

SEÑOR PRESIDENTE:

OBJETIVO:

Evaluar la implementación de la Red Privada Virtual (VPN) que el Instituto Nacional de Vitivinicultura ha dispuesto para el acceso remoto de los empleados del organismo en el marco de la pandemia COVID-19, analizando si se cumplen con las buenas prácticas y recomendaciones asociadas con este tipo de accesos. Además se evaluará el sistema de control interno y la gestión con relación a los aspectos enunciados dentro de la "Política de Seguridad de la Información Modelo" para este tipo de redes.

El presente trabajo está incorporado en la reformulación de la Planificación Anual de la Unidad de Auditoría Interna para el corriente año como Proyecto N° 12.

ALCANCE DE LA TAREA:

Las tareas se desarrollaron de acuerdo con las Normas de Auditoría Interna Gubernamental establecidas por Resolución N° 152/2002 de la SINDICATURA GENERAL DE LA NACION, ajustando su alcance a la aplicación de procedimientos de control de cumplimiento y sustantivos.

Se siguieron los lineamientos expuestos en la "POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN MODELO" aprobada en la Disposición 1/2015 de la Oficina Nacional de Tecnologías de la Información puesta en vigencia a través de la Decisión Administrativa 669/2004 de la Jefatura de Gabinete de Ministros, relacionados con los apartados de redes externas. Las tareas se ajustaron a la evaluación de los siguientes objetivos de control:

- Autenticación de Usuarios para Conexiones Externas
- Redes
- Buenas prácticas seguridad en VPN

Las tareas de campo se desarrollaron en Sede Central y en Sede de la UAI, lo cual incluyó las tareas previas, el relevamiento y tareas posteriores vinculadas a la preparación y análisis de los datos recabados.

En forma sintética se detallan a continuación las tareas realizadas de mayor significatividad:

- En el mes de Noviembre del año 2021 se realizó la actualización y análisis de información técnica y normativa vigente asociada a redes privadas virtuales.
- Mediante nota NO-2021-116713170-APN-UAI#INV ?Requerimientos Iniciales ? TI Auditoría Seguridad VPN? con fecha 01/12/2021 se solicitó al Responsable de Seguridad de la Información y Jefe del Departamento de Informática y Comunicaciones, la información y documentación de respaldo asociada a la implementación y administración de la Red Privada Virtual para el acceso remoto de los funcionarios del organismo:
 - Listado detallado de clientes VPN activos.
 - Detalle de los modos de conexión remota utilizados en el organismo (herramientas de acceso remoto utilizadas).
 - Listado detallado de clientes VPN activos.
 - Listado detallado de clientes remotos activos.
 - Documentación autorización clientes VPN / remoto.
 - Detalle de las VPN instaladas en equipos que no son propiedad del organismo.
 - Documentación configuración del servidor VPN utilizado, y de los certificados clientes. Configuración estándar de otras herramientas de acceso remoto utilizadas.
 - Detalles de redes implementadas para los cliente VPN
 - Descripción procedimiento monitoreo de actividad VPN.
 - Política de configuración de los registros de auditoría (logs) de seguridad del servidor VPN. Política de retención de esos registros.
 - Registro de incidentes de seguridad desde la habilitación masiva de VPN en el organismo.
 - Detalle de la capacitación impartida y de los empleados que la recibieron asociada a la metodología de trabajo

remoto.

- El día 08/12/2021 se recibió mediante nota NO-2021-119344768-APN-DIYC#INV, un pedido de prórroga en el plazo de entrega.
- El día 15/12/2021 se recibió mediante nota NO-2021-119671278-APN-UAI#INV la documentación solicitada en los Requerimientos Iniciales, y se comenzó a analizar la misma.
- Se entrevistó al Jefe del Departamento de Informática y Comunicaciones
- A partir del día 21/12/2021 se comenzaron a notificar las observaciones.

OBSERVACIONES MAS SIGNIFICATIVAS:

No se realizaron observaciones significativas en el presente informe.

CONCLUSIONES:

Considerando el alcance y tareas desarrolladas, observaciones y opinión del auditado; puede señalarse que las medidas adoptadas por el organismo en relación al acceso remoto de usuarios del organismo resultan satisfactorias, con las salvedades expuestas en el punto "Observaciones" del presente informe.