INFORME EJECUTIVO
INFORME DE AUDITORIA INTERNA Nº 009/2020
TI - Aud Seguridad VPN (Plan Emergencia)
Proyecto N° 8
Mendoza, 30 de Diciembre de 2020

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 Auditoria Interna para el corriente año como Proyecto N° 8.

ALCANCE DE LA TAREA:

Las tareas se desarrollaron de acuerdo con las Normas de Auditoria 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:

- Riesgos de seguridad
- 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:

- Relevamiento preliminar de la VPN habilitada para acceso remoto mediante la herramienta NMAP
- En el mes de Octubre del año 2020 se realizó la recopilación y análisis de información técnica y normativa vigente asociada a redes privadas virtuales.
- Mediante nota NO-2020-79152821-APN-UAI#INV "Requerimientos Iniciales - TI Auditoría Seguridad VPN" con fecha 17/11/2020 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.
  - Documentación autorización clientes VPN.
  - Detalle de los modos de conexión utilizados en el organismo (herramientas de acceso remoto utilizadas).
  - Información sobre las VPN que se utilizan 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.
  - Además de envié un cuestionario asociado a la gestión de esta red.
- El día 24/11/2020 se recibió mediante nota NO-2020-81326049-APN-DIYC#INV, un pedido de prórroga en el plazo de

entrega.

- El día 27/11/2020 se recibió mediante nota NO-2020-82414833-APN-DIYC#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 17/12/2020 se comenzaron a notificar las observaciones.

OBSERVACIONES MAS SIGNIFICATIVAS:

OBSERVACIÓN Nº 1	***METODO ACCESO REMOTO INSEGURO***

Algunos equipos del organismo utilizan como método de acceso un programa de escritorio remoto conocido como DWSERVICE. Este método no esta considerado dentro de las mejores prácticas en seguridad y presenta más riesgos que los accesos mediante VPN.

RECOMENDACIÓN

Se recomienda la utilización de un método más adecuado para el acceso a los equipos del organismo.

ESTADO: Con Acción Correctiva Informada

OBSERVACIÓN Nº 2	***CONTROLES RED VPN INSUFICIENTES***

La red de acceso para los clientes VPN, VPN-WARRIORS, no posee los mismos controles que las redes habilitadas para los usuarios en las distintas subredes del organismo; permitiendo el acceso en forma directa mediante diversos protocolos a los servidores del organismo.

RECOMENDACIÓN

Se recomienda crear una nueva red VPN configurada con los mismos niveles de acceso que las subredes del organismo y dirigir allí a las VPN's de los usuarios, dejando la VPN-WARRIORS para uso exclusivo de personal informático

ESTADO: Con Acción Correctiva Informada

OBSERVACIÓN Nº 3	***EQUIPOS CON RIESGOS DE SEGURIDAD***

Se ha habilitado el ingreso mediante VPN a equipos propiedad de funcionarios del organismo, los cuales no están bajo el control del DIC, lo que implica no saber si se cumplen las condiciones de seguridad mínimas (antivirus, actualizaciones, sistema operativo) al momento de conectarse a la red.

RECOMENDACIÓN

Se recomienda implementar una VPN tipo Portal para el acceso de estos equipos a los sistemas y archivos del organismo.

ESTADO: Con Acción Correctiva Informada

CONCLUSIONES:

En base a lo analizado, las observaciones realizadas y la opinión del auditado se considera necesario analizar una forma diferente de acceso y procedimientos que la soporten, para los equipos que no están incluidos en el dominio del organismo con el fin de mejorar la seguridad, sugiriendo que estos equipos utilicen una VPN donde se posea acceso a recursos puntuales (como los sistemas de gestión del organismo) pero no a toda la red.
Para los demás aspectos analizados en el presente informe, puede señalarse que las medidas adoptadas por organismo resultan satisfactorias, debiendo solucionar los aspectos observados de acuerdo a los compromisos asumidos.

Si bien no se puede obviar que el ingreso a la modalidad de trabajo remoto en el organismo se realizó de forma muy rápida y con un nivel de operatividad excelente, se debe considerar el crecimiento en la utilización de las VPN y la posible

extensión en el tiempo de la pandemia COVID-19 junto con los cambios que trae incorporada, por lo cual se debería avanzar en mejorar la seguridad de este tipo de conexiones de acuerdo con lo arriba expuesto.

TILLAR
Martin
Omar

Firmado
digitalmente por
TILLAR Martin Omar
Fecha: 2020.12.30
12:55:12 -03'00'