INSTITUTO NACIONAL DE VITIVINICULTURA
Unidad de Auditoria Interna

INFORME EJECUTIVO
INFORME DE AUDITORIA INTERNA Nº 002/2020
TI - Gestión de Comunicaciones y Operaciones
Proyecto N° 2
Mendoza, 30 de Junio de 2020

SEÑOR PRESIDENTE:

OBJETIVO:

Evaluar el cumplimiento del marco normativo y reglamentario vigente, evaluando el sistema de control interno y la gestión con relación a los aspectos enunciados dentro de la "Política de Seguridad de la Información Modelo" (Decisión Administrativa 669/2004) bajo el punto: 'GESTIÓN DE COMUNICACIONES Y OPERACIONES'.
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° 2.

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 iniciaron durante el año 2019 (07/10/2019) no pudiendo finalizarse durante el periodo planificado. Durante el corriente año las mismas se extendieron desde el 17/02/2020 hasta el 30/06/2020. Las tareas se ajustaron a la evaluación de los siguientes objetivos de control:

- Cambios en las Operaciones
- Código Malicioso
- Aprobación del Sistema
- Seguimiento y revisión de los servicios de las terceras partes
- Separación entre Instalaciones de Desarrollo e Instalaciones Operativas
- Gestión del cambio de los servicios de terceras partes
- Registro de fallas
- Separación de Funciones
- Resguardo de la información
- Seguridad de los medios en tránsito
- Administración de medios informáticos removibles
- Procedimientos y controles de intercambio de la información
- Registro de auditoría
- Seguridad de la documentación del sistema
- Eliminación de medios de información
- Documentación de los Procedimientos Operativos
- Planificación de la Capacidad
- Provisión de servicio
- Código Móvil
- Gestión de Comunicaciones y Operaciones
- Registro de actividades del personal operativo
- Sistemas de acceso público
- Riesgos de seguridad
- Procedimientos de manejo de la información
- Seguridad del gobierno electrónico
- Protección de los registros
- Política de correo electrónico
- Redes
- Sincronización de relojes
- Registro de actividad de administrador y operador
- Seguridad de los la mensajería

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 los elementos en el organismo alcanzados por los objetivos de control del proyecto 02/09/2019
- Mediante nota NO-2019-91127299-APN-UAI#INV "Requerimientos Iniciales - Auditoría Res 669/2004 - Gestión de Comunicaciones y Operaciones" con fecha 7/10/2019 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 COMUNICACIONES Y OPERACIONES' siguiendo los lineamientos expuestos en la Decisión Administrativa 669/2004 "POLITICA DE SEGURIDAD DE LA INFORMACION" de la Jefatura de Gabinete para las siguientes categorías:
Procedimientos y responsabilidades operativas
- Gestión de provisión de servicios
- Planificación y aprobación de sistemas
- Protección contra código malicioso
- Respaldo o Backup
- Gestión de la red
- Administración y Seguridad de los Medios de Almacenamiento
- Intercambios de información y software
- Seguridad del Correo Electrónico
- Seguimiento y Control
- El día 24/10/2019 se recibió mediante nota NO-2019-95880753-APN-DIYC#INV, un pedido de prórroga en el plazo de entrega.
- El día 11/11/2019 se recibió mediante nota NO-2019-100931337-APN-DIYC#INV la documentación solicitada en los Requerimientos Iniciales, y se comenzó a analizar la misma.
- Los días 28/02/2020 y 02/03/2020 se realizó una revisión de los principales procedimientos asociados a actividades críticas (Dominio, Backup, Actualización Sistemas Operativos Servidores, Antivirus y Firewall) con el propósito de verificar la ejecución y cumplimiento de 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
- Especialista en sistemas operativos basados en software libre y comunicaciones digitales.
- En el marco de la emergencia sanitaria decretada el día 12/03/2020 y debido al incremento en la actividad del departamento de Informática y Comunicaciones asociado a los cambios en la modalidad de trabajo y procedimientos operativos, se postergó la comunicación de observaciones del presente proyecto.
- A partir del día 09/06/2020 se comenzaron a notificar las observaciones.

OBSERVACIONES MAS SIGNIFICATIVAS:

OBSERVACIÓN Nº 1	***NORMATIVA GESTIÓN DE COMUNICACIONES Y OPERACIONES DESACTUALIZADA***

La política de Seguridad de la Información del Organismo se encuentra desactualizada.- El capítulo de GESTIÓN DE COMUNICACIONES Y OPERACIONES no está formalizado por el organismo, no obstante el mismo ya se encuentra aprobado por el COTYSIC.

RECOMENDACIÓN

Reglamentar el capítulo de la política de Seguridad de la Información asociado a la Gestión de Indicentes de Seguridad en los plazos acordados con SIGEN.

ESTADO: En Trámite

OBSERVACIÓN Nº 4	***POLITICA ACTUALIZACION SOFTWARE BASE SERVIDORES LINUX INEXISTENTE***

No existe una política para la actualización del software de base de los servidores Linux implementados en el organismo. Hay varios equipos corriendo software con versiones sin soporte por parte del fabricante. Tampoco están adecuadamente formalizados las programas que no pueden ser actualizados por problemas de operatividad.

RECOMENDACIÓN

Se recomienda generar una política que especifique las frecuencias y condiciones que se seguiran para la actualización de los servidores con software libre del organismo, explicitando las excepciones a las mismas y su justificación.

ESTADO: S/A Correctiva Informada

OBSERVACIÓN Nº 7	***DATOS DE VIRUS SOPHOS MUY ANTIGUOS***

Se ha verificado en varios clientes Sophos que la última actualización de la base de virus tiene fecha febrero 2020. No obteniendo certeza si esto es correcto o producto de una desactualización del producto.

RECOMENDACIÓN

Se recomienda analizar y confirmar si hay una nueva versión de la base de virus y proceder en consecuencia.

ESTADO: Regularizada

OBSERVACIÓN Nº 9	***INEXISTENCIA RESGUARDO LOGS SEGURIDAD***

Los registros de seguridad de los servidores de dominio no se almacenan en cinta. En el caso de los logs de seguridad de los firewalls del organismo, existe un proceso pero el mismo no está funcionando motivo por el cual esos logs tampoco se resguardaban.

RECOMENDACIÓN

Se recomienda almacenar los logs de seguridad de los servidores críticos junto con el resguardo en cinta del organismo.

ESTADO: Regularizada

OBSERVACIÓN Nº 11	***PROCEDIMIENTO ADMINISTRACIÓN EQUIPAMIENTO REMOTO SIN FORMALIZAR***

El procedimiento para "ADMINISTRACIÓN DEL EQUIPAMIENTO REMOTO" no ha sido formalizado mediante normativa adecuada. Además está incompleto ya que faltan algunos datos importantes como la configruación de OpenVPN y de SSH implementada.

RECOMENDACIÓN

Se recomienda completar y formlizar el mencionado documento

ESTADO: S/A Correctiva Informada

OBSERVACIÓN Nº 18	***REGISTROS SEGURIDAD SERVIDORES INSUFICIENTES***

Los registros de seguridad de los servidores de dominio tienen activada la reescritura con en base a un registro de tamaño muy pequeño.

RECOMENDACIÓN

Se recomienda configurar de forma efectiva los REGISTROS SEGURIDAD en los servidores de dominio para evitar la perdida de información ante eventos de seguridad.

ESTADO: Regularizada

CONCLUSIONES:

En base a lo analizado, las observaciones realizadas y la opinión del auditado se considera necesario finalizar la confección de la nueva política de seguridad del organismo lo antes posible, y generar todos los procedimientos que de ella se desprenden para que se reflejen los cambios en las actividades producto de la extensa evolución tecnológica que ha sufrido el organismo en los últimos 10 años.

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.

GALINDO Fernando Antonio

Firmado digitalmente por GALINDO Fernando Antonio
Fecha: 2020.06.30 16:55:58 -03'00'