

Habana, 18 de mayo de 2019  
"Año 61 de la Revolución"

## A: Todas las entidades de la Empresa de Gases Industriales.

### Asunto: Indicación de obligatorio cumplimiento del Control de Acceso a la Red de Gases Industriales para evitar que equipos vulnerables se conecten a la misma.

La Dirección de Informática y Comunicaciones de la Empresa de Gases Industriales de Cuba, teniendo en cuenta que:

- Desde el nodo se realizan levantamientos de vulnerabilidades críticas en las estaciones de nuestra red.
- La **OSRI** emite alertas sobre vulnerabilidades que afectan nuestras estaciones.
- Existe en Gases Industriales un proceso de reconfiguración, mantenimiento y chequeo del estado de los servidores WSUS.
- Está orientado que la instalación de los parches del Sistema Operativo y producto antivirus kaspersky controlado centralizadamente desde la consola KSC (Kaspersky Security Center) sea un paso en la preparación de una nueva PC antes de entregarla a los usuarios.
- No se da el seguimiento apropiado a las notificaciones que se envían desde el nodo y reciben las entidades periódicamente, para resolver en tiempo los problemas que reciben en el informe de auditoría.
- Los reportes abiertos por meses por el Grupo de Gestión no cuentan con notas sobre las acciones realizadas para solucionar los problemas que se informan con la acción anterior.
- No se puede permitir el acceso a la red a computadoras vulnerables, desactualizadas o sin antivirus.
- Es obligación de los Administradores de Red el chequeo periódico del estado de las actualizaciones de Windows y del producto antivirus de todas las estaciones y servidores.
- Las aplicaciones adquiridas de terceros, como el Distrá, no tienen soporte por el proveedor y genera gastos financieros si existen afectaciones por virus o fallas de seguridad.

### Resuelve:

1. Poner en práctica una nueva política de **Protección de Acceso a la Red (NAP, Network Access Protection)** para las estaciones detectadas en las siguientes categorías del informe de auditoría:
  - a. PCs vulnerables.
  - b. PCs sin contacto con WSUS.
  - c. PCs que no actualizan.
  - d. KSC: PCs sin agente.
  - e. KSC: AV en estado crítico.
  - f. U otras categorías críticas que se consideren.



2. A las estaciones que estén implicadas en alguna de las anteriores categorías, se le aplicarán las siguientes medidas automáticamente al ejecutarse la auditoría. Estas son ejecutadas periódicamente:
  - a. **Bloqueo del acceso a todos los servicios del Nodo Nacional.**
  - b. **Bloqueo del acceso al Servicio de Correo.**
  - c. **O alguno de estas medidas.**
3. Cuando las estaciones sean remediadas de sus fallas y las auditorías automáticas lo detecten serán reestablecidos automáticamente los servicios.
4. Los administradores de Red y el Grupo de Gestión del Nodo podrán ver las estaciones bloqueadas en la siguiente URL: <http://logparser.gases.co.cu:8080/nap.html>.
5. Desde el Centro de Gestión del Nodo y por los administradores de red de las entidades se atenderán los posibles reportes de usuarios, cuya pérdida de servicio es causada por la actual medida, para las estaciones bloqueadas. En estos se explicará las causas de la pérdida del acceso a los servicios.
6. Se le dará un trato diferenciado a las estaciones de trabajo que desempeñan una actividad laboral continua (Trabajo 24h), debido a la complejidad de estos puestos.
7. **Entrará en vigor a partir del 20 de Mayo del 2019.**

## Notas importantes

- En los servidores WSUS se ha trabajado en estandarizar la configuración y mantenimiento automático, normalmente no es necesario realizar ningún cambio de configuración, se aprobarán automáticamente los parches **Críticos y de Seguridad**.
- Si alguno de los servidores que necesitan comunicarse con el Nodo sale en las auditorías, toda la UEB perdería completamente el servicio que este brinda, por ejemplos: Controlador de Dominio, el Servidor de Correos, WSUS.

Aprobado por:

Ernesto Santana Rodríguez  
Director de Informática y Comunicaciones  
Empresa de Gases Industriales



Yamilet Fuentes Pardiñas  
Directora General  
Empresa de Gases Industriales



DIC-0001/19

C.C: Archivo, Leity Méndez López, Liliana Frontela