INFORME DE PRUEBAS DE INGENIERÍA SOCIAL

DOCUMENTO CONFIDENCIAL
Elaborado por:

Versión 1.0

Febrero, 2026 Santiago de Cali.

Historial de versiones

Id	Fecha (dd/mm/aa)	Versión	Descripción	Elaborado por	Revisado por
01	23/02/2026	1.0.	Informe de pruebas de ingeniería social Transmilenio	Password Consulting Services S.A.S	Coordinador del proyecto

CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. ALCANCE 3
4. DESCRIPCIÓN DE LAS PRUEBAS 4
5.RANGOS DE ACEPTACIÓN 0
6. RESULTADOS DE LAS PRUEBAS 0
6.1. Phishing 0
6.1.1. Características de la prueba 0
6.1.2. Resultados obtenidos 2
6.1.3. Indicadores 0
6.2. Tailgating 2
6.2.1. Características de la prueba 2
6.2.2. Desarrollo de la prueba 2
6.2.3. Indicadores y Resultados 3
6.2.4. Anexos 19
6.3. Pretexting 19
7. RECOMENDACIONES GENERALES 36
8. CONCLUSIÓN 36

1. INTRODUCCIÓN

En el presente documento se describe los resultados obtenidos en la ejecución del plan de pruebas de ingeniería social para Transmilenio S.A. Así como los indicadores y riesgos.

2. OBJETIVO

Presentar los resultados obtenidos de la ejecución del plan de pruebas de ingeniería social a Transmilenio S.A. Lo anterior con el fin de evaluar la efectividad de las medidas de seguridad existentes y la conciencia de los empleados frente a ataques de ingeniería social, específicamente:

- **Phishing:** Se enviaron correos electrónicos fraudulentos para medir la tasa de clics en enlaces maliciosos y la divulgación de información confidencial.

- **Pretexting:** Se implementó la técnica de Pretexting, mediante la participación de una actriz que representó el personaje *"La Bandera Costeña – Sepcilia*", utilizada como herramienta pedagógica y de sensibilización.

- **Tailgating:** La estrategia se desarrolló mediante la simulación de ingreso a diferentes dependencias, observando el comportamiento del personal frente a diferentes situaciones.

3. ALCANCE

El alcance de este documento, detalla los resultados obtenidos de la prueba de ingeniería social no presencial, realizado a Transmilenio S.A.
A continuación, se lista la actividad de Ingeniería Social Realizada:

- Pruebas de ingeniería social (no presencial): **Phishing.**
- Pruebas de ingeniería social (presencial): **Pretexting y Tailgating**

Nota aclaratoria: Para la ejecución de las pruebas anteriormente propuesta se debe tener en cuenta, que la información o resultados obtenidos de la prueba, será la fuente para la identificación de las malas prácticas.

4. DESCRIPCIÓN DE LAS PRUEBAS

Phishing: La prueba consistió en el envío de correos electrónicos con mensajes falsos que imitan comunicaciones legítimas, invitando a los colaboradores a diligenciar una encuesta, con el objetivo de verificar cómo reaccionan los usuarios finales ante solicitudes de información sensible o confidencial (Número de teléfono, numero de cedula, y dirección de residencia).

Tailgating: Esta técnica fue utilizada como mecanismo de validación práctica de los controles de seguridad física implementados en las instalaciones, permitiendo identificar posibles vulnerabilidades asociadas al acceso a zonas restringidas y a la protección de la información.

La estrategia se desarrolló mediante la simulación de ingreso a diferentes dependencias, observando el comportamiento del personal frente a situaciones como:

- Verificación de identidad antes de permitir el ingreso a áreas controladas.
- Cumplimiento de la política de no facilitar el acceso a terceros sin autorización.
- Reporte oportuno de personas no identificadas dentro de las instalaciones.

La actividad se ejecutó en un entorno controlado y con fines pedagógicos, orientada a fortalecer la cultura de seguridad, reforzar el cumplimiento de los controles físicos establecidos e identificar oportunidades de mejora en la gestión del acceso a las áreas críticas de la organización.

Pretexting: Se implementó la técnica de Pretexting, mediante la participación de una actriz que representó el personaje *"La Bandera Costeña – Sepcilia*", utilizada como herramienta pedagógica y de sensibilización.

La prueba se desarrolló el 10 de febrero de 2026 en las instalaciones de TM ubicadas en la Avenida Calle 26 No. 69 - 76, Torre 1 y Torre 4, mediante una intervención controlada articulada a través de una actividad de pausas activas dirigida a los funcionarios de Transmilenio, lo que permitió generar un entorno natural de interacción.

5.RANGOS DE ACEPTACIÓN

Para las pruebas se definieron unos rangos de aceptación evaluados en los indicadores establecidos, con la finalidad de validar los resultados esperados desde el punto de vista del **atacante**, en donde se pretendía que por lo menos el **5%** de los funcionarios sometidos a las pruebas entregaran algún tipo de información y desde el punto de vista de la entidad **Transmilenio S.A.** se esperaba que no supere el **3%**.

En la siguiente tabla se presentan los rangos de aceptación:

ID	Descripción	Desde >	Hasta <=
1	Raro	0%	3%
2	Poco probable	3%	10%
3	Posible	10%	30%
4	Probable	30%	50%
5	Casi cierta	50%	100%

Tabla Rangos de aceptación

6. RESULTADOS DE LAS PRUEBAS

6.1. Phishing

6.1.1. Características de la prueba

En la siguiente tabla se exponen las características implementadas para la ejecución de la prueba de Phishing:

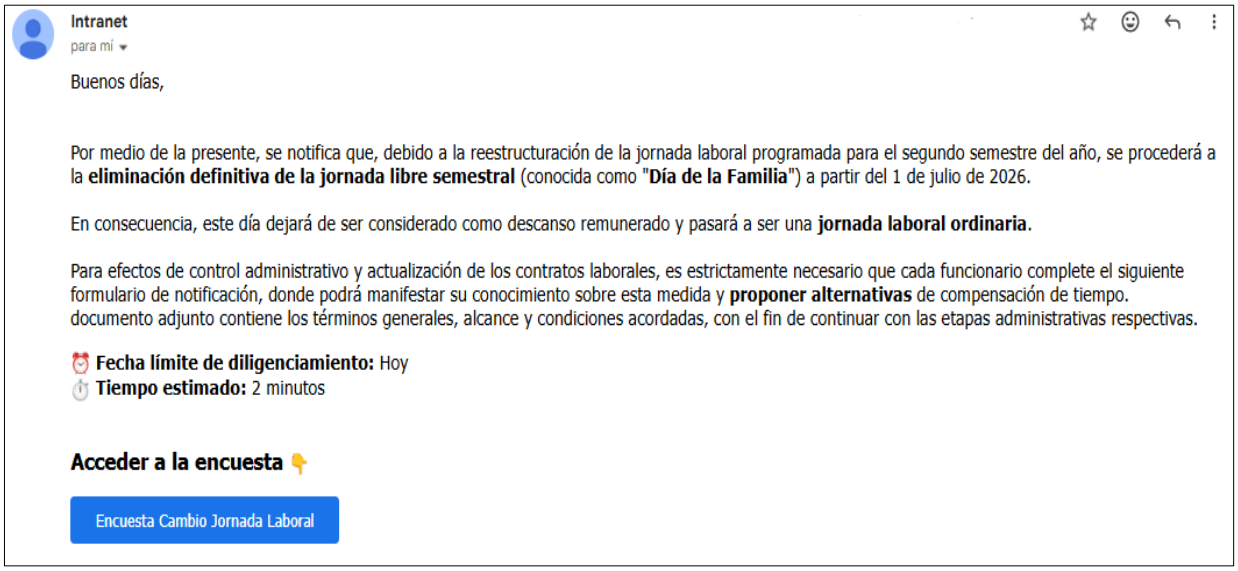
Fecha de Ejecución	10 de febrero de 2026, 8:35 am
Fecha de Finalización	12 de febrero a las 6:00 pm
Público Objetivo	30 cuentas de correo corporativas de funcionarios
Correo de envió falso	intranet@transmileniogov.com
Formulario de Captura de datos	https://forms.gle/mJgfYCCvewBGcWwD9

Herramientas Utilizadas	Aplicativo de campaña: Gophish. Servidor de Correo: Zoho mail Licencia de envió correos simultáneos: Zeptomail. Dominio suplantado: **transmileniogov.com**

Medios implementados para la prueba de Phishing

Correo Enviado

Asunto: [PRIORIDAD ALTA]: Encuesta interna requerida - Cese del beneficio "Día de la Familia" - Ley 2101 de 2021



Intranet
para mí

Buenos días,

Por medio de la presente, se notifica que, debido a la reestructuración de la jornada laboral programada para el segundo semestre del año, se procederá a la **eliminación definitiva de la jornada libre semestral** (conocida como "**Día de la Familia**") a partir del 1 de julio de 2026.

En consecuencia, este día dejará de ser considerado como descanso remunerado y pasará a ser una **jornada laboral ordinaria**.

Para efectos de control administrativo y actualización de los contratos laborales, es estrictamente necesario que cada funcionario complete el siguiente formulario de notificación, donde podrá manifestar su conocimiento sobre esta medida y **proponer alternativas** de compensación de tiempo. documento adjunto contiene los términos generales, alcance y condiciones acordadas, con el fin de continuar con las etapas administrativas respectivas.

⏰ **Fecha límite de diligenciamiento:** Hoy
⏱️ **Tiempo estimado:** 2 minutos

Acceder a la encuesta 👇

Encuesta Cambio Jornada Laboral

Formulario:



6.1.2. Resultados obtenidos

Cantidad de correos electrónicos enviados	**30**
Cantidad de funcionarios que abrieron el correo	**8**
Cantidad de veces que se dio "Click" en enlace URLs	**5**
Cantidad funcionarios que suministraron información	**3**
Cantidad de correos electrónicos reportados como malicioso	**2**

Tabla de Resultados obtenidos

	ID	Estado	Fecha de envió	Correo electrónico
1	MrtAD7o	Click en enlace	2026-02-10T13:37:02.429964369Z	alejandro.monroy@transmilenio.gov.co
2	2YmDP49	Correo abierto	2026-02-10T13:37:05.541674667Z	alexandra.alvarez@transmilenio.gov.co
3	0DMIj66	Correo abierto	2026-02-10T13:37:07.817780462Z	alicia.suarez@transmilenio.gov.co
4	p2EywLA	Click en enlace	2026-02-10T13:37:14.151711946Z	aura.camargo@transmilenio.gov.co
5	baVCCFd	Correo abierto	2026-02-10T13:37:16.54697265Z	camilo.oliveros@transmilenio.gov.co
6	krz2Kja	Correo enviado	2026-02-10T13:37:18.352998015Z	camilo.forero@transmilenio.gov.co
7	h6xu70W	Correo enviado	2026-02-10T13:37:31.427757088Z	cesar.torres@transmilenio.gov.co
8	SqoyQFe	Correo enviado	2026-02-10T13:37:33.580859593Z	cristina.nino@transmilenio.gov.co
9	iiPUgMA	Correo enviado	2026-02-10T13:37:50.313759373Z	edgar.galindo@transmilenio.gov.co

	ID	Estado	Fecha de envió	Correo electrónico
10	DBm2Ms6	Click en enlace	2026-02-10T13:37:52.670047402Z	edwin.castellanos@transmilenio.gov.co
11	9frchn5	Correo abierto	2026-02-10T13:37:53.854191637Z	freddy.cepeda@transmilenio.gov.co
12	cY6R8Au	Correo enviado	2026-02-10T13:37:58.050812471Z	german.naranjo@transmilenio.gov.co
13	wQ0do4b	Correo enviado	2026-02-10T13:37:59.883866584Z	helber.romero@transmilenio.gov.co
14	ZBVp02H	Click en enlace	2026-02-10T13:38:00.711083548Z	isabel.zapata@transmilenio.gov.co
15	2Eum9I8	Correo abierto	2026-02-10T13:38:01.442181276Z	jacqueline.torres@transmilenio.gov.co
16	t6W2NgS	Correo enviado	2026-02-10T13:38:02.24792764Z	jamis.torres@transmilenio.gov.co
17	u0iOFrq	Correo enviado	2026-02-10T13:38:02.993193953Z	jorge.castro@transmilenio.gov.co
18	Xac0zXz	Correo enviado	2026-02-10T13:38:03.753558486Z	juan.rueda@transmilenio.gov.co
19	esDv7la	Correo enviado	2026-02-10T13:38:04.561553827Z	juan.becaria@transmilenio.gov.co
20	PIT0XXJ	Correo enviado	2026-02-10T13:38:05.331634343Z	juanm.moreno@transmilenio.gov.co
21	aIM8bMB	Correo enviado	2026-02-10T13:38:06.11542093Z	katterine.lugo@transmilenio.gov.co
22	4ScM6Am	Click en enlace	2026-02-10T13:38:06.931444941Z	marcela.carrascal@transmilenio.gov.co
23	6P0oeiR	Correo abierto	2026-02-10T13:38:07.696955439Z	natalia.garcia@transmilenio.gov.co
24	XZhH1k0	Correo enviado	2026-02-10T13:38:08.474332216Z	rafael.avendano@transmilenio.gov.co
25	VyjmObP	Correo enviado	2026-02-10T13:38:09.228518893Z	sebastian.paramo@transmilenio.gov.co
26	ByQikUm	Correo enviado	2026-02-10T13:38:09.967986132Z	tania.bernal@transmilenio.gov.co
27	NzYOIgA	Correo abierto	2026-02-10T13:38:10.714045053Z	victor.mercado@transmilenio.gov.co
28	73asJ4m	Correo enviado	2026-02-10T13:38:11.471618368Z	winston.barrios@transmilenio.gov.co
29	PbZ9Nnn	Correo abierto	2026-02-10T13:38:12.22094148Z	gretta.bolano@transmilenio.gov.co
30	mKMmVpB	Correo enviado	2026-02-10T13:38:12.963586809Z	juan.buitrago@transmilenio.gov.co

Tabla de Resultados obtenidos

Color	Descripción
Verde	Correos enviados, y sin interacción por parte del usuario.
Naranja	Correos abierto por parte del usuario
Rojo	Usuarios que dieron click en el enlace

Información suministrada: Datos personales como (Número de teléfono, número de cedula, dirección de sus residencias y cuenta de correo corporativo).

Fecha	Hora	¿Usted ha programado el uso de su "Día de la Familia" para el segundo semestre de 2026?	Dada la eliminación del día libre, ¿cuál de estas opciones preferiría para recuperar ese tiempo de descanso?	Dirección de residencia	¿Fue notificado previamente sobre la eliminación del Día de la Familia a partir de julio de 2026?	Número de Teléfono	¿Estaría de acuerdo en cambiar el día libre por un bono económico equivalente a media jornada?	Número de Cédula	Para fines de validación de identidad ante la oficina, y respectiva notificación. Ingrese su correo electrónico:
10/02/2026	8:48 a. m.	No, aún no lo he programado	Trabajar una hora extra diaria durante una semana.	Carrera 14B # 161-54 Torre 14 Apto 304	No	3012918787	Si	39686356	isabel.zapata@transmilenio.gov.co
10/02/2026	8:55 a. m.	No, aún no lo he programado	Me es indiferente, acepto la eliminación.	Calle 163 # 59 a - 10	Si	3143550892	Si	24202509	alicia.suarez@transmilenio.gov.co
10/02/2026	10:45 a. m	No, aún no lo he programado	Trabajar una hora extra diaria durante una semana.	Calle 66a No. 96a-23	Si	3212765768	Si	27852574	Marcela.carrascal@transmilenio.gov.co

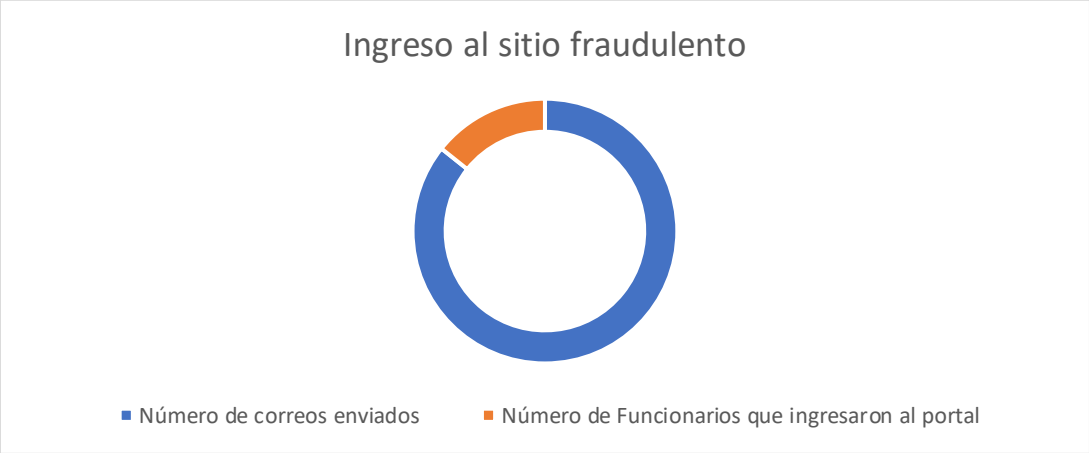
6.1.3. Indicadores

Resultados obtenidos

- **Ingresos al sitio fraudulento:**

$$\frac{\textbf{5}\text{ número de funcionarios que ingresaron al formulario}}{\textbf{30}\text{ número de funcionarios objetivo para la prueba}} * 100 = \textbf{16,6\%}$$

De acuerdo con el resultado del **indicador No.1**: El **16,6%** de los funcionarios ingresó al enlace malicioso; la probabilidad de que se materialice un riesgo tipo phishing es "**Posible**".

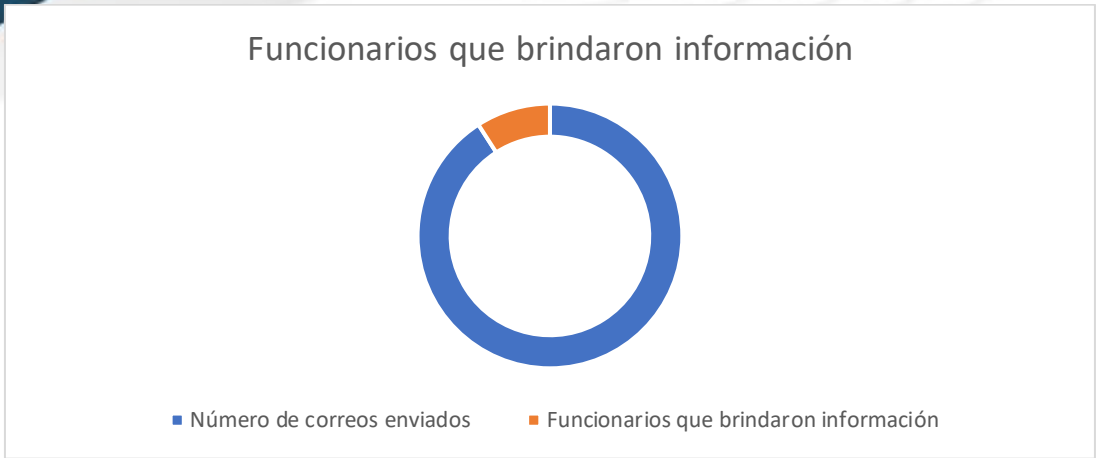


Gráfica indicador ingreso al sitio sospechoso

- **Usuarios que suministraron información:**

$$\frac{\textbf{3}\text{ número de funcionarios que suministraron información}}{\textbf{30}\text{ número de funcionarios objetivo para la prueba}} * 100 = \textbf{10\%}$$

De acuerdo con el resultado del **indicador No.2**: De los funcionarios que ingresaron al enlace malicioso, el **10%** suministro información confidencial, la probabilidad de que se filtre información con una actividad tipo phishing es "**Poco probable**".



Gráfica indicador funcionarios que brindaron información

- **Reporte de incidente:**

  2 número de funcionarios que reportaron el correo / **30** número de funcionarios objetivo para la prueba * **100 = 6.66%**

De acuerdo con el resultado del **indicador No 3**, De los funcionarios que recibieron y abrieron el correo, el **6.66%** reporto el correo en mención como un incidente de seguridad, o marcándolo como spam en su bandeja de entrada. la probabilidad de que los funcionarios reporten actividad tipo phishing es "**Poco probable**".

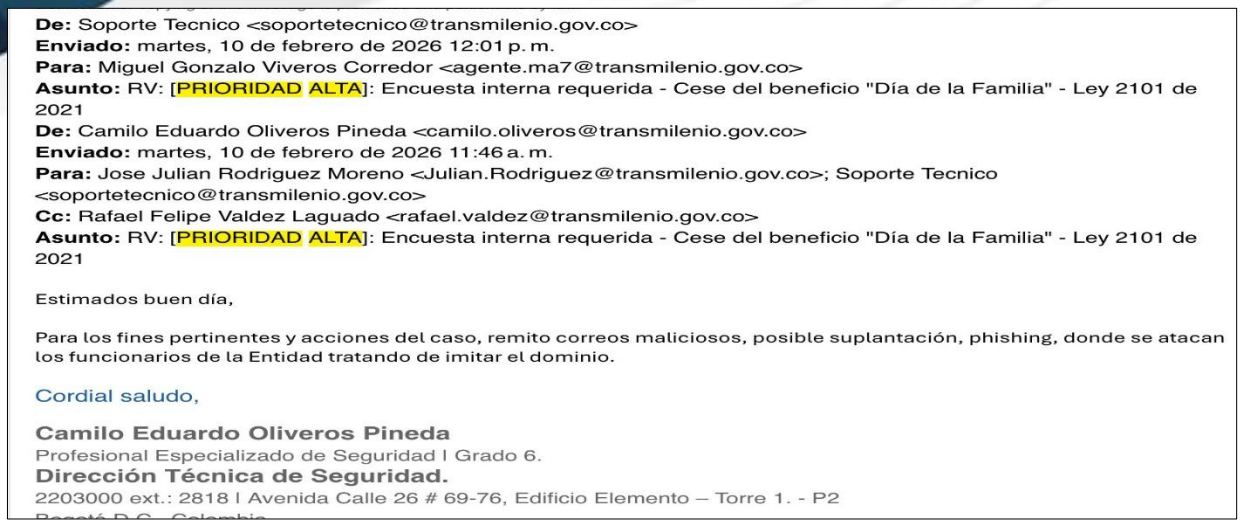
De: Alicia Suarez Rojas <alicia.suarez@transmilenio.gov.co>
Enviado: Tuesday, February 10, 2026 9:05:01 AM
Para: Direccion de TICs <DireccionTICs@transmilenio.gov.co>; Jose Julian Rodriguez Moreno <Julian.Rodriguez@transmilenio.gov.co>
Asunto: Fw: [PRIORIDAD ALTA]: Encuesta interna requerida - Cese del beneficio "Día de la Familia" - Ley 2101 de 2021

Buenos días; reenvío correo que me llegó a mi correo. Para su verificación correspondiente.

Gracias

Cordialmente

Alicia Suárez Rojas
Técnico de Enlace
Dirección Técnica de BRT
alicia.suarez@transmilenio.gov.co
Av. ElDorado No 69 – 76
Edificio Elemento Torre 1 Piso 4
Teléfono: 220 3000 Extensión 1832



De: Soporte Tecnico <soportetecnico@transmilenio.gov.co>
Enviado: martes, 10 de febrero de 2026 12:01 p. m.
Para: Miguel Gonzalo Viveros Corredor <agente.ma7@transmilenio.gov.co>
Asunto: RV: [PRIORIDAD ALTA]: Encuesta interna requerida - Cese del beneficio "Día de la Familia" - Ley 2101 de 2021
De: Camilo Eduardo Oliveros Pineda <camilo.oliveros@transmilenio.gov.co>
Enviado: martes, 10 de febrero de 2026 11:46 a. m.
Para: Jose Julian Rodriguez Moreno <Julian.Rodriguez@transmilenio.gov.co>; Soporte Tecnico <soportetecnico@transmilenio.gov.co>
Cc: Rafael Felipe Valdez Laguado <rafael.valdez@transmilenio.gov.co>
Asunto: RV: [PRIORIDAD ALTA]: Encuesta interna requerida - Cese del beneficio "Día de la Familia" - Ley 2101 de 2021

Estimados buen día,

Para los fines pertinentes y acciones del caso, remito correos maliciosos, posible suplantación, phishing, donde se atacan los funcionarios de la Entidad tratando de imitar el dominio.

Cordial saludo,

Camilo Eduardo Oliveros Pineda
Profesional Especializado de Seguridad I Grado 6.
Dirección Técnica de Seguridad.
2203000 ext.: 2818 I Avenida Calle 26 # 69-76, Edificio Elemento – Torre 1. - P2

6.2. Tailgating

6.2.1. Características de la prueba

Fecha de Ejecución	18 de febrero de 2026, 10:00 am
Fecha de Finalización	18 de febrero a las 1:00 pm
Público Objetivo	Torre 1 piso 2, 4 (nivel central), 5, 6 y piso 8 torre 4
Herramientas Utilizadas	Sticker de ingreso (QR) correspondiente a días anteriores

6.2.2. Desarrollo de la prueba

La prueba se desarrolló mediante una intrusión controlada orientada a evaluar la efectividad de los controles de acceso físico implementados en TM, la cual cuenta con un procedimiento formal de validación y autorización de ingreso.

El ejercicio fue diseñado para generar un escenario realista que permitiera observar el comportamiento del personal de seguridad y funcionarios frente a situaciones de acceso no irregulares. En este contexto se implementó la técnica de Tailgating, simulando el ingreso de un funcionario nuevo, el cual no contaba con un contacto disponible para la autorización del acceso.

La actividad incluyó la interacción directa con el personal de seguridad del edificio, permitiendo evaluar aspectos relacionados con:

- Verificación de la vigencia de credenciales o permisos temporales.
- Validación de identidad de colaboradores nuevos.
- Cumplimiento del procedimiento de autorización previa para el ingreso.
- Gestión de situaciones excepcionales ante ausencia de confirmación inmediata.
- Aplicación de criterios de control antes de permitir el acceso a las instalaciones.

De manera complementaria, la intrusión permitió validar la efectividad del mecanismo de autorización por parte de funcionarios internos y analizar el nivel de rigurosidad en la aplicación de los lineamientos institucionales de seguridad física.



6.2.3. Indicadores y Resultados

- **Piso 1**

La intrusión en la torre 1, piso uno (1) puerta principal comprendió la evaluación del control de acceso gestionado por el personal de seguridad ubicado en la portería y en las puertas principales de la torre; Durante la ejecución de la prueba de Tailgating, se generó un escenario controlado simulando el ingreso de un funcionario nuevo sin contacto disponible para autorizar su acceso, utilizando un sticker correspondiente al día 17 de febrero.

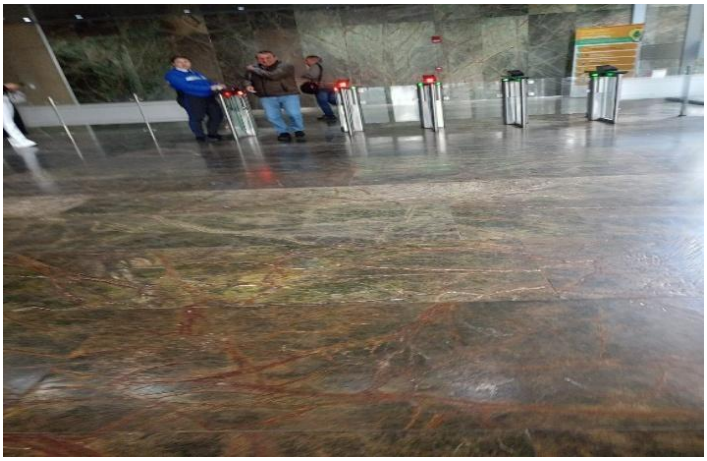
En el punto de control se encontraban cuatro (4) guardias de seguridad en la portería y dos (2) en la puerta principal, quienes realizaron la validación del permiso presentado.

Como resultado de la intervención, se evidenció lo siguiente:

- No fue permitido el ingreso con el sticker correspondiente a una fecha anterior, debido a la verificación de vigencia del permiso.
- El personal de seguridad exigió autorización formal para permitir el acceso al edificio.
- El ingreso fue posible mediante la intervención y autorización expresa de una funcionaria de TM, quien confirmó el acceso.

Los resultados evidencian una aplicación adecuada del procedimiento de control de acceso en lo relacionado con la verificación de vigencia de permisos temporales y la exigencia de autorización previa. No obstante, se identifica como aspecto a fortalecer la formalización y trazabilidad del mecanismo de autorización otorgado por funcionarios internos, con el fin de asegurar que este tipo de validaciones se realicen exclusivamente a través de los canales institucionales establecidos.

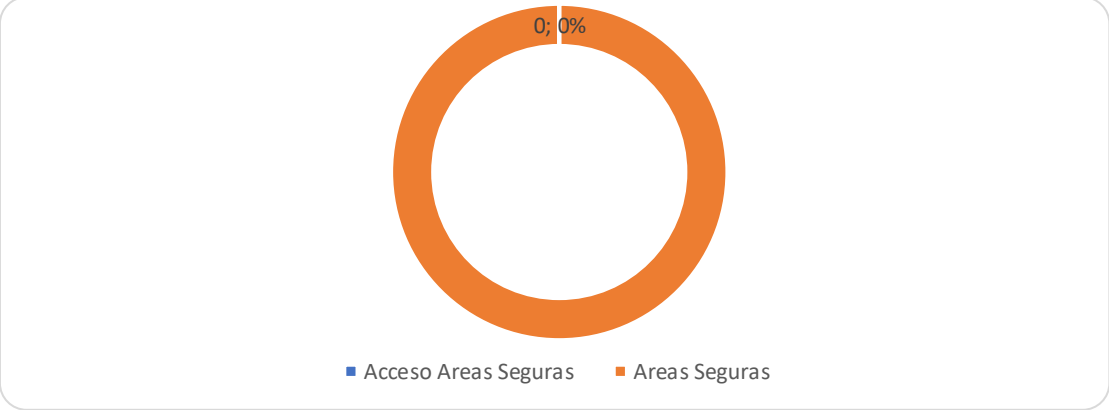
En términos generales, en el piso uno (1) se presentó un nivel de control efectivo frente a intentos de ingreso con credenciales vencidas, demostrando consistencia en la aplicación del protocolo de seguridad física.





- **Ingreso a áreas seguras:**

$$\frac{0 \text{ número de áreas seguras donde se ingreso}}{1 \text{ número de áreas seguras}} * 100\% = 0\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso a áreas seguras de TM, la probabilidad de que se pueda acceder es "**raro**".

- **Piso 2**

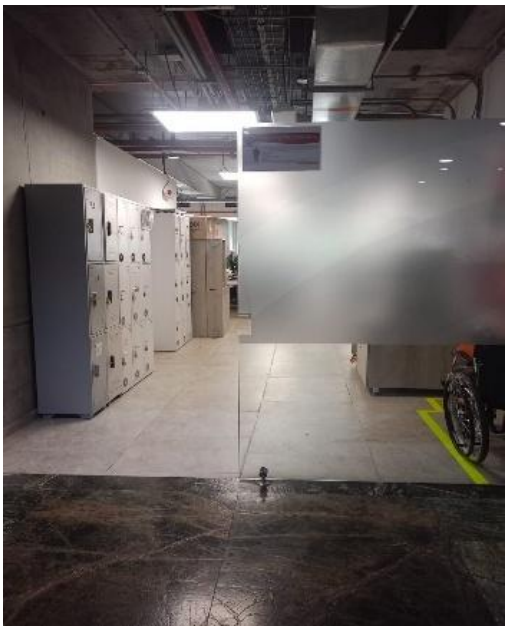
La intrusión en la torre1, el piso dos (2) comprendió las áreas generales del nivel y dos (2) zonas clasificadas como segura y restringida. Durante la actividad de Tailgating se

simuló el ingreso bajo el pretexto de realizar una actualización de inventario del inmobiliario, lo que permitió generar un entorno de interacción controlada.

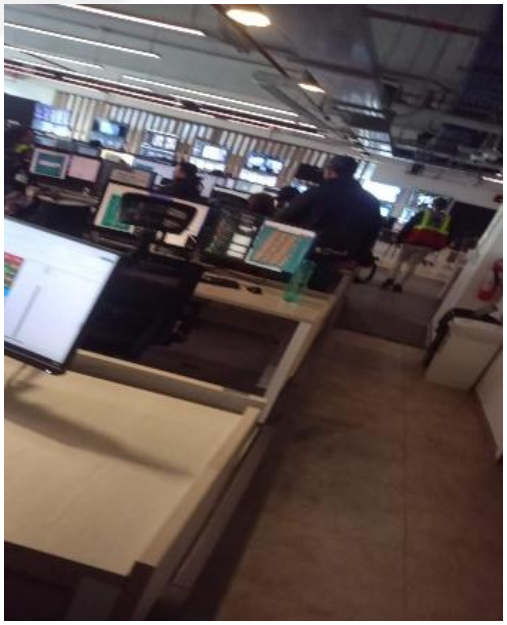
Como resultado de la evaluación, se identificaron las siguientes situaciones:

- Generación de tiquete de ingreso por parte del personal de seguridad para acceso a áreas generales.
- Ingreso sin acompañamiento inicial a dependencias del piso.
- Bloqueo efectivo al intentar acceder a zona segura y restringida.
- Solicitud de autorización formal mediante correo electrónico o acompañamiento de funcionario responsable.

Los hallazgos evidencian aplicación diferenciada de los controles de seguridad, con mayor rigurosidad en áreas clasificadas como restringidas. Aun así, se identifica oportunidad de fortalecimiento en la validación del alcance del permiso otorgado para actividades operativas dentro del piso.



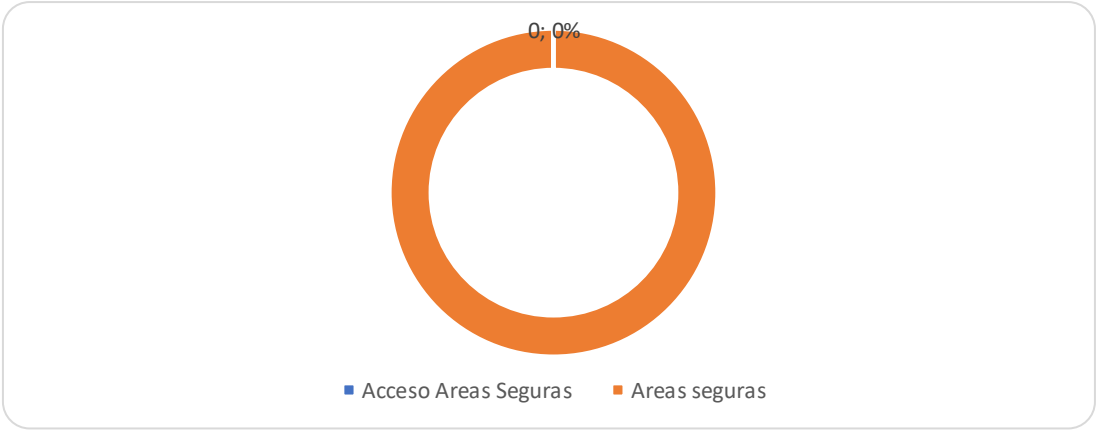






- **Ingreso a áreas seguras:**

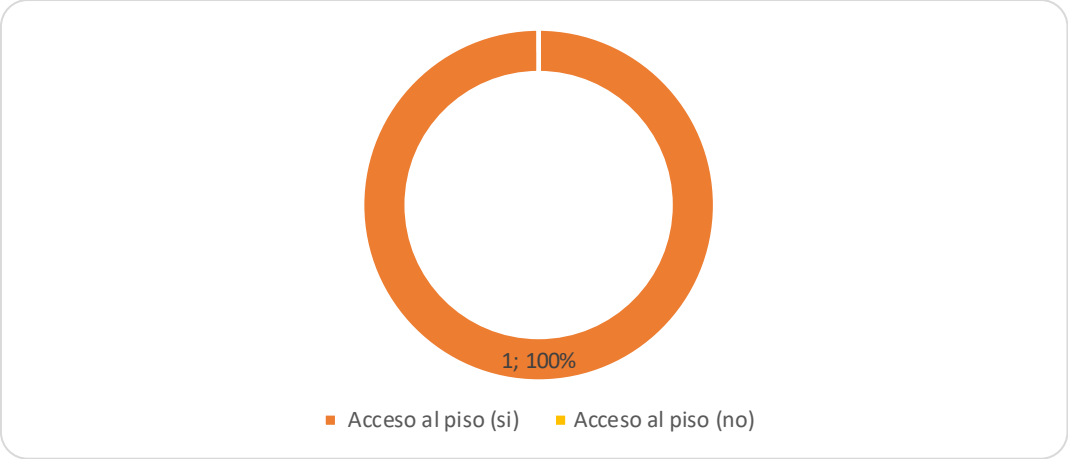
$$\frac{0 \text{ número de áreas seguras donde se ingreso}}{2 \text{ número de áreas seguras}} * 100\% = 0\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso a áreas seguras de TM, la probabilidad de que se pueda acceder es "**raro**".

- **Ingreso al piso:**

$$\frac{1 \text{ número de ingreso a pisos}}{1 \text{ número de pisos ingresados}} * 100\% = 100\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso al piso 2 de TM, la probabilidad de que se pueda acceder es "**Casi cierto**", considerando que el ingreso fue permitido sin una validación restrictiva equivalente a la aplicada en las zonas seguras.

➢ **Piso 4**

La intrusión en la torre, piso cuatro (4) comprendió las áreas generales del nivel y las zonas clasificadas como seguras y restringidas. Durante la actividad de Tailgating, se simuló el ingreso bajo un pretexto operativo previamente definido, con el objetivo de evaluar la efectividad de los controles de acceso físico implementados.

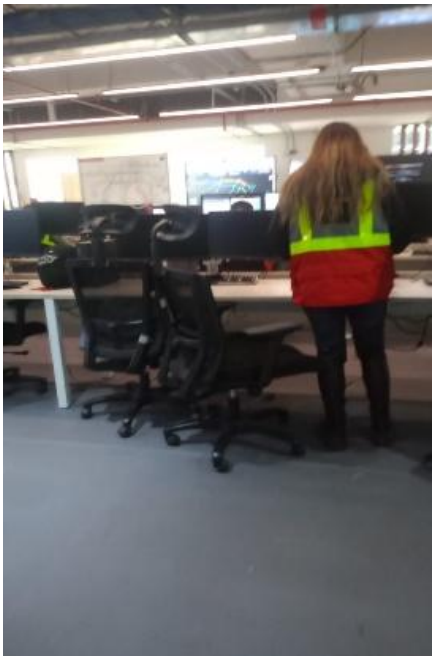
Como resultado de la evaluación, se identificaron las siguientes situaciones:

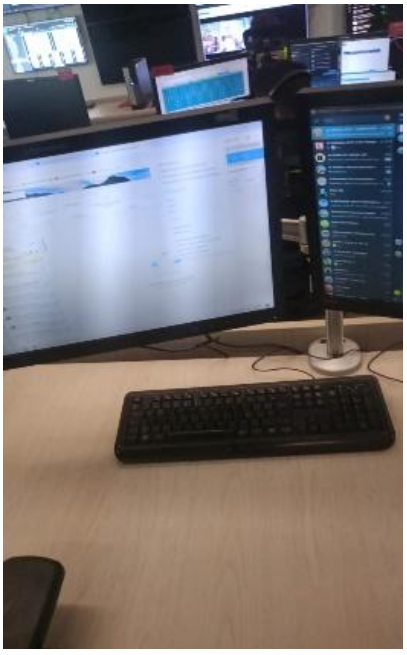
- Ingreso al piso sin solicitud de explicación o validación detallada por parte del personal de seguridad.
- Acceso permitido a áreas generales sin verificación del alcance o necesidad de la actividad informada.
- Restricción efectiva al intentar ingresar a zonas clasificadas como seguras y restringidas.
- Aplicación de controles más rigurosos únicamente en áreas críticas.

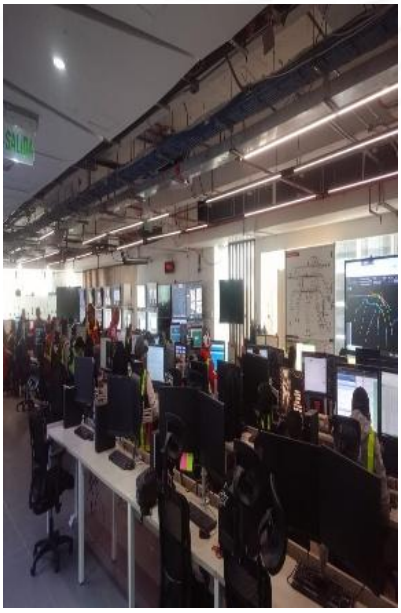
Los hallazgos evidencian una debilidad en el control de acceso general al piso, dado que no se realizó validación previa del motivo de ingreso ni verificación formal por parte del personal de vigilancia.







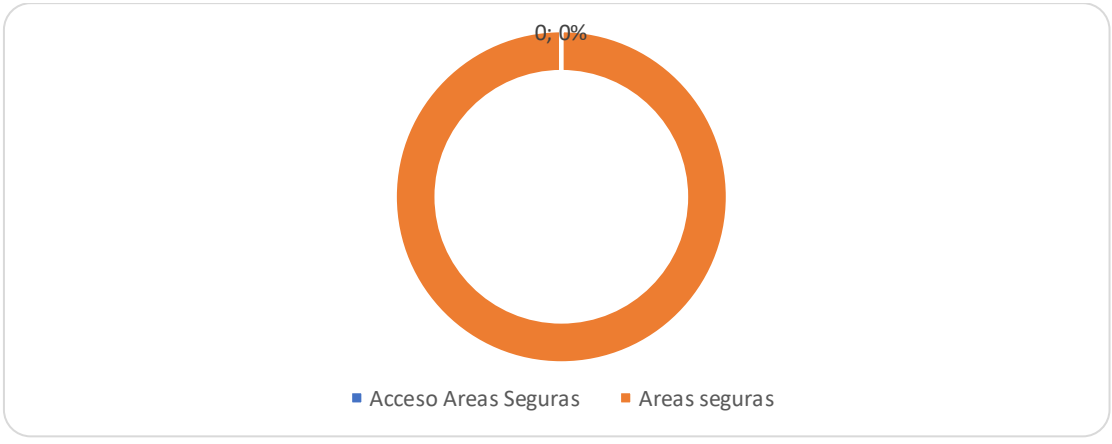




Durante la intervención realizada en el piso cuatro (4) se evaluó una (1) zona segura cumpliendo los controles de seguridad.

- **Ingreso áreas seguras:**

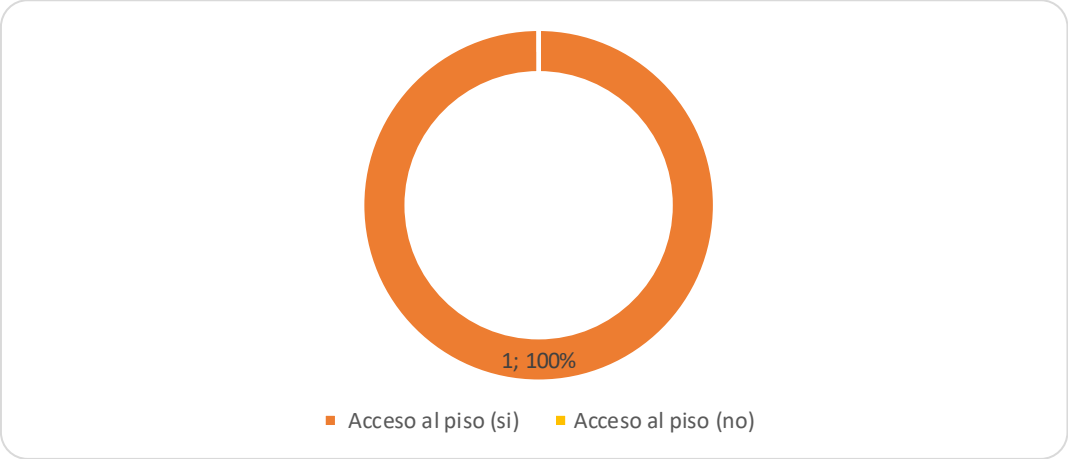
$$\frac{0 \text{ número de áreas seguras donde se ingreso}}{1 \text{ número de áreas seguras}} * 100\% = 0\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso a áreas seguras de TM, la probabilidad de que se pueda acceder es "**raro**".

- **Ingreso al piso:**

$$\frac{1 \text{ número de ingreso a pisos}}{1 \text{ número de pisos ingresados}} * 100\% = 100\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso al piso 4 de TM, la probabilidad de que se pueda acceder es "**Casi cierto**", considerando que el ingreso fue permitido sin una validación restrictiva equivalente a la aplicada en las zonas seguras.

➢ **Piso 5**

La intervención en la torre 1, piso cinco (5) comprendió las áreas generales del nivel y las zonas clasificadas como seguras y restringidas. Durante la actividad de Tailgating, se simuló el ingreso bajo un pretexto operativo previamente definido, con el objetivo de evaluar la efectividad de los controles de acceso físico implementados.

Como resultado de la evaluación, se identificaron las siguientes situaciones:

- Validación por parte del guardia de seguridad, quien informó que, debido a la condición de visitante (evidenciada mediante sticker), el ingreso debía realizarse con acompañamiento de un funcionario responsable, por lo cual en ese momento no fue posible continuar.
- Posteriormente, tras transcurrir un periodo de tiempo, se intentó nuevamente el ingreso, sin que se presentara objeción o verificación adicional por parte del personal de vigilancia.
- Restricción efectiva al intentar ingresar a zonas clasificadas como seguras y restringidas.
- Aplicación de controles más rigurosos únicamente en áreas seguras.

Los hallazgos evidencian una aplicación parcial de los controles de acceso físico. Si bien inicialmente se realizó una validación conforme al protocolo para visitantes, la falta de consistencia en la verificación permitió el ingreso sin acompañamiento, lo que representa una oportunidad de mejora en la aplicación uniforme de los controles en el acceso general al piso. No obstante, se observó adecuada efectividad en las zonas seguras, donde el acceso fue restringido.

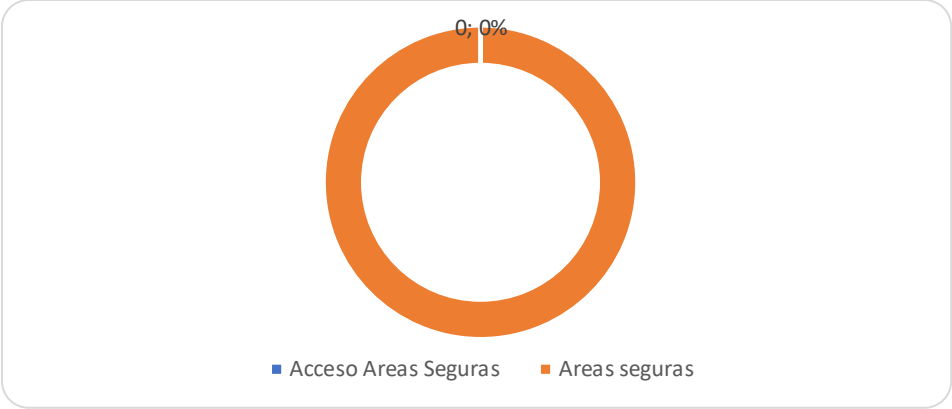






- **Ingreso áreas seguras:**

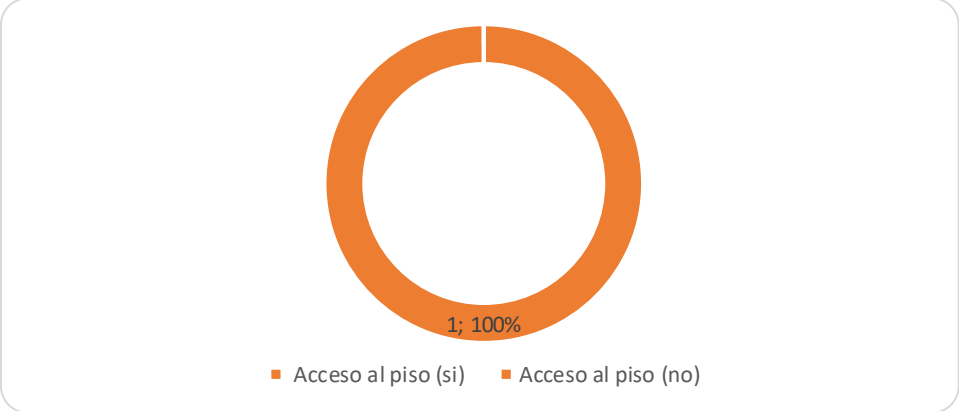
$$\frac{0 \text{ número de áreas seguras donde se ingreso}}{2 \text{ número de áreas seguras}} * 100\% = 0\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso a áreas seguras de TM, la probabilidad de que se pueda acceder es "**raro**".

- **Ingreso al piso:**

$$\frac{1 \text{ número de ingreso a pisos}}{1 \text{ número de pisos ingresados}} * 100\% = 100\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso al piso 4 de TM, la probabilidad de que se pueda acceder es "**Casi cierto**", considerando que el ingreso fue permitido sin una validación restrictiva equivalente a la aplicada en las zonas seguras.

- **Piso 6**

La intrusión en la torre 1, piso seis (6) comprendió las áreas generales del nivel y las zonas clasificadas como seguras y restringidas con el objetivo de evaluar la efectividad de los controles de acceso físico implementados.

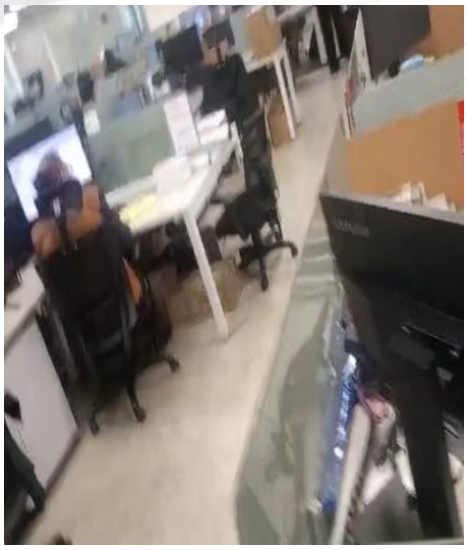
Como resultado de la evaluación, se identificaron las siguientes situaciones:

- Validación por parte del guardia de seguridad, el cual realiza inspección de maleta tanto al ingreso como a la salida, así como registro en minuta de los elementos ingresados.
- Acceso permitido al piso una vez realizada la validación correspondiente.
- Restricción efectiva al intentar ingresar a zonas clasificadas como seguras y restringidas.

Los hallazgos evidencian que los controles de acceso físico en el piso 6 presentan un nivel adecuado de aplicación en el acceso general, al realizarse inspección y registro de elementos conforme al protocolo establecido. Asimismo, se observó una adecuada efectividad en las zonas seguras, donde el acceso fue restringido conforme a los controles definidos.

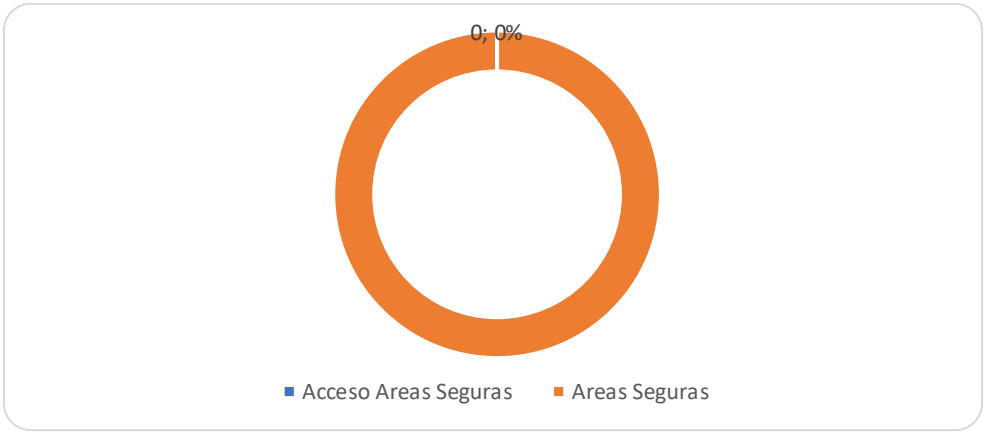






- **Ingreso áreas seguras:**

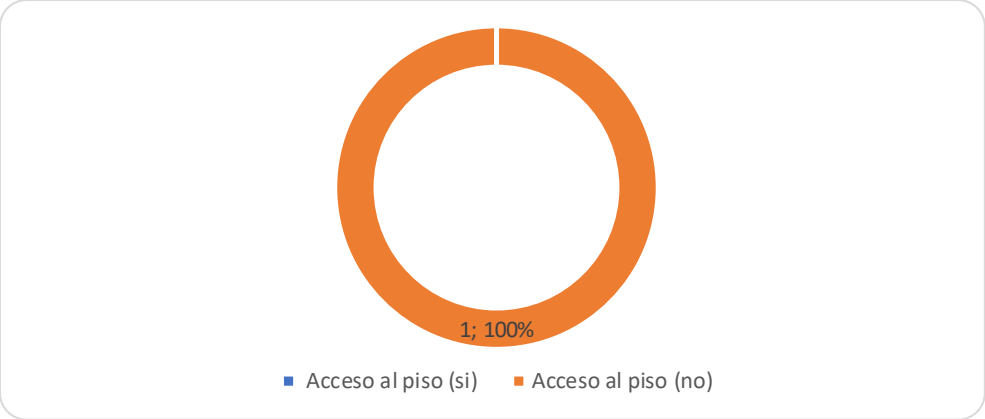
$$\frac{0 \text{ número de áreas seguras donde se ingreso}}{1 \text{ número de áreas seguras}} * 100\% = 0\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso a áreas seguras de TM, la probabilidad de que se pueda acceder es "**raro**".

- **Ingreso al piso:**

$$\frac{1 \text{ número de ingreso a pisos}}{1 \text{ número de pisos ingresados}} * 100\% = 100\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso al piso 4 de TM, la probabilidad de que se pueda acceder es "**Casi cierto**", considerando que el ingreso fue permitido, aun sin cuando se realiza inspección de elementos y la verificación de registros en minuta.

Torre 4 Piso 8

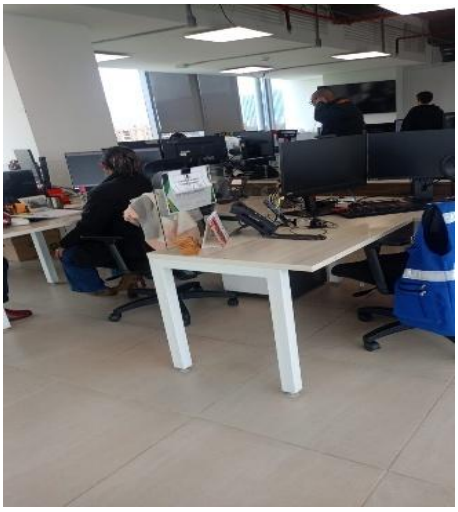
La intrusión en la torre cuatro (4) piso ocho (8) comprendió las áreas generales del nivel y las zonas clasificadas como seguras y restringidas, con el objetivo de evaluar la efectividad de los controles de acceso físico implementados.

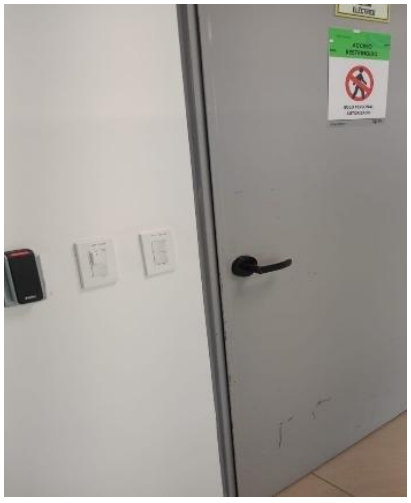
Como resultado de la evaluación, se identificaron las siguientes situaciones:

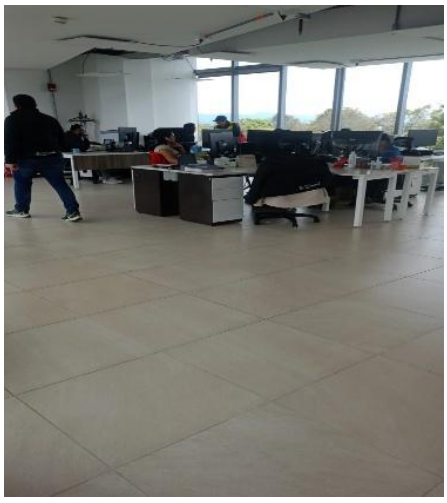
- Validación por parte del guardia de seguridad para el ingreso a la torre, realizando confirmación telefónica con el área correspondiente, quien autorizó el acceso.
- Restricción efectiva al intentar ingresar a zonas clasificadas como seguras y restringidas.
- Al momento de la salida, se evidenció ausencia del personal de vigilancia en el punto de control, lo que permitió retirarse sin validación de identidad. Lo que permitió un nuevo ingreso a la Torre uno (1) y a los pisos dos (2), cuatro (4), cinco (5) y seis (6) sin verificación adicional.

Los hallazgos evidencian que, si bien los controles de acceso físico presentan una adecuada aplicación en el ingreso inicial y en las zonas seguras, existe una debilidad significativa en el control de salida y en la continuidad de la verificación de identidad en los demás pisos de la torre 1. Esta situación representa una oportunidad de mejora en la supervisión permanente de los puntos de control y en la aplicación consistente de validación de ingreso y salida.



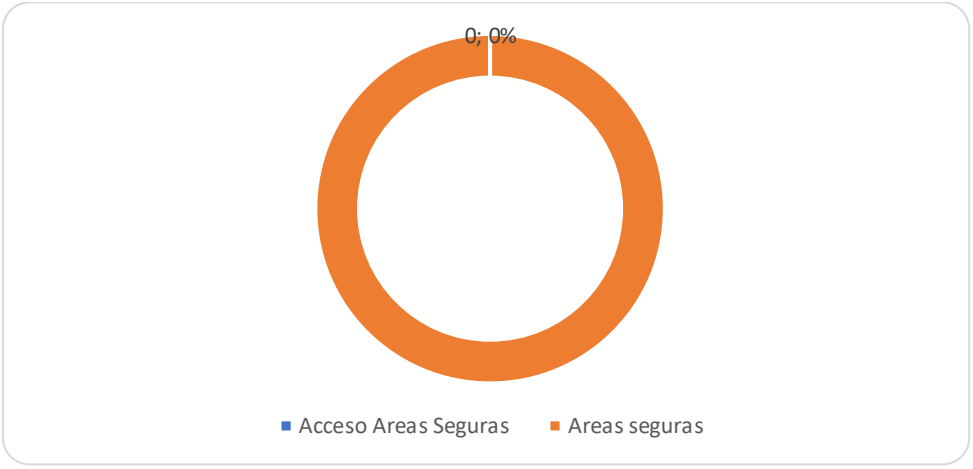






- **Ingreso áreas seguras:**

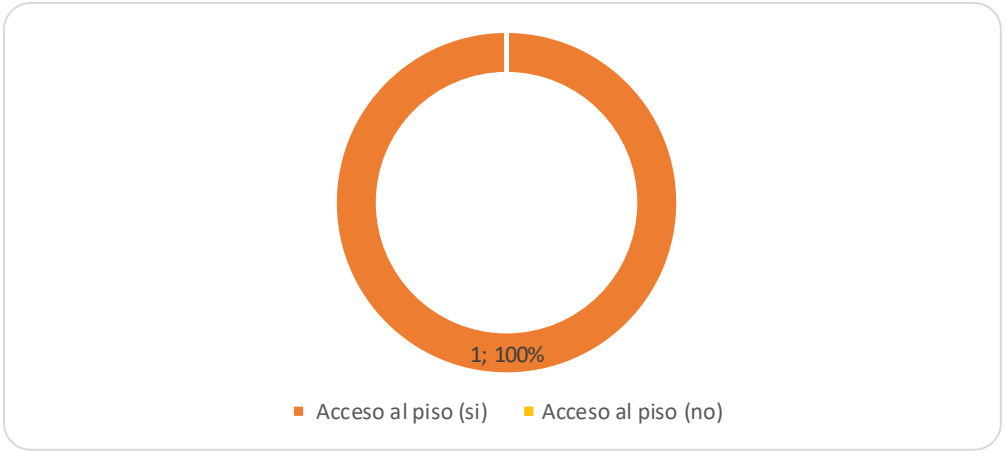
$$\frac{0 \text{ número de áreas seguras donde se ingreso}}{1 \text{ número de áreas seguras}} * 100\% = 0\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso a áreas seguras de TM, la probabilidad de que se pueda acceder es "**raro**".

- **Ingreso al piso:**

$$\frac{1 \text{ número de ingreso a pisos}}{1 \text{ número de pisos ingresados}} * 100\% = 100\%$$



De acuerdo con el resultado del **indicador**, del intento de ingreso al piso 4 de TM, la probabilidad de que se pueda acceder es "**Casi cierto**", considerando que el ingreso fue permitido sin una validación restrictiva.

6.2.4. Anexos

Evidencias Fotográficas

https://drive.google.com/drive/folders/1lwOwpz_fCFsRZKbA-6geLC7tQLsRiMEN?usp=drive_link

6.3. Pretexting

La prueba se desarrolló el 10 de febrero de 2026 en las instalaciones de TM ubicadas en la Avenida Calle 26 No. 69 - 76, Torre 1 y Torre 4, mediante una actividad de distracción controlada y articulada con TM a través de pausas activas dirigida a los funcionarios, lo que permitió generar un entorno natural de interacción.

En este contexto se implementó la técnica de Pretexting, mediante la participación de una actriz que representó el personaje *"La Bandera Costeña – Sepcilia*", utilizada como herramienta pedagógica y de sensibilización.

La actividad incluyó un componente de concientización en seguridad de la información, reforzando buenas prácticas relacionadas con:

- Bloqueo del equipo de cómputo al retirarse del puesto de trabajo.
- Evitar el uso de contraseñas genéricas o compartidas.
- Uso responsable de herramientas de Inteligencia Artificial (IA).
- Protección de la información en entornos físicos y digitales.
- Aplicación del principio de escritorio limpio.

De manera complementaria, se permitió validar el cumplimiento de controles de seguridad física y lógica mediante la observación directa de comportamientos y condiciones de los puestos de trabajo, identificando oportunidades de mejora en la aplicación de los lineamientos institucionales.



Nota: Es de mencionar que la ejecución de la prueba para el piso 7, no se logró completar, teniendo en cuenta que el piso se visitó finalizando la tarde y ya no se encontraba mucho personal, sin embargo, se realizó el recorrido de manera superficial.

Como resultado de la evaluación, se identificaron las siguientes oportunidades de mejora en los pisos visitados:

- Equipos de cómputo sin bloqueo de sesión en ausencia del funcionario responsable.
- Documentos impresos en bandejas de impresora sin la debida custodia.
- Información física expuesta en los puestos de trabajo sin las medidas de protección correspondientes.
- Carnets institucionales dejados sobre los puestos de trabajo.

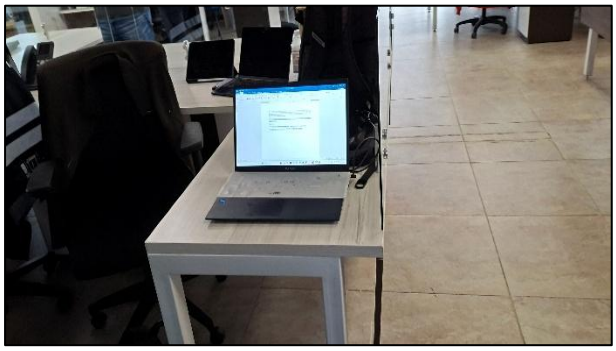
Los hallazgos evidencian debilidades en la aplicación del principio de escritorio limpio, el control de documentos impresos y la responsabilidad individual en la protección de la información institucional.

➢ **Piso 2**

En el Piso 2 se ingresó a las áreas de Seguridad, Dirección Técnica Zonal y Archivo.

Se evaluaron 94 puestos de trabajo, identificándose incumplimientos en los controles de seguridad analizados.







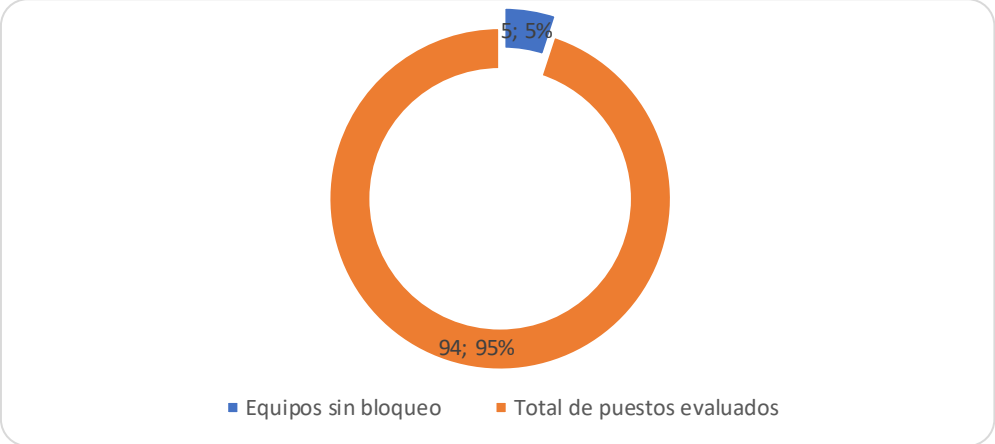


- **Equipos sin bloqueo**

$$\frac{\text{5: Cantidad de puestos de trabajo sin bloqueo de sesión}}{\text{94: Total de puestos de trabajo en las oficinas objetivo}} * 100\% = 5\%$$

De acuerdo con el resultado anterior, se puede determinar que es **"Raro"** que los funcionarios del piso 2, cumplan con los controles y vulnerabilidades que afecten los

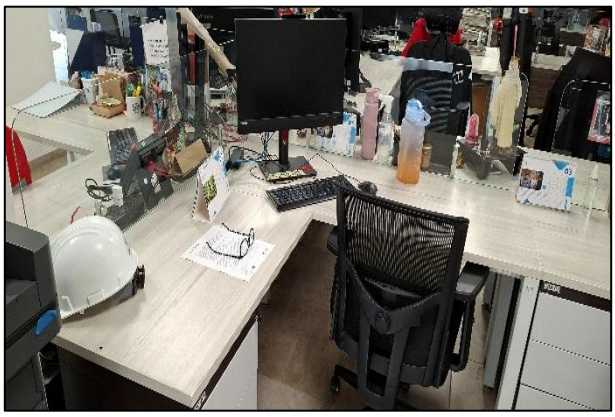
principios de seguridad de la información, como lo es el realizar el debido bloqueo de sesión.

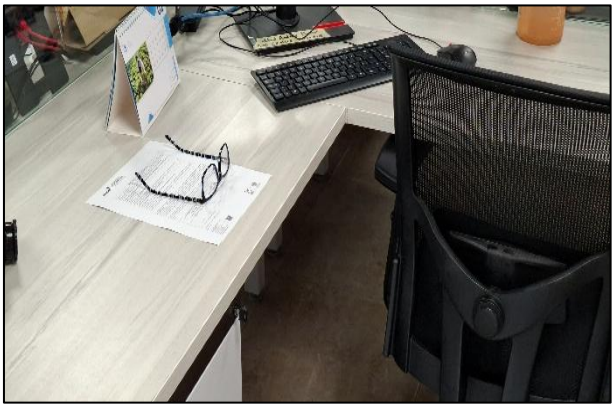


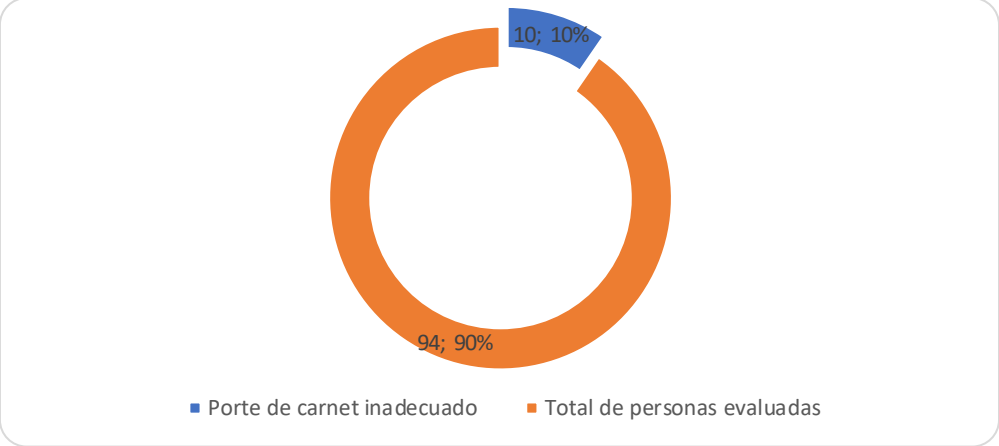
- **Control de Identificación - Porte de carnet**

$$\frac{10\text{: Cantidad de funcionarios sin portar el carnet}}{94\text{: Total de funcionarios observados en el piso}} * 100\% = 10\%$$

De acuerdo con el resultado anterior, se puede determinar que es **"Poco probable"** que los funcionarios del piso 2, cumplan con los controles y vulnerabilidades que afecten los principios de seguridad de la información, como lo es el porte del carnet de la entidad.







- **Piso 4**

En el Piso 4 se ingresó a las áreas de Planeación, Atención al Usuario y otras dependencias ubicadas en este nivel.

Se evaluaron 137 puestos de trabajo, identificándose incumplimientos en los controles de seguridad analizados.







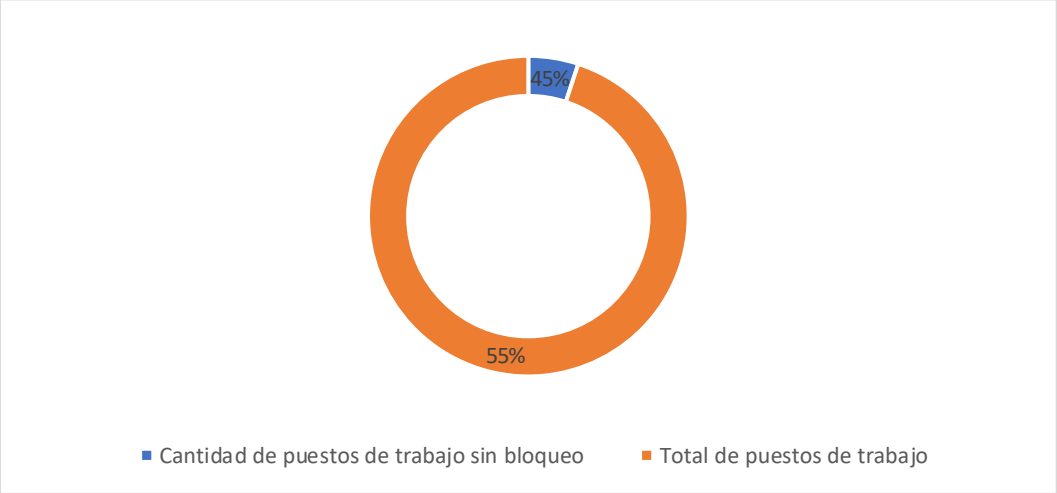


En el Piso 4 se evaluaron 137 puestos de trabajo, identificándose incumplimientos en los controles de seguridad analizados.

- **Equipos sin bloqueo:**

$$\frac{62\text{: Cantidad de puestos de trabajo sin bloqueo de sesión}}{137\text{: Total de puestos de trabajo en las oficinas objetivo}} * 100\% = 45\%$$

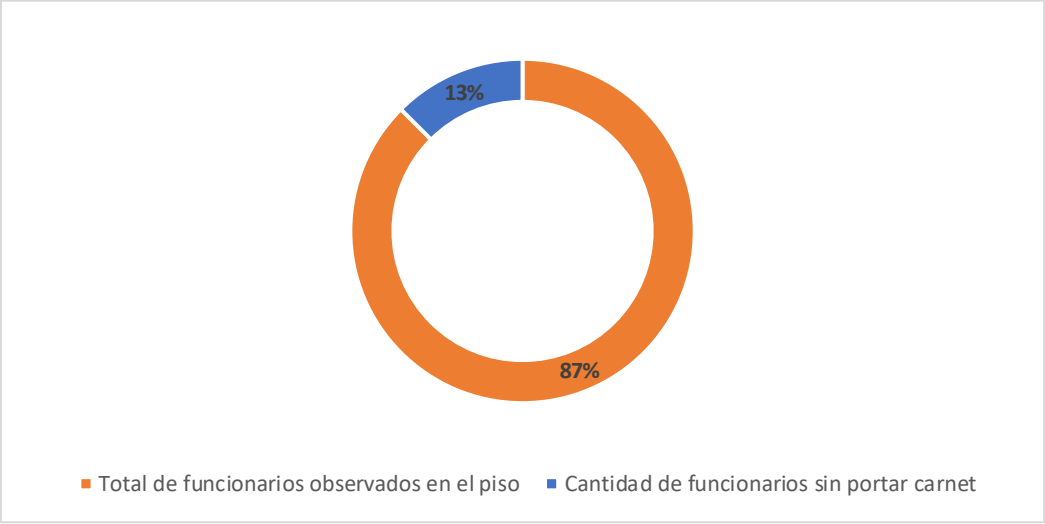
De acuerdo con el resultado anterior, se puede determinar que es **"Probable"** que los funcionarios del piso 4, cumplan con los controles y vulnerabilidades que afecten los principios de seguridad de la información, como lo es el realizar el debido bloqueo de sesión.



- **Control de Identificación - Porte de carnet:**

$$\frac{10\text{: Cantidad de funcionarios sin portar el carnet}}{137\text{: Total de funcionarios observados en el piso}} * 100\% = 7\%$$

De acuerdo con el resultado anterior, se puede determinar que es **"Poco probable"** que los funcionarios del piso 4, incumplan con los controles y vulnerabilidades que afecten los principios de seguridad de la información, como lo es el porte del carnet de la entidad.



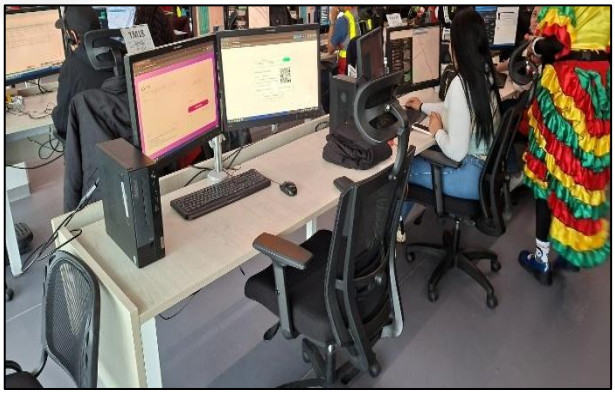
Piso 5

La intervención en el Piso 5, correspondiente al Centro de Control, permitió evaluar el cumplimiento de los lineamientos de seguridad de la información en un entorno de operación crítica y monitoreo continuo.

Se evaluaron 85 puestos de trabajo, identificándose incumplimientos en los controles de seguridad analizados.





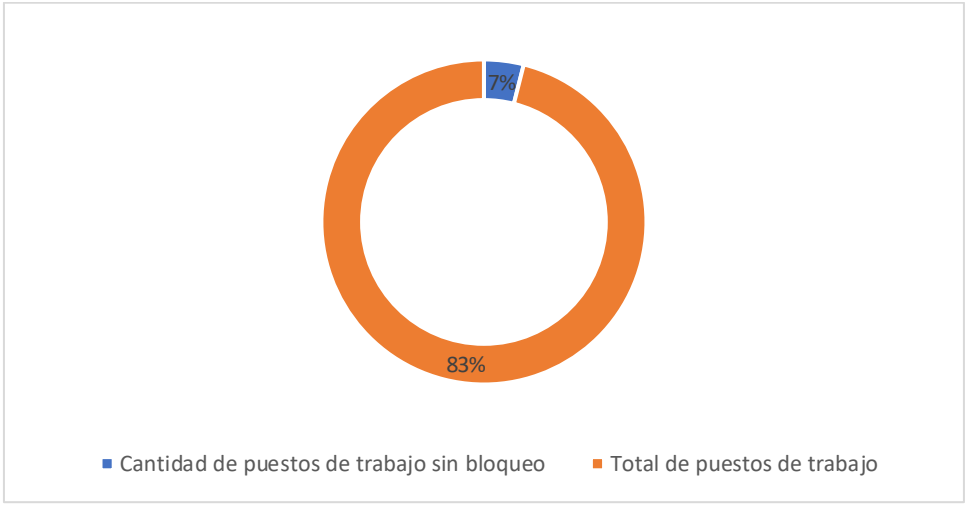




- **Control Lógico - Equipos sin bloqueo**

$$\frac{6\text{: Cantidad de puestos de trabajo sin bloqueo de sesión}}{85\text{: Total de puestos de trabajo en las oficinas objetivo}} * 100\% = 7\%$$

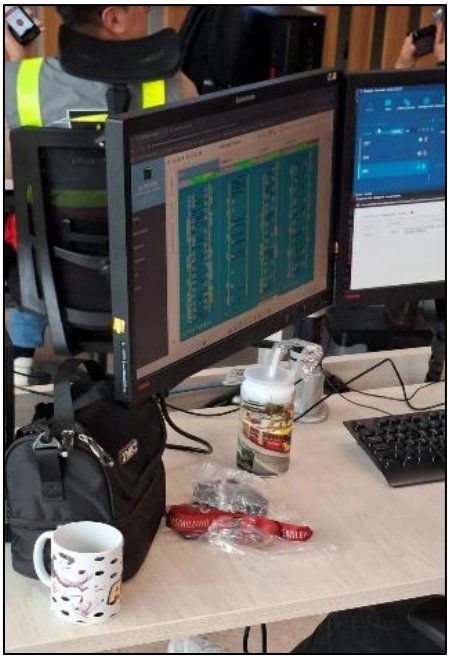
De acuerdo con el resultado anterior, se puede determinar que es **"Poco probable"** que los funcionarios del piso 5, cumplan con los controles y vulnerabilidades que afecten los principios de seguridad de la información, como lo es el realizar el debido bloqueo de sesión.



- **Control de Identificación - Porte de carnet**

$$\frac{3\text{: Cantidad de funcionarios sin portar el carnet}}{85\text{: Total de funcionarios observados en el piso}} * 100\% = 4\%$$

De acuerdo con el resultado anterior, se puede determinar que es **"Poco probable"** que los funcionarios del piso 6, incumplan con los controles y vulnerabilidades que afecten los principios de seguridad de la información, como lo es el porte del carnet de la entidad.

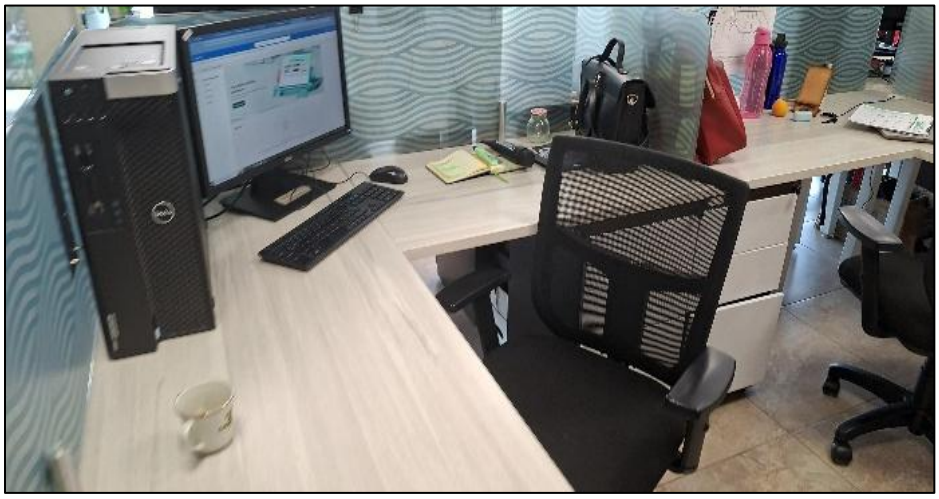


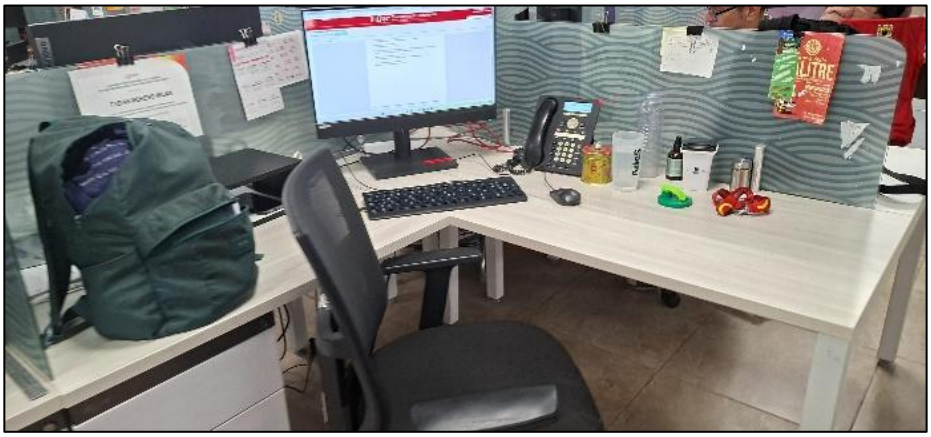


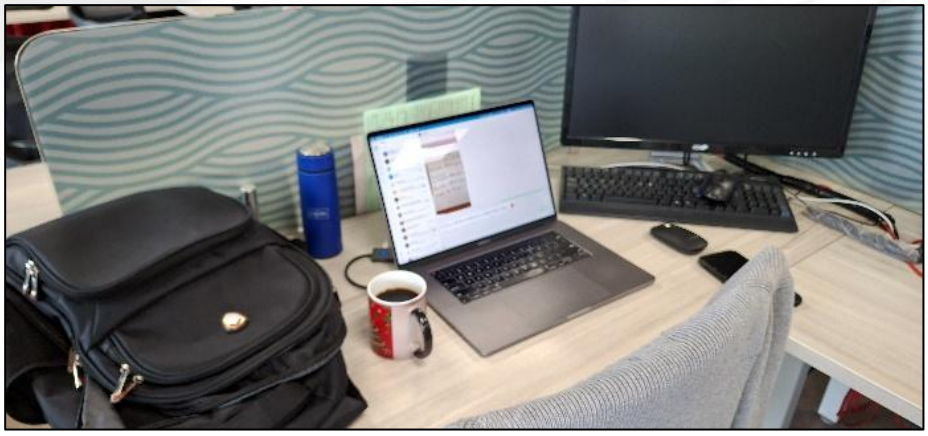
- **Piso 6**

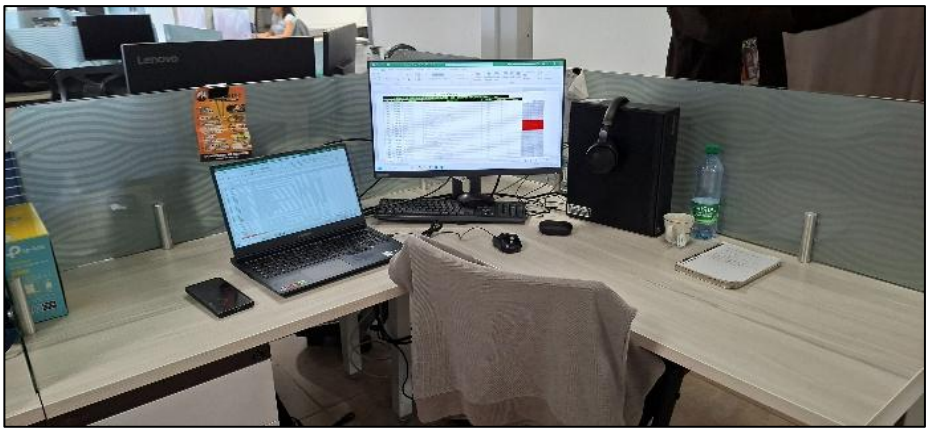
En el Piso 6 se ingresó a las áreas de Comunicaciones, Negocios e Infraestructura.

Se evaluaron 63 puestos de trabajo, identificándose incumplimientos en los controles de seguridad analizados.





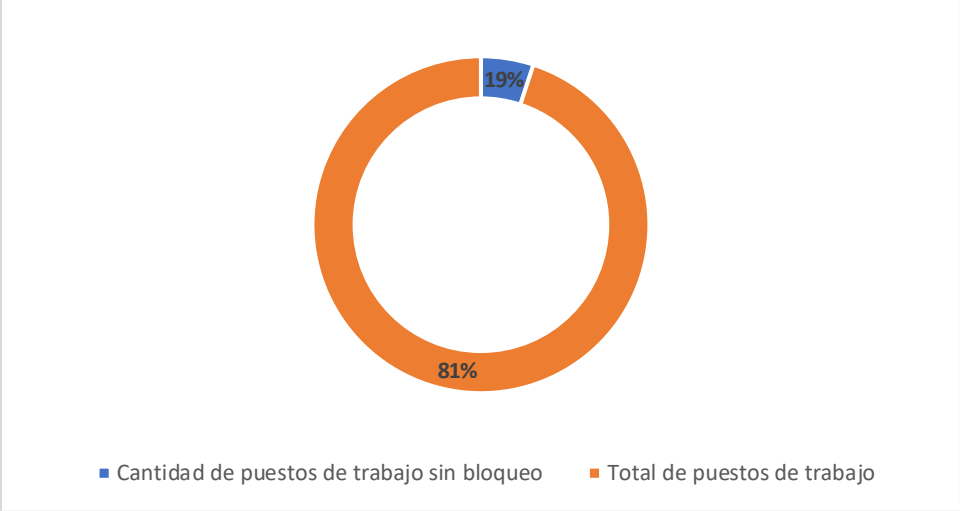




- **Equipos sin bloqueo:**

$$\frac{12\text{: Cantidad de puestos de trabajo sin bloqueo de sesión}}{63\text{: Total de puestos de trabajo en las oficinas objetivo}} * 100\% = 19\%$$

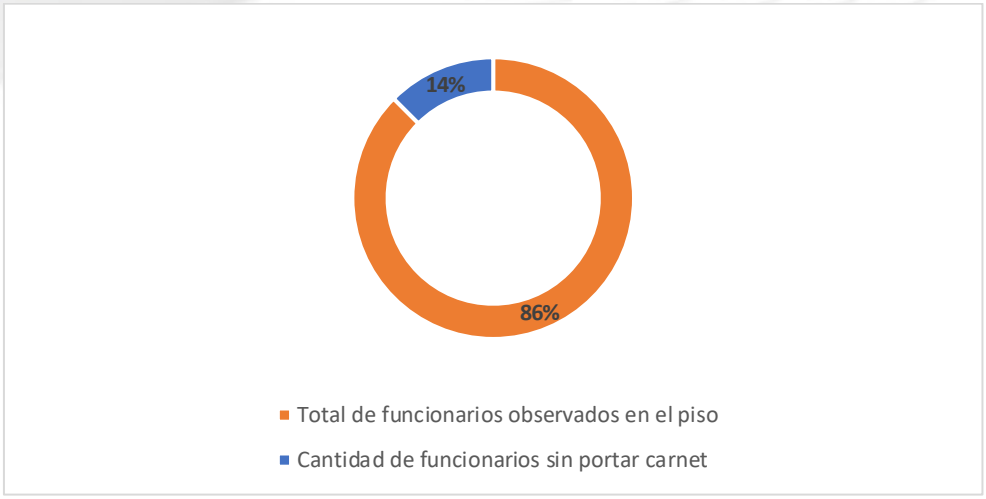
De acuerdo con el resultado anterior, se puede determinar que es **"Posible"** que los funcionarios del piso 6, cumplan con los controles y vulnerabilidades que afecten los principios de seguridad de la información, como lo es el realizar el debido bloqueo de sesión.



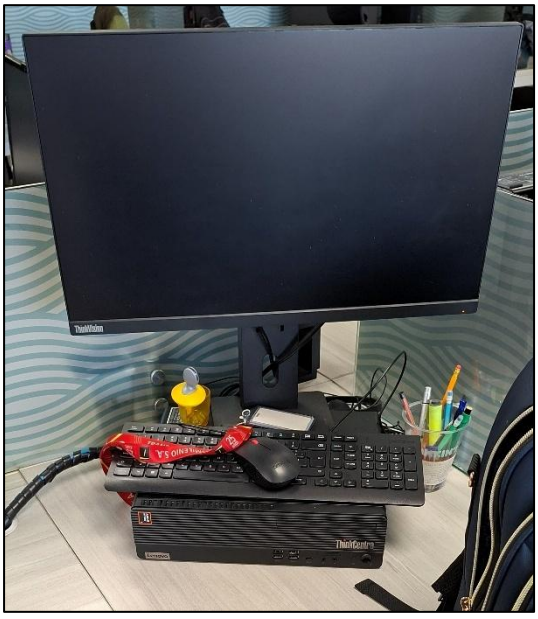
- **Identificación - Porte de carnet**

$$\frac{9\text{: Cantidad de funcionarios sin portar el carnet}}{63\text{: Total de funcionarios observados en el piso}} * 100\% = 14\%$$

De acuerdo con el resultado anterior, se puede determinar que es **"Posible"** que los funcionarios del piso 6, incumplan con los controles y vulnerabilidades que afecten los principios de seguridad de la información, como lo es el porte del carnet de la entidad.


14%
86%
Total de funcionarios observados en el piso
Cantidad de funcionarios sin portar carnet

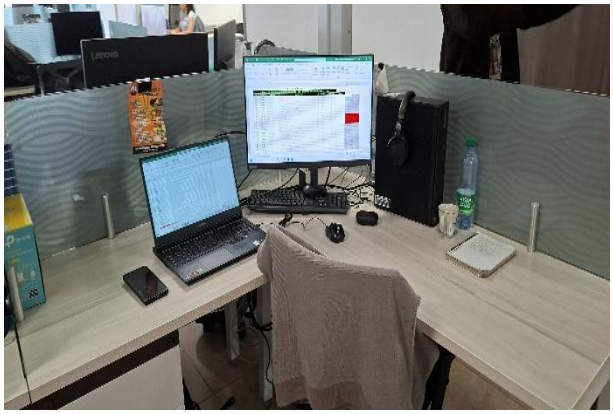




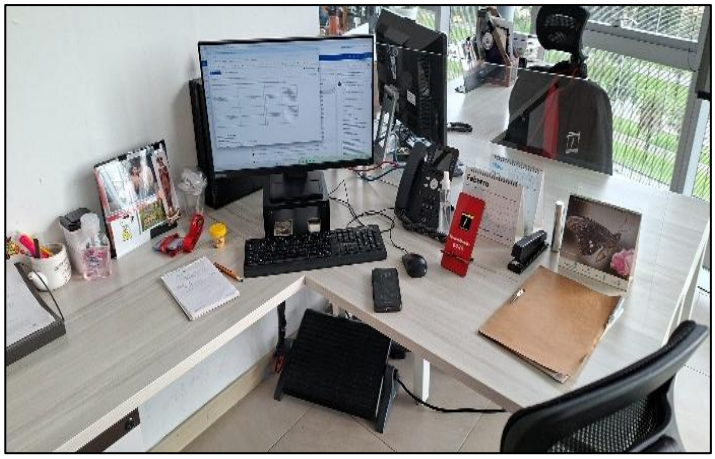
Piso 8

La intervención en el Piso 8, correspondiente a la Dirección Corporativa, permitió

Se evaluaron 73 puestos de trabajo, identificándose incumplimientos en los controles de seguridad analizados.



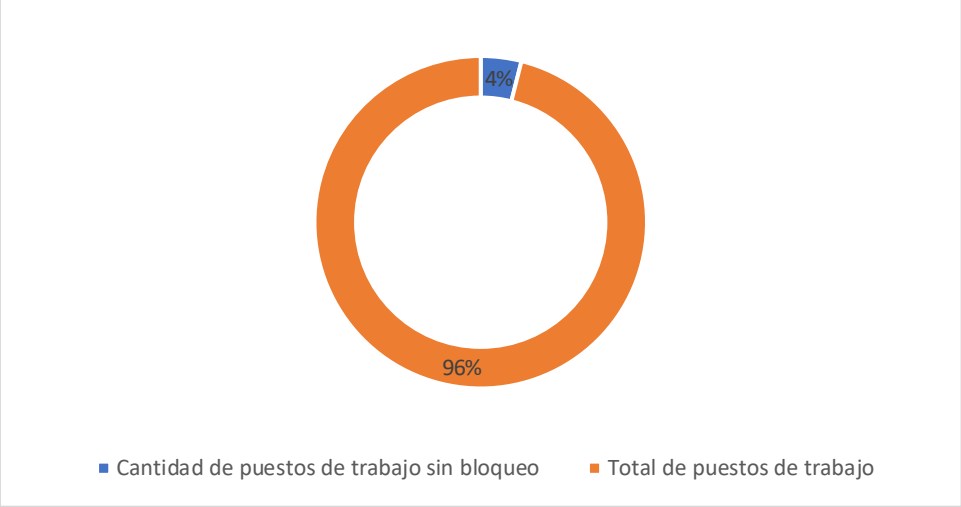




- **Control Lógico - Equipos sin bloqueo**

$$\frac{\text{3: Cantidad de puestos de trabajo sin bloqueo de sesión}}{\text{73: Total de puestos de trabajo en las oficinas objetivo}} * 100\% = 4\%$$

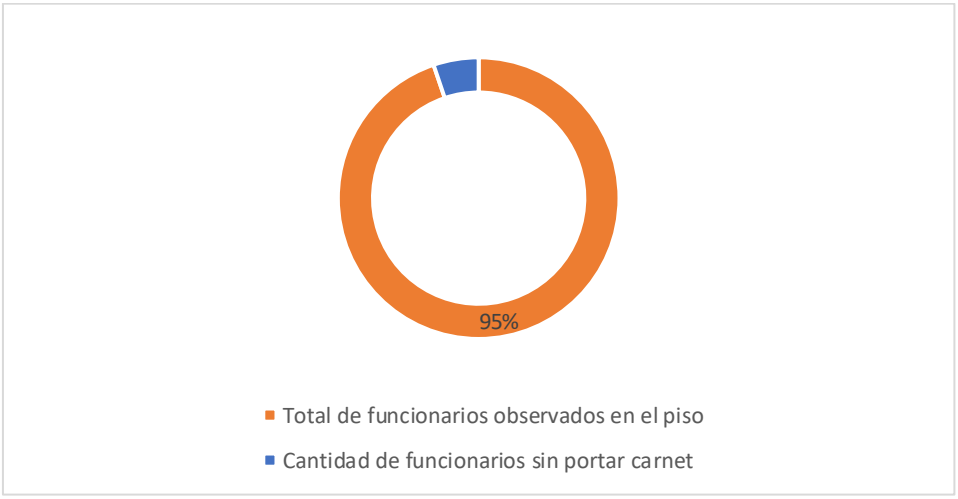
De acuerdo con el resultado anterior, se puede determinar que es **"Poco probable"** que los funcionarios del piso 8, incumplan con los controles y vulnerabilidades que afecten los principios de seguridad de la información, como lo es el porte del carnet de la entidad.

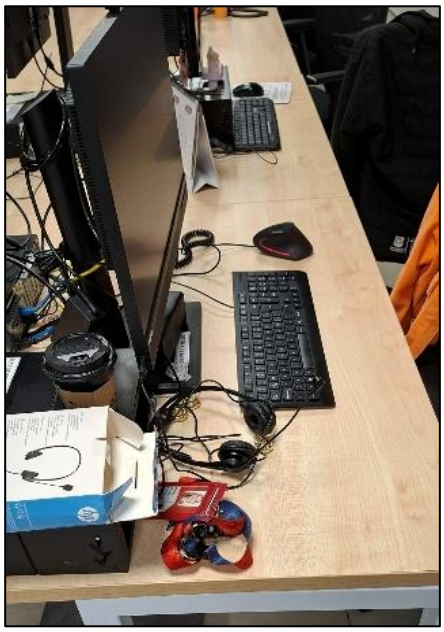


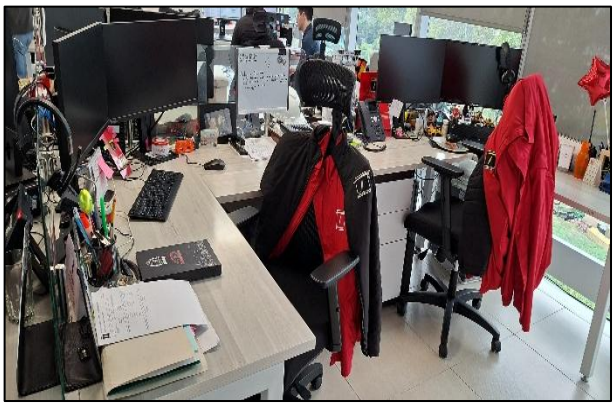
- **Control de Identificación - Porte de carnet**

$$\frac{4\text{: Cantidad de funcionarios sin portar el carnet}}{73\text{: Total de funcionarios observados en el piso}} * 100\% = 5\%$$

De acuerdo con el resultado anterior, se puede determinar que es **"Poco probable"** que los funcionarios del piso 8, incumplan con los controles y vulnerabilidades que afecten los principios de seguridad de la información, como lo es el porte del carnet de la entidad.







Fortalezas Identificadas

Durante la ejecución de la prueba de Pretexting se evidenciaron controles implementados de manera adecuada en los diferentes pisos intervenidos, los cuales contribuyen al fortalecimiento del entorno de seguridad de la información. Entre las principales fortalezas identificadas se destacan:

- Presencia permanente de guardas de seguridad en los accesos a los pisos y áreas intervenidas.
- Implementación de control de acceso mediante tarjeta de proximidad.
- Sistema de videovigilancia (CCTV) en funcionamiento.
- Áreas restringidas debidamente cerradas, limitando el ingreso no autorizado.
- Asignación de escarapela o sticker de seguridad para su porte visible durante la permanencia en las instalaciones.
- Acompañamiento del personal interno de la entidad durante la ejecución de la actividad.

Estas condiciones evidencian que la entidad cuenta con controles físicos y administrativos establecidos, los cuales constituyen una base sólida para el fortalecimiento continuo de la cultura de seguridad de la información.

7. RECOMENDACIONES GENERALES

- Utilizar diferentes mecanismos para la publicación de avisos de seguridad de la información, destacando a los funcionarios que hayan participado en actividades de seguridad de la información, reportando eventos o incidentes de seguridad de la información.
- Mantenerse actualizado en las últimas amenazas y formas de ataques de ingeniería social y comunicarlas en las jornadas de sensibilización.
- Continuar realizando pruebas de ingeniería social de manera periódica con el fin de evaluar el nivel de conciencia y cumplimiento de los funcionarios y contratistas frente a las políticas y prácticas relacionadas a la seguridad de la información, así mismo evaluar la eficacia de las campañas de sensibilización y las capacitaciones que se realicen.
- Realizar este tipo de ejercicio periódicamente para comprobar la concientización de los funcionarios de Transmilenio S.A. con un público objetivo de usuarios más grande, que involucre a los equipos de seguridad, TI y recursos humanos, para obtener una visión más completa de la seguridad de la organización.
- Fomentar una cultura de desconfianza hacia cualquier solicitud de información personal o corporativa.

8. CONCLUSIÓN

En términos generales, los resultados reflejan que el riesgo no se encuentra asociado a fallas estructurales o control físico, sino a hábitos operativos y prácticas cotidianas que pueden ser mitigadas mediante acciones continuas de sensibilización, supervisión y seguimiento.

En las pruebas evidenció la importancia de mantener estrategias periódicas de concientización y validación práctica de controles, como mecanismo para reforzar la interiorización de las políticas de seguridad de la información dentro del contexto operativo de la entidad.

Por otra parte, es importante dar a conocer los impactos que podría causar una pérdida de la **confidencialidad, integridad y disponibilidad** de los activos de información, tales como, implicaciones a nivel legal y procesos disciplinarios al interior de la entidad.