

INFORME FINAL N° 08/DVAGT-AI/2023.
AUDITORIA INFORMATICA A CONEXIONES REMOTAS

MACRO PROCESO: Gestión de Tecnología de Información	PROCESO: Gestión de TIC'S
DEPENDENCIA AUDITADA: Gerencia de Tecnología de Información	FECHA DE ELABORACIÓN DEL INFORME: 11/12/2023
DIRECTIVO RESPONSABLE: Lic. Diego Ruiz Díaz	DESTINATARIO: Gerente de Tecnología de Información
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° 49/A.I./2023 de fecha 28 de Setiembre del 2023.

2. ALCANCE

La Auditoria abarcó la seguridad del ámbito de las conexiones remotas contempladas en la Gerencia de Tecnología de Información.

El área sujeta a revisión fue el Dpto. Infraestructura y Operaciones TIC, con el Dpto. de Calidad Informática dependiente de la Gerencia de Tecnología de Información. 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.

El periodo auditado de este análisis corresponde del 28/09/2023 al 10/11/2023

3. OBJETIVOS

- Verificar los procedimientos adecuados de protección de cualquier dispositivo móvil y/o removible, del cual se accede a los Sistemas Corporativos de la Compañía, según la Política de Sistemas de Seguridad de la Información en su punto **3.8.1 Computación Móvil**.

- Revisar las *Normas y Procedimientos* para el Trabajo Remoto, según la Política de Sistemas de Seguridad de la Información de la Compañía, en su punto **3.8.2 Trabajo Remoto**.
- Evaluar los Controles y Disposiciones para los accesos remotos, como también los registros de incidentes para la falla de seguridad de este tipo de acceso, según la Política de Sistemas de Seguridad de la Información en su punto **3.8.2**, en el párrafo de **Controles de Acceso**.

4. DOCUMENTOS

- Política de Seguridad de Sistema de Información (P.S.S.I.).
- Instructivo Conexión Remota del 02/04/2020.

5. TRABAJOS REALIZADOS:

- Revisión de los informes enviados por el Dpto. Infraestructura y Operaciones TIC, conjuntamente con el Dpto. Calidad Informática.

6. 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, “(CI)” para las observaciones de Control Interno, “(D)” para los Descargos, “(R)” para las Recomendaciones y “(PMF)” para Plan de Mejoramiento Funcional

7. SEGURIDAD DE CONEXIONES REMOTAS

Este Equipo Auditor realizó la verificación de los documentos enviados por las dependencias comprendidas en la auditoria correspondiente, de la cual se puntualiza cuanto sigue a continuación:

7.1 Observación (CI): Se constataron que no existen procedimientos para el trabajo remoto tales como seguridad física, ambiente de trabajo remoto, seguridad de comunicaciones del mismo, ya que cada usuario utiliza su propia comunicación a internet para establecer la conexión remota. En la **Política de Seguridad de Sistemas de Información**, en el **punto 3.8.2 Trabajo Remoto**, se citan las normas y procedimientos del Trabajo Remoto, tales como :

- a) *“La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.*
- b) *El ambiente de trabajo remoto propuesto.*



- c) *Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos de la Compañía, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del Sistema interno.*
- d) *La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.*
- e) *Evitar la instalación / desinstalación de software no autorizada por la Compañía.”.....*

Descargo del Dpto. Infraestructura y Operaciones TIC/ Dpto. Calidad Informática:

(D) *“El procedimiento vigente para la habilitación de conexiones remotas se encuentra establecido en el Instructivo de Conexión Remota del 02/04/2020.*

Todos los accesos remotos se realizan en forma segura, implementadas a través de conexiones VPN (red privada virtual) que utilizan protocolo encriptados. Para cada conexión se requiere la creación e instalación de un certificado individual como método de seguridad. Los usuarios remotos solo tienen la posibilidad de acceder a los sistemas habilitados y de acuerdo a los roles previamente asignados a los mismos.

El Departamento de Infraestructura y Operaciones TIC se encuentra actualmente en etapa de revisión y actualización del mismos, en el que serán incluidas las tareas y responsabilidades de las áreas que intervienen en el ciclo de vida de estas conexiones, incluidas las del control”

Opinión del Equipo Auditor

Evaluado el descargo, este Equipo Auditor levanta la observación.

7.2 Observación (H): Se constataron que los casos de acceso remoto y registros de incidentes de fallas de los mismos, se registran vía correo electrónico conexiones@copaco.Com.py.

La Política de Seguridad de Sistemas de Información en su punto 3.8.2 Trabajo Remoto, en el párrafo final, establece lo siguiente: *“Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.”*

Descargo del Dpto. Infraestructura y Operaciones TIC/ Dpto. Calidad Informática:

(D) *“Actualmente se está evaluando la posibilidad de que este tipo de conexiones sea gestionada a través del formulario electrónico “Solicitud de Acceso a los Sistemas Informáticos”, a modo de centralizar en un único punto de contacto la atención de solicitudes e incidentes para este tipo de conexiones.”*

VISIÓN
MISSION
VALORES

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

Opinión del Equipo Auditor

Evaluable el descargo este Equipo Auditor, se mantiene en la observación, considerando la importancia del control de los incidentes de fallas de seguridad en este tipo de conexiones. Se solicita la elaboración del Plan de Mejoramiento Funcional (PMF).

Recomendación

(R) Que el Jefe del Dpto. Calidad Informática en coordinación con la Gerencia de Tecnología de Información, realicen las gestiones necesarias para implementar la solicitud de conexiones remotas, a través de un formulario electrónico, contemplando los posibles incidentes de fallas de seguridad y los responsables para la corrección de los mismos.



Augusto F. Hermosilla D.
Auditor Actuante



Lic. Juan Bautista Flores G.
Coordinador



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