INSTITUTO NACIONAL DE VITIVINICULTURA
Unidad de Auditoria Interna

INFORME EJECUTIVO
INFORME DE AUDITORIA INTERNA Nº 008/2012
TI - Proceso de Desarrollo y Mant. de Sistemas
Proyecto N° 2
Mendoza, 11 de Junio de 2021

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 las 'Normas de Control Interno para Tecnología de la Información para el Sector Público Nacional' (Resolución 48/2005) bajo el punto: 'DESARROLLO, MANTENIMIENTO O ADQUISICIÓN DE SOFTWARE DE APLICACIÓN' y los aspectos enunciados en la "Política de Seguridad de la Información Modelo" (Decisión Administrativa 669/2004) bajo el punto: "ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS".

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 25/02/2021 hasta el 31/05/2021.
Se analizó el proceso de desarrollo y mantenimiento de todos los sistemas de información del organismo cuya modificación está bajo la órbita del Departamento de Información y Comunicaciones. Se incluyeron sistemas de Fiscalización y Apoyo de acuerdo a las categorías definidas por el organismo. Se excluyeron los sistemas mantenidos por otros organismos independientemente de donde se alojan los servidores.
Las tareas se ajustaron a la evaluación de los siguientes objetivos de control:

- Procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas.
- Formulación y documentación de requerimientos
- Criterio para el establecimiento de prioridades entre los distintos requerimientos.
- Tratamiento Solicitudes de emergencia.
- Aprobación de las áreas usuarias sobre las especificaciones elaboradas.
- Participación de la unidad de auditoría interna durante el desarrollo.
- Utilización de estándares de diseño, programación y documentación.
- Planificación y realización de pruebas en las distintas etapas del desarrollo.
- Pasaje del sistema aprobado desde el ambiente de desarrollo/prueba al de producción
- Control de las versiones del software.
- Preparación y actualización documentación de soporte.
- Capacitación al personal de las áreas usuarias y de la unidad de TI.
- Contratación de servicios externos de desarrollo y mantenimiento de sistemas.
- Requerimientos de seguridad de los sistemas.
- Seguridad en los sistemas de aplicación.
- Controles criptográficos.
- Seguridad de los archivos del sistema.
- Seguridad de los procesos de desarrollo y soporte.
- Gestión de vulnerabilidades técnicas .

Las tareas de campo se desarrollaron en Sede de la UAI y mediante la modalidad de teletrabajo, lo cual incluyó las tareas previas, el relevamiento y tareas posteriores vinculadas a la preparación y análisis de los datos recabados. No pudo realizarse la tarea in situ de comparación de los archivos en los servidores contra los del repositorio, debido a las restricciones vigentes relacionadas a la Pandemia del COVID-19 durante las fechas planificadas para dicha tarea.

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

- *Mediante nota NO-2021-29363607-APN-UAI#INV – "Requerimientos Iniciales" con fecha 05/04/2021 se solicitó al Jefe del Departamento de Informática y Comunicaciones, la información y documentación de respaldo asociada al "Proceso de Desarrollo, Mantenimiento y Adquisición de software de Aplicación" de acuerdo al siguiente detalle:*

- *Estándares aplicados durante las etapas de Análisis, Diseño, Programación y Documentación de las aplicaciones.*
- *Procedimiento para la formulación y documentación de los requerimientos por parte de las áreas usuarias.*
- *Procedimiento para la asignación de Prioridades sobre los requerimientos recibidos.*
- *Metodología utilizada para la aprobación de las Especificaciones de Análisis/Diseño.*
- *Procedimiento de Aseguramiento de la Calidad del Software / pruebas sobre los desarrollos realizados.*
- *Procedimiento utilizado para la aprobación formal del usuario a los desarrollos probados.*
- *Descripción de la implementación de la Política de uso de controles criptográficos del organismo en las actividades de desarrollo de software del organismo.*
- *Procedimiento de pasaje a producción*
- *Procedimiento de generación y actualización de versiones de software.*
- *Manual de usuario sistema de Versionado y Pasaje a Producción.*
- *Estándar de implementación y configuración GitLab.*
- *Detalle designación roles y responsabilidades pasaje a producción.*
- *Normativa de la asignación de Responsables técnicos para cada aplicación vigente en el organismo.*
- *Identificación (con numero de exp) de los servicios vigentes en el organismo durante el año 2020/2021.*

Además se requirió documentación técnica de las siguientes aplicaciones:

- *Sistema de Automotores*
- *DDJJ de Cosecha*
- *DDJJ de Espumantes*
- *Gestión Personal*
- *Listado resumido de los requerimientos de desarrollo/modificación realizados al departamento de informática durante el periodo 2020/2021 asociados a las aplicaciones arriba mencionadas.*
- *Listado resumido de las versiones pasados a producción durante el periodo 2020/2021 asociados a las aplicaciones arriba mencionadas.*

- *El día 12/04/2021 se recibió mediante nota NO-2021-31372231-APN-DIYC#INV, un pedido de prórroga en el plazo de entrega.*
- *El día 19/04/2021 se recibió mediante nota NO-2021-33792033-APN-DIYC#INV la respuesta a la documentación solicitada en los Requerimientos Iniciales, y se comenzó a analizar la misma.*
- *El día 19/04/2021 se obtuvo acceso al repositorio de código del organismo a través de un usuario veedor asociado al auditor de sistemas.*
- *El día 11/05/2021 se obtuvo acceso a los directorios de las aplicaciones que contenían la documentación técnica solicitada en los requerimientos iniciales.*
- *Se realizaron consultas mediante medios electrónicos y telefónicos a los siguientes funcionarios:*
  - *Jefe del Departamento de Informática y Comunicaciones*
  - *Administrador de Infraestructura*
  - *Jefe División Desarrollo*
- *A partir del día 21/05/2021 se comenzaron a notificar las observaciones.*

OBSERVACIONES MAS SIGNIFICATIVAS:

OBSERVACIÓN Nº 1	***DOCUMENTACIÓN CONTROLES NUEVOS DESARROLLOS INSUFICIENTE***

Los sistemas desarrollados bajo la nueva metodología no han incluido en su etapa de análisis/diseño la especificacón de controles que aseguren la validez de los datos ingresados o sobre los datos de salida. Además no se generó documentación para sobre estandares asociados al diseño y programación utilizados en los mismos.

RECOMENDACIÓN

Se recomienda incluir en la documentación de los nuevos desarrollos un detalle de los estándares de programación que deben implementarse en materia de seguridad del sistema, junto con un detalle de los controles que debe implementar el mismo desde el punto de vista operativo y de seguridad.

ESTADO: S/A Correctiva Informada

OBSERVACIÓN Nº 3	***AUTORIZACION DATOS PRUEBAS INFORMAL***

Se observa que no se ha identificado documentación formal de la autorización para la utilización de las bases operativas en el ambiente de pruebas.

RECOMENDACIÓN

Se recomienda formalizar la autorización para la utilización de bases de datos productivas en el ambiente de pruebas

ESTADO: S/A Correctiva Informada

OBSERVACIÓN Nº 4	***GESTIÓN DE VULNERABILIDADES INSUFICIENTE***

El organismo no realiza test de penetración en forma periódica para los sistemas que posee. Se han realizado algunas actividades aisladas las cuales han contribuido a mejorar la seguridad de las aplicaciones.

RECOMENDACIÓN

Se recomienda realizar en forma periodica revisiones de seguridad de los sistemas de información del organismo, ya se mediante servicios externos o capacitando al personal interno.

ESTADO: Con Acción Correctiva Informada

OBSERVACIÓN Nº 5	***METODOLOGÍA DESARROLLO, MANTENIMIENTO Y ADQUISICIÓN DE SOFTWARE APLICATIVO SIN REGLAMENTAR***

La metodología para las actividades de Análisis, Desarrollo y Mantenimiento de sistemas, generada por el DIC no ha sido reglamentada mediante mediante la normativa correspondiente. La comunicación mediante una nota no es un acto asministrativo suficiente para la implementación de la misma.

RECOMENDACIÓN

Se debe formalizar la metodología mediante un acto admninstrativo con el nivel correspondiente que detemine el procedimiento.

ESTADO: Con Acción Correctiva Informada

OBSERVACIÓN Nº 10	***REPOSITORIO EN GITLAB INCOMPLETO***

El repositorio de código fuente del organismo implementado en GITLab no incluye el código, ni la versión productiva de todos los sistemas vigentes del organismo.

RECOMENDACIÓN

Se recomienda incluir en el repositorio los sistemas que se encuentran en vigentes en el organismo no incluidos actualmente.

ESTADO: Regularizada

CONCLUSIONES:

De acuerdo a lo analizado, se han verificado significativos avances en la mayoría de los temas asociados con el proceso bajo revisión. Principalmente la adopción de una metodología de ciclo de vida de desarrollo de sistemas y la implementación de un software de versionado.
Considerando el alcance y tareas desarrolladas, observaciones y opinión del auditado; puede señalarse que las medidas adoptadas para el proceso de DESARROLLO y MANTENIMIENTO DE SISTEMAS del organismo resultan satisfactorias, debiendo solucionar los aspectos observados de acuerdo a los compromisos asumidos.

TILLAR
Martin Omar

Firmado digitalmente
por TILLAR Martin Omar
Fecha: 2021.06.11
12:17:44 -03'00'