INSTITUTO NACIONAL DE VITIVINICULTURA
Unidad de Auditoria Interna

INFORME EJECUTIVO
INFORME DE AUDITORIA INTERNA Nº 015/2022
TI - Gestión de Accesos
Proyecto N° 11
Mendoza, 29 de Diciembre de 2022

SEÑOR PRESIDENTE:

OBJETIVO:

Evaluar el cumplimiento del marco normativo y reglamentario vigente, verifiando el sistema de control interno y la gestión con relación a los aspectos enunciados dentro de los 'Requisitos Mínimos de Seguridad de la Información para Organismos' (Decisión Administrativa 641/2021), bajo el punto 'Autenticación, Autorización y Control de Accesos' y la 'Política de Seguridad de la Información del INV' (Resolución 8/2022 INV), bajo el punto 'GESTIÓN DE ACCESOS'.

El presente trabajo está incorporado en la Planificación Anual de la Unidad de Auditoria Interna para el corriente año como Proyecto N° 11.

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. Las mismas se extendieron desde el 8/8/2022 hasta el 30/12/2022.

El alcance del presente proyecto no incluyó la revisión de permisos de acceso de los usuarios a los sistemas de información del organismo, ni tampoco incluyó la revisión de usuarios en bases de datos del organismo. Esta reducción del alcance fue necesaria para adecuarse a las horas disponibles en la UAI en la segunda mitad del año 2022.

Las tareas se ajustaron a la evaluación de los siguientes objetivos de control:

- Sistema de Administración de Contraseñas.
- Administración de Contraseñas Críticas.
- Uso de Contraseñas.
- Camino Forzado.
- Subdivisión de Redes.
- Política de Gestión de Accesos.
- Gestión de Contraseñas de Usuario.
- Acceso a Internet.
- Autenticación de Usuarios para Conexiones Externas.
- Identificación y Autenticación de los Usuarios.
- Seguridad de los Servicios de Red.
- Registración de Usuarios.
- Gestión de Privilegios.

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 las redes del organismo 15/08/2022
- Mediante nota NO-2022-88327907-APN-UAI#INV 'Requerimientos Iniciales' con fecha 24/08/2022 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 'GESTIÓN DE ACCESOS' de acuerdo al siguiente detalle:
  - Capítulo de la política de seguridad del organismo referido a la Gestión de Accesos.
  - Listado de dominios implementados en el organismo
  - Identificación de los servidores que actúan como controladores de dominio, servidores web, servidores de base de datos y firewall en el ambiente producción del organismo
  - Listado de los usuarios registrados en los dominios del organismo.
  - Listado de los usuarios registrados en los servidores web, de base de datos y firewall en el ambiente producción del organismo.
  - Identificación de cuentas de usuarios con las cuales es posible efectuar actividades críticas en los servidores de detallados en el punto 3.

- Procedimiento para la administración de contraseñas de los usuarios identificados en el punto anterior (act. críticas).
- Listado de cuentas genéricas implementadas en los servidores requeridos.
- Documentación asociada a la política de usuarios locales habilitados en los servidores.

- El día 01/09/2022 se recibió mediante nota NO-2022-92124238-APN-DIYC#INV, un pedido de prórroga en el plazo de entrega.
- El día 29/09/2022 se recibió mediante nota NO-2022-103644739-APN-DIYC#INV la documentación solicitada en los Requerimientos Iniciales, y se comenzó a analizar la misma.
- Los días 12, 13 y 14/12/2022 se realizó una revisión de los principales servidores del organismo asociados a actividades críticas (Dominio; WebServer, LAPD, Firewall) con el propósito de verificar los parámetros de seguridad implementados en los mismos.
- Se entrevistaron a los siguientes funcionarios:
  - Jefe del Departamento de Informática y Comunicaciones
  - Jefe de la División de Administración de Sistemas del DIC
  - Administrador de Infraestructura
- A partir del día 21/12/2022 se comenzaron a notificar las observaciones.

OBSERVACIONES MAS SIGNIFICATIVAS:

OBSERVACIÓN Nº 3	***USUARIOS DESARROLLO CON PRIVILEGIOS ADMINISTRACION***

Se han identificados usuarios de la div desarrollo con perfiles de admistrador/superusuario en los servidores web de producción de acuerdo al siguiente detalle:

MALBEC6-2 dla***, mmi***,
MARSELAN dla***, mmi***,
HMARSELAN dla***, mmi***,
HMENCIA fvi***,
XMENCIA-proyec fvi***

RECOMENDACIÓN

Se debería retirar todo los provilegios de los usuarios de desarrollo en el entorno productivo.

ESTADO: En Implementación

OBSERVACIÓN Nº 5	***REGISTRO MODIFICACIONES INSUFICIENTE ADMINISTRACION USUARIOS***

La aplicacion de Administración de Usuarios de los Sistemas de Gestión (originales) no registra de forma clara los datos de los operadores que realizan modificaicones/bajas sobre un login y sus perfiles.

RECOMENDACIÓN

La aplicación de adminitración de usuarios debe permitir un registro preciso de todas las modificaciones de privilegios que se realizan sobre los usaurios del sistema.

ESTADO: S/A Correctiva Informada

OBSERVACIÓN Nº 7	***USUARIOS DESVINCULADOS EN GRUPOS CRITICOS***

Se identificaron usuarios de dominio en el Grupo de Seguridad "Admins. del Dominio" que se encuentran desvinculados de la institución.

RECOMENDACIÓN

Se recomienda implementar un checklist de verificación para la eliminación de los todos usuarios "especiales" cuando se desvincula un empleado del DIC.

ESTADO: Regularizada

OBSERVACIÓN Nº 8	***PARAMETROS ERRONEOS CONFIGURACION CONTRASEÑA SERVIDORES LINUX***

Los parámetros de configuración de la contraseñas de los servidores Linux de producción del organismo no respeta los parámetros estipulados en la Política de Seguridad del Organismo (IF-2022-129222798-APNDIYC#INV) en lo referido a caducidad, complejidad, reutilización y tiempo de vida.

RECOMENDACIÓN

Se recomienda ajustar los parámetros de contraseñas a todos los servidore LINUX de acuerdo a lo establecido en la política de seguridad del organismo.

ESTADO: S/A Correctiva Informada

OBSERVACIÓN Nº 11	***UTILIZACION USUARIOS CRITICOS GENERICOS***

Se identificó la utilización del superusuario genérico "root" en los servidores Linux de la DMZ del organismo.

RECOMENDACIÓN

Se recomienda no utilizar estos usuarios en forma habitual, poniendo sus claves a reguardo y utilizarlos sólo para emergencias.

ESTADO: S/A Correctiva Informada

CONCLUSIONES:

De acuerdo a lo analizado, se han verificado avances en la mayoría de los temas asociados con el proceso bajo revisión, principalmente la aprobación de la nueva versión de la política de Seguridad de la Información del organismo. Sin embargo se observa que es alto el número de observaciones de informes anteriores que se repiten al momento de realizar el presente proyecto, por esto se considera necesario generar a la brevedad posible los procedimientos que se desprenden de la nueva Política de Seguridad de la Información del organismo en materia de Autenticación, Autorización y Control de Accesos a los efectos de mejorar la gestión de los procesos asociados.

Considerando el alcance y tareas desarrolladas, observaciones y opinión del auditado; puede señalarse que las medidas adoptadas para el proceso de GESTION DE ACCESOS del organismo resultan satisfactorias, con excepción de los aspectos 'Gestión de Privilegios' y 'Administración de Contraseñas Criticas' los cuales resultan aceptables. Se deberían solucionar los aspectos observados de acuerdo a los compromisos asumidos.

TILLAR Martin Omar

Firmado digitalmente por TILLAR Martin Omar
Fecha: 2022.12.29 12:40:27 -03'00'