INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO
Nº 4200000-807-2024

El Asesor de Despacho de la Consejería Distrital TIC de la Secretaría General de la Alcaldía Mayor de Bogotá D.C., obrando como Supervisor del Contrato y/o Convenio Nro. 4200000-807-2024 presenta informe con el fin de proceder al reporte de cumplimiento en los siguientes términos:

1. INFORMACIÓN DE LA EJECUCIÓN DEL CONTRATO O CONVENIO			
Contratista:	**EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP - ETB S.A. ESP**		
Objeto:	Proveer una plataforma omnicanal de orquestación que incluya chatbot, tablero de control que permita pagos e interacción de servicios Distritales y que integre soluciones a la plataforma asegurando una experiencia unificada y coherente para el usuario.		
Valor del contrato:	319,974,540.00 incluido IVA	**Valor de la adición (si hay lugar a ello):**	No aplica
Valor total del contrato:	319,974,540.00 incluido IVA	**Valor ejecutado:**	$91.659.525
Plazo inicial del contrato:	5 mes(es)	**Prórroga (si se llevó a cabo):**	No aplica
Plazo final del contrato:	5 mes(es)	**Fecha de suscripción:**	31/07/2024
Fecha de iniciación:	31/07/2024	**Fecha de suspensión (si hay lugar a ello):**	No aplica
Fecha de reinicio (si se llevó a cabo):	No aplica	**Fecha de terminación:**	30/12/2024
Dependencia donde presta el servicio (solo para persona natural)	No aplica	**Sede donde presta el servicio (solo para persona natural)**	No aplica

2. CUMPLIMIENTO DE LAS OBLIGACIONES:

Que conforme con la ejecución de dicho acuerdo de voluntades, me permito certificar el desarrollo de las siguientes actividades en cumplimiento del objeto y las obligaciones contractuales:

OBLIGACIONES	ACTIVIDADES	ANEXOS	Nro. CARPETA Y DE FOLIO EN EL EXPEDIENTE CONTRACTUAL EN EL QUE REPOSA LA EVIDENCIA. (Incluir nombre del archivo con el cual fue cargado en SECOP).
1. Realizar la configuración, personalización y puesta en operación de Chatico, con 23 flujos generales y hasta 300 intenciones en un segundo nivel de navegación, conforme a lo solicitado en el presente Anexo Técnico.	N/A	N/A	N/A

INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO Nº 4200000-807-2024

2. Realizar cada una de las actividades previstas en los documentos integrantes del proceso, de acuerdo con la programación aprobada por el supervisor del contrato y deberá cumplir con los entregables correspondientes al numeral "8.4.3. Documentación técnica a entregar de la plataforma omnicanal de orquestación (SaaS), del Anexo Técnico	2.1. Realizó y entregó los soportes relacionados el numeral 8.4.3 del anexo técnico.	2.1.1 Entregó los soportes relacionados con la obligación.	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • ID del contrato en SECOP CO1.PCCNTR.6583693 • Carpeta de Pago Dos https://bit.ly/4fjIQHP
3. Asistir a los comités y reuniones de seguimiento programados por la supervisión del contrato a fin de analizar el avance normal de las diferentes actividades según cronograma de actividades	3.1 Asistió a todas las reuniones de seguimiento a las que se le convocó en el mes de Septiembre de 2024.	3.1.1 Entregó los soportes relacionados con la obligación.	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • ID del contrato en SECOP CO1.PCCNTR.6583693 • Carpeta de Pago Dos https://bit.ly/4fjIQHP
4. Aportar al supervisor del contrato la información necesaria para liquidar el contrato.	N/A	N/A	N/A
5. Responder en los plazos que la SGAB establezca en cada caso, los requerimientos de aclaración o de información que le formule.	N/A	N/A	N/A
6. Entrega del documento de escalamientos con números de contacto, correos electrónicos y nombres de los involucrados en el proceso de soporte y atención, y deberá mantenerlo actualizado durante la vigencia del contrato.	N/A .	N/A	N/A
7. Cumplir con las condiciones establecidas en el Anexo y en los demás documentos	N/A	N/A	N/A

INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO Nº 4200000-807-2024

integrantes del proceso de contratación.			
8. El Contratista debe garantizar que el valor del contrato incluye todos los gastos, costos, derechos, impuestos, tasas y demás contribuciones relacionadas con el cumplimiento del objeto del presente contrato, cuando estos apliquen.	8.1 El contratista relacionó la evidencia correspondiente durante el mes de Septiembre de 2024.	8.1.1. Entregó los informes mensuales junto a las facturas correspondientes.	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • ID del contrato en SECOP CO1.PCCNTR.6583693 • Carpeta de Pago Dos https://bit.ly/4fjIQHP
9. El Contratista deberá contar con las capacidades necesarias para el buen desempeño de la plataforma omnicanal de orquestación y dar cumplimiento a los ANS establecidos en el presente Anexo Técnico.	9.1 Realizó y entregó los soportes relacionados al numeral 5.1 del anexo técnico.	9.1.1. Entregó los soportes relacionados con la obligación.	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • ID del contrato en SECOP CO1.PCCNTR.6583693 • Carpeta de Pago Dos https://bit.ly/4fjIQHP
10. El contratista debe garantizar que el servicio de plataforma omnicanal de orquestación cumpla con lineamientos de seguridad basados en las normas y las mejores prácticas de la industria y debe estar protegida contra ataques informáticos al igual que toda la aplicación e infraestructura contratada.	10.1. El contratista presentó informes de análisis de Seguridad de la información, de forma mensual, garantizando el cumplimiento de los lineamientos de seguridad basados en las normas y las mejores prácticas de la industria.	10.1.1. Entregó documento de análisis sobre pruebas de seguridad.	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • ID del contrato en SECOP CO1.PCCNTR.6583693 • Carpeta de Pago Dos https://bit.ly/4fjIQHP
11. El contratista deberá proveer los planes, plataformas alternas y procesos de contingencia del servicio de la plataforma omnicanal de orquestación que aseguren la continuidad del servicio en un porcentaje del 99,6% para las conversaciones de los ciudadanos requeridas y con el tiempo de respuesta y la	11.1. El contratista presentó el informe mensual de comportamiento transaccional en cada una de las entregas.	11.1.1. Entregó informe mensual del comportamiento transaccional, tiempos de respuesta, componentes tecnológicos, servicio de respaldo y backups.	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • ID del contrato en SECOP CO1.PCCNTR.6583693 • Carpeta de Pago Dos https://bit.ly/4fjIQHP

INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO Nº 4200000-807-2024

calidad que garanticen la satisfacción del cliente.			
12. El contratista debe informar mensualmente la disponibilidad operativa de la plataforma principal.	12.1. Presentó informes mensuales de Diseño Centrado en el Usuario.	12.1.1. El informe mensual presentado en cada uno de los periodos consolida el ejercicio de Diseño Centrado en el Usuario, sujeto de análisis en el mes correspondiente.	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • ID del contrato en SECOP CO1.PCCNTR.6583693 • Carpeta de Pago Dos https://bit.ly/4fjIQHP
13. El contratista deberá proveer mejoras en rendimiento o en funcionalidad que el contratista libere para sus clientes o específicamente para la Secretaría General de la Alcaldía Mayor de Bogotá con el fin de dar mejoramiento continuo al respectivo servicio para el buen desempeño transaccional y pondrá a disposición de la SGAB las versiones o *upgrades* de otros clientes y que sean beneficiosas para la SGAB.	N/A	N/A	N/A
14. El contratista deberá entregar un informe mensual del comportamiento transaccional, tiempos de respuesta, componentes tecnológicos, servicios de respaldo y *backups* que sustenten la correcta administración de la plataforma. El informe mensual debe ir con los soportes de ejecución establecidos en la forma de pago. Estos se deben presentar en las fechas entregadas por la entidad, y deberán ser entregados a más tardar los tres (3) primeros días	14.1. El contratista presentó el informe mensual de comportamiento transaccional en cada una de las entregas.	14.1.1. Entregó informe mensual del comportamiento transaccional, tiempos de respuesta, componentes tecnológicos, servicio de respaldo y backups.	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • ID del contrato en SECOP CO1.PCCNTR.6583693 • Carpeta de Pago Dos https://bit.ly/4fjIQHP

INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO
Nº 4200000-807-2024

hábiles posteriores a la fecha de entrega establecida, para la revisión y aprobación de SGAB. Esta aprobación por parte del supervisor del contrato designado por SGAB deberá hacerse máximo en los tres (3) días hábiles siguientes a la presentación de dicho informe.			
15. El Contratista deberá proveer de forma adecuada la disponibilidad y seguridad para la creación de usuarios de Administrador y de Gestores de base de conocimiento del orquestador con los respectivos controles de contraseñas y logs de auditoría.	N/A	N/A	N/A
16. El Contratista deberá informar previamente a la SGAB, cualquier mantenimiento programado o de emergencia que se requiera en la aplicación, infraestructura o componentes tecnológicos que estén siendo utilizados por la SGAB detallando el cambio, el riesgo y las acciones de mitigación. Adicionalmente para los cambios solicitados por la SGAB, deberá cumplir las fechas que se pacten entregando la documentación exigida por la SGAB para el control de cambios, como: documento técnico del cambio, riesgos, roll back (como devolverse), minutograma, responsables.	16.1. El contratista presentó el informe mensual de disponibilidad operativa de la plataforma principal.	16.1.1. El informe mensual referido estableció los cronogramas de actividades previas a los despliegues a realizar en ambiente productivo.	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • ID del contrato en SECOP CO1.PCCNTR.6583693 • Carpeta de Pago Dos https://bit.ly/4fjIQHP

INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO Nº 4200000-807-2024

17. El contratista deberá realizar la transferencia de conocimiento de conformidad con lo establecido en el presente anexo técnico.	N/A	N/A	N/A
18. El contratista deberá prestar los soportes, documentación técnica e informes establecidos en el Anexo técnico.	18.1. El contratista proporcionó los informes mensuales relacionados en el numeral 8.4 del anexo técnico.	18.1.1. Entregó los soportes relacionados con la obligación.	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • ID del contrato en SECOP CO1.PCCNTR.6583693 • Carpeta de Pago Dos https://bit.ly/4fjIQHP
19. De conformidad con lo estipulado en el Decreto 332 de 2020 “Por medio del cual se establecen medidas afirmativas para promover la participación de las mujeres en la contratación del Distrito Capital”, se debe tener en cuenta que tanto para la presentación de las hojas de vida en la oferta, como para la ejecución del contrato que resulte, se debe observar lo establecido en el artículo 3°.	N/A	N/A	N/A
20. El contratista deberá entregar al finalizar el contrato toda la información generada que sea de propiedad de la Secretaría General, derivada de la ejecución del objeto contractual y el presente Anexo Técnico.	N/A	N/A	N/A

INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO
Nº 4200000-807-2024

3. GESTIÓN DE PAGOS, DESEMBOLSOS O RECAUDOS:

De acuerdo con lo establecido, se ha realizado a la fecha 31/10/2024 un total de Un (1) pago, por valor de NOVENTA Y UN MILLONES SEICCIENTOS CINCUENTA Y NUEVE MIL QUINIENTOS VENTICINCO PESOS ($91.659.525) MONEDA CORRIENTE INCLUIDO IVA, de acuerdo con la entrega de los bienes, productos y/o servicios estipulados en la cláusula 4 del contrato, así:

(Si el informe corresponde a un informe parcial, se debe diligenciar la tercera columna con N/A.)

PAGO Nro. 1		
Requisitos	**Descripción**	**Nro. Carpeta y de folio en el expediente contractual en el que reposa la evidencia o enlace de acceso al SECOP donde están publicados los documentos** (incluir nombre del archivo con el cual fue cargado en SECOP)**.**
Facturas o documentos equivalentes	Factura electrónica No. FC 001000095444	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • Carpeta de Pago Uno https://bit.ly/4fjIQHP
Anexos (Actas de Comité) (Informes)	**N/A**	
Periodo certificado por parte del supervisor (01/09/2024) a (30/09/2024)	Certificado de recibo a satisfacción No 4685 del 17 de octubre de 2024	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • Carpeta de Pago Uno https://bit.ly/4fjIQHP
Acreditación de pago de aportes al Sistema Integral de Seguridad Social y Parafiscales	de revisor fiscal correspondiente a parafiscales del mes de septiembre de 2024	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • Carpeta de Pago Uno https://bit.ly/4fjIQHP
Comprobante de ingreso de elementos a almacén.	N/A	**N/A**
Orden de pago	Pago en tramite	Todas las evidencias fueron cargadas oportunamente en la plataforma SECOP 2, en la siguiente ruta: • Ejecución del contrato • Documentos de ejecución del contrato • Carpeta de Pago Uno https://bit.ly/4fjIQHP

INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO
Nº 4200000-807-2024

Nota: No existen reintegros o devoluciones.

(En caso de que el contrato o convenio suscrito implique un recaudo de dinero por parte de la Secretaría General se debe diligenciar el siguiente cuadro)

De acuerdo con lo establecido en la cláusula _____ del contrato/convenio, se han realizado a la fecha __/__/____ un total de _____ facturas, por valor de _____ PESOS ($_____), y un total de _____ cuentas de cobro, por valor de _____ PESOS ($_____), de acuerdo con la entrega de los bienes, productos y/o servicios estipulados en la cláusula _____ del contrato, así:

FACTURA Nro. ____			
Requisitos	**Descripción**	**Nro. Carpeta y de folio en el expediente contractual en el que reposa la evidencia o enlace de acceso al SECOP donde están publicados los documentos.**	**Observaciones**
N/A	N/A	N/A	N/A

Se presenta Mora en el pago para el mes de _____: SÍ ____ NO____
Reporte de seguimiento al pago en Mora:

CUENTA DE COBRO Nro. ____			
Requisitos	**Descripción**	**Nro. Carpeta y de folio en el expediente contractual en el que reposa la evidencia o enlace de acceso al SECOP donde están publicados los documentos.**	**Observaciones**
N/A	N/A	N/A	N/A

Se presenta Mora en el pago para el mes de _____: SÍ ____ NO____
Reporte de seguimiento al pago en Mora:

(En caso de que el contrato o convenio suscrito implique un recaudo de dinero por parte de la Secretaría General en la Red CADE se debe diligenciar el siguiente cuadro)

De acuerdo con los servicios prestados y lo estipulado en las obligaciones del convenio/contrato _____, el valor ejecutado por concepto de gastos de administración y arrendamiento asciende a la suma de_____ PESOS ($_____), con corte al ___ de _____ de _____, así:

NO. FAC	FECHA DE FACTURA	PERIODO	CONCEPTO	VALOR NETO	VALOR CONSIGNADO	FECHA CONSIGNACIÓN
N/A	N/A	N/A	N/A	N/A	N/A	N/A

La relación anterior refleja los cobros y recaudos establecidos de forma mensual _____, según la forma de pago establecida en el convenio/contrato, por lo anterior SÍ____ NO____ se generaron intereses moratorios para el periodo comprendido entre el ___ de _____ de _____ al ___ de _____ de _____.

INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO
Nº 4200000-807-2024

4. DESARROLLO DEL CONTRATO

La aprobación de la garantía única se produjo el día 31/07/2024, la cual se constituyó así:

PÓLIZA No.	AMPAROS	VALORES ASEGURADOS	VIGENCIAS	
			FECHA INICIO	FECHA FINAL
74563	CUMPLIMIENTO DELCONTRATO	$ 31,997,454.00	31/07/2024	01/05/2025
74563	PAGO DE SALARIOS,PRESTACIONES SOCIALES E INDEMNIZACIONES	$ 15,998,727.00	31/07/2024	31/12/2027
74563	CALIDAD DEL SERVICIO	$ 31,997,454.00	31/07/2024	01/05/2025

4.1 MODIFICACIONES

Que el contrato tuvo las siguientes modificaciones contractuales:

CLASE DE MODIFICACIÓN	FECHA	VALOR (En caso de ser adición)	TIEMPO (En caso de que sea prórroga)	Nro. CARPETA Y DE FOLIO EN EL EXPEDIENTE CONTRACTUAL
No aplica	**No aplica**	**No aplica**	**No aplica**	**No aplica**

5. EL SUPERVISOR Y/O INTERVENTOR DEL CONTRATO Y/O CONVENIO CERTIFICA QUE:

(Si el informe corresponde a un informe de supervisión parcial, el supervisor deberá diligenciar el siguiente cuadro)

TIPO DE INFORME	CUMPLIMIENTO	MARQUE CON UNA X EN CASO DE QUE SEA POSITIVA LA RESPUESTA, EN CASO CONTRARIO INDIQUE LAS RAZONES POR LAS CUALES HA INCUMPLIDO EL CONTRATISTA
INFORME PARCIAL	El(la) contratista a la fecha viene cumpliendo a satisfacción el objeto del contrato.	X
	Que el supervisor del contrato certifica al Ordenador del Gasto, que las obligaciones contractuales vienen siendo ejecutadas de conformidad con lo pactado y en su totalidad a la fecha de corte del informe, con oportunidad y diligencia	X
	Que el (la) contratista a la fecha viene cumpliendo durante la ejecución del contrato y corte del periodo, con el pago de los aportes al Sistema General de Seguridad Social en Salud, Pensión y Riesgos Laborales o la certificación emitida por el Representante Legal y/o Revisor Fiscal de la	X

INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO Nº 4200000-807-2024

	firma donde indica que la precitada persona jurídica se encuentra al día con el Sistema de Seguridad Social, Pensiones, etc., de conformidad con las normas legales vigentes	
	Que verifiqué el cumplimiento de las obligaciones contractuales y recibí los informes y/o productos correspondientes pactados entre las partes, los cuales fueron cargados y revisados oportunamente en la plataforma SECOP según sea el caso.	X
	Que su ejecución presupuestal ha obedecido a los pagos y desembolsos pactados contractualmente y las modificaciones si a ello hubiere lugar.	X

(Si el informe corresponde a un informe de supervisión final, el supervisor deberá diligenciar el siguiente cuadro)

TIPO DE INFORME	CUMPLIMIENTO	MARQUE CON UNA X EN CASO DE QUE SEA POSITIVA LA RESPUESTA, EN CASO CONTRARIO INDIQUE LAS RAZONES POR LAS CUALES HA INCUMPLIDO EL CONTRATISTA
INFORME FINAL	El(la) contratista cumplió a satisfacción el objeto del contrato.	**N/A**
	Que el supervisor del contrato certifica al Ordenador del Gasto, que las obligaciones contractuales fueron ejecutadas de conformidad con lo pactado y en su totalidad, con oportunidad y diligencia.	**N/A**
	Que el (la) contratista cumplió durante la ejecución del contrato, con el pago de los aportes al Sistema General de Seguridad Social en Salud, Pensión y Riesgos Laborales o la certificación emitida por el Representante Legal y/o Revisor Fiscal de la firma donde indica que la precitada persona jurídica se encuentra al día con el Sistema de Seguridad Social, Pensiones, etc., de conformidad con las normas legales vigentes	**N/A**
	Que verifiqué el cumplimiento de las obligaciones contractuales y recibí los informes y/o productos correspondientes pactados entre las partes, los cuales fueron cargados y revisados oportunamente en la plataforma SECOP según sea el caso.	**N/A**
	Que su ejecución presupuestal obedeció a los pagos y desembolsos pactados contractualmente y las modificaciones si a ello hubiere lugar.	**N/A**

6. CONTROL SOBRE LAS OBLIGACIONES POST CONTRACTUALES (SI APLICA)

A continuación, se describen las obligaciones post contractuales resultantes de la ejecución del presente contrato o convenio No_____ de _____ y la forma en que se realizará el seguimiento de su cumplimiento por parte de la supervisión:

INFORME PARCIAL DE SUPERVISIÓN CONTRATO Y/O CONVENIO
Nº 4200000-807-2024

DESCRIPCIÓN DE LAS OBLIGACIONES POST CONTRACTUALES	MODO DE SEGUIMIENTO POR PARTE DE LA SUPERVISIÓN	FECHA ESTIMADA DE CULMINACIÓN DE LA OBLIGACIÓN POST CONTRACTUAL	DESCRIPCIÓN DEL SOPORTE DEL SEGUIMIENTO (Deberá encontrarse cargado en el SECOP)
N/A	N/A	N/A	N/A

(En caso de que no se presenten obligaciones post contractuales no se debe diligenciar el cuadro anterior)

7. MATERIALIZACIÓN DE LOS RIESGOS ASOCIADOS AL CONTRATO O CONVENIO

No hubo materialización de los riesgos asociados a este contrato.

8. OBSERVACIONES

Describa las situaciones que requiera señalar en desarrollo del informe parcial o final que necesite documentar, de lo contrario no diligencie.

7. FIRMAS

NOMBRE DEL SUPERVISOR/INTERVENTOR	CARGO	FIRMA
Juan Carlos Parada Gallardo	Asesor Consejería Distrital de TIC	

En caso de que el contrato se ejecute en un punto de atención de la Red CADE se deberá diligenciar el siguiente cuadro:

NOMBRE DEL APOYO A LA SUPERVISÓN	CARGO	FIRMA
No aplica	Responsable del insumo técnico.	No aplica
No aplica	Responsable del insumo jurídico.	No aplica
No aplica	Responsable del insumo financiero.	No aplica

EL ASESOR DE DESPACHO DE LA SECRETARIA GENERAL DE LA ALCALDIA MAYOR DE BOGOTA D.C. EN SU CALIDAD DE SUPERVISOR(ES) DEL CONTRATO INTERADMINISTRATIVO DE CÓDIGO No. 4130000-807-2024

CERTIFICA QUE:

Que (el/la) EMPRESA DE TELECOMUNICACIONES DE BOGOTÁ S.A. ESP - ETB S.A. ESP, identificado con NIT No. 899999115, en desarrollo del objeto del CONTRATO INTERADMINISTRATIVO No. 4130000-807-2024, cumplió a satisfacción con las obligaciones derivadas del mismo, durante el periodo comprendido entre el 1 de septiembre de 2024 y el 30 de septiembre de 2024. Cta. Bco. 6029. Teniendo en cuenta que:

CONSIDERACIONES RESPECTO AL CUMPLIMIENTO	INDICAR S/N E INCLUYA SI ES NECESARIO LA JUSTIFICACIÓN
El(la) contratista a la fecha viene cumpliendo a satisfacción el objeto del contrato.	SI .
Que el supervisor del contrato certifica al Ordenador del Gasto, que las obligaciones contractuales vienen siendo ejecutadas de conformidad con lo pactado y en su totalidad a la fecha de corte del informe, con oportunidad y diligencia.	SI .
Que verifiqué el cumplimiento de las obligaciones contractuales y recibí los informes y/o productos correspondientes pactados entre las partes, los cuales fueron cargados y revisados oportunamente en las plataformas de SECOP 1 o SECOP 2 según sea el caso.	SI .
Que el (la) contratista a la fecha viene cumpliendo durante la ejecución del contrato y corte del periodo, con el pago de los aportes al Sistema General de Seguridad Social en Salud, Pensión y Riesgos Laborales o la certificación emitida por el Representante Legal y/o Revisor Fiscal de la firma donde indica que la precitada persona jurídica se encuentra al día con el Sistema de Seguridad Social, Pensiones, etc., de conformidad con las normas legales vigentes.	SI .
Que su ejecución presupuestal ha obedecido a los pagos y desembolsos pactados contractualmente y las modificaciones si a ello hubiere lugar.	SI .

La presente certificación se expide para efectos de pago por el valor de veintiun millones treinta mil seiscientos nueve pesos m/cte. ($21,030,609.00), tal como lo estipula la cláusula TERCERA del contrato: Valor y Forma de Pago, de conformidad con la(s) factura(s) NO. FC 001000096268 del 25 de octubre de 2024.

El valor se debe afectar de la siguiente manera:

R.P./RES.	Rubro Presupuestal	Plan cuentas - Fuente financiación - PEP	Valor a Pagar
1640 VIG	O2301172301202402290300 4-8109 - IMPLEMENTACIÓN DE LA ESTRATEGIA DE CIUDAD INTELIGENTE PARA MEJORAR LA CALIDAD DE VIDA DE LA CIUDADANÍA EN BOGOTÁ D.C.	O232010100502030101-Paquetes de software Fuente: 1-100-F001 PEP: PM/0104/0103/23010040229	21,030,609.00

Centros de Costo

RP/RES	Rubro Pptal	Nombre del Rubro Presupuestal	Centro de Costo	Vr Centro Costo
1640	O2301172301202402290300 4	8109 - IMPLEMENTACIÓN DE LA ESTRATEGIA DE CIUDA	OFICINA CONSEJERÍA DISTRITAL - TIC	21,030,609.00

Descripción: Pago por servicios prestados a satisfacción durante el periodo del 1 al 30 de septeimbre de 2024. Radicado SIGA 1-2024-42540

El pago se debe abonar a la cuenta bancaria asociada al contrato o convenio celebrado.

Se expide la presente certificación en Bogotá D.C., a los 29 días del mes de octubre de 2024.

JUAN CARLOS PARADA GALLARDO
Asesor De Despacho

Solicitud No: 4973



S O L U C I O N E S C O R P O R A T I V A S
244700_000003
SECRETARIA GENERAL DE LA ALCALDIA CTO 42000008072
NIT 899999061
CRA 8 NO. 10 - 65
Bogotá/Cundinamarca

Factura Electrónica de Venta No. FC 001000096268
PERIODO FACTURADO Septiembre 01 al 30
Fecha de Expedición Octubre 25 de 2024 - 12:51 h.

NÚMERO CUENTA PARA PAGOS:	FECHA DE PAGO PARA EVITAR SUSPENSIÓN :	TOTAL A PAGAR
12055422360	Noviembre 22 de 2024	$ 21,030,609.00

M E S A N T E R I O R

VALOR FACTURA ANTERIOR	- PAGO RECIBIDO

M E S A C T U A L

+ FACTURA ACTUAL	+ NOTAS CRÉDITO	+ AJUSTE A LA DECENA	= ESTADO DE CUENTA
$21,030,609.00			$ 21,030,609.00

R E S U M E N D E F A C T U R A E L E C T R Ó N I C A D E V E N T A

ITEM	SERVICIO	SUBTOTAL	IVA	TOTAL
1	Hora para mejoras, nuevas funcionalides e integraciones	$ 2.658.100.00	$ 505.039.00	$ 3.163.139.00
2	Paquete de Conversaciones	$ 15.821.570.00	-	$ 15.821.570.00
3	Paquete de Notificaciones Proactivas	$ 2.045.900.00	-	$ 2.045.900.00
	TOTAL FACTURADO	$ 20,525,570.00	$ 505,039.00	**$ 21,030,609.00**

"Si cancelas después de la fecha límite, los intereses se cobrarán en la siguiente factura. Adicionalmente se cobrarán cargo por reconexión por cada Servicio individual: $18.000; Plan Dúo: $26.000; Plan Trío: $29.000, valores con IVA incluido"

VALOR TOTAL A PAGAR

(415)7707181500017(8020)100100009626 81(3900)0021030609(96)202411

REFERENCIA DE PAGO 1-001000096268-1
FACTURA ELECTRÓNICA DE VENTA NO. FC 001000096268
FORMA DE PAGO: Crédito
MEDIO DE PAGO: Otro
FECHA LÍMITE DE PAGO PARA EVITAR SUSPENSIÓN Noviembre 22 de 2024
VALOR TOTAL A PAGAR **$ 21,030,609.00**

CANALES DIGITALES DE ATENCIÓN:

LÍNEA DE ATENCIÓN EMPRESAS
WHATSAPP
305 777 7772

MI ETB
EMPRESAS & CIUDADES INTELIGENTES
MI ETB

¡HOLA SOY LUZ! TU ASISTENTE VIRTUAL

Denuncie
De la explotación sexual a menores de edad
teprotejo.org

Superintendencia de Industria y Comercio – SIC KR 13 27 00 Pi 1/3 BOGOTA D. C. Contact Center 601 5920400 – 018000 910 165 CONTACTENOS@SIC.GOV.CO, www.sic.gov.co

Autoridad Nacional de Televisión - ANTV CL 72 12 77 ED Fernando Gómez Agudelo BOGOTA D. C PBX: 601 7957000 - Fax 601 7957000 ext: 1107 – 018000516072, informacion@antv.gov.co, www.antv.gov.co
Facturador: Revchain Solutions LLC Sucursal Colombia Nit 900.817.668-1 Software: Revchain Con Cesión parcial del contrato a: Techrea, con NIT: 900.306.554-8

Carvajal Soluciones de Comunicación S.A.S. NIT: 800.096.812-8



SOLUCIONES CORPORATIVAS

ETB protege el derecho a la intimidad de los consumidores

Por eso te invitamos a seleccionar los canales por los cuales quieres que te contacten con fines comerciales, publicitarios y de gestión de cartera.

Selecciónalos ingresando a: etb.com/ley2300

Mientras tanto, continuaremos contactándote por los canales habituales.



ESCANEA EL CÓDIGO QR PARA SELECCIONAR LOS CANALES

CANALES DIGITALES DE ATENCIÓN AL CLIENTE

WHATSAPP 305 777 7772

MI ETB EMPRESAS & CIUDADES INTELIGENTES

MI ETB

¡HOLA SOY LUZ! TU ASISTENTE VIRTUAL

CHAT ETB.COM

CUFE: bab9071da90cc618e6abe1a05a902ada34700f1c786a27b8ebde74356b1ef87b99ad447f4eb5bbb544310be68b54f1a1

CONSULTE SU FACTURA ELECTRÓNICA DE VENTA EN MI ETB EMPRESAS Y CIUDADES INTELIGENTES

CENTROS DE SERVICIO

CENTRO	Cra. 7 No. 20-65
CHICÓ	Cra. 15 No. 90-13
KENNEDY	Cra. 78H No. 36-65 Sur
OLAYA	Av. Caracas 24 - 60 Sur

Para mayor información sobre la factura de su empresa, marque: A nivel nacional 01 8000 123 737

Ingrese a etb.com para PQR (Peticiones, Quejas y Recursos) escriba al correo solucion_grandes_clientes@etb.com y para soporte a helpdesketb@etb.com.co

Descarga tu factura electrónica de venta >>>>

OFICINA DE ATENCIÓN DE PQR (PETICIONES, QUEJAS Y RECURSOS) SEGÚN RÉGIMEN DE PROTECCIÓN AL USUARIO SIC.

24

HELP DESK PREMIUM

Para mayor información y atención de PQR's (Peticiones, Quejas y Recursos), marque gratis a nuestras líneas de Atención Telefónica 01 8000 123 737 a Nivel Nacional

RECUERDE: Si paga su factura fuera de la fecha, se aplicará una Tasa de Recargo Mora de 2.09% ETB SA ESP – NIT 899.999.115-8 Somos agentes autorretenedores – Resolución DIAN 0547 de Enero 2002 y agentes retenedores para terceros – Decreto 2885 de 2001. Régimen Común. Agente retenedor impuesto sobre las ventas. Grandes contribuyentes – Resolución 9061 del 10 de diciembre de 2020. Autorretenedores de rendimientos financieros. (Resolución 2863 de 2018) Agente retenedor permanente ICA. Actividad Económica 6110, tarifa 9.98 por mil. Catalogada como Entidad de Derecho Público para efectos de retención ICA Bogotá D.C. Aplican tarifas de IVA así: Servicio telefónico – 19%; Telefonía Móvil Celular – 19% y 4% por Impuesto al Consumo; Otros bienes y servicios – 19%. Según lo dispuesto en el artículo 192 de la Reforma Tributaria (Ley 1819 de 2016): "La tarifa del impuesto sobre las ventas aplicable a los contratos celebrados con entidades públicas o estatales, será la vigente en la fecha de la resolución o acto de adjudicación, o suscripción del respectivo contrato" Si tales contratos son adicionados, a dicha adición le son aplicables las disposiciones vigentes al momento de la celebración de dicha adición. " Apreciado Cliente: Es importante que revise las instalaciones telefónicas internas (dentro de su vivienda, edificio o predio) ya que son de su responsabilidad. De ésta manera prevendrá posibles fraudes con su línea. Además, ETB tiene a su disposición los servicios gratuitos de Código Secreto y Local Exclusivo, que le permiten restringir las llamadas de su línea telefónica. Para solicitar la restricción de llamadas a los servicios que cobren tarifa con prima acérquese a cualquier CADE o Centro de Servicios." "Señor cliente, los ajustes resultado del trámite de cambio de plan, se verán reflejados en su próxima factura". Resolución DIAN para facturación electrónica No. 18764069865682 del 30 de Abril de 2024 Prefijo FC, Autoriza desde 1000000000 al 1000396000. Vigencia de 24 meses

USO DE LOS CÓDIGOS DE BARRAS: Esta factura presenta dos códigos de barras, los cuales se usan para fechas de pago que superan los 30 días. El uso de los cupones de código de barras es exclusivamente entre sí. El cupón de Mes 1 sirve para pagar los cargos de la presente factura. El cupón de Saldo Total sirve para pagar los cargos que a la fecha tiene pendientes por pagar al momento de la emisión de la presente factura. En caso de no pagar en las fechas establecidas se generarán intereses de mora y posible suspensión del servicio.

RECUERDE: EN CASO DE PRESENTAR UNA RECLAMACIÓN EN RELACIÓN CON EL MONTO DE SU FACTURA, DEBERÁ PROCEDER AL PAGO DE LAS SUMAS QUE NO SEAN OBJETO DE RECLAMACION, ANTES DE LA FECHA DEL PAGO OPORTUNO.

PUNTOS DE PAGO

PAGO EN ENTIDADES NO BANCARIAS
Efecty

PAGO CAJEROS ELECTRÓNICOS
ATH, Red Multicolor, Bancos, Servibanca

RED CADE
Cades, Rapicades y Supercades

DOMICILIACIÓN Y/O DÉBITO AUTOMÁTICO
Consulte con su Banco para mayor información

PAGOS POR INTERNET
www.etb.com/pagos/
www.etb.com/Empresas/mietb
www.bancodebogota.com.co
www.bancopopular.com.co
www.bbva.com.co
www.bcsc.com.co
www.colpatria.com.co
www.davivienda.com.co
www.gnbsudameris.com.co
www.itau.co
www.mispagosaldia.com

PAGO TELEFÓNICO
BCSC 601 3077030
Bogotá 601 3820000
Citibank 601 6383838
Scotiabank Colpatria 601 7561616
Davivienda 601 3383838
GNB Sudameris 601 3077707

PAGO EN OFICINAS DE ENTIDADES FINANCIERAS
BCSC Bogotá, Citibank Itaú, Colpatria (Clientes) GNB Sudameris, Banco Pichincha Popular

PAGO EN OFICINAS ESPECIALIZADAS (BANCOS)
BCSC, Colpatria, Bogotá, Davivienda

Corvajal Soluciones de Comunicación S.A.S. NIT. 800.096.812-8



SECRETARIA GENERAL DE LA ALCALDIA CTO 42000008072

CUENTA CLIENTE 12055422360 **PERIODO FACTURADO: Septiembre 01 al 30**
FACTURA ELECTRÓNICA DE VENTA No. FC 001000096268

ANEXO DETALLE POR NÚMERO DE CONEXIÓN

DETALLE POR SERVICIO

Negocios Especiales **TOTAL: $ 21,030,609.00**

SERVICIO	PERIODO	ID SERVICIO	CAPACIDAD	DIRECCIÓN / CIUDAD INSTALACIÓN	VALOR SIN IMPUESTOS	VALOR CON IMPUESTOS
OFIMATICA_REV_CFM	01-Sep-24 / 30-Sep-24	STI00055570		Bogotá	$ 17,867,470.00	$ 17,867,470.00
OFIMATICA_REV_CFM	01-Sep-24 / 30-Sep-24	STI00081908		Bogotá	$ 2,658,100.00	$ 3,163,139.00

Superintendencia de Industria y Comercio – SIC KR 13 27 00 P1 1/3 BOGOTA D. C. Contact Center 601 5920400 – 018000 910 165 CONTACTENOS@SIC.GOV.CO, www.sic.gov.co

Autoridad Nacional de Televisión - ANTV CL 72 12 77 ED Fernando Gómez Agudelo BOGOTA D. C. PBX: 601 7957000 - Fax: 601 7957000 ext. 1107 – 018000516072, informacion@antv.gov.co, www.antv.gov.co

Carvajal Soluciones de Comunicación S.A.S. NIT. 800.096.812-8

DIAN

Formulario del Registro Único Tributario

001

2. Concepto 0 2 Actualización

4. Número de formulario 14968743686

(415)7707212489984(8020) 000001496874368 6

5. Número de Identificación Tributaria (NIT)	6. DV	12. Dirección seccional	14. Buzón electrónico
8 9 9 9 9 9 1 1 5	8	Operativa de Grandes Contribuyentes 3 1	

IDENTIFICACIÓN

24. Tipo de contribuyente	25. Tipo de documento	26. Número de Identificación	27. Fecha expedición
Persona jurídica 1			

Lugar de expedición	28. País	29. Departamento	30. Ciudad/Municipio

31. Primer apellido	32. Segundo apellido	33. Primer nombre	34. Otros nombres

35. Razón social

EMPRESA DE TELECOMUNICACIONES DE BOGOTA SA ESP PUDIENDO IDENTIFICARSE PARA TODOS LOS EFECTOS CON LA SIGLA ETB S.A. E.S.P

36. Nombre comercial	37. Sigla
	ETB SA ESP

UBICACIÓN

38. País	39. Departamento	40. Ciudad/Municipio
COLOMBIA 1 6 9	Bogotá D.C. 1 1	Bogotá, D.C. 0 0 1

41. Dirección principal

CR 8 20 56

42. Correo electrónico gestioncorrespondencia@etb.com.co

43. Código postal	44. Teléfono 1	45. Teléfono 2
	2 4 2 2 7 2 0	

CLASIFICACIÓN

Actividad económica				Ocupación	
Actividad principal		Actividad secundaria		Otras actividades				
46. Código	47. Fecha inicio actividad	48. Código	49. Fecha inicio actividad	50. Código	1	2	51. Código	52. Número establecimientos
6 1 1 0	2 0 1 3 0 1 1 1	6 1 9 0	2 0 1 3 0 1 1 1	6 3 1 1	4 6 5 2			19

Responsabilidades, Calidades y Atributos

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
53. Código	5	7	8	9	1 0	1 3	1 4	1 5	3 3	4 2	4 5	4 8	5 2	5 5	5 9											

05- Impto. renta y compl. régimen ordinar
07- Retención en la fuente a título de rent
08- Retención timbre nacional
09- Retención en la fuente en el impuesto
10- Obligado aduanero
13- Gran contribuyente
14- Informante de exogena
15- Autorretenedor
33- Impuesto nacional al consumo
42- Obligado a llevar contabilidad
45- Autorretenedor de rendimientos financi
48 - Impuesto sobre las ventas - IVA
52 - Facturador electrónico
55 - Informante de Beneficiarios Finales
59 - Autorretención especial renta

Usuarios aduaneros										
	1	2	3	4	5	6	7	8	9	10
54. Código	2 2	2 3								
	11	12	13	14	15	16	17	18	19	20

Exportadores					
55. Forma	56. Tipo	Servicio	1	2	3
1	2	57. Modo	2		
		58. CPC	8 4		

IMPORTANTE: Sin perjuicio de las actualizaciones a que haya lugar, la inscripción en el Registro Único Tributario -RUT-, tendrá vigencia indefinida y en consecuencia no se exigirá su renovación

Para uso exclusivo de la DIAN

59. Anexos SI [ ] NO [X] 60. No. de Folios: 0 61. Fecha 2023 - 12 - 21 / 12 : 30: 14

La información suministrada a través del formulario oficial de inscripción, actualización, suspensión y cancelación del Registro Único Tributario (RUT), deberá ser exacta y veraz; en caso de constatar inexactitud en alguno de los datos suministrados se adelantarán los procedimientos administrativos sancionatorios o de suspensión, según el caso, Parágrafo del artículo 1.6.1.2.6 del Decreto 1625 del 2016. De igual manera al formalizar el trámite el usuario fue informado y acepta la política de tratamiento de datos ley 1581 de 2012.

Firma del solicitante:

Sin perjuicio de las verificaciones que la DIAN realice.

Firma autorizada:

984. Nombre BLANCO RIVEIRA ALEXIS JAVIER

985. Cargo Representante legal Certificado

COPIA CERTIFICADO DOCUMENTO SIN COSTO

Fecha generación documento PDF: 10-01-2024 03:30:19PM

Deloitte & Touche S.A.S.
Nit. 860.005.813-4
Carrera 9 No. 78-31 Piso 1
Bogotá, D.C.
Colombia

Tel: +57 (601) 426 2000
www.deloitte.com/co

El Suscrito Revisor Fiscal Principal de
Empresa de Telecomunicaciones de Bogotá S.A. E.S.P.
NIT 899.999.115-8

CONSIDERANDO QUE:

1. De conformidad con el artículo 2 de la Ley 43 de 1990, demás previsiones legales y pronunciamientos jurisprudenciales existentes en la materia, la Revisoría Fiscal es una actividad relacionada con la ciencia contable ejercida por un Contador Público quien lleva a cabo sus funciones con fundamento en las normas, principios y procedimientos propios de dicha profesión; dentro de las cuales se encuentra la función de certificación que tiene carácter de prueba cuando se expide con fundamento en los libros de contabilidad y en el sistema contable de la compañía.

2. La Administración de la Compañía es responsable por la correcta preparación de los registros contables, los cuales se deben realizar con fundamento en el marco técnico normativo aplicable en Colombia en materia de información contable y financiera.

3. A la fecha se encuentra en curso mi examen sobre los estados financieros de la compañía por el año que terminará al 31 de diciembre de 2024.

4. Para efectos de la expedición de la presente certificación he obtenido la información que he considerado necesaria y he realizado los siguientes procedimientos:

   - Cruce de los saldos de los auxiliares contables de las cuentas: 24150181 - Aportes de Pensión, 24150191 - Aportes de Salud, 24150201 - Aportes ICBF y Sena, 24150321 - Aportes ARL y 25112401 - Aportes Caja del mes de septiembre de 2024 contra las planillas PILA de mismo corte.

   - Verificación de los pagos de las planillas PILA que se relacionan a continuación, de acuerdo con las fechas establecidas por el Decreto 923 del 31 de mayo de 2017.

Planillas empleados activos	
No. de planilla	Fecha de pago
80557650	04/10/2024

Planilla empleados pensionados	
No. De planilla	Fecha de pago
80547222	04/10/2024

De acuerdo con las anteriores consideraciones a continuación expedimos la certificación solicitada por Empresa de Telecomunicaciones de Bogotá S.A. E.S.P.

Deloitte se refiere a una o más entidades de Deloitte Touche Tohmatsu Limited ("DTTL"), su red global de firmas miembro y sus sociedades afiliadas a una firma miembro (en adelante "Entidades Relacionadas") (colectivamente, la "organización Deloitte"). DTTL (también denominada como "Deloitte Global") así como cada una de sus firmas miembro y sus Entidades Relacionadas son entidades legalmente separadas e independientes, que no pueden obligarse ni vincularse entre sí con respecto a terceros. DTTL y cada firma miembro de DTTL y su Entidad Relacionada es responsable únicamente de sus propios actos y omisiones, y no de los de las demás. DTTL no provee servicios a clientes. Consulte www.deloitte.com/co/conozcanos para obtener más información.

Deloitte.

CERTIFICA QUE:
(Cifras Expresadas en Pesos Colombianos)

De acuerdo con registros contables, los soportes de pago y demás documentos soporte suministrados por Empresa de Telecomunicaciones de Bogotá S.A. E.S.P., la Compañía ha realizado el pago por concepto de aportes al Sistema de Seguridad en salud para el mes de octubre de 2024; así como, los aportes a las Cajas de Compensación Familiar, riesgos profesionales, pensiones, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje correspondiente al mes de septiembre de 2024 mediante las planillas integradas de liquidación que se relacionan a continuación:

Planilla	No. de Planilla	Periodo Pensiones, ARL y Parafiscales	Periodo salud	Fecha de pago	Valor causado	Valor pagado
Planilla activos	80557650	2024-09	2024-10	04/10/2024	$4.843.462.200	$4.863.462.200
Planilla pensionados	80547222	2024-09	2024-10	04/10/2024	$11.453.200	$11.453.200

Sin perjuicio de las limitaciones establecidas por las normas legales y contables para el ejercicio de la Revisoría Fiscal, el alcance de mi trabajo en lo que se refiere a lo certificado se limita únicamente al cruce de información contable contra los soportes de pago de las Plantillas PILA que me ha suministrado la Compañía.

Se expide en Bogotá D.C. a los cuatro (04) días del mes de octubre de 2024, por solicitud de la Administración de Empresa de Telecomunicaciones de Bogotá S.A. E.S.P. en cumplimiento de lo establecido por las leyes 789 de 2002 y 828 de 2003.

Alejandro Perdomo Córdoba
Revisor Fiscal Principal
Tarjeta Profesional No. 124911-T
Designado por Deloitte & Touche S.A.S.

DOCUMENTATION VERIFIED

10 ANOS
IDENTIAN®
CREANDO TERRITORIOS CIBERSEGUROS

Informe Ejecutivo Retest Análisis de Vulnerabilidades

versión 1.0



Presentado a:

Silice

Enero de 2024

TABLA DE CONTENIDO

Capítulo		Página
1.	INTRODUCCIÓN	4
2.	ALCANCE	5
3.	CUMPLIMIENTO NORMATIVO	6
4.	MARCO METODOLOGÍCO DE LAS PRUEBAS	7
4.1.	Marco Metodológico De Ejecución	9
5.	DEFINICIÓN DE ESCENARIOS Y OBJETIVOS	10
5.1.	Plataforma Tecnológica	10
5.2.	Fecha de ejecución	10
5.3.	Escenario y vector de ejecución	10
6.	CRITERIOS PARA EVALUACIÓN DEL RIESGO	11
6.1.	Calculo y Valoración	11
6.2.	Niveles de Criticidad	12
7.	DESCRIPCION GLOBAL DE VULNERABILIDADES	13
7.1.	Resultados Generales	13
7.2.	Vulnerabilidades identificadas por nivel de riesgo	14
7.3.	Vulnerabilidades por activo (Dominio/ IP /HOST)	14
7.4.	Análisis Diferencial Test Vs Retest	14
8.	RECOMENDACIONES GENERALES	15
9.	CONCLUSIONES	16

CONFIDENCIAL

TABLA DE ILUSTRACIONES

Ilustración 1. Metodologías de Trabajo, OWASP 7
Ilustración 2. Metodología de Trabajo, OSSTMM 8
Ilustración 3. Metodología de Trabajo, PTEST 8
Ilustración 4. Fases del Proyecto 9
Ilustración 5. Escenarios de Pruebas 10
Ilustración 6. Objetivos Ethical Hacking Interno SILICE (LATAM PAU) 10
Ilustración 7. Relación valor cualitativo – cuantitativo del IMPACTO 12
Ilustración 8. Relación valor cualitativo – cuantitativo Factor de Ocurrencia 12
Ilustración 9. Calculo para la Valoración del Riesgo 12
Ilustración 10. Representación Niveles de Criticidad 12
Ilustración 11. Vulnerabilidades Identificadas 13
Ilustración 12. Vulnerabilidades encontradas 14
Ilustración 13. Vulnerabilidades encontradas por activo 14
Ilustración 14. Vulnerabilidades encontradas – Analisis diferencial 14
Ilustración 15. Resultado General 16

CONFIDENCIAL

1. INTRODUCCIÓN

El objetivo de este documento es presentar el resultado de las pruebas de **ETHICAL HACKING EXTERNO** realizadas sobre los dispositivos pertenecientes a la plataforma tecnológica de **SILICE** estipulados en el alcance del proyecto, estas pruebas se llevaron a cabo de acuerdo a los lineamientos de las metodologías manejadas por **IDENTIAN**.

Toda la información que se muestra a continuación se ha obtenido lícitamente mediante permisos formales por nuestro cliente. Sus conclusiones son el fruto de un minucioso estudio sobre los resultados de las pruebas.

CONFIDENCIAL

2. ALCANCE

El objetivo del servicio es validar y definir claramente los niveles de exposición en que se encuentra la plataforma tecnológica de **SILICE** frente a posibles ataques e incursiones no autorizadas por parte de delincuentes informáticos, con el fin de lograr que la configuración de la infraestructura tecnológica implementada actualmente, cumpla con los más altos estándares de seguridad, de manera que se minimice el riesgo en cuanto a la integridad, disponibilidad y confidencialidad de la información de la red de datos de **SILICE.**

De acuerdo con lo anterior, las pruebas se encuentran enmarcadas en la evaluación de características asociadas al sistema operativo y configuración de servicios en cada dispositivo, de acuerdo con las especificaciones definidas por parte de la gerencia del proyecto en **SILICE** en conjunto con la consultoría y las cuales comprenden los siguientes escenarios:

- Escenario 1 – **Pruebas Hacking Ético Caja Gris Externo**
- Escenario 2 – **Pruebas Hacking Ético Caja Blanca Externo**
-

CONFIDENCIAL

3. CUMPLIMIENTO NORMATIVO

De acuerdo con las metodologías utilizadas en la ejecución del proyecto, **IDENTIAN** considera dentro del contexto de las pruebas y de la compañía la aplicabilidad de los siguientes estándares, normas y las directrices metodológicas según sea requerido por la compañía:

a. **Circular externa 007 de la Superintendencia Feneciera de Colombia:** En su numeral 4.2. Protección y detección establece: Las entidades deben desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos. Las entidades deben:

4.2.1. Adoptar procedimientos y mecanismos para identificar y analizar los incidentes de ciberseguridad que se presenten.
4.2.2. Gestionar las vulnerabilidades de aquellas plataformas que soporten activos de información críticos y que estén expuestos en el ciberespacio.
4.2.3. Realizar un monitoreo continuo a su plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la entidad**.**

b. **Estándar PCI DSS:** La norma PCI DSS en su requisito 11.2, determina pruebas sobre análisis de vulnerabilidades internos, externos y ethical hacking, 11.3 pruebas de penetración y segmentación. Lo anterior garantiza que el entorno de datos de tarjeta de crédito se encuentra protegido.

c. **ISO 27001:** Para asegurar los tres pilares de la seguridad de la información (Disponibilidad, Integridad y Confidencialidad) en su numeral 18.2.3, se realizarán pruebas técnicas sobre la infraestructura de la compañía. Adicionalmente el numeral 12.6 menciona implementar un sistema de gestión de vulnerabilidades para prevenir incidentes de seguridad.

d. **C042:** Los lineamientos para fortalecer la seguridad de la información de los clientes y usuarios que están vigilados por la Súper Financiera de Colombia, mencionan realizar pruebas de vulnerabilidad y test de penetración anualmente. Adicionalmente asegurar la segregación de los ambientes y establecer un sistema de análisis de vulnerabilidades.

CONFIDENCIAL

4. MARCO METODOLOGÍCO DE LAS PRUEBAS

El juego de pruebas a partir de la información recolectada contó con un amplio margen de detección de vulnerabilidades potenciales incluyendo aquellas que son automatizadas, es decir que son detectadas a partir del uso de herramientas de software especializadas y en las cuales dichos programas evalúan, categorizan e identifican automáticamente las posibles vulnerabilidades presentes en cada uno de los activos evaluados, por medio de algoritmos que comparan las características de cada sistema en particular contra su base de datos propia y de otra parte se realizó la detección manual de vulnerabilidades la cual se basa en el conocimiento del consultor a través de la información recopilada en cada uno de los activos evaluados y sobre la cual se ejecutan ataques controlados de manera específica con el fin de evidenciar fallos a nivel de configuración, puertos y servicios habilitados, versiones del sistema, entre otros.

Estas vulnerabilidades, relacionadas directamente con los componentes a evaluar; serán parte de pruebas a ejecutar a lo largo del ejercicio **ETHICAL HACKING EXTERNO**, teniendo en cuenta factores como las características propias de cada servidor (puertos, servicios, versiones del software, sistema operativo, etc.), las aplicaciones, arquitectura y todas aquellas particularidades que permiten identificar inicialmente la posible existencia de un riesgo.

Las pruebas de seguridad se encuentran soportadas en estándares internacionales establecidos para el desarrollo de pruebas de vulnerabilidad y penetración enumeradas a continuación:

- **OWASP: Open Web Application Security Project**
- **OSSTMM: Open Source Security Testing Methodology Manual**
- **PTES: Penetration Testing**

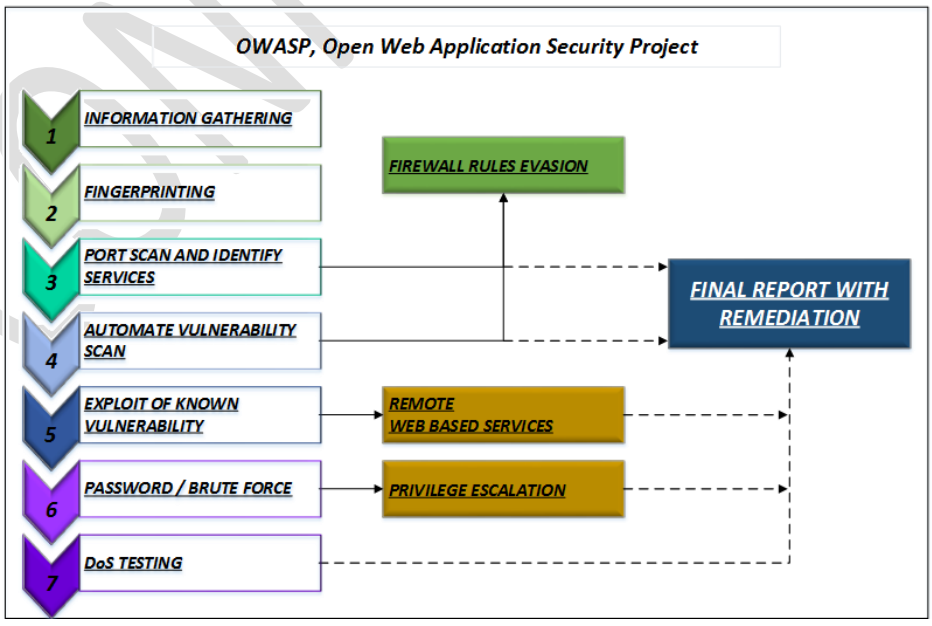


Ilustración 1. Metodologías de Trabajo, OWASP

CONFIDENCIAL

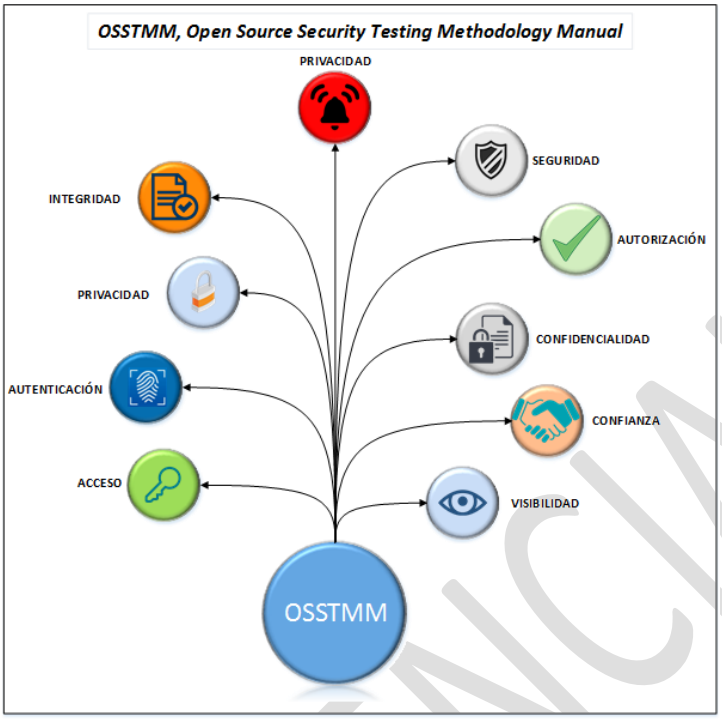


Ilustración 2. Metodología de Trabajo, OSSTMM

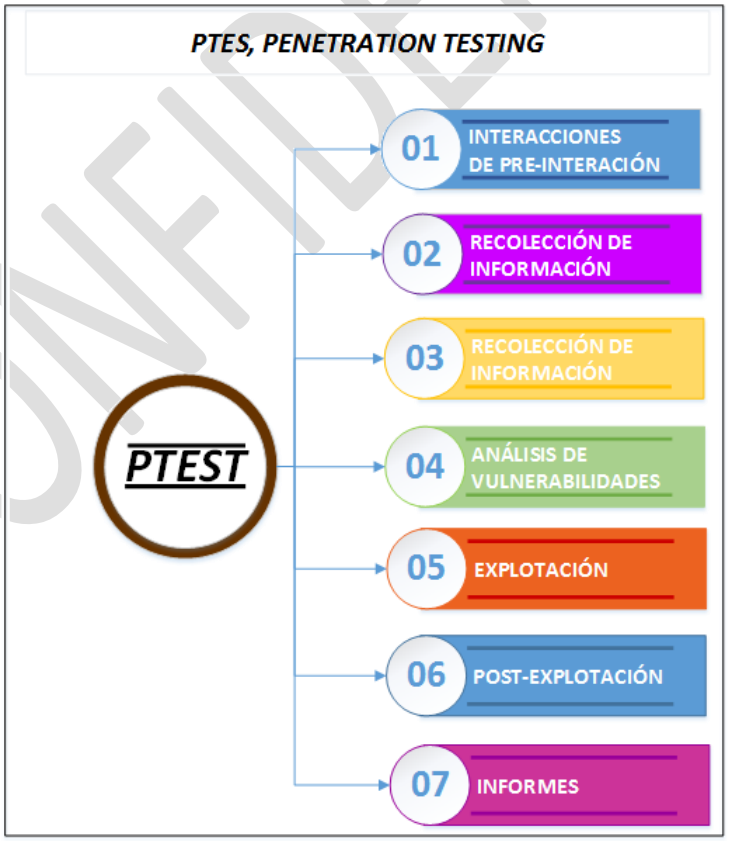


Ilustración 3. Metodología de Trabajo, PTEST

CONFIDENCIAL

4.1. Marco Metodológico De Ejecución

Con el propósito de alcanzar los objetivos esperados, el proyecto se estructura de la siguiente forma:

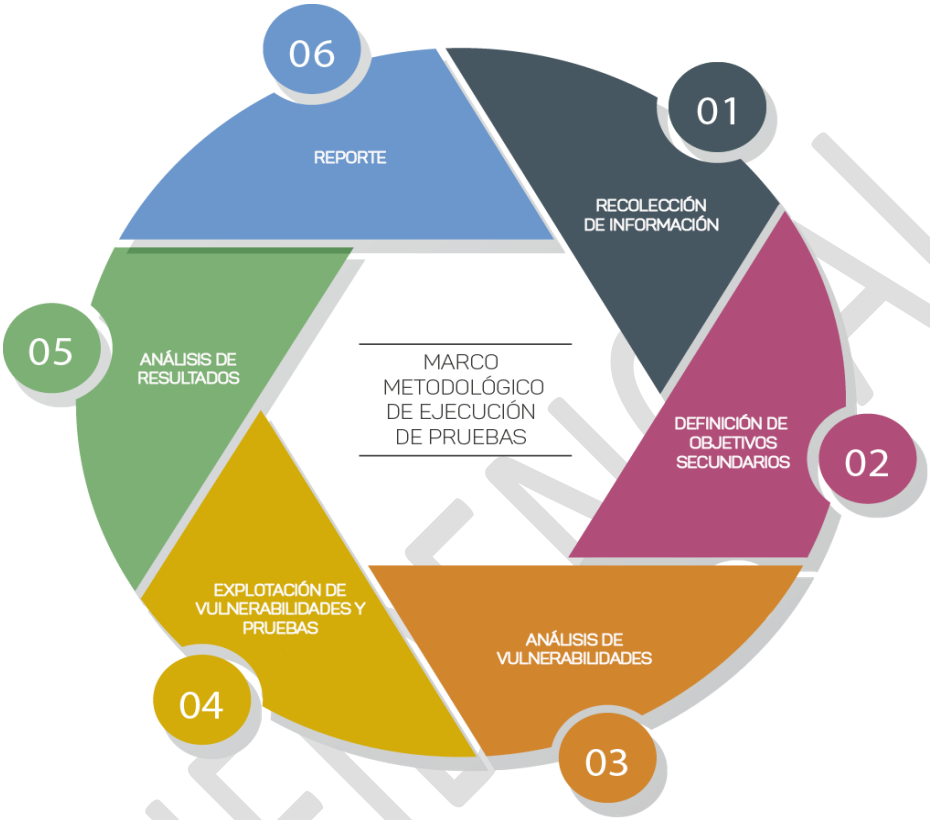


Ilustración 4. Fases del Proyecto

CONFIDENCIAL

5. DEFINICIÓN DE ESCENARIOS Y OBJETIVOS

Define los lugares desde donde el consultor realizará las pruebas de seguridad.

Escenario	Descripción	Aplica
Escenario 1	Pruebas internas: las pruebas se realizan desde un punto de acceso asignado por la empresa, en el cual se tiene visibilidad directa a los objetivos.	NO
Escenario 2	Pruebas externas: las pruebas se realizan desde una red externa a la de la empresa. En la mayoría de los casos se hace desde Internet.	SI

Ilustración 5. Escenarios de Pruebas

5.1. Plataforma Tecnológica

Bajo este esquema, los recursos que se sometieron a pruebas de vulnerabilidad en **SILICE** de acuerdo con lo definido por el área de Infraestructura fueron los siguientes:

Aplicaciones Internas		
No.	**Dominio**	**URL**
1	latam.pau.zone	https://latam.pau.zone/
2	api-latam.pau.zone	https://api-latam.pau.zone/

Ilustración 6. Objetivos Ethical Hacking Interno SILICE (LATAM PAU)

5.2. Fecha de ejecución

Las pruebas fueron ejecutadas en un escenario Externo controlado, en un espacio de tiempo entre el 15 y el 24 de enero de 2024 en un horario intermitente de 8:00 am a 1:00 am.

5.3. Escenario y vector de ejecución

Las pruebas se ejecutaron de manera Remota desde una ubicación publica cuya IP: 190.84.117.125 y 181.51.9.236. sin considerar ningún permiso adicional.

Las pruebas se ejecutan en modalidad Caja Negra, Caja Gris y con usuario valido en la aplicación, tipo Caja Blanca.

CONFIDENCIAL

6. CRITERIOS PARA EVALUACIÓN DEL RIESGO

El riesgo se entiende como la combinación de dos factores: la probabilidad de un evento y su impacto (*ISO Guide 73*), por lo que la evaluación del riesgo comprende la consideración sistemática de lo siguiente:

- ***Probabilidad*:** Es la medida real de la probabilidad de ocurrencia de un evento (o de un suceso de seguridad) teniendo como parámetros las amenazas, vulnerabilidades y controles más frecuentes que se tengan implementados en la compañía para proteger los activos.
- ***Impacto*:** Es el daño que probablemente puede resultar de la ocurrencia de un evento de seguridad, teniendo como referencia las consecuencias potenciales derivadas de la pérdida o falla en alguno de los criterios propios de la información (Confidencialidad, Integridad, Disponibilidad). Generalmente se deriva del valor de recuperación del activo en caso de pérdida.

La metodología de análisis de riesgo utilizada en este proceso de evaluación de vulnerabilidades y pruebas de **ETHICAL HACKING EXTERNO**, está enfocada a realizar un análisis de tipo "***Cualitativo***", es decir, valorar y medir todos los componentes del análisis, los activos, las probabilidades de ocurrencia de los eventos, el impacto y el riesgo propiamente dicho, en escalas de nivel, sin entrar en la utilización de valores estimados de costos en dinero. Teniendo en cuenta lo anterior, la evaluación de probabilidad o factor de ocurrencia se encuentra definida bajo un marco de estimación estadístico mundial que permite identificar el comportamiento histórico frente a la ocurrencia de eventos relacionados con la explotación de vulnerabilidades y generación de ataques.

Dentro de las pruebas se analiza cada uno de los dispositivos evaluados como un activo de información teniendo como base que un activo es algo que tiene valor y que es de utilidad para una compañía, la operación de su negocio y su propia continuidad. Cabe aclarar que determinar el valor de cada uno de estos activos en forma detallada se enmarca dentro de un análisis de riesgos global en toda la compañía y el cual se constituye como un procedimiento de alta rigurosidad que para este caso no ha sido realizado, no obstante la evaluación de riesgo realizada en estas pruebas se deriva de un análisis de alto nivel frente a la criticidad de la plataforma y los objetivos de negocio identificados, los cuales a su vez se encuentran enmarcados en la clasificación de vulnerabilidades y su impacto según la industria a nivel mundial.

6.1. Calculo y Valoración

El cálculo realizado para estimar el nivel de riesgo asociado a la plataforma evaluada se encuentra definido bajo los siguientes criterios:

- **Impacto**: Suma del Valor de la Confidencialidad, la Disponibilidad e Integridad para cada activo de información, teniendo en cuenta:

CONFIDENCIAL

Valor Cualitativo	Valor Cuantitativo
Catastrófico	5
Mayor	4
Moderado	3
Menor	2
Bajo	1

Ilustración 7. Relación valor cualitativo – cuantitativo del IMPACTO

Valor Cualitativo	Valor	Descripción
Casi Seguro	5	Se espera que ocurra en la mayoría de las circunstancias
Probable	4	Probablemente ocurra en la mayoría de las circunstancias
Posible	3	Podría ocurrir en algún momento
Improbable	2	Pudo ocurrir en algún momento
Raro	1	Puede ocurrir solo en circunstancias excepcionales

Ilustración 8. Relación valor cualitativo – cuantitativo Factor de Ocurrencia



Ilustración 9. Calculo para la Valoración del Riesgo

6.2. Niveles de Criticidad

A continuación, se describen los niveles de criticidad bajo los que se realiza el análisis.

Crítico CVSS 9.0-10.0	Alto CVSS 7.0-8.9	Medio CVSS 4.0-6.9	Bajo CVSS 0.1-3.9
En esta clasificación se encuentran las vulnerabilidades de seguridad que pueden comprometer un sistema.	En esta clasificación se encuentran las vulnerabilidades de seguridad que pueden otorgar privilegios a un atacante sobre el sistema.	En esta clasificación se encuentran las vulnerabilidades de seguridad que individualmente no afectan de forma grave el sistema pero que pueden llevar a un ataque al combinarse con otras.	En esta clasificación se encuentran las vulnerabilidades de seguridad que suministran información a un atacante pero no genera un riesgo para la integridad o disponibilidad del sistema.

Ilustración 10. Representación Niveles de Criticidad

La ilustración 10 presenta el nivel de riesgo o grado de exposición del sistema; su función es establecer la importancia de las vulnerabilidades identificadas; es un insumo primordial del plan de mitigación que permite gestionar y mitigar las debilidades mediante su priorización.

CONFIDENCIAL

7. DESCRIPCION GLOBAL DE VULNERABILIDADES

Las pruebas de vulnerabilidades consistieron en determinar problemas de seguridad en la etapa de identificación de Información en los activos escaneados. Estos problemas de seguridad, se pueden determinar usando herramientas especializadas automáticas o de manera manual, ahora bien, estas pruebas se caracterizaron por la presencia de controles de seguridad, que limitaban el escaneo de puertos y de vulnerabilidades constantemente.

7.1. Resultados Generales

La identificación de vulnerabilidades contribuye a la medición del riesgo existente en la infraestructura tecnológica, desde el punto de vista de configuraciones de software implementado, falta de actualización o una configuración errónea de los mismos. A continuación, se muestran los resultados de las vulnerabilidades identificadas:

Riesgo	Vulnerabilidades
BAJO	5
MEDIO	2
ALTO	1
CRITICO	0
TOTAL	8

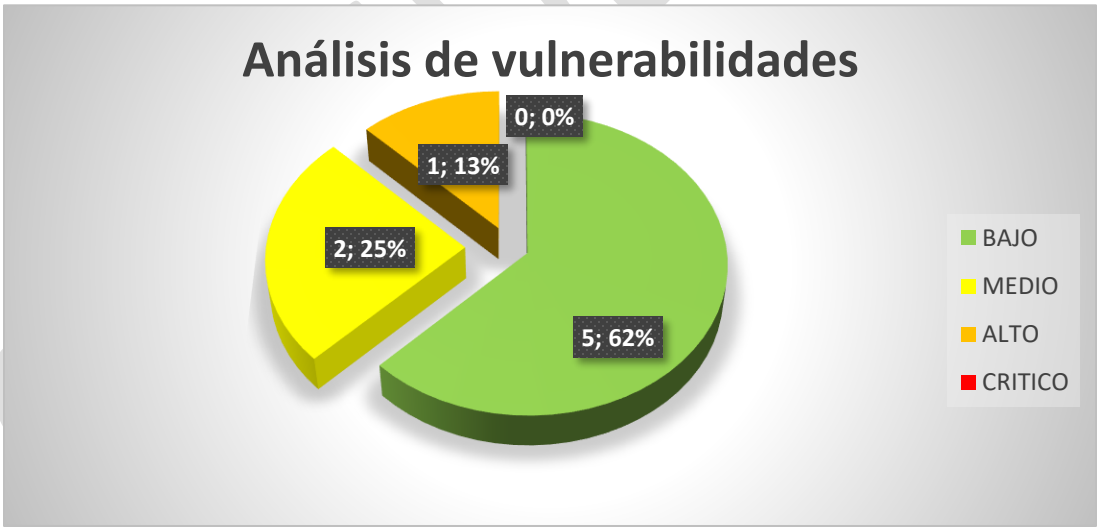


Ilustración 11. Vulnerabilidades Identificadas

Ilustración 11: En el análisis realizado, se identifica una (1) vulnerabilidad con riesgo alto, dos (2) vulnerabilidades con severidad media, y cinco (5) vulnerabilidades con severidad baja.

7.2. Vulnerabilidades identificadas por nivel de riesgo

ID	RIESGO	NOMBRE DE LA VULNERABILIDAD	HOST IP / DOMINIO
1	ALTO	Out-of-date Version (Apache)	latam.pau.zone, api-latam.pau.zone
2	MEDIO	SSL Certificate Cannot Be Trusted	latam.pau.zone
3	MEDIO	SSL Self-Signed Certificate	latam.pau.zone
4	BAJO	Login page password-guessing attack	api-latam.pau.zone
5	BAJO	HSTS Missing From HTTPS Server (RFC 6797)	latam.pau.zone
6	BAJO	Content Security Policy (CSP) not implemented	latam.pau.zone
7	BAJO	Version Disclosure (Apache)	latam.pau.zone
8	BAJO	Autocomplete Enabled	latam.pau.zone

Ilustración 12. Vulnerabilidades encontradas

Remitir al documento anexo "Matriz Análisis de Vulnerabilidades Silice RETEST PAU-DSP externa Enero 2024" para más información de las vulnerabilidades identificadas.

7.3. Vulnerabilidades por activo (Dominio/ IP /HOST)

A continuación, se entrega el detalle de la cantidad de vulnerabilidades por cada uno de los activos, esto nos ayuda a tomar decisiones y priorizar el plan de acción y remediación.

Vulnerabilidades por Activo						
No.	IP / Dominio	Critico	Alto	Medio	Bajo	Total
1	latam.pau.zone	0	1	2	4	7
2	api-latam.pau.zone	0	1	0	1	2

Ilustración 13. Vulnerabilidades encontradas por activo

7.4. Análisis Diferencial Test Vs Retest

A continuación, se presenta un comparativo, entre las vulnerabilidades identificadas en el test inicial ejecutado en el mes Agosto de 2023 y las identificadas en el mes de Enero de 2024.

Análisis diferencial - Test Vs Retest					
Item	Criticas	Altas	Medias	Bajas	Total
Análisis Inicial Agosto 2023	0	1	2	6	9
Retest - Enero 2024	**0**	**1**	**2**	**5**	8
Vulnerabilidades Remediadas	0	0	0	1	1
Vulnerabilidades persistentes	0	1	2	5	8
Vulnerabilidades nuevas	0	0	0	0	0

Ilustración 14. Vulnerabilidades encontradas – Analisis diferencial

Se identifica la remediación de una (1) vulnerabilidad de riesgo bajo.

CONFIDENCIAL

8. RECOMENDACIONES GENERALES

A continuación, se presentan las recomendaciones generales que ayudaran a mitigar el nivel de riesgo al cual se encuentra expuesto los objetivos evaluados para **SILICE:**

- Corregir los hallazgos de riesgo alto identificados durante la ejecución de las pruebas.
- Actualizar las tecnologías identificadas que contienen vulnerabilidades conocidas.
- Evitar la exposición de archivos y directorios que no sean necesarios en las aplicaciones, restringiendo el acceso desde internet.
- Aplicar controles anti repeticiones automáticas en las api, evitando ataques automatizados de credenciales y otros.
- Mantener portales de administración filtrados, evitando su acceso desde cualquier ubicación en internet, esto mediante listas de acceso o métodos de autenticación basados en segundo factor de autenticación.
- Realizar auditorías de seguridad en caso de que la plataforma tecnológica se actualice o sufra un cambio importante con el fin de descartar problemas de seguridad que se puedan presentar por estos procesos.
- Seguir las recomendaciones que se presentan en los apartados anteriores con el fin de corregir las diferentes vulnerabilidades identificadas en los dispositivos evaluados.

CONFIDENCIAL

9. CONCLUSIONES

El estudio realizado sobre la plataforma tecnológica de **SILICE**, muestra aspectos o puntos de mejora, que pueden ser ajustados mediante un plan de remediación, en el cual se incluyan actualizaciones, configuraciones de acuerdo con las necesidades y requerimientos de seguridad de la información, para el adecuado funcionamiento de las operaciones y el negocio en general.

De acuerdo a lo anterior las vulnerabilidades identificadas, se clasifican en su nivel de riesgo según el CVE (Common Vulnerabilities and Exposures) vulnerabilidades y exposiciones, las cuales se encuentran en la base de datos internacional (NVD) y un marco de estimación estadístico mundial. Con lo anterior se define el nivel de criticidad sobre un marco específico para **SILICE**, que pretende alertar y mostrar de ser necesario el impacto sobre el uso de este tipo de servicios, los cuales muchas veces son evaluados sin la adecuada atención en la gestión de seguridad informática, pero que sin duda y basado en las estadísticas de ataques a nivel mundial, constituyen una amenaza frente a la probabilidad de ataques de diferente tipo.

PLATAFORMA SILICE	
CRITICO	
ALTO	
MEDIO	X
BAJO	

Ilustración 15. Resultado General

La ilustración 15 muestra el resultado general de la evaluación realizada sobre la plataforma tecnológica de **SILICE**, de acuerdo con la metodología utilizada para el análisis de riesgo y su aplicación dentro del escenario evaluado.

En nivel de riesgo de la infraestructura evaluada se cataloga como MEDIO, esto debido a los hallazgos explotables identificados.

CONFIDENCIAL

10 ANOS
IDENTIAN®
CREANDO TERRITORIOS CIBERSEGUROS

Informe Ejecutivo Análisis de Vulnerabilidades y Hackign Ético

versión 1.0



Presentado a:

Silice

Agosto de 2023

TABLA DE CONTENIDO

Capítulo	Página
1. ALCANCE	4
2. CUMPLIMIENTO NORMATIVO	4
3. MARCO METODOLOGÍCO DE LAS PRUEBAS	5
4. DEFINICIÓN DE ESCENARIOS Y OBJETIVOS	5
4.1. Plataforma Tecnológica	6
4.2. Fecha de ejecución	6
4.3. Escenario y vector de ejecución	6
5. CRITERIOS PARA EVALUACIÓN DEL RIESGO	7
5.1. Calculo y Valoración	7
5.2. Niveles de Criticidad	8
6. DESCRIPCION GLOBAL DE VULNERABILIDADES	9
6.1. Resultados Generales	9
6.2. Vulnerabilidades identificadas por nivel de riesgo	10
6.3. Vulnerabilidades por activo (Dominio/ IP /HOST)	11
8. RECOMENDACIONES GENERALES	12
9. CONCLUSIONES	13

INTRODUCCIÓN

El objetivo de este documento es presentar el resultado de las pruebas de **ETHICAL HACKING EXTERNO** realizadas sobre los dispositivos pertenecientes a la plataforma tecnológica de **SILICE** estipulados en el alcance del proyecto, estas pruebas se llevaron a cabo de acuerdo a los lineamientos de las metodologías manejadas por **IDENTIAN**.

Toda la información que se muestra a continuación se ha obtenido lícitamente mediante permisos formales por nuestro cliente. Sus conclusiones son el fruto de un minucioso estudio sobre los resultados de las pruebas.

1. ALCANCE

El objetivo del servicio es validar y definir claramente los niveles de exposición en que se encuentra la plataforma tecnológica de **SILICE** frente a posibles ataques e incursiones no autorizadas por parte de delincuentes informáticos, con el fin de lograr que la configuración de la infraestructura tecnológica implementada actualmente, cumpla con los más altos estándares de seguridad, de manera que se minimice el riesgo en cuanto a la integridad, disponibilidad y confidencialidad de la información de la red de datos de **SILICE.**

De acuerdo con lo anterior, las pruebas se encuentran enmarcadas en la evaluación de características asociadas al sistema operativo y configuración de servicios en cada dispositivo, de acuerdo con las especificaciones definidas por parte de la gerencia del proyecto en **SILICE** en conjunto con la consultoría y las cuales comprenden los siguientes escenarios:

- Escenario 1 – **Pruebas Hacking Ético Caja Gris Externo**
- Escenario 2 – **Pruebas Hacking Ético Caja Blanca Externo**

2. CUMPLIMIENTO NORMATIVO

De acuerdo con las metodologías utilizadas en la ejecución del proyecto, **IDENTIAN** considera dentro del contexto de las pruebas y de la compañía la aplicabilidad de los siguientes estándares, normas y las directrices metodológicas según sea requerido por la compañía:

a. **Circular externa 007 de la Superintendencia Feneciera de Colombia:** En su numeral 4.2. Protección y detección establece: Las entidades deben desarrollar e implementar actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad. La función de protección y detección permite el descubrimiento oportuno de eventos e incidentes de ciberseguridad y cómo protegerse ante los mismos. Las entidades deben:

b. **Estándar PCI DSS:** La norma PCI DSS en su requisito 11.2, determina pruebas sobre análisis de vulnerabilidades internos, externos y ethical hacking, 11.3 pruebas de penetración y segmentación. Lo anterior garantiza que el entorno de datos de tarjeta de crédito se encuentra protegido.

c. **ISO 27001:** Para asegurar los tres pilares de la seguridad de la información (Disponibilidad, Integridad y Confidencialidad) en su numeral 18.2.3, se realizarán pruebas técnicas sobre la infraestructura de la compañía. Adicionalmente el numeral 12.6 menciona implementar un sistema de gestión de vulnerabilidades para prevenir incidentes de seguridad.

d. **C042:** Los lineamientos para fortalecer la seguridad de la información de los clientes y usuarios que están vigilados por la Súper Financiera de Colombia, mencionan realizar pruebas de vulnerabilidad y test de penetración anualmente. Adicionalmente asegurar la segregación de los ambientes y establecer un sistema de análisis de vulnerabilidades.

3. MARCO METODOLOGÍCO DE LAS PRUEBAS

El juego de pruebas a partir de la información recolectada contó con un amplio margen de detección de vulnerabilidades potenciales incluyendo aquellas que son automatizadas, es decir que son detectadas a partir del uso de herramientas de software especializadas y en las cuales dichos programas evalúan, categorizan e identifican automáticamente las posibles vulnerabilidades presentes en cada uno de los activos evaluados, por medio de algoritmos que comparan las características de cada sistema en particular contra su base de datos propia y de otra parte se realizó la detección manual de vulnerabilidades la cual se basa en el conocimiento del consultor a través de la información recopilada en cada uno de los activos evaluados y sobre la cual se ejecutan ataques controlados de manera específica con el fin de evidenciar fallos a nivel de configuración, puertos y servicios habilitados, versiones del sistema, entre otros.

Estas vulnerabilidades, relacionadas directamente con los componentes a evaluar; serán parte de pruebas a ejecutar a lo largo del ejercicio **ETHICAL HACKING EXTERNO**, teniendo en cuenta factores como las características propias de cada servidor (puertos, servicios, versiones del software, sistema operativo, etc.), las aplicaciones, arquitectura y todas aquellas particularidades que permiten identificar inicialmente la posible existencia de un riesgo.

Las pruebas de seguridad se encuentran soportadas en estándares internacionales establecidos para el desarrollo de pruebas de vulnerabilidad y penetración enumeradas a continuación:

- **OWASP: Open Web Application Security Project**
- **OSSTMM: Open Source Security Testing Methodology Manual**
- **PTES: Penetration Testing**

4. DEFINICIÓN DE ESCENARIOS Y OBJETIVOS

Define los lugares desde donde el consultor realizará las pruebas de seguridad.

Escenario	Descripción	Aplica
Escenario 1	Pruebas internas: las pruebas se realizan desde un punto de acceso asignado por la empresa, en el cual se tiene visibilidad directa a los objetivos.	NO
Escenario 2	Pruebas externas: las pruebas se realizan desde una red externa a la de la empresa. En la mayoría de los casos se hace desde Internet.	SI

Ilustración 1. Escenarios de Pruebas

4.1. Plataforma Tecnológica

Bajo este esquema, los recursos que se sometieron a pruebas de vulnerabilidad en **SILICE** de acuerdo con lo definido por el área de Infraestructura fueron los siguientes:

Aplicaciones Internas		
No.	**Dominio**	**URL**
1	latam.pau.zone	https://latam.pau.zone/
2	api-latam.pau.zone	https://api-latam.pau.zone/

Ilustración 2. Objetivos Ethical Hacking Interno SILICE (PAU y DSP)

4.2. Fecha de ejecución

Las pruebas fueron ejecutadas en un escenario Externo controlado, en un espacio de tiempo entre el 27 de julio al 18 de agosto de 2023 en un horario intermitente de 8:00 am a 1:00 am.

4.3. Escenario y vector de ejecución

Las pruebas se ejecutaron de manera Remota desde una ubicación publica cuya IP: 190.84.117.125 y 181.51.9.236. sin considerar ningún permiso adicional.

Las pruebas se ejecutan en modalidad Caja Negra, Caja Gris y con usuario valido en la aplicación, tipo Caja Blanca.

5. CRITERIOS PARA EVALUACIÓN DEL RIESGO

El riesgo se entiende como la combinación de dos factores: la probabilidad de un evento y su impacto (*ISO Guide 73*), por lo que la evaluación del riesgo comprende la consideración sistemática de lo siguiente:

- ***Probabilidad*:** Es la medida real de la probabilidad de ocurrencia de un evento (o de un suceso de seguridad) teniendo como parámetros las amenazas, vulnerabilidades y controles más frecuentes que se tengan implementados en la compañía para proteger los activos.
- ***Impacto*:** Es el daño que probablemente puede resultar de la ocurrencia de un evento de seguridad, teniendo como referencia las consecuencias potenciales derivadas de la pérdida o falla en alguno de los criterios propios de la información (Confidencialidad, Integridad, Disponibilidad). Generalmente se deriva del valor de recuperación del activo en caso de pérdida.

La metodología de análisis de riesgo utilizada en este proceso de evaluación de vulnerabilidades y pruebas de **ETHICAL HACKING EXTERNO**, está enfocada a realizar un análisis de tipo "***Cualitativo***", es decir, valorar y medir todos los componentes del análisis, los activos, las probabilidades de ocurrencia de los eventos, el impacto y el riesgo propiamente dicho, en escalas de nivel, sin entrar en la utilización de valores estimados de costos en dinero. Teniendo en cuenta lo anterior, la evaluación de probabilidad o factor de ocurrencia se encuentra definida bajo un marco de estimación estadístico mundial que permite identificar el comportamiento histórico frente a la ocurrencia de eventos relacionados con la explotación de vulnerabilidades y generación de ataques.

Dentro de las pruebas se analiza cada uno de los dispositivos evaluados como un activo de información teniendo como base que un activo es algo que tiene valor y que es de utilidad para una compañía, la operación de su negocio y su propia continuidad. Cabe aclarar que determinar el valor de cada uno de estos activos en forma detallada se enmarca dentro de un análisis de riesgos global en toda la compañía y el cual se constituye como un procedimiento de alta rigurosidad que para este caso no ha sido realizado, no obstante la evaluación de riesgo realizada en estas pruebas se deriva de un análisis de alto nivel frente a la criticidad de la plataforma y los objetivos de negocio identificados, los cuales a su vez se encuentran enmarcados en la clasificación de vulnerabilidades y su impacto según la industria a nivel mundial.

5.1. Calculo y Valoración

El cálculo realizado para estimar el nivel de riesgo asociado a la plataforma evaluada se encuentra definido bajo los siguientes criterios:

- **Impacto**: Suma del Valor de la Confidencialidad, la Disponibilidad e Integridad para cada activo de información, teniendo en cuenta:

Valor Cualitativo	Valor Cuantitativo
Catastrófico	5
Mayor	4
Moderado	3
Menor	2
Bajo	1

Ilustración 3. Relación valor cualitativo – cuantitativo del IMPACTO

		Descripción
Casi Seguro	5	Se espera que ocurra en la mayoría de las circunstancias
Probable	4	Probablemente ocurra en la mayoría de las circunstancias
Posible	3	Podría ocurrir en algún momento
Improbable	2	Pudo ocurrir en algún momento
Raro	1	Puede ocurrir solo en circunstancias excepcionales

Ilustración 4. Relación valor cualitativo – cuantitativo Factor de Ocurrencia



Ilustración 5. Calculo para la Valoración del Riesgo

5.2. Niveles de Criticidad

A continuación, se describen los niveles de criticidad bajo los que se realiza el análisis.

Crítico CVSS 9.0-10.0	Alto CVSS 7.0-8.9	Medio CVSS 4.0-6.9	Bajo CVSS 0.1-3.9
En esta clasificación se encuentran las vulnerabilidades de seguridad que pueden comprometer un sistema.	En esta clasificación se encuentran las vulnerabilidades de seguridad que pueden otorgar privilegios a un atacante sobre el sistema.	En esta clasificación se encuentran las vulnerabilidades de seguridad que individualmente no afectan de forma grave el sistema pero que pueden llevar a un ataque al combinarse con otras.	En esta clasificación se encuentran las vulnerabilidades de seguridad que suministran información a un atacante pero no genera un riesgo para la integridad o disponibilidad del sistema.

Ilustración 6. Representación Niveles de Criticidad

La ilustración 6 presenta el nivel de riesgo o grado de exposición del sistema; su función es establecer la importancia de las vulnerabilidades identificadas; es un insumo primordial del plan de mitigación que permite gestionar y mitigar las debilidades mediante su priorización.

6. DESCRIPCION GLOBAL DE VULNERABILIDADES

Las pruebas de vulnerabilidades consistieron en determinar problemas de seguridad en la etapa de identificación de Información en los activos escaneados. Estos problemas de seguridad, se pueden determinar usando herramientas especializadas automáticas o de manera manual, ahora bien, estas pruebas se caracterizaron por la presencia de controles de seguridad, que limitaban el escaneo de puertos y de vulnerabilidades constantemente.

6.1. Resultados Generales

La identificación de vulnerabilidades contribuye a la medición del riesgo existente en la infraestructura tecnológica, desde el punto de vista de configuraciones de software implementado, falta de actualización o una configuración errónea de los mismos. A continuación, se muestran los resultados de las vulnerabilidades identificadas:

Riesgo	Vulnerabilidades
BAJO	6
MEDIO	2
ALTO	1
CRITICO	0
TOTAL	9

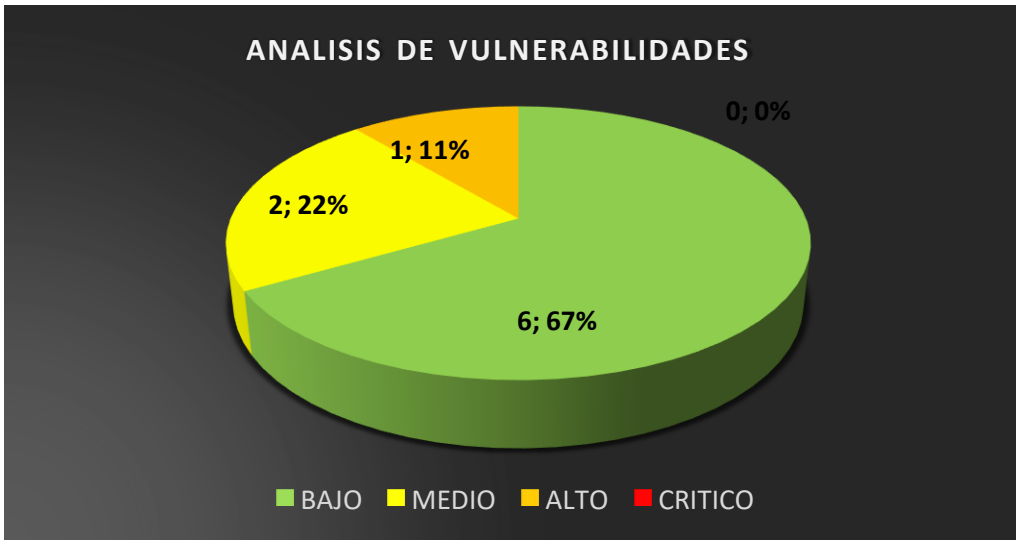


Ilustración 7. Vulnerabilidades Identificadas

Ilustración 7: En el análisis realizado, se identifica una (1) vulnerabilidades con nivel de riesgo alto, dos (2) vulnerabilidades con severidad media, y seis (6) vulnerabilidades con severidad baja.

6.2. Vulnerabilidades identificadas por nivel de riesgo

ID	RIESGO	NOMBRE DE LA VULNERABILIDAD	HOST IP / DOMINIO
1	ALTO	Out-of-date Version (Apache)	latam.pau.zone, api-latam.pau.zone
2	MEDIO	Login page password-guessing attack	api-latam.pau.zone
3	MEDIO	Inactive session time greater than 1 hour	latam.pau.zone
4	BAJO	Cookie without Secure flag set	latam.pau.zone
5	BAJO	Cookie without HttpOnly flag set	latam.pau.zone
6	BAJO	HSTS Missing From HTTPS Server (RFC 6797)	latam.pau.zone
7	BAJO	Content Security Policy (CSP) not implemented	latam.pau.zone
8	BAJO	Version Disclosure (Apache)	latam.pau.zone, api-latam.pau.zone
9	BAJO	Autocomplete Enabled	latam.pau.zone

Ilustración 8. Vulnerabilidades encontradas

Remitir al documento anexo "Matriz Análisis de Vulnerabilidades Silice LATAM_PAU externa agosto de 2023" para más información de las vulnerabilidades identificadas.

6.3. Vulnerabilidades por activo (Dominio/ IP /HOST)

A continuación, se entrega el detalle de la cantidad de vulnerabilidades por cada uno de los activos, esto nos ayuda a tomar decisiones y priorizar el plan de acción y remediación.

Vulnerabilidades por Activo						
No.	**IP / Dominio**	**Critico**	**Alto**	**Medio**	**Bajo**	**Total**
1	latam.pau.zone	0	1	1	6	8
2	api-latam.pau.zone	0	1	1	1	3

Ilustración 9. Vulnerabilidades encontradas por activo

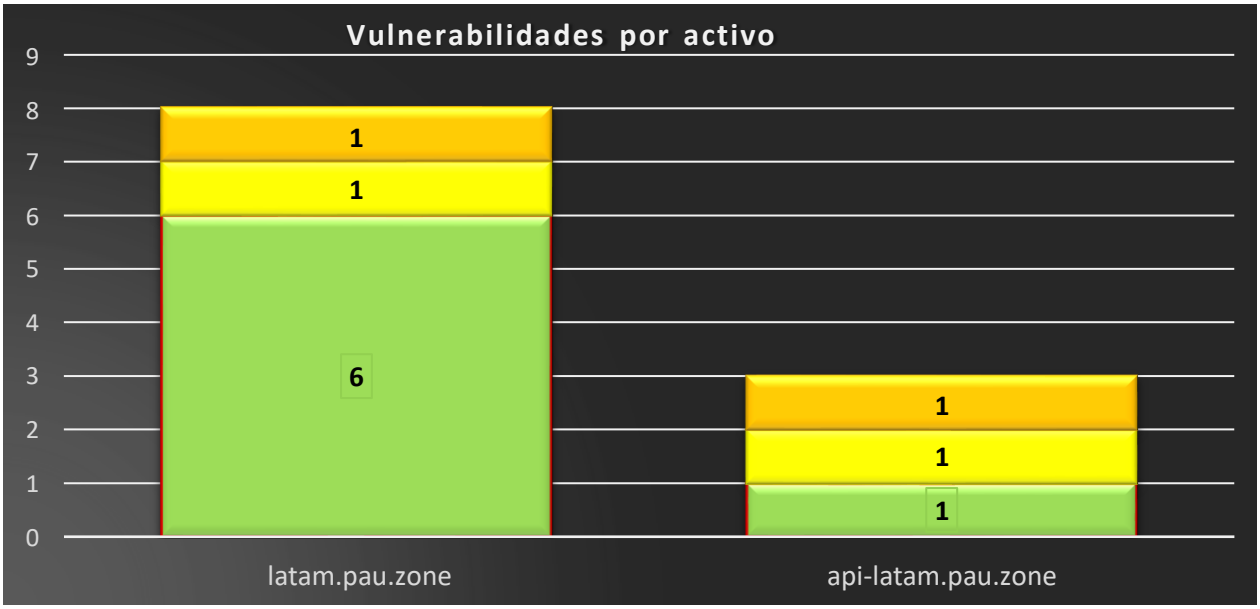


Ilustración 10. Diagrama de barras – Vulnerabilidades encontradas por activo

8. RECOMENDACIONES GENERALES

A continuación, se presentan las recomendaciones generales que ayudaran a mitigar el nivel de riesgo al cual se encuentra expuesto los objetivos evaluados para **SILICE:**

- Corregir los hallazgos de riesgo alto identificados durante la ejecución de las pruebas.
- Actualizar las tecnologías desactualizadas que contienen vulnerabilidades conocidas.
- Aplicar controles anti-repeticiones automáticas en las api, evitando ataques automatizados de credenciales y otros.
- Mantener portales de administración filtrados, evitando su acceso desde cualquier ubicación en internet, esto mediante listas de acceso o métodos de autenticación basados en segundo factor de autenticación.
- Realizar auditorías de seguridad en caso de que la plataforma tecnológica se actualice o sufra un cambio importante con el fin de descartar problemas de seguridad que se puedan presentar por estos procesos.
- Seguir las recomendaciones que se presentan en los apartados anteriores con el fin de corregir las diferentes vulnerabilidades identificadas en los dispositivos evaluados.

9. CONCLUSIONES

El estudio realizado sobre la plataforma tecnológica de **SILICE**, muestra aspectos o puntos de mejora, que pueden ser ajustados mediante un plan de remediación, en el cual se incluyan actualizaciones, configuraciones de acuerdo con las necesidades y requerimientos de seguridad de la información, para el adecuado funcionamiento de las operaciones y el negocio en general.

De acuerdo a lo anterior las vulnerabilidades identificadas, se clasifican en su nivel de riesgo según el CVE (Common Vulnerabilities and Exposures) vulnerabilidades y exposiciones, las cuales se encuentran en la base de datos internacional (NVD) y un marco de estimación estadístico mundial. Con lo anterior se define el nivel de criticidad sobre un marco específico para **SILICE**, que pretende alertar y mostrar de ser necesario el impacto sobre el uso de este tipo de servicios, los cuales muchas veces son evaluados sin la adecuada atención en la gestión de seguridad informática, pero que sin duda y basado en las estadísticas de ataques a nivel mundial, constituyen una amenaza frente a la probabilidad de ataques de diferente tipo.

PLATAFORMA SILICE	
CRITICO	
ALTO	
MEDIO	X
BAJO	

Ilustración 11. Resultado General

La Ilustración 11 muestra el resultado general de la evaluación realizada sobre la plataforma tecnológica de **SILICE**, de acuerdo con la metodología utilizada para el análisis de riesgo y su aplicación dentro del escenario evaluado.

En nivel de riesgo de la infraestructura evaluada se cataloga como MEDIO, esto debido a los hallazgos explotables identificados.

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	899999115-8	ETB S.A ESP		CRA 8 No 20 00	2426094	alexander.felicianoc@etb.com.co	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		
SUCURSAL	A – Más de 200 cot	PRINCIPAL	PPAL	BOGOTÁ D. C.	BOGOTÁ, D.C.		SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					2108	66
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2024-10	2024-09	E		80557650	$4.843.462.200	

TOTALES POR SUBSISTEMAS

TOTALES SALUD

Código EPS	Nombre	NIT	Cotización Obligatoria	UPC Adicional	Incapacidades		Licencia Maternidad		Días Mora	Valor Mora Cotización	Valor Mora UPC	Total a Pagar	No. Afiliados
					No. Autorización	Valor	No. Autorización	Valor					
EPS001	ALIANSALUD EPS S.A.	830113831-0	68.227.700	0		0		0	0	0	0	68.227.700	48
EPS002	Salud Total EPS	800130907-4	19.079.700	0		0		0	0	0	0	19.079.700	40
EPS005	Sanitas EPS	800251440-6	418.505.700	0		0		0	0	0	0	418.505.700	410
EPS008	Compensar EPS	860066942-7	319.448.500	34.915.500		0		0	0	0	0	354.364.000	547
EPS010	EPS Sura	800088702-2	79.017.100	0		0		0	0	0	0	79.017.100	77
EPS017	Famisanar EPS	830003564-7	61.650.300	0		0		0	0	0	0	61.650.300	118
EPS037	Nueva EPS	900156264-2	241.102.700	0		0		0	0	0	0	241.102.700	913
EPS041	NUEVA E.P.S. S.A. MOV	900156264-2	325.000	0		0		0	0	0	0	325.000	2
EPS042	EPS COOSALUD	900226715-3	78.900	0		0		0	0	0	0	78.900	1
EPSC34	Recaudo SGP Capital Salud	900298372-9	1.300.000	0		0		0	0	0	0	1.300.000	8
ESSC24	EPS-S Coosalud	900226715-3	162.500	0		0		0	0	0	0	162.500	1
MIN001	Fondo Sol y Gar Min Salud	901037916-1	4.601.700	0		0		0	0	0	0	4.601.700	4
MIN002	MIN002 Fondo Sol y Gar Min Salud	901037916-1	7.206.200	0		0		0	0	0	0	7.206.200	5

TOTALES PENSIÓN

Código AFP	Nombre	NIT	Cotización Obligatoria	Aporte Voluntario Afiliado	Aporte Voluntario Aportante	Aporte FSP - Solidaridad	Aporte FSP - Subsistencia	Días Mora	Valor Mora Cotización	Valor Mora FSP	Total a Pagar	No. Afiliados
230201	Proteccion (ING + Proteccion)	800229739-0	162.858.200	0	0	4.413.600	5.037.800	0	0		172.309.600	125
230301	Porvenir	800224808-8	178.237.000	0	0	4.566.900	5.257.600	0	0		188.061.500	147
230901	Skandia Pensiones Obligatorias	800253055-2	99.537.400	500.000	0	3.069.000	4.615.000	0	0		107.721.400	43
231001	Colfondos	800227940-6	213.324.400	0	0	6.186.900	6.576.000	0	0		226.087.300	142
25-14	Colpensiones	900336004-7	1.695.241.600	0	0	39.074.400	43.014.000	0	0		1.777.330.000	1546

TOTALES RIESGOS LABORALES

Código ARL	Nombre	NIT	Cotización Obligatoria	Incapacidades		Aportes Otros Sistemas	Valor Neto Cotización	Días Mora	Valor Mora Cotización	Subtotal Cotización	No. Radicado Saldo a Favor	Valor Saldo a Favor	Fondo Solidaridad	Total a Pagar	No. Afiliados
				No. Autorización	Valor										
14-23	Positiva Seguros	860011153-6	164.936.700				164.936.700	0	0	164.936.700			1.649.367	164.936.700	2067

TOTALES CAJAS

Código CCF	Nombre	NIT	Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
CCF03	Comfenalco Antioquia	890900842-6	2.999.800	0	0	2.999.800	8
CCF06	Combarranquilla	890102002-2	1.181.200	0	0	1.181.200	4
CCF21	Cafam	860013570-3	571.003.900	0	0	571.003.900	1962

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

compensar | miplanilla.com

PLANILLA INTEGRADA DE AUTOLIQUIDACION DE APORTES

DATOS DEL APORTANTE						
TIPO	NÚMERO	NOMBRE APORTANTE		DIRECCIÓN	TELÉFONO	CORREO	EXONERADO PAGO PARAFISCALES Y SALUD
NI	899999115-8	ETB S.A ESP		CRA 8 No 20 00	2426094	alexander.felicianoc@etb.com.co	
FORMA PRESENTACIÓN	CLASE APORTANTE	NOMBRE SUCURSAL	CÓDIGO	DEPARTAMENTO	CIUDAD / MUNICIPIO		
SUCURSAL	A – Más de 200 cot	PRINCIPAL	PPAL	BOGOTÁ D. C.	BOGOTÁ, D.C.		SI

DATOS DE LA PLANILLA						
PLANILLA ASOCIADA	FECHA PAGO ASOCIADA (DIA/MES/AÑO)	TIPO PLANILLA	FECHA PAGO (DIA/MES/AÑO)	NÚMERO PLANILLA	CANTIDAD	
					EMPLEADOS	UPC
					2108	66
PERIODO SALUD	PERIODO PENSIONES				TOTAL A PAGAR	
2024-10	2024-09	E		80557650	$4.843.462.200	

CCF34	Cofrem	892000146-3	2.696.300	0	0	2.696.300	7
CCF35	Caja Fliar Nariño	891280008-1	484.300	0	0	484.300	1
CCF36	Comfaoriente	890500675-6	1.516.100	0	0	1.516.100	14
CCF40	Comfenalco Santander	890201578-7	1.685.400	0	0	1.685.400	4
CCF44	Comfamiliar Risaralda	891480000-1	915.500	0	0	915.500	2
CCF50	Comfenalco	890700148-4	1.015.100	0	0	1.015.100	2
CCF56	Comfenalco Valle	890303093-5	796.400	0	0	796.400	3

TOTALES PARAFISCALES				
Valor Aporte	Días Mora	Valor Mora Aporte	Total a Pagar	No. Afiliados
SENA				
146.845.000	0	0	146.845.000	512
ICBF				
220.255.200	0	0	220.255.200	512
ESAP				
MEN				

TOTALES POR SUBSISTEMA			
Tipo Administradora	No. Administradoras Reportadas	Valor antes de IGE, LMA, IRP y Mora	Total a Pagar
Salud	13	1.255.621.500	1.255.621.500
Pensión	5	2.471.509.800	2.471.509.800
Riesgos Laborales	1	164.936.700	164.936.700
CCF	10	584.294.000	584.294.000
ESAP	0	0	0
ICBF	1	220.255.200	220.255.200
MEN	0	0	0
SENA	1	146.845.000	146.845.000
TOTALES	31	4.843.462.200	4.843.462.200

PAGADO 958790106

Este documento está clasificado como PRIVADO por parte de Compensar Operador de Información

UNIDAD ADMINISTRATIVA ESPECIAL **JUNTA CENTRAL DE CONTADORES**

Certificado No:

7 5 3 6 E 4 8 5 0 0 A 7 8 4 8 A

LA REPUBLICA DE COLOMBIA

MINISTERIO DE COMERCIO, INDUSTRIA Y TURISMO

UNIDAD ADMINISTRATIVA ESPECIAL

JUNTA CENTRAL DE CONTADORES

CERTIFICA A:
QUIEN INTERESE

Que el contador público **ALEJANDRO PERDOMO CORDOBA** identificado con CÉDULA DE CIUDADANÍA No 80201300 de BOGOTA, D.C. (BOGOTA D.C) Y Tarjeta Profesional No 124911-T SI tiene vigente su inscripción en la Junta Central de Contadores y desde la fecha de Inscripción.

NO REGISTRA ANTECEDENTES DISCIPLINARIOS * * *

Deloitte & Touche S.A.S.
Nit. 860.005.813-4
Carrera 9 No. 78-31 Piso 1
Bogotá, D.C.
Colombia

Tel: +57 (601) 426 2000
www.deloitte.com/co

El Suscrito Revisor Fiscal Principal de
Empresa de Telecomunicaciones de Bogotá S.A. E.S.P.
NIT 899.999.115-8

CONSIDERANDO QUE:

1. De conformidad con el artículo 2 de la Ley 43 de 1990, demás previsiones legales y pronunciamientos jurisprudenciales existentes en la materia, la Revisoría Fiscal es una actividad relacionada con la ciencia contable ejercida por un Contador Público quien lleva a cabo sus funciones con fundamento en las normas, principios y procedimientos propios de dicha profesión; dentro de las cuales se encuentra la función de certificación que tiene carácter de prueba cuando se expide con fundamento en los libros de contabilidad y en el sistema contable de la compañía.

2. La Administración de la Compañía es responsable por la correcta preparación de los registros contables, los cuales se deben realizar con fundamento en el marco técnico normativo aplicable en Colombia en materia de información contable y financiera.

3. A la fecha se encuentra en curso mi examen sobre los estados financieros de la compañía por el año que terminará al 31 de diciembre de 2024.

4. Para efectos de la expedición de la presente certificación he obtenido la información que he considerado necesaria y he realizado los siguientes procedimientos:

   - Cruce de los saldos de los auxiliares contables de las cuentas: 24150181 - Aportes de Pensión, 24150191 - Aportes de Salud, 24150201 - Aportes ICBF y Sena, 24150321 - Aportes ARL y 25112401 - Aportes Caja del mes de septiembre de 2024 contra las planillas PILA de mismo corte.

   - Verificación de los pagos de las planillas PILA que se relacionan a continuación, de acuerdo con las fechas establecidas por el Decreto 923 del 31 de mayo de 2017.

Planillas empleados activos	
No. de planilla	Fecha de pago
80557650	04/10/2024

Planilla empleados pensionados	
No. De planilla	Fecha de pago
80547222	04/10/2024

De acuerdo con las anteriores consideraciones a continuación expedimos la certificación solicitada por Empresa de Telecomunicaciones de Bogotá S.A. E.S.P.

Deloitte se refiere a una o más entidades de Deloitte Touche Tohmatsu Limited ("DTTL"), su red global de firmas miembro y sus sociedades afiliadas a una firma miembro (en adelante "Entidades Relacionadas") (colectivamente, la "organización Deloitte"). DTTL (también denominada como "Deloitte Global") así como cada una de sus firmas miembro y sus Entidades Relacionadas son entidades legalmente separadas e independientes, que no pueden obligarse ni vincularse entre sí con respecto a terceros. DTTL y cada firma miembro de DTTL y su Entidad Relacionada es responsable únicamente de sus propios actos y omisiones, y no de los de las demás. DTTL no provee servicios a clientes. Consulte www.deloitte.com/co/conozcanos para obtener más información.

Deloitte.

CERTIFICA QUE:
(Cifras Expresadas en Pesos Colombianos)

De acuerdo con registros contables, los soportes de pago y demás documentos soporte suministrados por Empresa de Telecomunicaciones de Bogotá S.A. E.S.P., la Compañía ha realizado el pago por concepto de aportes al Sistema de Seguridad en salud para el mes de octubre de 2024; así como, los aportes a las Cajas de Compensación Familiar, riesgos profesionales, pensiones, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje correspondiente al mes de septiembre de 2024 mediante las planillas integradas de liquidación que se relacionan a continuación:

Planilla	No. de Planilla	Periodo Pensiones, ARL y Parafiscales	Periodo salud	Fecha de pago	Valor causado	Valor pagado
Planilla activos	80557650	2024-09	2024-10	04/10/2024	$4.843.462.200	$4.863.462.200
Planilla pensionados	80547222	2024-09	2024-10	04/10/2024	$11.453.200	$11.453.200

Sin perjuicio de las limitaciones establecidas por las normas legales y contables para el ejercicio de la Revisoría Fiscal, el alcance de mi trabajo en lo que se refiere a lo certificado se limita únicamente al cruce de información contable contra los soportes de pago de las Plantillas PILA que me ha suministrado la Compañía.

Se expide en Bogotá D.C. a los cuatro (04) días del mes de octubre de 2024, por solicitud de la Administración de Empresa de Telecomunicaciones de Bogotá S.A. E.S.P. en cumplimiento de lo establecido por las leyes 789 de 2002 y 828 de 2003.

Alejandro Perdomo Córdoba
Revisor Fiscal Principal
Tarjeta Profesional No. 124911-T
Designado por Deloitte & Touche S.A.S.

DOCUMENTATION VERIFIED

Deloitte & Touche S.A.S.
Nit. 860.005.813-4
Carrera 9 No. 78-31 Piso 1
Bogotá, D.C.
Colombia

Tel: +57 (601) 426 2000
www.deloitte.com/co

El Suscrito Revisor Fiscal Principal de
Empresa de Telecomunicaciones de Bogotá S.A. E.S.P.
NIT 899.999.115-8

CONSIDERANDO QUE:

1. De conformidad con el artículo 2 de la Ley 43 de 1990, demás previsiones legales y pronunciamientos jurisprudenciales existentes en la materia, la Revisoría Fiscal es una actividad relacionada con la ciencia contable ejercida por un Contador Público quien lleva a cabo sus funciones con fundamento en las normas, principios y procedimientos propios de dicha profesión; dentro de las cuales se encuentra la función de certificación que tiene carácter de prueba cuando se expide con fundamento en los libros de contabilidad y en el sistema contable de la compañía.

2. La Administración de la Compañía es responsable por la correcta preparación de los registros contables, los cuales se deben realizar con fundamento en el marco técnico normativo aplicable en Colombia en materia de información contable y financiera.

3. A la fecha se encuentra en curso mi examen sobre los estados financieros de la compañía por el año que terminará al 31 de diciembre de 2024.

4. Para efectos de la expedición de la presente certificación he obtenido la información que he considerado necesaria y he realizado los siguientes procedimientos:

   - Cruce de los saldos de los auxiliares contables de las cuentas: 24150181 - Aportes de Pensión, 24150191 - Aportes de Salud, 24150201 - Aportes ICBF y Sena, 24150321 - Aportes ARL y 25112401 - Aportes Caja desde el mes de abril de 2024 al mes de septiembre de 2024 contra las planillas PILA de los mismos cortes.

   - Verificación de los pago de las planillas PILA que se relacionan a continuación, de acuerdo con las fechas establecidas por el Decreto 923 del 31 de mayo de 2017.

Planillas empleados activos	
No. de planilla	Fecha de pago
76597841	03/05/2024
77384334	06/06/2024
78207567	05/07/2024
78937651	05/08/2024
79697516	05/09/2024
80557650	04/10/2024

Planilla empleados pensionados	
No. De planilla	Fecha de pago
76577342	03/05/2024
77376402	06/06/2024
78191760	05/07/2024
78935736	05/08/2024
79697237	05/09/2024
80547222	04/10/2024

De acuerdo con las anteriores consideraciones a continuación expedimos la certificación solicitada por Empresa de Telecomunicaciones de Bogotá S.A. E.S.P.

Deloitte se refiere a una o más entidades de Deloitte Touche Tohmatsu Limited ("DTTL"), su red global de firmas miembro y sus sociedades afiliadas a una firma miembro (en adelante "Entidades Relacionadas") (colectivamente, la "organización Deloitte"). DTTL (también denominada como "Deloitte Global") así como cada una de sus firmas miembro y sus Entidades Relacionadas son entidades legalmente separadas e independientes, que no pueden obligarse ni vincularse entre sí con respecto a terceros. DTTL y cada firma miembro de DTTL y su Entidad Relacionada es responsable únicamente de sus propios actos y omisiones, y no de los de las demás. DTTL no provee servicios a clientes. Consulte www.deloitte.com/co/conozcanos para obtener más información.

Deloitte.

CERTIFICA QUE:
(Cifras Expresadas en Pesos Colombianos)

De acuerdo con registros contables, los soportes de pago y demás documentos soporte suministrados por Empresa de Telecomunicaciones de Bogotá S.A. E.S.P., la Compañía ha realizado el pago por concepto de aportes al Sistema de Seguridad en salud correspondientes a los meses comprendidos de mayo de 2024 a octubre de 2024; así como, los aportes a las Cajas de Compensación Familiar, riesgos profesionales, pensiones, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje correspondiente a los meses comprendidos desde abril de 2024 a septiembre de 2024 mediante las planillas integradas de liquidación que se relacionan a continuación:

Planilla	No. de Planilla	Periodo Pensiones, ARL y Parafiscales	Periodo salud	Fecha de pago	Valor causado	Valor pagado
Planilla activos	76597841	2024-04	2024-05	03/05/2024	5.555.660.100	5.555.660.100
Planilla pensionados	76577342	2024-04	2024-05	03/05/2024	11.453.200	11.453.200
Planilla activos	77384334	2024-05	2024-06	06/06/2024	4.963.264.100	4.963.264.100
Planilla pensionados	77376402	2024-05	2024-06	06/06/2024	11.453.200	11.453.200
Planilla activos	78207567	2024-06	2024-07	05/07/2024	7.742.849.500	7.742.849.500
Planilla pensionados	78191760	2024-06	2024-07	05/07/2024	11.453.200	11.453.200
Planilla activos	78937651	2024-07	2024-08	05/08/2024	4.916.288.100	4.916.288.100
Planilla pensionados	78935736	2024-07	2024-08	05/08/2024	11.453.200	11.453.200
Planilla activos	79697516	2024-08	2024-09	05/09/2024	$4.703.710.600	$4.703.710.600
Planilla pensionados	79697237	2024-08	2024-09	05/09/2024	$11.453.200	$11.453.200
Planilla activos	80557650	2024-09	2024-10	04/10/2024	$4.843.462.200	$4.863.462.200
Planilla pensionados	80547222	2024-09	2024-10	04/10/2024	$11.453.200	$11.453.200

Sin perjuicio de las limitaciones establecidas por las normas legales y contables para el ejercicio de la Revisoría Fiscal, el alcance de mi trabajo en lo que se refiere a lo certificado se limita únicamente al cruce de información contable contra los soportes de pago de las Plantillas PILA que me ha suministrado la Compañía.

Se expide en Bogotá D.C. a los cuatro (04) días del mes de octubre de 2024, por solicitud de la Administración de Empresa de Telecomunicaciones de Bogotá S.A. E.S.P. en cumplimiento de lo establecido por las leyes 789 de 2002 y 828 de 2003.

Alejandro Perdomo Córdoba
Revisor Fiscal Principal
Tarjeta Profesional No. 124911-T
Designado por Deloitte & Touche S.A.S.

Informe de Monitoreo
Chatico

Septiembre 2024

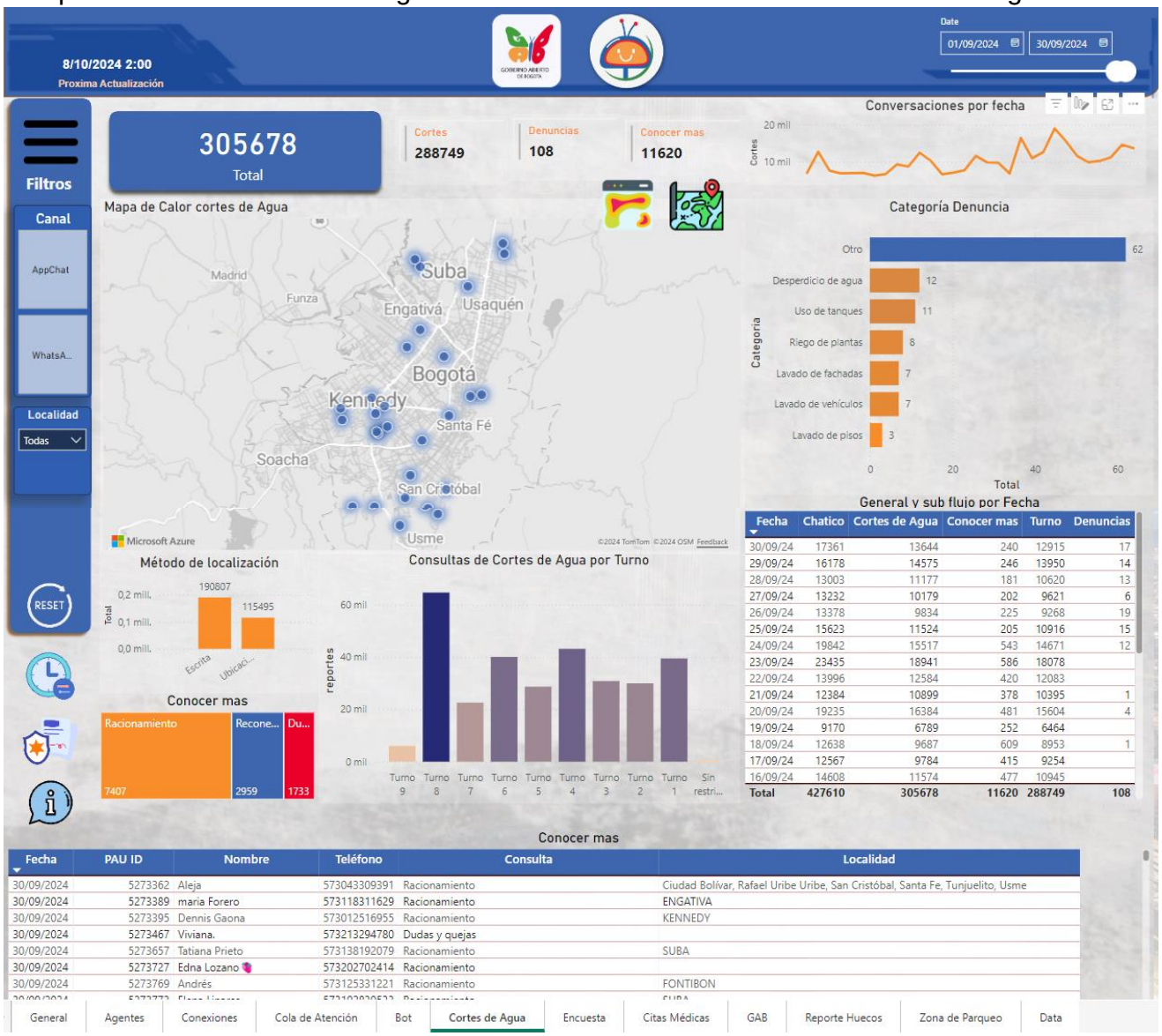
Gobierno Abierto de Bogotá

Comportamiento Agente Virtual Chatico
Septiembre 2024

El presente informe de agende virtual Chatico corresponde al mes de Septiembre, con corte al día 30 se Septiembre. Este servicio digital tiene como objetivo comunicar ágilmente diferentes temas relacionados con la ciudad, información sobre trámites y que son de interés general, para este mes de Septiembre mostraremos los resultados del comportamiento en relación con los diferentes flujos que actualmente se manejan y elcomportamiento general de la plataforma.

- **Continuación Flujo de Agua**

En razón a la coyuntura sobre desabastecimiento de los embalses de Bogotá, el flujo de agua permanece durante el mes de Septiembre, las funcionalidades de este flujo son con el propósito de informar a los habitantes de la ciudad sobre las medidas para mitigar la contingencia.



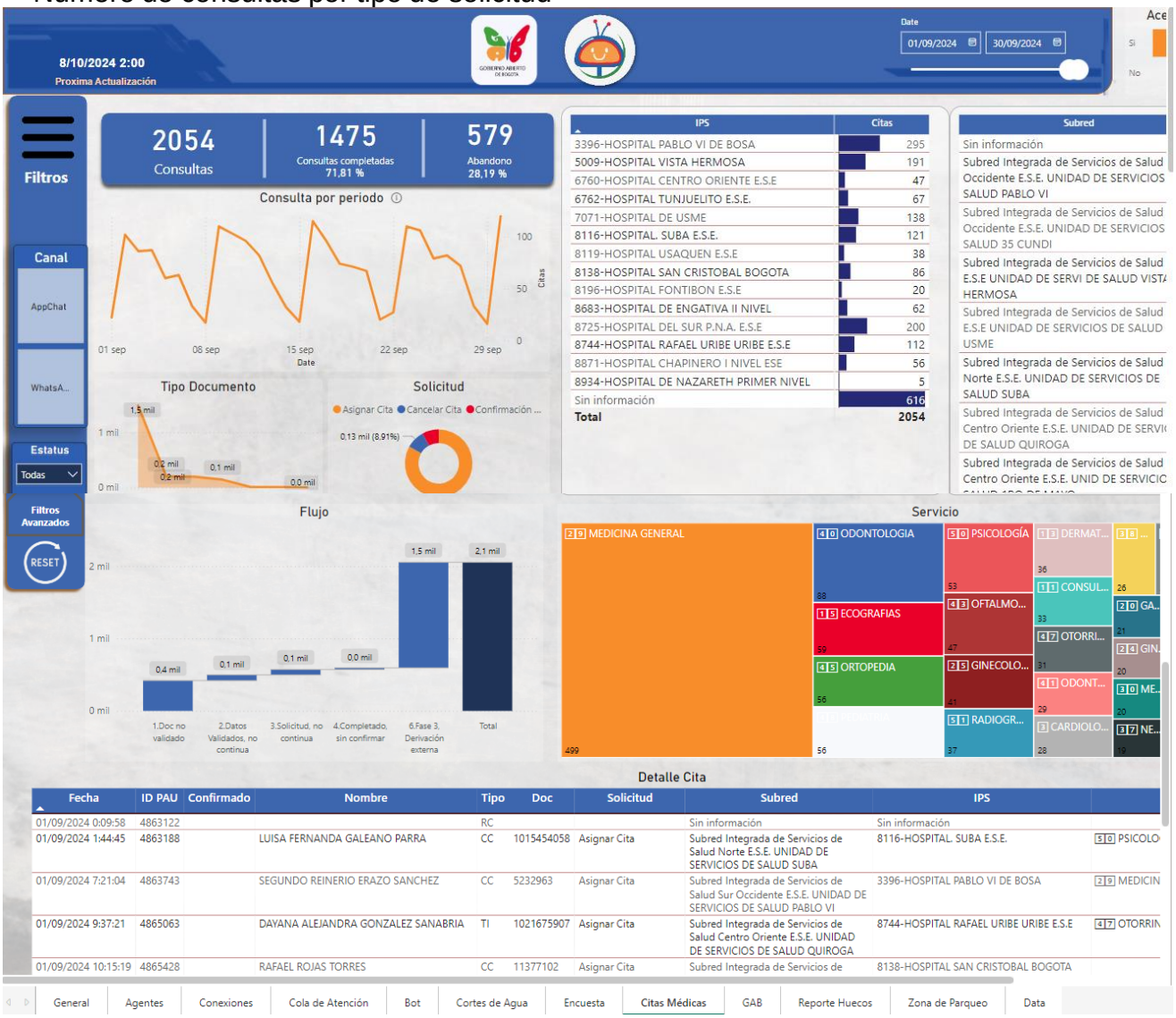
Fecha	Chatico	Cortes de Agua	Conocer mas	Turno	Denuncias
30/09/24	17361	13644	240	12915	17
29/09/24	16178	14575	246	13950	14
28/09/24	13003	11177	181	10620	13
27/09/24	13232	10179	202	9621	6
26/09/24	13378	9834	225	9268	19
25/09/24	15623	11524	205	10916	15
24/09/24	19842	15517	543	14671	12
23/09/24	23435	18941	586	18078	
22/09/24	13996	12584	420	12083	
21/09/24	12384	10899	378	10395	1
20/09/24	19235	16384	481	15604	4
19/09/24	9170	6789	252	6464	
18/09/24	12638	9687	609	8953	1
17/09/24	12567	9784	415	9254	
16/09/24	14608	11574	477	10945	
Total	**427610**	**305678**	**11620**	**288749**	**108**

Fecha	PAU ID	Nombre	Teléfono	Consulta	Localidad
30/09/2024	5273362	Aleja	573043309391	Racionamiento	Ciudad Bolívar, Rafael Uribe Uribe, San Cristóbal, Santa Fe, Tunjuelito, Usme
30/09/2024	5273389	maria Forero	573118311629	Racionamiento	ENGATIVA
30/09/2024	5273395	Dennis Gaona	573012516955	Racionamiento	KENNEDY
30/09/2024	5273467	Viviana.	573213294780	Dudas y quejas	
30/09/2024	5273657	Tatiana Prieto	573138192079	Racionamiento	SUBA
30/09/2024	5273727	Edna Lozano	573202702414	Racionamiento	
30/09/2024	5273769	Andrés	573125331221	Racionamiento	FONTIBON

- **Flujo Citas Médicas**

A continuación, se muestra en gráficos datos del flujo de salud – Citas Médicas en donde se contempla la siguiente información:

• Total, de consultas para citas médicas
• Flujo de citas médicas completado
• Flujo de citas médicas no completado.
• Número de consultas por IPS o Número de consultas por Subred
• Número de consultas por tipo de solicitud



Fuente: Tablero de control ETBPAU (proveedor Chatico). Fecha consultada del 01 al 30 de Septiembre del 2024

- **Atención de Agentes Humanos.**

A continuación, comportamiento de atención de agentes detallados en la siguiente gráfica:



Fuente: Tablero de control ETBPAU (proveedor Chatico). Fecha consultada del 01 al 30 de Septiembre del 2024

Cifras de Comportamiento General
Periodo 1 al 30 de Septiembre
Interacciones de Chatico



De A	do.	lu.	ma.	mi.	ju.	vi.
00:00-01:00	365	433	284	288	274	236
01:00-02:00	207	210	146	122	171	129
02:00-03:00	147	151	91	105	88	108
03:00-04:00	123	213	149	153	125	119
04:00-05:00	206	863	598	534	515	422
05:00-06:00	410	2921	1910	1789	1519	1162
06:00-07:00	1518	4888	3175	2949	2527	2135
07:00-08:00	2600	5084	3927	3882	3396	3145
08:00-09:00	3288	6244	3855	3779	3194	3034
09:00-10:00	3423	7	8789	9038	3044	7650
10:00-11:00	3152	7	3288	4256	9239	12959
11:00-12:00	2913	4987	2863	3608	3	3166
12:00-13:00	3044	4789	2902	7	3702	3677
13:00-14:00	3501	4877	2971	3493	2468	3134
14:00-15:00	2582	3987	2607	2603	2251	2749
15:00-16:00	2409	3843	2518	2422	2053	2976
16:00-17:00	2427	4019	2619	2406	2169	2856
17:00-18:00	2769	3925	2632	2608	2243	2677
18:00-19:00	3419	4283	3004	2939	2504	2970
19:00-20:00	3639	7	3516	3554	2870	3813
20:00-21:00	3014	4628	3471	3635	2669	2967
21:00-22:00	3212	3584	3627	3901	1020	2268

PAU ID	Fecha Inicio	Fecha Fin	Cliente	Teléfono	Asunto
5290720	30/09/2024 23:58:56	01/10/2024 0:31:22	Juan Pablo García H	573132193383	Cortes agua
5290719	30/09/2024 23:58:31	30/09/2024 23:59:43	Gloria	573132075390	Cortes agua
5290718	30/09/2024 23:58:21	01/10/2024 0:31:21	De La Mano Con Dios	573043605160	Cortes agua
5290717	30/09/2024 23:57:42	30/09/2024 23:59:40	D Y	573115491885	Cortes agua
5290716	30/09/2024 23:57:16	01/10/2024 0:29:22	cococo	573127478329	Cortes agua
5290715	30/09/2024 23:56:47	01/10/2024 0:29:22	Vivi	573222291051	Educación en Bogotá
5290714	30/09/2024 23:56:36	01/10/2024 0:29:22	Canas	573138935289	Cortes agua
5290713	30/09/2024 23:56:24	30/09/2024 23:58:13	Isabella	573108630940	Cortes agua
5290712	30/09/2024 23:55:57	01/10/2024 0:28:22		573133507668	Cortes agua
5290711	30/09/2024 23:55:51	01/10/2024 0:28:21	Ginita	573117075620	Movilidad
5290710	30/09/2024 23:55:08	01/10/2024 0:27:21	Martha Yate	573012091218	Apertura y Abandono
5290709	30/09/2024 23:55:00	01/10/2024 0:26:21	Yenny Nova	573103933356	Apertura y Abandono

Fuente: Tablero de control ETBPAU (proveedor Chatico). Fecha consultada del 1 al 30 de Septiembre del 2024

Durante el periodo del 1 al 30 del mes de Septiembre, se tuvieron en total 427.610 conversaciones, las cuales, se discriminan de la siguiente manera:

Mes	WhatsApp	Web	TOTAL	% WAPP	% WEB
Sep-24	412985	14.625	427.610	96,6%	3,4%

Historial Interacciones Chatico Julio 2022 / Septiembre 2024

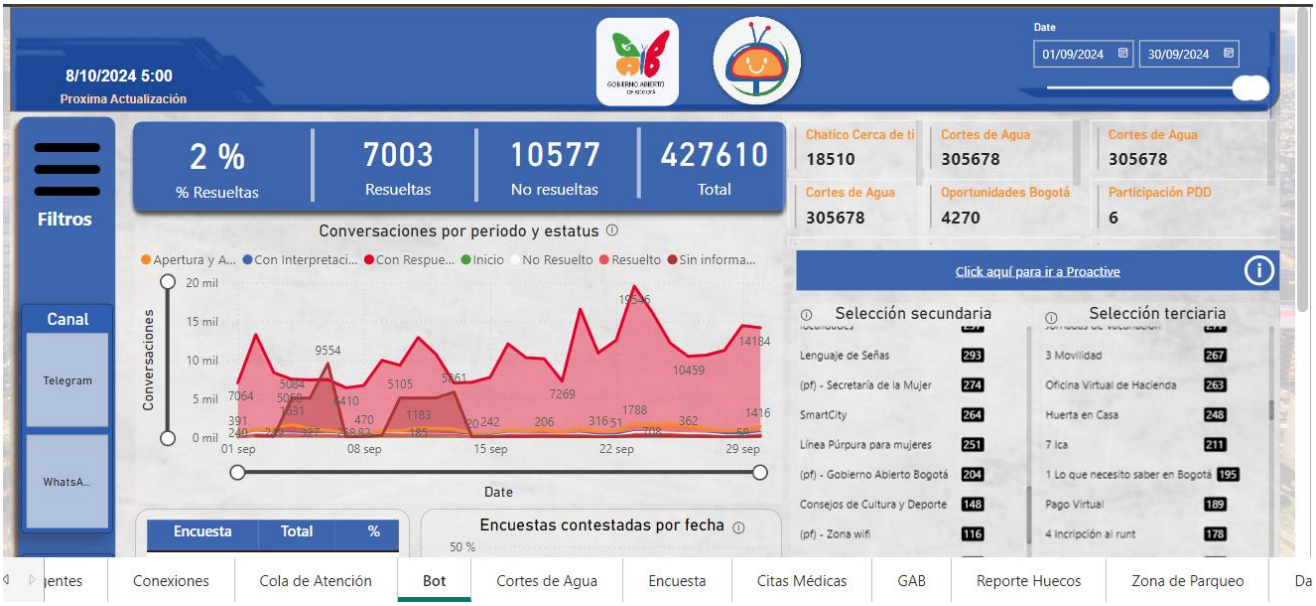
A continuación, historial de interacciones chatico Durante los meses de julio 2022 a Septiembre de 2024.

Mes	WhatsApp	Web	TOTAL	% WAPP	% WEB
jul-22	33	1.483	1.516	2,2%	97,8%
ago-22	1.323	2.725	4.048	32,7%	67,3%
sep-22	25.133	11.956	37.089	67,8%	32,2%
oct-22	164.995	19.348	184.343	89,5%	10,5%
nov-22	2.645	11.097	13.742	19,2%	80,8%
dic-22	15.743	11.227	26.970	58,4%	41,6%
ene-23	75.974	20.114	96.088	79,1%	20,9%
feb-23	54.325	16.292	70.617	76,9%	23,1%
mar-23	54.032	14.808	68.840	78,5%	21,5%
abr-23	45.580	11.574	57.154	79,7%	20,3%
may-23	7.522	24.553	32.075	23,5%	76,5%
jun-23	12.973	56.320	69.293	18,7%	81,3%
jul-23	10.772	49.666	60.438	17,8%	82,2%
ago-23	27.035	16.067	43.102	62,7%	37,3%
sep-23	31.839	10.175	42.014	75,8%	24,2%
oct-23	36.026	9.841	45.867	78,5%	21,5%
nov-23	202.724	10.065	212.789	95,3%	4,7%
dic-23	24.024	6.654	30.678	78,3%	21,7%
ene-24	33.226	14.463	47.689	69,7%	30,3%
feb-24	38.718	17.798	56.516	68,5%	31,5%
mar-24	85.011	12.481	97.492	87,2%	12,8%
abr-24	698.473	26.338	724.811	96,4%	3,6%
may-24	396.372	12.996	409.368	96,8%	3,2%
jun-24	443.681	13.586	457.267	97,0%	3,0%
Julio-24	319.719	15.305	335.024	95.4%	4,6%
Ago-24	303.126	14.699	317.825	95,4%	4,6%
Sep-24	412985	14.625	427.610	96,6%	3,4%

Mensajes Proactivos

En el mes de septiembre se enviaron 40,455 mensajes proactivos de devolución de Plan Distrital de Desarrollo.

Las métricas de los mensajes proactivos se incluyeron en la venta Bot del BI para identificar la cantidad de usuarios que interactuaron a través del mensaje.



Bogotá D. C, 01 de Octubre de 2024

Señores:
Consejería Distrital TIC
JUAN CARLOS PARADA GALLARDO
CONTRATO 4200000-807-2024
SECRETARIA GENERAL ALCALDÍA MAYOR DE BOGOTÁ

Asunto: DOCUMENTACIÓN PRUEBAS DE SEGURIDAD

En el marco del contrato interadministrativo 4200000-807-2024 entre la Secretaría General de la Alcaldía Mayor de Bogotá y ETB, se relacionan los siguientes documentos que corresponden a las pruebas realizadas y dan garantía de seguridad según lo establecido en el Anexo técnico.

- 07.Informe Ejecutivo Ethical Hacking SILICE LATAM_PAU
- 07. Informe Ejecutivo Retest de vulnerabilidades RETEST SILICE LATAM_PAU 2024 V1.1-
- 07.SIL.IT.POL.05-002 - Estructura de Normativa de Seguridad de la Información_signed

Los archivos mencionados se encuentran en la carpeta **07. Documento pruebas de seguridad- Pago 02**

Cordialmente.



Miguel Rodriguez Pestana
Ingeniero posventa ETB
Móvil: 3057408673

Estructura de Normativa de Seguridad de la Información

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

Registro de cambios

Fecha	Autor	Versión	Referencia de cambio
28/06/2022	Jeannine D'Enjoy	1.0	Versión inicial
21/09/2023	Fabian Camargo	1.1	1-Se adiciona al numeral 4.2 - Codificación, el tipo de documento Anexo (ANX). 2-Se incluyen los responsables de aprobar los documentos. 3-Se hace revisión general del documento y ajustes de forma.

Revisores

Fecha	Autor	Versión Revisada	Referencia de cambio
28/06/2022	Jeannine D'Enjoy	1.0	
25/09/2023	Jeannine D'Enjoy	1.1	

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

Hoja de firmas y revisiones



Jeannine D'Enjoy
Director de Operaciones y Continuidad del servicio

Fabián Camargo S.

Fabian Camargo
Chief Information Security Officer

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

ÍNDICE

1. OBJETIVO ***4***

2. ÁMBITO DE APLICACIÓN ***4***

3. DOCUMENTOS RELACIONADOS ***5***

4. DESARROLLO ***5***

4.1.1 Política Corporativa de Seguridad de la Información 5

4.1.2 Normativa de Seguridad de la Información 6

4.1.3 Estándares de Seguridad 9

4.1.4 Procedimientos Operativos de Seguridad 9

4.1.5 Guías de Seguridad 9

4.2 Codificación **10**

4.3 Ciclo de vida para los documentos del Marco Normativo **11**

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"

ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

1. OBJETIVO

El presente documento detalla la estructura, codificación y ciclo de vida de la documentación que formará el Marco Normativo de Seguridad de la información en SILICE, la cual regirá para la protección de activos informáticos, así como la implantación de la Política Corporativa de Seguridad de la Información.

2. ÁMBITO DE APLICACIÓN

Todas las líneas de negocio de SILICE y para otras entidades colaboradoras o terceros involucrados en la utilización de la información y sistemas que la soportan.

3. DOCUMENTOS RELACIONADOS

- SIL.IT.POL.05-001 - Política Corporativa de Seguridad de la Información.
- SIL.IT.POL.05-003 - Normativa de Seguridad de la Información
- SIL.IT.MAF.06-002 - Estructura de Seguridad

4. DESARROLLO

El Marco Normativo de Seguridad de la Información constituye el conjunto de documentos, tanto administrativos como técnicos que definen y especifican las directrices establecidas en la Política Corporativa de Seguridad de la Información.

Dicho marco normativo está estructurado en cuatro niveles estableciendo el "*QUÉ*" se tiene que cumplir y el "*COMO*" se implanta. (ver la figura 1 "Estructura Marco Normativo de Seguridad de la información"):

- Políticas de Seguridad.
- Estándares de Seguridad.
- Procedimientos Operativos de Seguridad.
- Guías de Seguridad.

En los apartados siguientes se define y se desarrolla con más en detalle cada uno de los niveles de esta estructura.

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

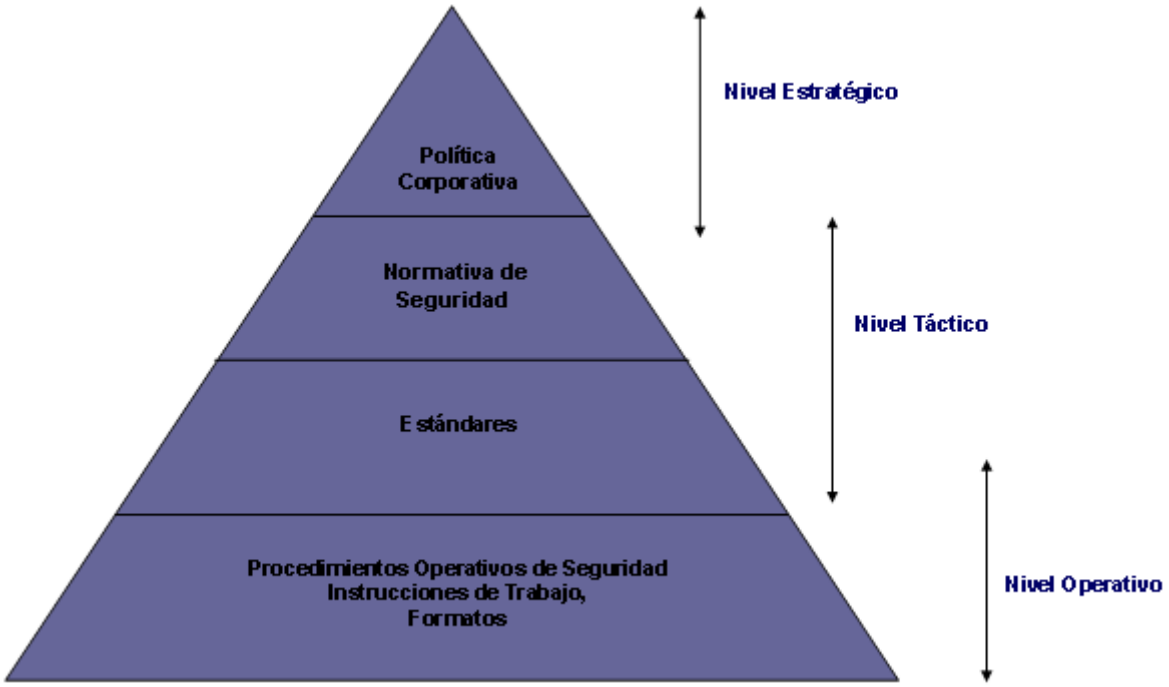


Figura 1: Estructura del Marco Normativo de Seguridad de la Información

4.1.1 Política Corporativa de Seguridad de la Información

Declaración de alto nivel de objetivos, directrices y compromiso de la Dirección General para acometer la gestión de la Seguridad de la Información.

Los demás componentes del Marco Normativo Seguridad de la Información se basan y se desarrollan a partir de esta Política Corporativa de Seguridad de la Información.

4.1.2 Normativa de Seguridad de la Información

La Normativa de Seguridad de la Información es un documento, que basado en la Política Corporativa de Seguridad de la Información, contendrá directrices de alto nivel en algún contexto determinado (como los dominios del estándar ISO27001 e ISO27002) que deben ser implantadas con el propósito de resguardar los activos de información y sus sistemas.

Las directrices que contenga una determinada política serán:

- De obligado cumplimiento,

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

- ➢ De índole técnica y/u organizativa,
- ➢ Independientes de la tecnología,

Su ámbito de aplicación serán los sistemas de información, la información que es procesada o almacenada en dichos sistemas y los usuarios que acceden a la misma.

El contenido de la normativa siempre cumplirá con lo establecido en la Política Corporativa de Seguridad de la Información y su función será desarrollar el contenido de la misma dentro del ámbito de la seguridad de la información.

La normativa considera los dominios del estándar ISO 27002 y estarán divididas según el dominio de la seguridad de la información que desarrollen, como se detalla a continuación.

- **Gestión de activos**

  - ➢ **Clasificación y Tratamiento de Información:** Directrices relativas para clasificar la información en función de su importancia para la organización y el tratamiento que se ha de hacer de la misma en función de dicha clasificación.

  - ➢ **Gestión de activos:** Directrices relativas al proceso de adquisición, inventario, identificación, asignación y etiquetado de los activos de información.

  - ➢ **Uso adecuado de activos de información:** Directrices para el uso adecuado y la protección de los activos informáticos propiedad de SILICE que son otorgados al personal para la realización de sus actividades.

- **Gestión de comunicaciones y operaciones**

  - ➢ **Copias de Respaldo y Recuperación:** Directrices relativas a los procedimientos de copias de respaldo y recuperación de la información.
  - ➢ **Registro y Monitorización:** Directrices relativas a los registros históricos y pistas de auditoría, obtenidos de los sistemas de

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

información, su tratamiento, almacenamiento, gestión y monitorización de eventos.

- ➢ **Gestión y distribución de medios de almacenamiento removibles:** Directrices relativas a la identificación, entrada, salida, distribución, reutilización y almacenamiento de medios de almacenamiento con información de la empresa.

- **Control de acceso**

  - ➢ **Identificación y Autenticación:** Directrices relativas a la identificación y autenticación de los usuarios en el acceso a la información y a los sistemas; a las propiedades de las contraseñas: a los procedimientos de gestión de identificadores y contraseñas.
  - ➢ **Control de Acceso:** Directrices relativas al otorgamiento, modificación y eliminación de derechos de acceso de los usuarios a los sistemas de información, una vez que estos han sido identificados y autenticados; a la utilización de roles y perfiles de acceso de acuerdo a las actividades de los usuarios en la organización para la asignación de privilegios; a los procedimientos de gestión de roles, privilegios y perfiles de usuario.
  - ➢ **Segmentación de redes:** Directrices para la separación, control y gestión de las redes y subsegmentos que permitan separar los sistemas de acuerdo al nivel de clasificación de la información que está siendo procesada o almacenada en los mismos. proteger los sistemas y aplicaciones que utilizan estas redes, así como la información en tránsito.

- **Adquisición, desarrollo y mantenimiento de sistemas de información**

  - ➢ **Adquisición, Desarrollo y Mantenimiento de Sistemas:** Directrices relativas a la seguridad de la información en el proceso de adquisición, desarrollo y mantenimiento de sistemas.
  - ➢ **Control de Software:** Directrices relativas a la protección contra códigos maliciosos, software autorizado, actualizaciones en los sistemas de información, licencias.

- **Gestión de incidentes de Seguridad de la Información**

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

- ➢ **Gestión de Incidentes**: Directrices relativas a los procedimientos de notificación, gestión y respuesta a los incidentes de seguridad de la información.

- **Gestión de la continuidad del negocio**

  - ➢ **Continuidad y recuperación del negocio**: Directrices relativas a la elaboración, implantación y verificación de planes que permitan una recuperación ordenada de los procesos de negocio ante contingencias o desastres que afecten a los sistemas sobre los que se soportan.

- **Conformidad**

  - ➢ **Retención y Eliminación de Datos:** Directrices relativas a los medios de almacenamiento, tiempos de retención, métodos y registros de la eliminación de datos considerando los requerimientos legales o de estándares de la industria de las distintas líneas de negocio de SILICE.
  - ➢ **Documento de Seguridad LFPDPPP:** Contiene los lineamientos, organización, inventario, avisos/cláusulas de privacidad, procedimientos ARCO de acuerdo a lo establecido por la LFPDPPP y su reglamento.
  - ➢ **Manual del entorno de datos de tarjetahabiente:** Documento que describe aquellos procesos de la organización que adquieren, procesan, almacenan o transmiten información de tarjetas de pago, los activos y personas que lo conforman, las terceras partes que participan así como los flujos de datos que involucran este tipo de datos en GGG SOLUTIONS.

4.1.3 Estándares de Seguridad

Documentos que recogen modelos, patrones o parámetros que deben ser utilizados para lograr el cumplimiento de las directrices establecidas en las Políticas de Seguridad de la Información.

4.1.4 Procedimientos Operativos de Seguridad

Documentos que recogen el conjunto de tareas detalladas y específicas con el fin de soportar, en la operación diaria, todos los aspectos establecidos en los niveles superiores del Marco Normativo de Seguridad de la Información.

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

Los procedimientos operativos de Seguridad de la Información podrán estar acompañados de la documentación adicional necesaria para la realización del mismo y para ayudar a la recolección de registros tales como formatos y listas de verificación.

Serán documentos que se usen en la gestión cotidiana, totalmente específicos para tecnologías, procesos o sistemas específicos.

4.1.5 Guías de Seguridad

Documentos que apoyan el cumplimiento del Marco Normativo de Seguridad al sugerir mejores prácticas, tecnologías, herramientas que faciliten la realización de alguna actividad.

4.2 Codificación

Cada política, estándar, procedimiento y guía para desarrollar la Política Corporativa de Seguridad de la Información será identificada con un código para facilitar su referencia.

La codificación será la siguiente:

SIL.DD.TT.DOM-XXX

Donde:

- **SLI** - SILICE
- **DD** - Departamento, según la siguiente tabla:

DEPARTAMENTO	CÓDIGO
Ventas	VE
Marketing y Comunicaciones	MC
Projects Managers	PM
Consultoría	IT
Desarrollo	IT
Soporte	IT
Infraestructura	IT
Plataforma	PL
Experiencia	EX
Finanzas	FI
Country Manager	CM
Administración	AD

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

➢ **TT** - Tipo de documento, según la siguiente tabla:

DOCUMENTO	CÓDIGO
Política	POL
Procedimiento	POS
Guía/ Formato	FOR
Estándar	EST
Manual de Funciones	MAF
Anexo	ANX

➢ **DOM** - Dominio ISO 27000, según la siguiente tabla:

DOMINIO	CÓDIGO
Política de seguridad	05
Aspectos organizativos de la seguridad de la información	06
Gestión de activos	07
Seguridad ligada a los recursos humanos	08
Seguridad física y ambiental	09
Gestión de comunicaciones y operaciones	10
Control de acceso	11
Adquisición, desarrollo y mantenimiento de los sistemas de información	12
Gestión de incidentes de seguridad de la información	13
Gestión de la continuidad del negocio	14
Cumplimiento	15

➢ **XXX** - Consecutivo

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA

4.3 Ciclo de vida para los documentos del Marco Normativo

Para los tipos de documentos que componen el Marco Normativo de Seguridad de la Información, se han identificado las fases de la gestión del ciclo de vida de la documentación, dichas fases se indican a continuación.

- **Elaboración:** El desarrollo del contenido del documento, realizado a partir de mejores prácticas, regulación vigente y/o a partir de las prácticas internas de SILICE.
- **Revisión**: La consulta al personal involucrado, obteniendo retroalimentación para mejorar el documento.
- **Aprobación:** Un requisito para la distribución "formal" del documento, su aceptación y publicación. La aprobación de los documentos se dará por parte del líder de la Dirección de Operaciones y del CISO.
- **Publicación**: Hacer el documento disponible al personal de SILICE a través de la Intranet.
- **Revisiones:** La repetición de las fases anteriores debido a modificaciones de sistemas o de legislación, mejoras propuestas o como resultado de informes de auditoría.

LAS COPIAS IMPRESAS DE ESTE DOCUMENTO SE CONSIDERAN "COPIAS NO CONTROLADAS"
ESTE DOCUMENTO ES DE USO EXCLUSIVO DE SILICE, QUEDA ESTRICTAMENTE PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL SIN AUTORIZACIÓN PREVIA