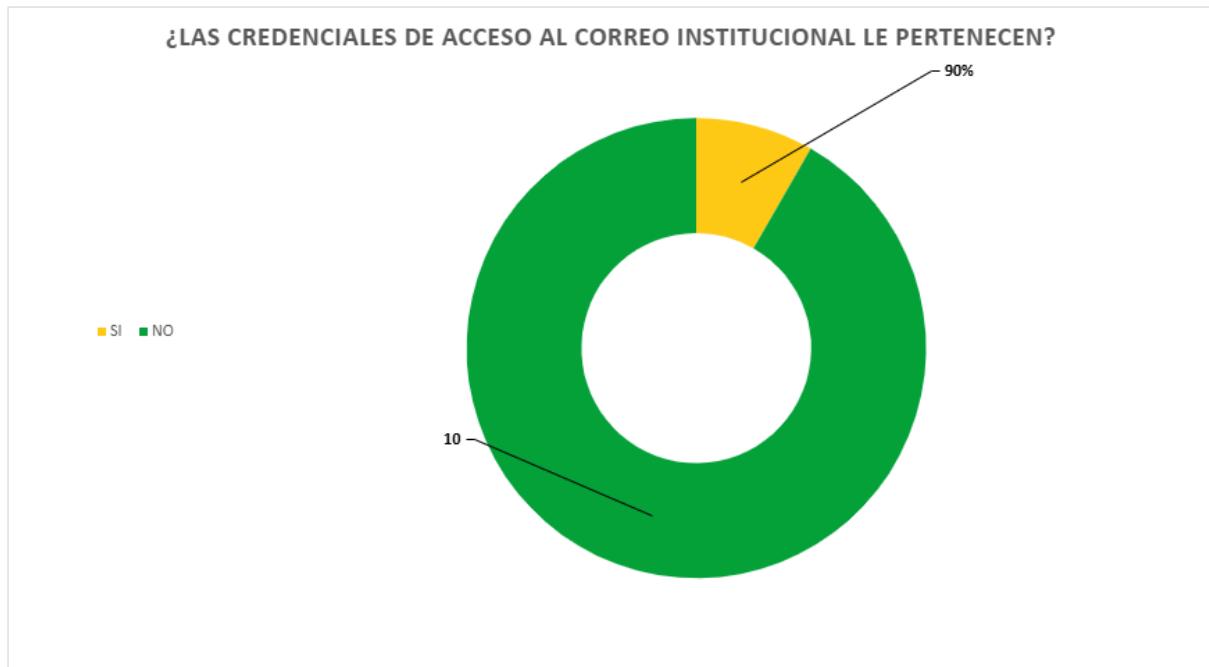


El 60% está utilizando correos personales, esto puede ser indicativo de que no se están siguiendo las políticas internas para garantizar la seguridad de los datos y evitar la filtración de información sensible, y aunque el 40% esté utilizando el correo institucional, esto sigue representando solo una parte del total. Esto quiere decir que aún existe un gran porcentaje de contratistas / funcionarios que no están completamente alineados con las políticas de seguridad.

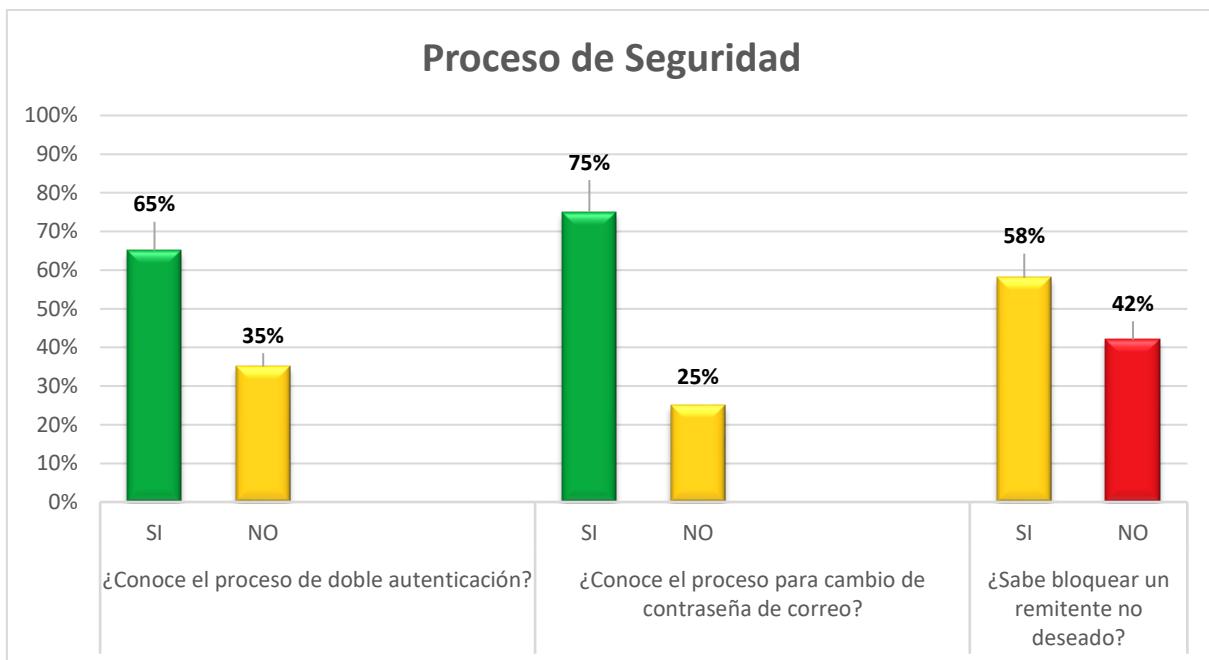
¿CUÁNDO SE LEVANTA DE SU ESCRITORIO BLOQUEA LA SESIÓN?



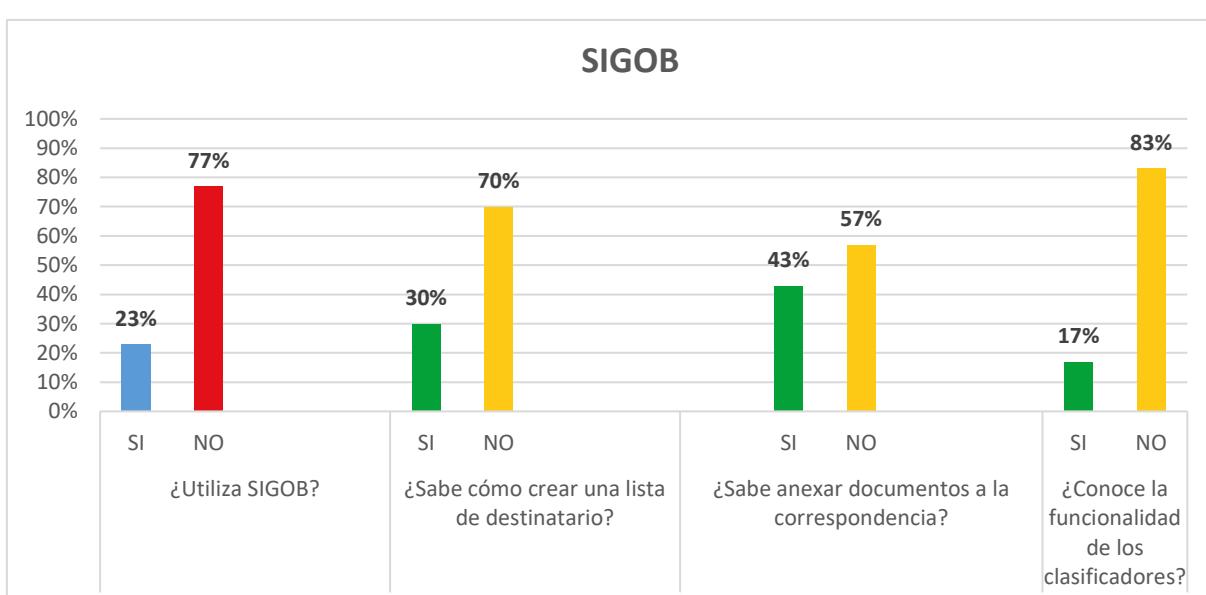
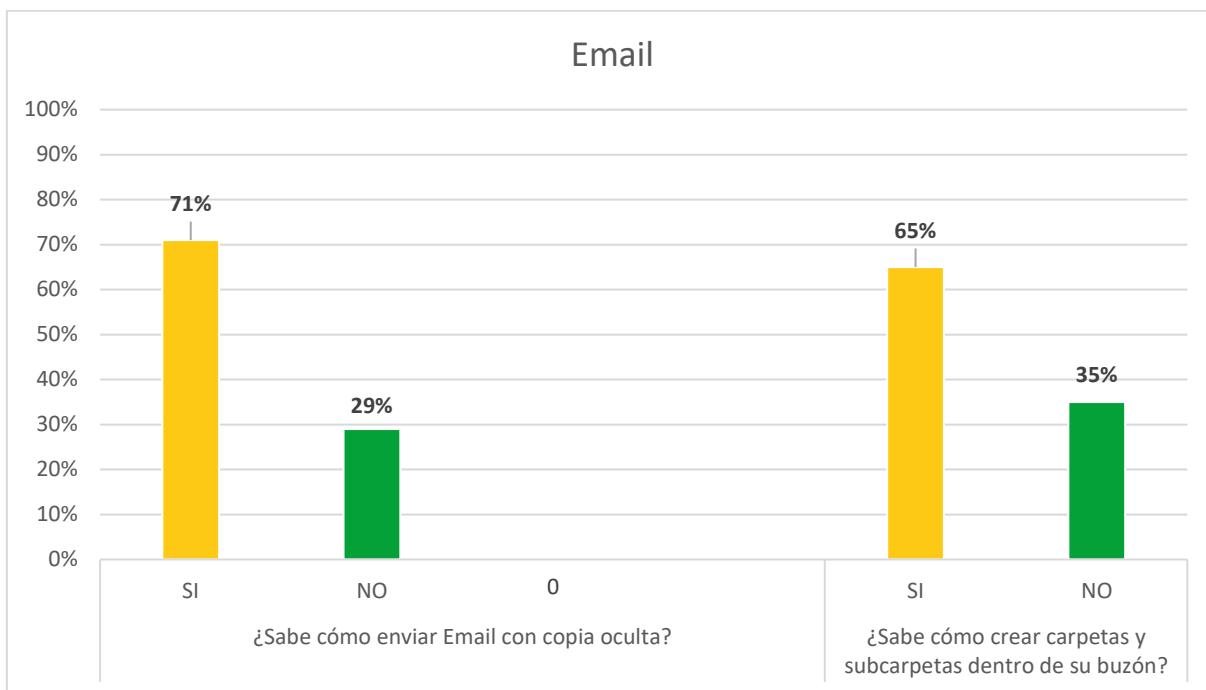
El 77% es un resultado que demuestra la buena práctica desde el punto de vista de la seguridad física. Bloquear la sesión impide que personas no autorizadas accedan a información confidencial cuando el usuario no está presente, sin embargo, ese 23% que no lo hace puede ser un indicativo de que las políticas de seguridad no están lo suficientemente reforzadas o no se han establecido normas claras sobre la necesidad de bloquear las sesiones. Se debe informar sobre la concientización de la seguridad..



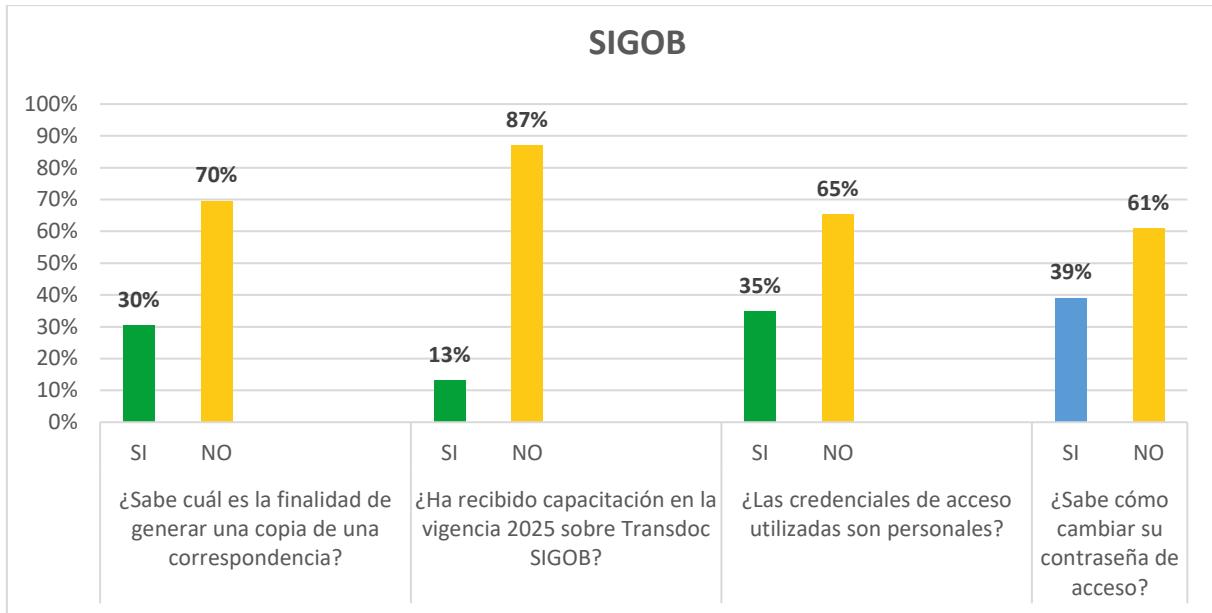
El hecho que el 90% de los usuarios tengan control sobre sus credenciales de acceso al correo institucional es positivo, ya que esto indica que tienen responsabilidad sobre sus cuentas y ese 10% que no tiene control, se debe revisar el por qué sucede y corregirlo para que cada usuario tenga el control necesario sobre su cuenta y así evitar problemas en la seguridad de la información.



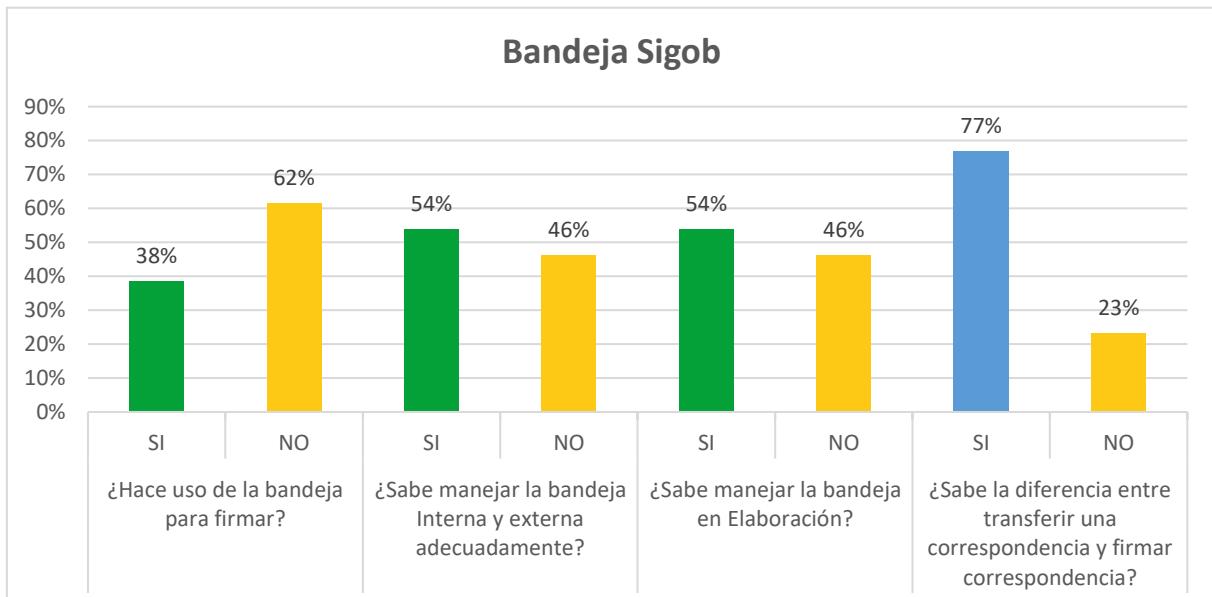
El resultado que el 65% de los contratistas/funcionarios conozcan el proceso de doble autenticación es positivo, pero aún hay un 35% que no está familiarizado con esta herramienta crítica de seguridad la cual se debe capacitar; Si bien el 75% tiene conocimiento de cambio de contraseña, es posible que aún no estén implementando las mejores prácticas en términos de protección de cuentas y esto significa que hay una brecha significativa en cuanto a la seguridad del correo electrónico y la protección contra phishing. Por último, el 42 % que no sabe bloquear un remitente, se les debe indicar que es una buena práctica para evitar el spam o correos molestos, aunque no es suficiente para protegerse contra phishing, malware u otros tipos de ataques que pueden venir a través de correos electrónicos.



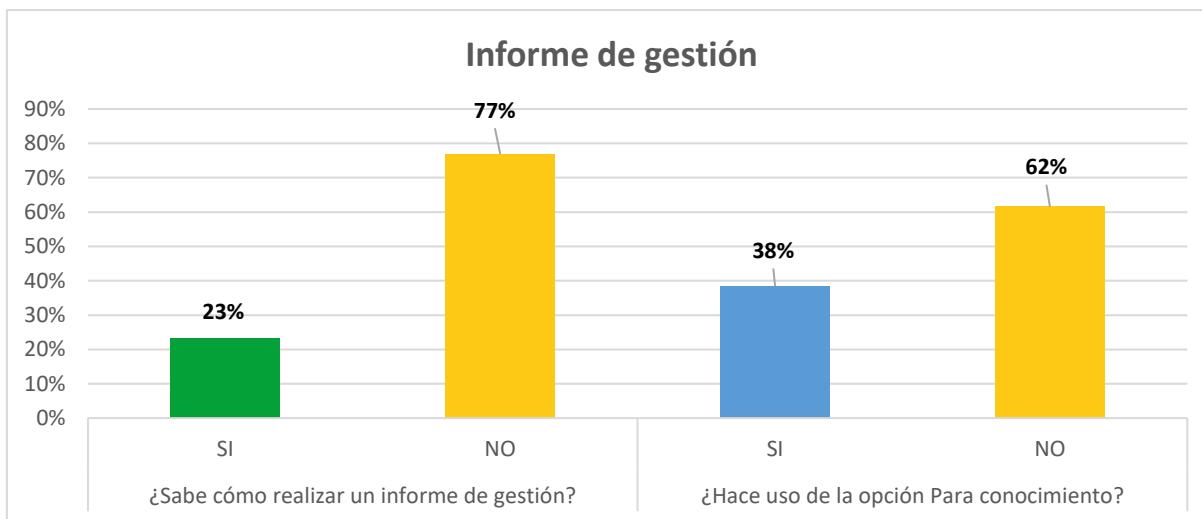
La mayoría usa SIGOB (77%) y tiene conocimientos sólidos sobre la creación de listas de destinatarios (70%) y los clasificadores (83%). Estos son aspectos clave de la plataforma, lo que indica que el grupo tiene un buen dominio de las funcionalidades básicas y avanzadas de SIGOB. La creación de destinatarios podría necesitar más capacitación, ya que solo el 57% lo sabe hacer. Aunque el conocimiento de los clasificadores es alto (83%), sería útil enseñar su uso práctico y aplicaciones dentro del flujo de trabajo de SIGOB.



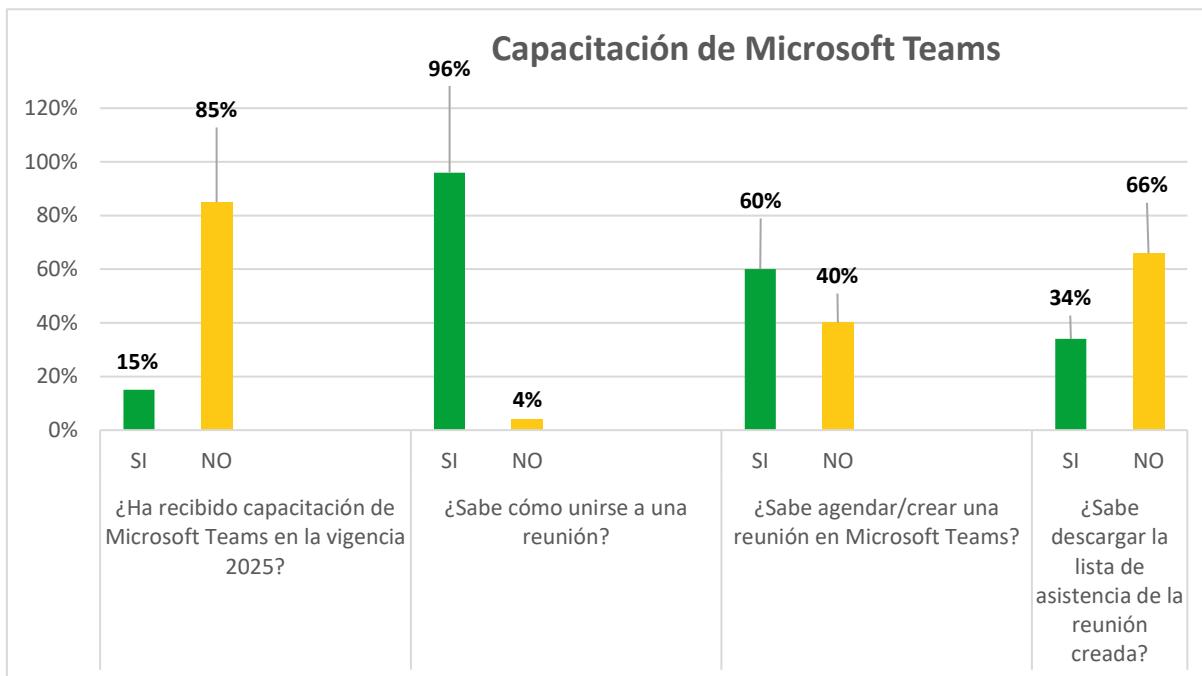
Estos resultados demuestran tres puntos a considerar: **Capacitación continua:** Ofrecer actualizaciones regulares sobre SIGOB, especialmente en funciones específicas que necesitan más atención (como la creación de destinatarios y el cambio de contraseñas); **Fomentar el uso de credenciales propias:** Garantizar que todos los usuarios tengan credenciales individuales para mejorar la seguridad y **Refuerzo en seguridad:** Proporcionar más orientación sobre la gestión de contraseñas para asegurar que todos sepan cómo cambiar su contraseña y proteger su cuenta.



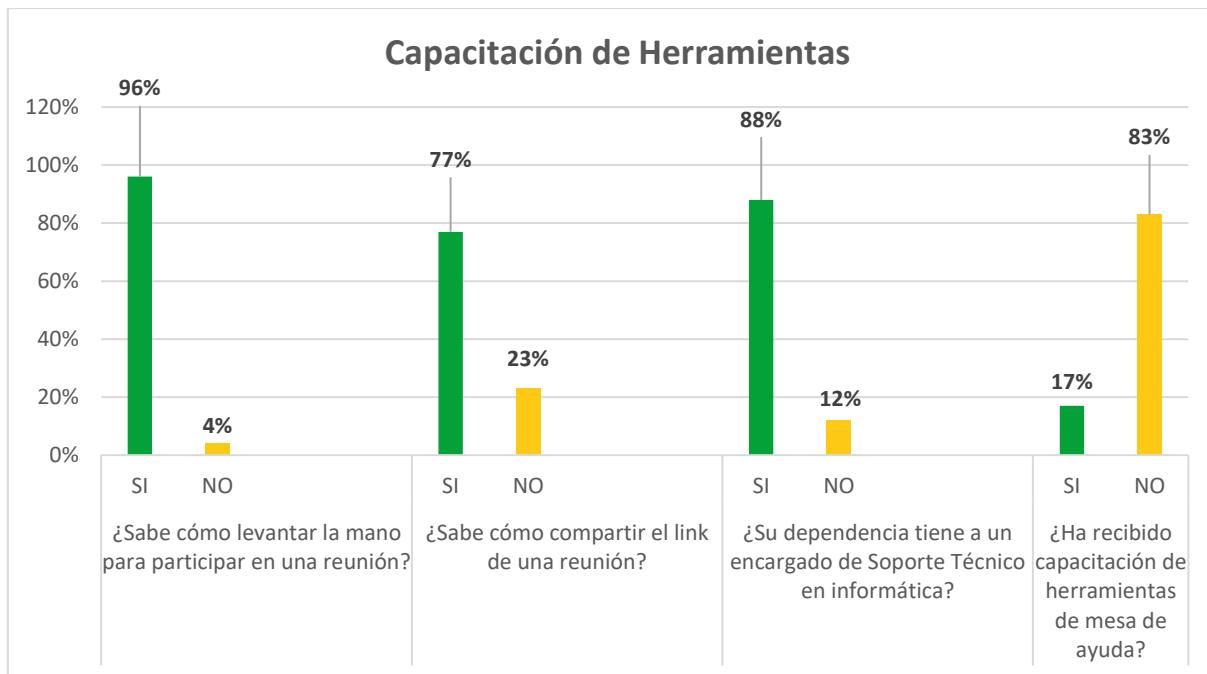
Una mayoría significativa no utiliza la bandeja para firmar, lo cual indica que son contratistas que no tienen acceso a la misma;. El 56% parece tener conocimientos adecuados sobre bandeja interna y externa, aunque casi la mitad aún presenta dificultades. Esto sugiere una necesidad de refuerzo formativo; El 54% maneja la bandeja de elaboración, pero casi la mitad de los encuestados admite no manejarla correctamente la cual se debe enfocar parte de la formación en esta bandeja en particular, mostrando ejemplos reales de su uso en el flujo de trabajo; y el 77% conoce la diferencia entre correspondencia y firmar correspondencia, se debe Aprovechar esta fortaleza para reforzar el resto del conocimiento sobre el sistema.



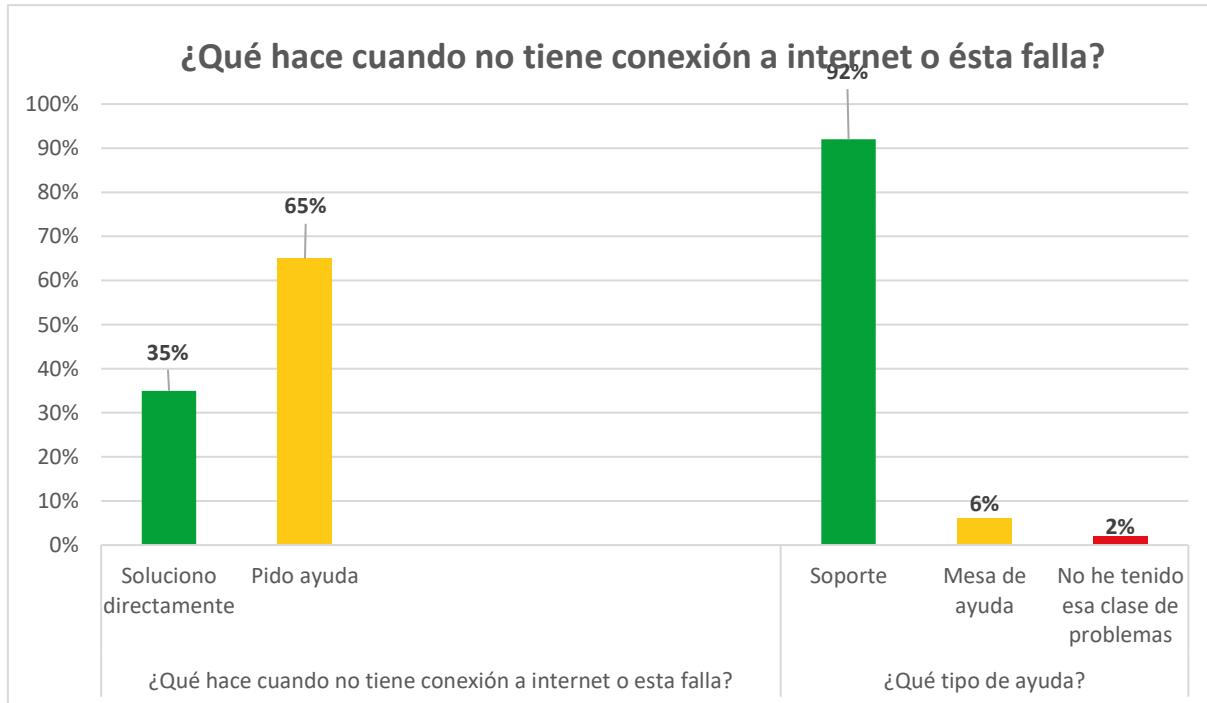
Que el 77% no conozca cómo realizar un informe de gestión se convierte en una **debilidad crítica**. Solo una cuarta parte de los encuestados sabe cómo elaborar un informe de gestión. Esto puede deberse a falta de formación, escasa experiencia o ausencia de lineamientos claros que traiga y puede generar reportes mal estructurados o la inexistencia de reportes en ciertos procesos, lo que afecta la trazabilidad y la toma de decisiones. Se recomienda hacer talleres prácticos. El hecho que sólo el 38% haga uso de la opción para su conocimiento hace incluir esta función en las capacitaciones como un componente estratégico de gestión documental.



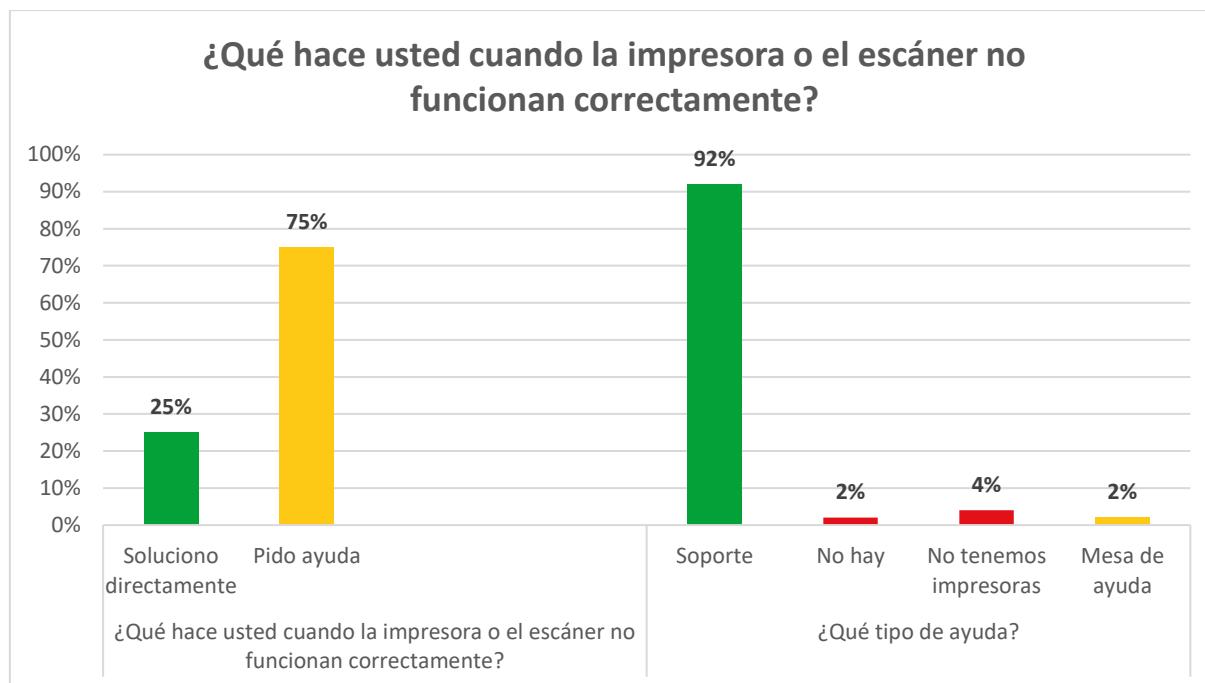
La capacidad de uso básico de Microsoft Teams (como unirse a reuniones) está bien desarrollada (96%), Sin embargo, el uso avanzado o administrativo (crear reuniones y gestionar listas de asistencia) aún presenta vacíos importantes. El 85% no ha recibido capacitación en 2025, lo que evidencia que la mayoría ha adquirido conocimientos de forma empírica o a través de terceros.



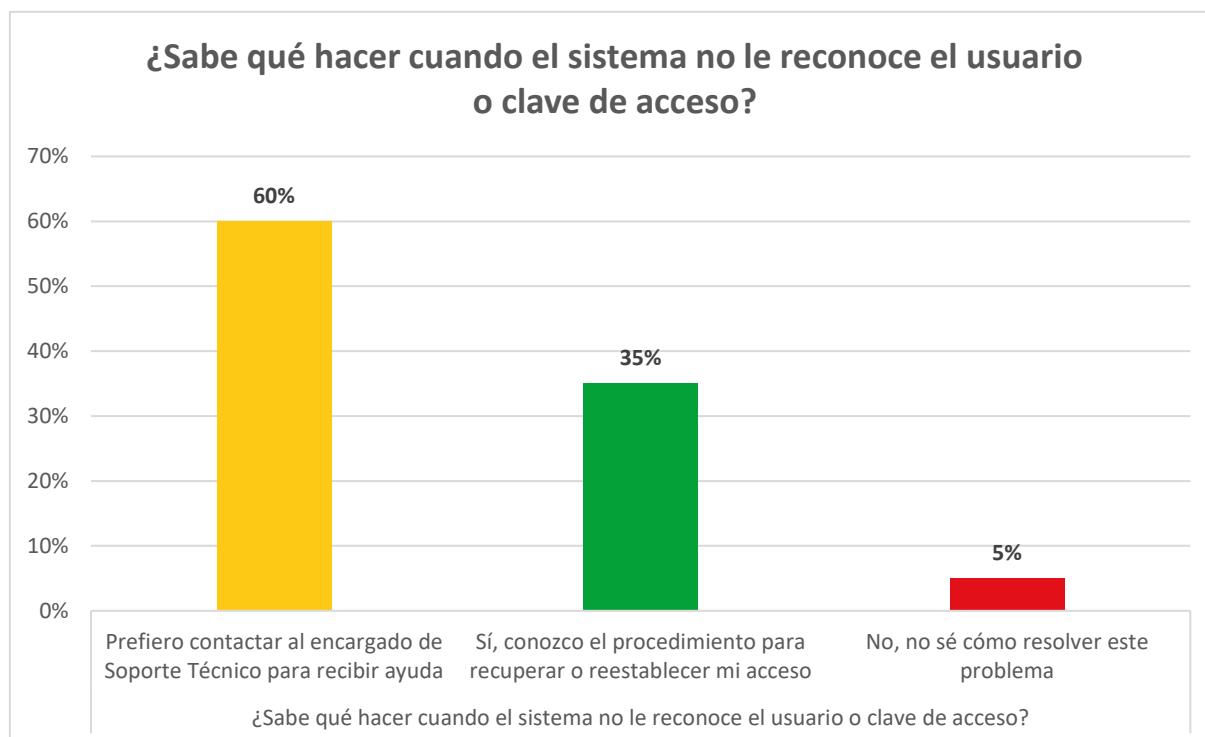
Hay un alto nivel de conocimiento en funcionalidades básicas de reuniones virtuales. Las áreas con mayor debilidad se relacionan con la capacitación formal, en especial la de herramientas de soporte (solo 17% la ha recibido). A pesar de que la mayoría cuenta con soporte técnico, el bajo acceso a formación sugiere que los colaboradores dependen más del acompañamiento directo que de una autonomía digital. Se recomienda fortalecer las capacitaciones en herramientas de mesa de ayuda, con sesiones prácticas y recursos didácticos. Promover manuales o guías rápidas sobre funciones básicas como compartir enlaces y Evaluar la cobertura de soporte técnico en las dependencias faltantes, buscando soluciones remotas si es necesario.



Una mayoría significativa (65%) depende de apoyo externo para resolver fallas de conexión, lo cual evidencia una brecha en autonomía tecnológica. Solo 1 de cada 3 usuarios es autosuficiente en este aspecto. La respuesta casi unánime a favor del soporte técnico (92%) indica que ésta es la principal fuente de solución frente a problemas de conectividad. La mesa de ayuda tiene muy baja incidencia (6%), lo cual puede deberse a falta de conocimiento, confianza o acceso a dicha herramienta. El 2% sin problemas es estadísticamente poco representativo, pero muestra que los fallos de conexión son prácticamente universales.



La mayoría del personal no cuenta con habilidades básicas para solucionar fallos con impresoras o escáneres. El soporte técnico es indispensable, pero su uso intensivo puede provocar demoras si no se acompaña de otros recursos. El desconocimiento o baja efectividad de la Mesa de ayuda se repite como patrón preocupante. Se recomienda Realizar talleres prácticos sobre solución de problemas comunes con impresoras y escáneres (instalación de drivers, errores frecuentes, configuración de red), Promover activamente la Mesa de ayuda como canal alternativo, Diseñar guías rápidas y de fácil acceso para solucionar los problemas más frecuentes con estos dispositivos e Implementar un sistema de seguimiento para medir tiempos y efectividad de atención entre soporte y mesa de ayuda.



La mayoría del personal prefiere contactar al área de soporte cuando enfrenta problemas de acceso, lo que sugiere que no se sienten seguros o no están familiarizados con el proceso de recuperación de credenciales, Autonomía técnica moderada (35%). Un poco más de un tercio conoce cómo recuperar o restablecer su acceso sin ayuda, lo cual es positivo, pero aún insuficiente para reducir la carga sobre el equipo de soporte técnico y Desconocimiento preocupante (5%). Un pequeño grupo admite no saber qué hacer ante este problema, lo que podría derivar en retrasos operativos o pérdida de productividad.

4.2 Encuesta de Satisfacción Final

4.2.1 Percepción de conectividad

El problema principal no es la disponibilidad del servicio, sino su desempeño (velocidad). La instalación de un canal adicional podría mejorar significativamente la experiencia de los usuarios y reducir la necesidad de solicitar ayuda técnica por lentitud o fallos menores.

4.2.2 Compromisos Resueltos

- Se da instrucciones para empezar caracterización para los colegios y validando una reunión para el tema.
- Se programa capacitación de Sigo para el jueves 27 de marzo. Esperando confirmación de horario.
- Se programa reunión para dar solución al GLPI Saus
- Se aclaran dudas existentes en cuanto a Sigob de escritorio y web
- Se hace cambio cable de red a computador del funcionario Rafael Galvis Jiménez en la oficina 1704 Inspección y Vigilancia.

4.2.3 Comentarios

5. Otros

Registro Fotográfico

Introducción a la Estrategia – Participación de los Contratistas y Funcionarios

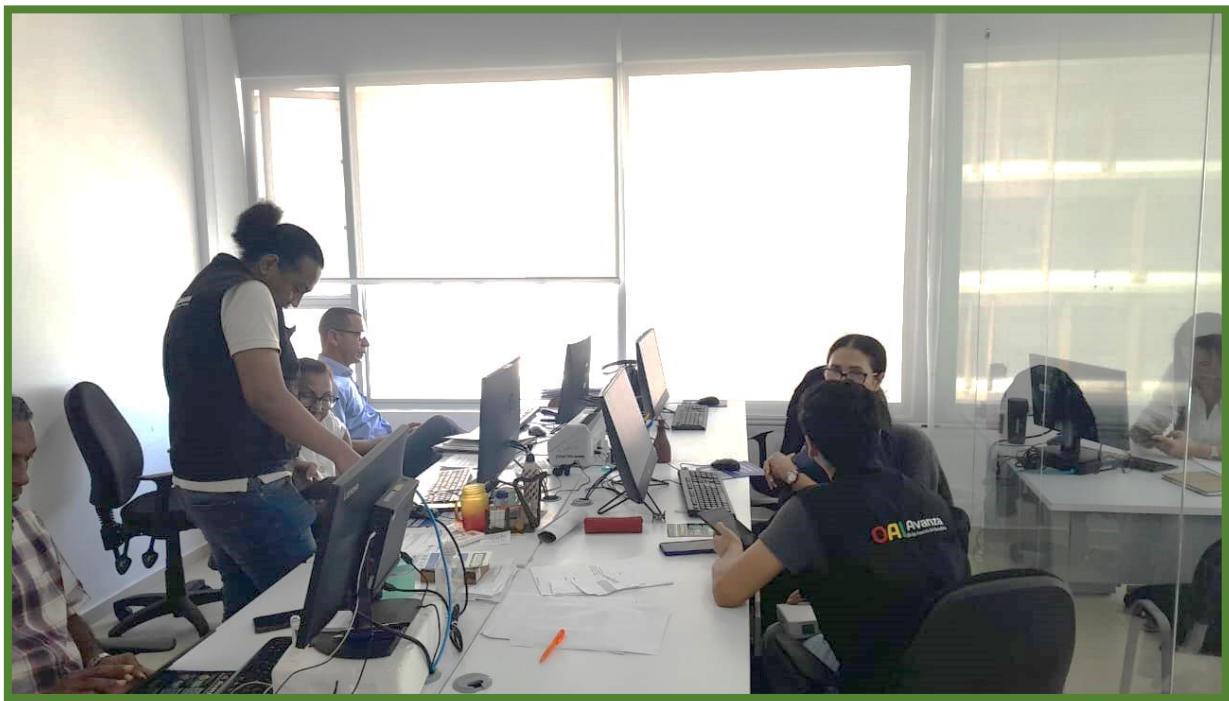


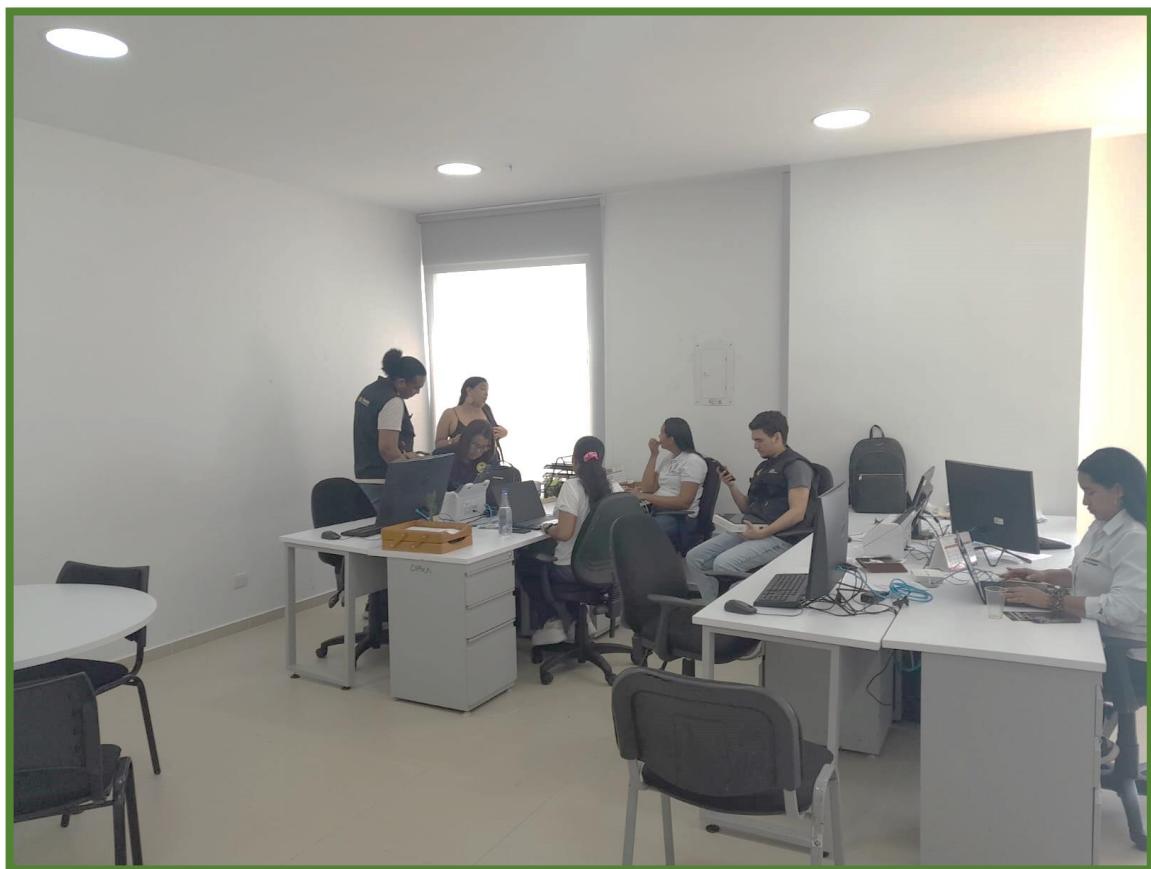
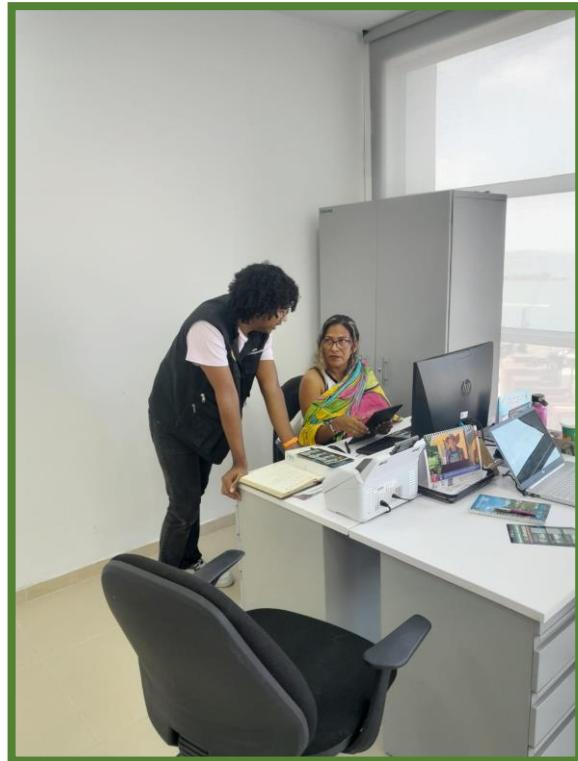
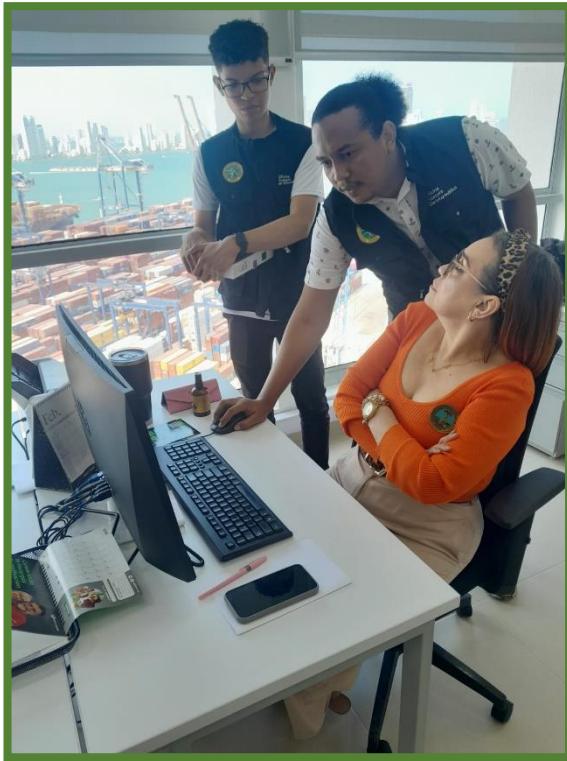






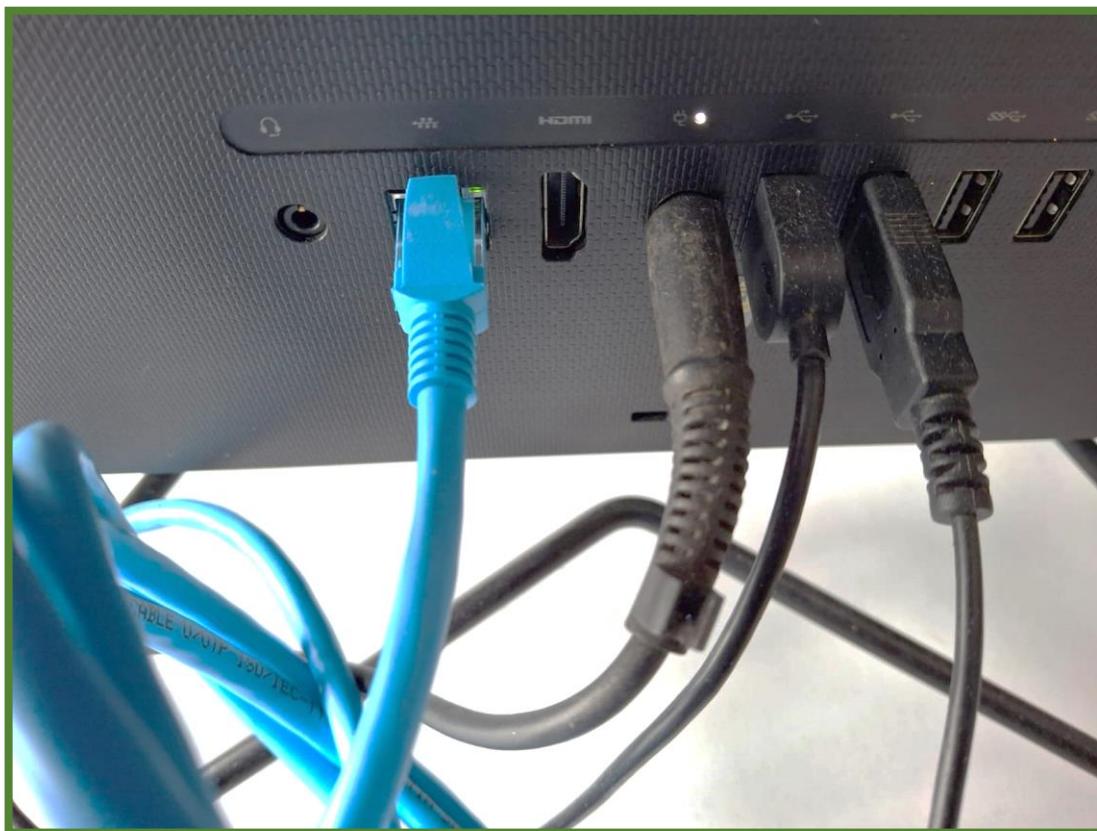
Validación Cumplimiento Políticas de Seguridad y Encuesta Diagnóstica







Soporte Técnico – Cambio Cable de red



CONTROL DE CAMBIOS		
FECHA	DESCRIPCIÓN DEL CAMBIO	VERSIÓN
17/05/202 4	Elaboración de Documento	1.0