INFORME EJECUTIVO
INFORME DE AUDITORIA INTERNA Nº 007/2018
TI - DA 669/2004 - Gestión de Accesos
Proyecto N° 5
Mendoza, 10 de Julio de 2018

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 ACCESOS".
El presente trabajo está incorporado en la Planificación Anual de la Unidad de Auditoria Interna para el corriente año como Proyecto N° 5.

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 19/2/2017 hasta el 10/07/2017.

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

- *Sistema de Administración de Contraseñas*
- *Camino Forzado*
- *Uso de Utilitarios de Sistema*
- *Política de Control de Accesos*
- *Restricción del Acceso a la Información*
- *Subdivisión de Redes*
- *Identificación y Autenticación de los Usuarios*
- *Limitación del Horario de Conexión*
- *Registración de Usuarios*
- *Autenticación de Usuarios para Conexiones Externas*
- *Trabajo Remoto*
- *Protección de los Puertos de Diagnóstico Remoto*
- *Registro y Revisión de Eventos*
- *Seguridad de los Servicios de Red*
- *Administración de Contraseñas Críticas*
- *Acceso a Internet*
- *Revisión de Derechos de Acceso de Usuarios*
- *Ruteo de Red*
- *Gestión de Privilegios*
- *Gestión de Contraseñas de Usuario*
- *Procedimientos y Áreas de Riesgo*
- *Conexión a la Red*
- *Protección de los Puertos de Diagnóstico Remoto*
- *Generación informes periódicos de gestión a la dirección.*

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 19/02/2018
- Mediante nota NO-2018-24828561-APN-UAI#INV 'Requerimientos Iniciales' con fecha 24/05/2018 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*
- *Inventario actualizado de los principales servidores de aplicación*
- *Inventario actualizado de servidores de base de datos productivos.*
- *Procedimiento formal de registro de usuarios para otorgar y revocar el acceso a los activos de información*
- *Metodología implementada para la declaración de confidencialidad asociada a los usuarios del organismo.*
- *Procedimiento para administración de contraseñas*
- *Listado de los usuarios registrados en los dominios del organismo*
- *Listado de los usuarios registrados en los servidores de base de datos del organismo.*
- *Identificación de cuentas de usuarios con las cuales es posible efectuar actividades críticas.*
- *Procedimiento para la administración de contraseñas de los usuarios identificados en el punto anterior (act. críticas)*
- *Detalle de redes y subredes implementadas en el organismo, incluyendo las rutas permitidas en cada una.*
- *Política implementada para el acceso a las diferentes redes del organismo.*
- *Listado de Redes Privadas Virtuales implementadas en el organismo.*
- *Procedimiento implementado para el acceso remoto a las redes del organismo.*
- *Listado de usuarios autorizados para el acceso remoto*
- *Detalle de las herramientas de acceso remoto instaladas en servidores y estaciones de trabajo, junto con la configuración las mismas.*
- *Documentación asociada a la definición de Grupos de acceso a Internet, junto con sus configuraciones*
- *Listado de cuentas genéricas implementadas en los principales servidores.*
- *Detalle de Documentación asociada a la política de desconexión y bloqueo de terminales.*
- *Documentación asociada a la política de usuarios locales habilitados en los servidores y equipos cliente.*
- *Detalle de Documentación asociada a la aplicación Administracion de Usuarios del sistema de gestión.*
- *Listado de perfiles implementados en la aplicación de Administracion de Usuarios .*
- *Metodología utilizada para el registro de modificaciones sobre el sistema de Administracion de Usuarios.*
- *Detalle de los reportes implementados en la aplicación de Administracion de Usuarios*
- *Documentación asociada a la Configuración de los registros de seguridad del dominio y de los servidores principales*
- *Procedimiento de monitoreo y revisión de registros de auditoria (logs) del dominio y los servidores principales*

- El día 01/06/2018 se recibió mediante nota NO-2018-26098224-APN-DIYC#INV, un pedido de prórroga en el plazo de entrega.
- El día 08/06/2018 se recibió mediante nota NO-2018-24828561-APN-UAI#INV la documentación solicitada en los Requerimientos Iniciales, y se comenzó a analizar la misma.
- Los días 23, 25 y 26/06/2018 se realizó una revisión de los principales servidores del organismo asociados a actividades críticas (Dominio; Base de Datos, 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 Base de Datos e infraestructura
  - Especialista en sistemas operativos basados en software libre y comunicaciones digitales.
- A partir del día 04/07/2018 se comenzaron a notificar las observaciones.

OBSERVACIONES MAS SIGNIFICATIVAS:

OBSERVACIÓN Nº 1	***NORMATIVA GESTION DE ACCESOS DESACTUALIZADO***

La política de Seguridad de la Información del Organismo se encuentra desactualizada.- NO está definido un capítulo de GESTION DE ACCESOS en el cual se cumplan los lineamientos señanlados en la “Política de Seguridad de la Información Modelo” aprobada por la ONTI.

RECOMENDACIÓN

Se recomienda avanzar con la confección del capítulo de "Gestión de Accesos" siguiendo los lineamientos señanlados en la "Política de Seguridad de la Información Modelo" aprobada por la ONTI.

ESTADO: En Trámite

OBSERVACIÓN Nº 4	***MODIFICACIONES ENTORNO PRODUCTIVO***

	PERSONAL DIV DESARROLLO

Se han identificados algunas modificaciones en los privilegios de los Sistemas de Gestión realizadas por usuarios de la div desarrollo. También se han detectado usuarios de la división desarrollo con nivel de acceso superusuario en el ambiente de producción.

RECOMENDACIÓN

El personal de la división desarrollo NO puede tener la posibilidad de modificar los datos en un entorno productivo, ya sea en una aplicación productiva o en la administración de usuarios.

ESTADO: En Trámite

OBSERVACIÓN Nº 9	***PROCEDIMIENTO ADMINISTRACION ACTIVIDADES CRITICAS INEXISTENTE***

El procedimiento de asignación temporaria de privilegios para efectuar actividades críticas no esta formalizado, lo cual dificulta el control de las actividades críticas realizadas por cuentas de usuarios habituales asociadas a personal del DIC .

RECOMENDACIÓN

Desarrollar un procedimiento documentado y normado de asigancián y seguimiento de privilegios para la ejecución de actividades críticas.

ESTADO: En Trámite

OBSERVACIÓN Nº 11	***USUARIOS DESARROLLO EN SERVIDORES DE BASE DE DATOS PRODUCTIVOS***

Segun lo informado se han identificado usuarios activos asociados a personal de la división desarrollo en los servidores de base de datos de producción de acuerdo al siguiente detalle:

- BMALPIVOT dlanzavechia, mmirabile,
- MALBEC6-2 dlanzavechia, mmirabile,
- MARSELAN dlanzavechia, mmirabile,
- HMENCIA fvidela

RECOMENDACIÓN

No permitir usuarios asociados a la división desarrollo en los servidores de base de datos productivos. Se debería capacitar a personal de la División Administración para que ejecute las tareas necesarias

ESTADO: S/A Correctiva Informada

OBSERVACIÓN Nº 14	***UTILIZACION USUARIOS CRITICOS GENERICOS EN FORMA HABITUAL***

Se identificó la utilización en forma regular/habitual de los usuarios genéricos Administrador en el dominio, root y postgres en el servidor HSEMILLON y de root en el Firewall.

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

OBSERVACIÓN Nº 18	***LOG SEGURIDAD SISTEMAS DE GESTION INEXISTENTE***

Los sistemas de gestión del organismo que se autentican vía ZIMBRA no registran ningún evento de seguridad. Para estos

sistemas no se generan registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

RECOMENDACIÓN

Se recomienda actualizar el sistema de validación y registro de usuario para los sistemas de gestión del organismo para que registren todos eventos relativos a la seguridad dispuestos por la política modelo.

ESTADO: En Trámite

OBSERVACIÓN Nº 19	***PROCEDIMIENTO REVISION DE REGISTROS DE AUDITORÍA INEXISTENTE***

No existe un procedimiento de monitoreo y revisión de registros de auditoria (logs) del dominio y los servidores principales que permita detectar fallas o amenazas antes de que los mismos se realice.

RECOMENDACIÓN

Desarrollar un procedimiento documentado y normado de revisión de registros de auditoría que especifique todos los aspectos relacionados con el control preventivo de los eventos almacenados.

ESTADO: En Trámite

OBSERVACIÓN Nº 20	***PROCEDIMIENTO MODALIDAD DE TRABAJO REMOTO INEXISTENTE***

La normativa vigente no contempla un procedimiento formalmente establecido donde se establezca el proceso de autorización del trabajo remoto, ambiente de trabajo, modalidad del trabajo permitido, revisión y monitoreo de la seguridad y procedimientos de auditoría específicos realizados regularmente sobre la utilización de los accesos remotos.

RECOMENDACIÓN

Desarrollar un procedimiento documentado y normado que regule la forma la modalidad de trabajo desde un lugar externo al orgaismo siguiendo los lineamientos señalados en la Política de Seguridad de la Información Modelo aprobada por la ONTI.

ESTADO: En Trámite

CONCLUSIONES:

Considerando el alcance y tareas desarrolladas puede señalarse que se presentan falencias en los aspectos de 'Requerimientos para el control de acceso', 'Administración de accesos de usuarios', 'Control de acceso al sistema operativo', 'Control de acceso a las aplicaciones', 'Monitoreo del acceso y uso de los sistemas' y 'Dispositivos móviles y trabajo remoto'; originadas en su mayoría en la falta de normativa actualizada. 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 aceptables, debiendo solucionar los aspectos observados de acuerdo a los compromisos asumidos.

GALINDO Fernando Antonio

Firmado digitalmente por GALINDO Fernando Antonio
Nombre de reconocimiento (DN): serialNumber=CUIL 20108466252, c=AR, cn=GALINDO Fernando Antonio
Fecha: 2018.07.10 17:33:40 -03'00'