

MEMORÁNDUM N° 67/DVAGT-DPAG-AI/2.024.


A : Departamento Auditoría de Gestión.
De : División Auditoría de Gestión Técnica.
Ref. : Remisión de Informe Final N° 04/DVAGT-DPAG-AI/2024
Fecha : 27/06/2.024. **ID N° 1.459.124.-**

Se remite el Informe Final correspondiente a la Auditoría practicada por la División Auditoría de Gestión Técnica, que consistió en la Seguridad del Servicio de Telefonía IP correspondiente al Plan Piloto de la Nueva Línea Baja para clientes de la Central de Villa Elisa, y en cumplimiento a la Orden de Trabajo N° 18/A.I./2024.

Solicito que el presente trabajo sea remitido a la **Presidencia del Directorio**, para conocimiento y/o acciones futuras y por intermedio de ésta a la **Departamento Servicios de Red IP – Gerencia Técnica**, para que tomen conocimiento de las recomendaciones y **elaboren los Planes de Mejoramiento Funcionales (PMF)** con relación a los ítems solicitados en un plazo no mayor a 5 (cinco) días contados a partir de la recepción del presente.

Se recuerda a los responsables de las áreas auditadas que deben realizar la carga de las acciones a ser implementadas y demás datos según los respectivos PMF en el Sistema Integrado de la Auditoría General del Poder Ejecutivo –SIAGPE.

Atentamente,



Ing. Víctor Daniel Acuña Fretez.
Encargado de Despacho
División Auditoría de Gestión Técnica

Folio del 1 al 7, incluyendo el presente Memorándum.

Adjunto

- Informe Final N° 04/DVAGT-DPAG-AI/2024 – 6 (seis) páginas.

AUDITORÍA INTERNA	
DEPARTAMENTO AUDITORÍA DE GESTIÓN	
Recibido por:	Lic. Ana María
Fecha:	7 JUN 2024 Hora: 13:40



INFORME FINAL N° 04/DVAGT-DPAG-AI/2024
AUDITORÍA A LA SEGURIDAD DEL SERVICIO DE TELEFONÍA IP

MACRO PROCESO:
Gestión de Redes y Servicios

PROCESO:
Gestión de Sistemas

DEPENDENCIA AUDITADA:
Departamento Servicios de Red IP

FECHA DE ELABORACIÓN DEL INFORME: 27/06/2024

DIRECTIVO RESPONSABLE:
Jorge A. Villalba G.

DESTINATARIO:
Gerencia Técnica

ASPECTOS GENERALES DEL PROCESO DE AUDITORIA

1. ANTECEDENTES

El presente trabajo fue realizado en el marco del Plan de Trabajo Anual de la Auditoría Interna y en cumplimiento de la Orden de Trabajo N° 18/A.I./2024 de fecha 17 de abril de 2024.

2. OBJETIVO GENERAL

Evaluar que los sistemas de información ofrezcan un grado de seguridad razonable y satisfaga las necesidades de los usuarios.

3. OBJETIVO ESPECIFICO

- ✓ Verificar la existencia de procedimientos y la aplicación correcta de la seguridad y prevención contra vulnerabilidades sobre las llamadas en el Servicio de Telefonía IP de la Compañía.
- ✓ Revisar la existencia de procedimientos y la aplicación correcta para la creación del cliente correcto aprovisionamiento en el servidor de telefonía IP.
- ✓ Revisar las Normas y Procedimientos utilizados para asegurar el procesamiento de los registros de llamadas realizados por el Servicio de Telefonía IP de la Compañía.

4. ALCANCE

La Auditoría abarcó la integridad y seguridad del Servicio de Telefonía IP correspondiente al proyecto de implementación de la Nueva Línea Baja, que actualmente se encuentra como Plan Piloto para los clientes de la Central de Villa Elisa, como primera etapa.

El área sujeta a revisión fue el Departamento Servicios de Red IP dependiente de la Gerencia Técnica. La auditoría fue realizada de acuerdo a las funciones y responsabilidades conferidas por los procedimientos que regulan las mismas y otras disposiciones legales concordantes y aplicables.

El presente informe es el resultado de la aplicación de procedimientos de control y del análisis de los documentos proveídos a los auditores. La ejecución y formalización de las operaciones examinadas son de exclusiva responsabilidad de los empleados de las áreas auditadas.

La Auditoría no incluye una revisión detallada e integral de todas las operaciones de las áreas auditadas, por lo tanto, el presente informe no puede considerarse como una exposición de todas las deficiencias o medidas que podrían adoptarse para corregirlas.

La Auditoría abarco el análisis de todo lo mencionado en el objetivo general y los objetivos específicos, arriba descriptos.

5. DOCUMENTOS

- ✓ Política de Seguridad de la Información (P.S.I.).
- ✓ Memorándum N° 43/DVAGT-AI/2024 – Solicitud de documentaciones del Servicio Telefonía IP.
- ✓ Presentación del SIPWISE – Nueva Línea Baja.
- ✓ Presentación del Proyecto de Implementación de la Nueva Línea Baja.
- ✓ Manual de Operaciones Sipwise NGCP

6. TRABAJOS REALIZADOS:

- ✓ Análisis documental de los documentos recibidos del Dpto. de Servicios de Red IP.
- ✓ Revisión documental del proyecto de Implementación del Servicio de Telefonía IP – Nueva Línea Baja.
- ✓ Evaluación del informe presentado en respuesta al Memorándum N° 43/DVAGT-AI/2024.

7. DESARROLLO DEL INFORME:

Como parte del desarrollo del trabajo, el Equipo Auditor procede a la identificación de los diferentes tipos de observaciones y para los mismos se utilizarán los códigos: "(H)" para Hallazgos y "(CI)" para Control Interno.

8. SEGURIDAD DE LAS LLAMADAS DEL SERVICIO DE TELEFONÍA IP

Por Memorándum N° 43/DVAGT-AI/2024, se solicitó a la **Gerencia Técnica**, la siguiente documentación:

"1. Informes de procedimientos utilizados o proyecto de implementación contra vulnerabilidades sobre las llamadas del servicio de Telefonía IP de la Compañía. Los ataques que pueden sufrir las llamadas pueden citarse a manera de ejemplo: llamadas a cuenta, bloqueo por DoS, suplantación de identidad, espionaje de llamadas."



VISION Ser una empresa nacional confiable y sustentable en el rubro de las telecomunicaciones, en constante crecimiento, con talento humano capaz y comprometido.
MISION Satisfacemos las necesidades de comunicación de nuestros clientes, con servicios de calidad y cobertura en todo el territorio nacional, contribuyendo al desarrollo del país.
VALORES Transparencia - Integridad - Honestidad - Igualdad e Inclusión - Eficiencia y Eficacia - Responsabilidad - Compromiso - Lealtad.

El Departamento Servicios de Red IP, informó lo siguiente:

"La plataforma de la Nueva línea Baja NGCP (next generation communication platform) cuenta con 4 niveles de seguridad, las cuales se explican a continuación:

A. Nivel 1, es el nivel más bajo y esta dado a nivel de servidor, la cual cuenta con una estructura de seguridad AAA (Authentication, authorization, and accounting) para operadores y administradores, además de una red aislada para su administración.

B. Nivel 2, nivel de servicio de Red y cuentas SIP, la plataforma cuenta con el feature de seguridad fail2ban a nivel IP y nivel de cuenta SIP (cuenta de usuario), el primero destinado a ataques DoS y el segundo contra intentos de robos de identidad de cuentas SIP (robo de contraseña) por el método de fuerza bruta.

C. Nivel 3, nivel de servicio SIP, La plataforma cuenta con la posibilidad de encriptar el tráfico VoIP mediante el protocolo de encriptación TLS (la cual recomendamos) para los usuarios SIP y peers que así lo deseen usar o lo soporten, con dicha posibilidad las llamadas son encriptadas de cliente a servidor y servidor a cliente, evitando las escuchas de llamadas por terceros.

D. Nivel 4, nivel de control de llamadas fraudulentas, este nivel se define en el perfil de ' cada cliente, y consiste en poner un tope de monto monetario diario, que al alcanzar dicho tope se bloquean las llamadas salientes del cliente. Esta funcionalidad evita que clientes que hayan sido víctimas de robo de sus credenciales de sus cuentas SIP no sean perjudicados con llamadas internacionales costosas o dicho de otro modo que los números nativos de la Nueva línea Baja sean utilizadas para transito de llamadas fraudulentas a destinos internacionales.

No está demás mencionar que se cuentan con las funcionalidades de cambio de contraseña (similar al utilizado por las líneas IP de COPACO S.A), así como la posibilidad de disponer de un reporte detallado de las llamadas realizadas por un determinado cliente.

Como evolución de la plataforma y cuando COPACOS.A cuente con su propia APP y HardPhone/ATA personalizado cada cliente podrá ser interconectado directamente a través de un túnel VPN directo a la Plataforma de la Nueva línea Baja (Con esto se evitaría cualquier bloqueo ya sea de IP o Puerto de otro ISP hacia las IP o Puertos utilizados por la plataforma de la Nueva Línea Baja). Esto no quiere decir que hoy en día no se cuente con este nivel más de seguridad, sino que, en el lado cliente se dificulta la instalación/configuración, por ejemplo, teniendo que intalar 2 APP (uno para realizar llamadas VoIP y otra para VPN) o un equipo hardphone/ATA que no tenga la funcionalidad de interconexión VPN integrada en el firmware."

De la visita realizada por este Equipo Auditor a las instalaciones del Departamento Servicios de Red IP, se pudo observar que la implementación del nuevo sistema para el servicio de Telefonía IP, aún se encuentra en desarrollo.

8.1 Observación (CI): No se cuenta con procedimientos aprobados para el Servicio de Telefonía IP.

Descargo del Jefe del Departamento Servicio de Red IP:

"Se ha solicitado mediante el Memorándum N.º 168/DPSTI-GT/2024 a la Gerencia Comercial para que en conjunto con este Departamento se proceda a la elaboración de los procedimientos que son utilizados para la comercialización y carga de contratos de este nuevo servicio. En el mismo se solicita incluir las áreas responsables y tareas a realizar así como los sistemas a ser utilizados para creación, activación y facturación del servicio."

Opinión del Equipo Auditor:

Se toma conocimiento de la situación mencionada, sin embargo, este Equipo Auditor considera importante la gestión y el seguimiento a fin de definir políticas y procedimientos, para reducir los riesgos que puedan afectar la implementación del servicio de llamadas IP – Nueva Línea Baja.

Considerando lo mencionado y evaluado el descargo, este Equipo Auditor, se mantiene en la observación en el punto 8.1. Se solicita la elaboración del Plan de Mejoramiento Funcional (PMF), para dar cumplimiento a la siguiente recomendación:

Recomendación al Departamento Servicios de Red IP:

En coordinación con el Gabinete Técnico, a fin de elaborar los procedimientos, funciones y responsabilidades de las cuales estarán sujetas el servicio de Telefonía IP.

Definir en coordinación con la Gerencia de Tecnología de Información, las normas y procedimientos que serán aplicados en todo el ciclo del aplicativo implementado del Servicio de Telefonía IP y la infraestructura de la cual se apoya, además de todos los aspectos de seguridad establecidos en la Política de Seguridad de la Información (P.S.I.).

9. REGISTRACIÓN DE USUARIOS DEL SERVICIO DE TELEFONÍA IP

Por Memorándum N° 43/DVAGT-AI/2024, se solicitó a la Gerencia Técnica, la siguiente documentación:

"2. Cuáles son los procedimientos utilizados para un correcto aprovisionamiento o creación de un cliente en el servidor SIPWISE del servicio de telefonía IP"

El Departamento Servicios de Red IP, informó lo siguiente:

"Para garantizar el aprovisionamiento eficiente del servicio, se empleará un sistema completamente automatizado, eliminando así la intervención humana en la plataforma de telefonía IP.

Este proceso implica una secuencia coordinada: primero, se carga el contrato en el sistema BOSS con el estado NUEVO. Luego, el sistema Monitor detecta este nuevo contrato y, mediante un script, configura la nueva línea IP en la plataforma. Además, el sistema Monitor se encarga de enviar las credenciales de acceso al cliente, ya sea por correo electrónico o SMS. Los datos de contacto del cliente, como su correo electrónico y número de teléfono, se extraen del sistema BOSS, siendo ingresados por el operador comercial al momento de cargar el contrato. Es importante destacar que sin estos datos, la cuenta SIP correspondiente no será creada en la plataforma.

Una vez que la línea está configurada y se detecta el primer registro, se activa en el sistema BOSS mediante el Web Service Monitor - BOSS.

Finalmente, el sistema BOSS lleva a cabo la facturación electrónica, siguiendo el mismo procedimiento utilizado para otros servicios IP.

Es importante resaltar que este mecanismo de aprovisionamiento es similar al utilizado para la creación de usuarios y activaciones del servicio GPON. Ha demostrado ser altamente eficaz, con muy pocos inconvenientes y una alta capacidad para manejarla creciente cantidad de clientes."



De la visita realizada por este Equipo Auditor a las instalaciones del Departamento Servicios de Red IP, se pudo observar que la carga se puede realizar tanto por el Sistema Monitor, como por el Sistema BOSS.

9.1 Observación (CI): No se encuentra definido los responsables de carga de clientes.

Descargo del Jefe del Departamento Servicio de Red IP:

"Se tendrá muy en cuenta este punto en el momento de la realización del procedimiento."

Opinión del Equipo Auditor:

Se toma conocimiento de la situación mencionada, sin embargo, este Equipo Auditor considera importante la gestión y el seguimiento a fin de definir políticas y procedimientos, para reducir los riesgos que puedan afectar la implementación del servicio de llamadas IP – Nueva Línea Baja.

Considerando lo mencionado y evaluado el descargo, este Equipo Auditor, se mantiene en la observación en el punto 9.1. Se solicita la elaboración del Plan de Mejoramiento Funcional (PMF), para dar cumplimiento a la siguiente recomendación:

Recomendación al Departamento Servicios de Red IP:

En coordinación con la Gerencia Comercial, a fin de definir los parámetros que serán necesarios para el correcto registro de los clientes contemplando las situaciones de cada cliente.

10. PROCESAMIENTO DE ARCHIVOS CDR's DEL SERVICIO DE TELEFONÍA IP

Por Memorándum N° 43/DVAGT-AI/2024, se solicitó a la Gerencia Técnica, la siguiente documentación:

"3. Cuáles son los procedimientos utilizados para un correcto procesamiento de los CDR's de las llamadas del servicio de Telefonía IP, para el servidor SIPWISE que se está implementando."

El Departamento Servicios de Red IP, informó lo siguiente:

"Teniendo como referencia la solución actual de IMS, se entrega un archivo CDR por día a GTI contemplando los mismos campos, orden y secuencia la cual se expresa en el documento "Campos utilizados en sipwise.docx", dicho documento contempla los campos actuales y los adicionales los cuales son consensuados y probados con el grupo de desarrollo de GTI. Para el formateo de estos campos se utiliza un servidor middleware el cual funge de traductor de manera automática entre Servidor SIPWISE y GTI, dicho servidor se encuentra alojada en la granja de servidores del datacenter a cargo del Departamento de Servicios de Red IP."





De la visita realizada por este Equipo Auditor a las instalaciones del Departamento Servicios de Red IP, se pudo observar que la entrega de los CDR, se realiza conforme a las especificaciones consensuadas con el grupo de desarrollo de GTI.

CONCLUSIÓN

De la verificación realizada, el Equipo Auditor realiza las siguientes conclusiones:

- No se cuenta con un procedimiento aprobado para el Servicio de Telefonía IP – Nueva Línea Baja.
- No se encuentran definidos los responsables de carga de clientes, considerando que la carga de los mismos se puede realizar tanto por el Sistema Monitor y por el Sistema BOSS.

Augusto F. Hermosilla D.
Auditor Actuante
Coordinador

Ing. Víctor D. Acuña F.
Encargado de Despacho
División Auditoría de Gestión Técnica