

IDENTIFICACION DE LA NO CONFORMIDAD

Codigo	82
Tipo	NO CONFORMIDAD
Origen	DETECCION INTERNA
Clasificacion	MEJORA
Persona que levanta NC	RENZO MUNOZ
Proceso origen	INFORMATICA
Proceso destino	INFORMATICA
Norma	ISO 9001
Clausula normativa	ANÁLISIS DE DATOS
Estado	CERRADA

DESCRIPCION NO CONFORMIDAD

Fecha compromiso: 05/07/2024

Fecha registro: 12/09/2024

El departamento TI se percata que existe una falla en el sistema local (carpetas compartidas, servidores y softwares), realizan una verificación de la estructura digital constatando que el sistema operativo central VMWare se encuentra pega, contactan al proveedor TECNOTEC quien presta servicios a la organización mediante el respaldo de la información digital , realizan una serie de acciones, principalmente el reinicio del sistema operativo quienes logran percatare la presencia de un virus de tipo ransomware producto de un ciberataque el que se afecta a varios de sus clientes incluido Pinto Piga Seeds.

Este ciberataque produjo la eliminación de los archivos en las carpetas compartidas que la organización mantenía en sus servidores y la encriptación de la información de respaldo de TECNOTEC.

Responsables de no conformidad	MANUEL ROSAS
Responsables de accion inmediata	MANUEL ROSAS
Notificar a - personas	SEBASTIAN CAYUL, GONZALO FUENZALIDA, CARLOS UBILLA, MATIAS TOBAR, RODRIGO GIRONES
Notificar a - grupos	Audidores Internos
Notificar a - cargos	-

ACCION INMEDIATA

Fecha compromiso: 06/07/2024

Fecha registro: 21/09/2026

Frente a la confirmación del ataque, se procedió a tomar medidas bajo 2 etapas:

I Etapa: (Acción inmediata)

1. Desconectar la red de la organización.
2. Apagar los servidores físicos no infectados.
3. Cortar toda comunicación digital con el proveedor.
4. Se envía un comunicado a las Jefaturas para que instruyan a sus colaboradores no encender sus laptops.
5. Verificación de los sistemas directo por las diferentes áreas.

II Etapa:

1. Cambio claves operativas.
2. Recolección de todas las laptops y PC de la organización.
3. Conformación de un equipo para labores en TI.
4. Revisión de los equipos en busca de archivos infectados para posteriormente respaldar información local y formatear.
5. Contratación asesor de seguridad digital.
6. Aumento seguridad por medio de autenticación multifactor (MFA)

Responsables de analisis de causa	MANUEL ROSAS
Notificar a - personas	SEBASTIAN CAYUL, GONZALO FUENZALIDA, CARLOS UBILLA, MATIAS TOBAR, RODRIGO GIRONES
Notificar a - grupos	Audidores Internos
Notificar a - cargos	-

ANALISIS DE CAUSA

Fecha compromiso: 09/07/2024

Fecha registro: 21/09/2026

Preliminarmente el ciberataque sufrido por el proveedor se genero por no mantener la última actualización de la infraestructura del sistema quedando vulnerables, esto permitió la suplantación de su sitio web corporativo desde donde se habrían accedido a la ruta de las bases de datos.

Responsables de accion correctiva	MANUEL ROSAS
Notificar a - personas	SEBASTIAN CAYUL, GONZALO FUENZALIDA, CARLOS UBILLA, MATIAS TOBAR, RODRIGO GIRONES
Notificar a - grupos	Audidores Internos
Notificar a - cargos	-

ACCION CORRECTIVA/PREVENTIVA

Fecha compromiso: 30/12/2024

Fecha registro: 21/09/2026

La organización por medio de la alta dirección y en asesoría con el especialista en ciberseguridad han dispuesto realizar:

1. Cambio del proveedor contemplando la verificación periódica de las actualizaciones de su software
2. Cambio en el método de respaldo
3. Cambio en la infraestructura y seguridad de la red física.
4. Definición de procedimiento(s) de ciberseguridad para la organización
5. Políticas de seguridad restrictivas (filtro contenido / descargas)
6. Restricción usuarios con permisos básicos.
7. Cambio de antivirus.

Responsables de efectividad de	RENZO MUNOZ
Notificar a - personas	SEBASTIAN CAYUL, GONZALO FUENZALIDA, CARLOS UBILLA, MATIAS TOBAR, RODRIGO GIRONES
Notificar a - grupos	Audidores Internos
Notificar a - cargos	-

EFECTIVIDAD DE LA ACCION TOMADA

Fecha compromiso: 30/12/2025

Fecha registro: 21/09/2026

Las indicaciones señaladas en el Plan de acción 2, permitieron realizar cambios cultural necesarios para la protección y resguardo de la estructura digital de la organización. Con esto, se realizó la eliminación de carpetas compartidas dentro de la red eliminando el riesgo de archivos maliciosos, el cambio físico se efectuó a través del respaldo por medio de la nube con microsoft 360. Al igual, el cambio del proveedor del servicio con mayor experiencia en el mercado informático.

A lo anterior, se ha sumado la concientización e información que el Dpto. TI realiza por medio de cartillas informativas a los email de los colaboradores la identificación de archivos phishing y el bloqueo de acceso libre a sitios web con mayor incidencia de ataque.

Por último, se desarrollaron las políticas de ciberseguridad, habilitación y control de credenciales.

Las medidas descritas e implementadas, han reunido las condiciones suficiente para escudar el manejo y respaldo de la información de la organización, no presentándose nuevo hechos de igual o similar condición al cierre de esta NC.

Notificar a - personas	SEBASTIAN CAYUL, GONZALO FUENZALIDA, CARLOS UBILLA, GUSTAVO RAMIREZ, RODRIGO GIRONES
Notificar a - grupos	Audidores Internos
Notificar a - cargos	-