2017

USUARIO ADMINISTRADOR DE PC'S

INFORME DE AUDITORÍA Nº 008/2017

Ministerio de
Trabajo, Empleo
y Seguridad Social

Unidad de Auditoría Interna

Ministerio de
Trabajo, Empleo
y Seguridad Social

UNIDAD DE AUDITORÍA INTERNA

Auditor Interno Titular
Lic. Ariel Ernesto DILEVA

Auditor Adjunto de Gestión de Recursos y Procesos de Apoyo
Dr. José Norberto DE NARDO

Supervisor de Auditoría de Tecnología de la Información
Lic. Maximiliano Antonio IORGI

Auditor Técnico
Sr. Alberto Carlos IGLESIAS

Contenido

INFORME EJECUTIVO

INFORME ANALÍTICO

INFORME

EJECUTIVO

INFORME EJECUTIVO DE AUDITORÍA

USUARIO ADMINISTRADOR DE PC'S

I) OBJETO

Examinar la asignación de derechos de "Administrador de PC's" a usuarios de recursos informáticos, el procedimiento para su habilitación y las medidas de control adoptadas al respecto por la Dirección General de Informática e Innovación Tecnológica (en adelante DGIIT), dependiente de la Subsecretaría de Coordinación.

II) ALCANCE

La tarea fue realizada en el período comprendido entre los meses de enero y marzo de 2017, de acuerdo con las Normas de Auditoria Interna Gubernamental aprobadas por Resolución SIGEN Nº 152/2002, aplicándose algunos de los procedimientos allí enumerados u otros que se consideraron necesarios en la circunstancia.

El informe se encuentra referido a las observaciones y recomendaciones sobre el objeto de la tarea hasta el período precedentemente indicado y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido

III) PRINCIPALES OBSERVACIONES Y RECOMENDACIONES

A continuación se transcriben las principales observaciones[1] y recomendaciones:

2. Observación

De acuerdo a la información relevada con el SCCM y a una calificación realizada por la CSI, surge que existen 106 aplicaciones. En el Anexo A se expone la nómina de tales aplicaciones instaladas que podrían poner en riesgo la seguridad, integridad y confidencialidad de la información y red del Organismo.

Unidad Auditoría Interna MTEySS

[1] **El número de observación detallado guarda correspondencia con el asignado en el Informe de Auditoría Analítico.**

Recomendación

La DGIIT, por intermedio de las áreas que intervienen en la autorización y control de los usuarios Administradores de PC's, debe evaluar los casos críticos y, en los casos que corresponda, proceder a su desinstalación previa comunicación a los respectivos usuarios.

3. Observación

Del relevamiento realizado sobre el circuito administrativo utilizado en el alta de los Usuarios Administradores de Pc's, surge que la CSI no interviene en el mismo.

Recomendación

La DGIIT debe evaluar el circuito administrativo descripto en el **Anexo B** y contemplar la intervención de la CSI en forma activa, realizando tareas de control o verificación sobre el usuario y su equipo en forma previa, establecer contacto a modo informativo con el usuario solicitante y comunicarle sus responsabilidades y los riesgos que involucra este tipo de permisos.

10. Observación

Se verifican demoras significativas en el proceso de remediación de los hallazgos detectados por la CSI en sus actividades de monitoreo. Esta situación incrementa el nivel del riesgo de control.

Recomendación

La DOyS junto con la CSI deben evaluar el procedimiento establecido como resultante del Monitoreo de Usuarios Administradores, establecer un cronograma para las acciones de monitoreo y reducir el tiempo insumido hasta la remediación de los hallazgos.

IV) CONCLUSIÓN

Sobre la base de las tareas desarrolladas, conforme al objeto y al alcance de las mismas, esta Unidad de Control estima que el procedimiento y las medidas de control adoptadas para la asignación de derechos de "Administrador de PC's" resultan adecuados.

Unidad Auditoría Interna MTEySS

De la respuesta brindada al Informe Preliminar se desprende el reconocimiento de los hallazgos formulados y la adopción de acciones correctivas que permitirán reducir el nivel de riesgo en aspectos vinculados a la seguridad, integridad y confidencialidad de la información y red del Organismo.

Buenos Aires, 3 de abril de 2017.

Lic. Maximiliano Antonio IORGI
Supervisor de Auditoría de
Tecnología de la Información

Dr. CP José Norberto DE NARDO
Auditor Adjunto de Gestión de Recursos y
Procesos de Apoyo

Lic. Ariel Ernesto DILEVA
Auditor Interno Titular

INFORME

ANALÍTICO

INFORME DE AUDITORÍA ANALÍTICO

USUARIO ADMINISTRADOR DE PC'S

I) OBJETO

Examinar la asignación de derechos de "Administrador de PC's" a usuarios de recursos informáticos, el procedimiento para su habilitación y las medidas de control adoptadas al respecto por la Dirección General de Informática e Innovación Tecnológica (en adelante DGIIT), dependiente de la Subsecretaría de Coordinación.

II) ALCANCE

La tarea fue realizada en el período comprendido entre los meses de enero y marzo de 2017, de acuerdo con las Normas de Auditoria Interna Gubernamental aprobadas por Resolución SIGEN Nº 152/2002, aplicándose algunos de los procedimientos allí enumerados u otros que se consideraron necesarios en la circunstancia.

El informe se encuentra referido a las observaciones y recomendaciones sobre el objeto de la tarea hasta el período precedentemente indicado y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido

III) ANTECEDENTES

NORMATIVOS

- Ley N° 24.156 - Ley de Administración Financiera y de los Sistemas de Control del Sector Público Nacional.
- Decreto N° 1344/2007 – Aprueba el Reglamento de la Ley de Administración Financiera y de los Sistemas de Control del Sector Público Nacional N° 24.156;
- Resolución SGN N° 152/2002 – Aprueba las "Normas de Auditoría Interna Gubernamental".
- Resolución SGN N° 172/2014 – Aprueba las "Normas Generales de Control Interno".
- Resolución MTEySS 1012/2014 – Aprueba las "Políticas de Seguridad de la Información del MTEySS".

Unidad Auditoría Interna MTEySS

- Resolución SSC N° 267/2015 – Aprueba el "Manual de Reglas de Gestión de Seguridad Informática".

DOCUMENTALES

- Formulario "Gestión de Privilegios Avanzados sobre Equipos";
- DTACyR-0005-10 – Documento Técnico - Permisos Temporales;
- SSC-DPR-DGIIT-DOyS-01 - Creación Cuentas Recursos;
- SSC-POI-DGIIT-14.07.07 - Administración de Información de Puestos de Trabajo;
- SSC-POI-DGIIT-14.08.01 - Gestión de Usuarios con Privilegios Avanzados en Puestos de Trabajo;
- Informe de "Monitoreo de Usuarios Administradores" Ejecuciones 2016 – 2017 elaborado por la Coordinación de Seguridad Informática (CSI) de la DGIIT;

INFORMÁTICOS

- Permiso de acceso de solo lectura al sitio de intranet del Sector Administración Cuentas y Recursos (ACyR): http://intranet/Lists/PermisosTemporalesBis/AllItems.aspx
- Detalle de Solicitudes (SR) registradas en el aplicativo informático *System Center Service Manager* (SCSM) al 12/01/2017;
- Reporte del *System Center Configuration Manager* (SCCM) generado por el área de Microinformática;

MARCO DE REFERENCIA

Se denomina usuario a una persona física u organismo que utiliza los recursos informáticos que el MTEySS pone a su disposición. Para ello debe poseer una "cuenta de acceso" asignada por el administrador de sistemas.

Existe la posibilidad que un usuario sea "Administrador de su puesto de trabajo", situación que lo habilita a realizar ciertas actividades críticas, como ser la instalación y administración de sistemas y de hardware no homologados, parametrización de preferencias (ej. fecha y hora), modificación de registros, habilitación y deshabilitación de servicios, instalación/actualización de aplicativos, creación, modificación y eliminación de cuentas, tener acceso a todos los archivos del sistema, compartir recursos locales con otros puestos de trabajo, etc.

Unidad Auditoría Interna MTEySS

Tal configuración representa un riesgo potencial a la seguridad de la información del organismo, pero se pueden otorgar dichos privilegios avanzados cuando se presente la necesidad. Para ello debe realizarse una solicitud formal a través del formulario electrónico "Privilegios Avanzados sobre Equipos" que se encuentra en la intranet, acompañando una adecuada fundamentación y justificación del pedido.

IV) TAREA REALIZADA

Descripción

La tarea realizada consistió en la ejecución de los siguientes procedimientos de auditoría y/o verificaciones:

1. Análisis normativo;
2. Recopilación de documentación;
3. Entrevistas con personal responsable del área ACyR, vinculados en la administración y creación de usuarios y otorgamiento de permisos a usuarios;
4. Entrevistas con personal del área Microinformática.
5. Entrevistas con personal de la CSI, responsable del monitoreo y cumplimiento de las Políticas de Seguridad del Organismo;
6. Consulta y obtención de información y documentación del sitio de intranet perteneciente al área ACyR de la Dirección de Operaciones y Servicios de la DGIIT, destinado al seguimiento de solicitudes (SR);
7. Relevamiento del circuito administrativo;
8. Solicitud y obtención y análisis de documentación de respaldo;
9. Generación de un reporte con el listado de usuarios administradores de puestos de trabajo;
10. Generación de un reporte con el detalle de los aplicativos informáticos instalados en puestos de trabajo de usuarios con privilegios de administrador local.

En forma previa a la emisión del presente Informe de Auditoria, se remitió a la DGIIT un "Informe Preliminar" a fin que efectuara los comentarios que estimase apropiados. Bajo el acápite "Respuesta del Sector Auditado", se incorporan al presente informe los comentarios efectuados por la DGIIT mediante Nota Nº ME-2017-04841976-APN-DGIIT#MT, recibida el 29/03/2017.

Unidad Auditoría Interna MTEySS

V) DESCRIPCIÓN, OBSERVACIONES Y RECOMENDACIONES

A continuación se describen los aspectos verificados, las observaciones surgidas de la labor y las recomendaciones que esta Unidad de Control sugiere para optimizar la gestión y operatoria en aquellos aspectos que constituyeron materia de examen.

A.- Análisis de puestos de trabajo

Descripción

La DGIIT posee una herramienta informática denominada *"System Center Configuration Manager 2007" (SCCM),* que permite obtener un detalle de los usuarios que poseen derechos de acceso como administrador en los puestos de trabajos conectados a la red del Organismo.

Como resultado de una consulta realizada por intermedio del SCCM se obtuvo la siguiente información:

TIPO	CANTIDAD
Clientes Activos[1]	2.332
Clientes Inactivos[2]	165
Clientes No Instalados[3]	17
Registros de equipos con administradores	82

De acuerdo a la información relevada con el SCCM en los equipos utilizados por Administradores de PC's, se obtuvo un detalle de 17.790 aplicaciones instaladas en 74 equipos. Luego del análisis realizado por esta Unidad de Auditoría Interna se remitió a la Coordinación de Seguridad Informática un listado conteniendo 2.902 aplicaciones para que las evalúen y clasifiquen, ya que podrían comprometer la seguridad, integridad y confidencialidad de la información del Ministerio y el normal funcionamiento de la red de datos.

RIESGO	ALTO	MEDIO	BAJO	NULO	TOTAL
Cantidad	44	62	314	2482	**2902**

Unidad Auditoría Interna MTEySS

[1] Clientes Activos: Es un equipo con el agente de recolección de datos instalado y funcionando que reporta al servidor al menos en los últimos 7 días.
[2] Clientes Inactivos: Son equipos con el agente de recolección de datos instalado cuya última fecha de reporte es mayor a 7 días.
[3] Clientes no instalados: Son equipos detectados en la red a los cuales no pudo instalarse el cliente de reporte de forma automática.

1. Observación

La herramienta SCCM no permite identificar la totalidad de los equipos conectados a la Red, debido a situaciones tales como Clientes Inactivos o No Instalados. Estas limitaciones impiden determinar con certidumbre el universo de usuarios habilitados como "Administrador de PC's".

Recomendación

La DGIIT deberá planificar una revisión del software instalado (cliente) en los puestos de trabajo y evaluar las medidas necesarias para escanear los equipos que se encuentran en desuso, con el fin de relevar el universo de puestos de trabajo conectados a la red del Organismo y optimizar los controles sobre los usuarios que tengan asignados derechos de acceso como "Administradores de PC's".

Respuesta del Sector Auditado

Existen dos casos a evaluar:

1. *Cliente no instalado: Se generara una planificación semanal de Mitigación de los clientes no instalados, generando tras cada detección un SR con los Equipos donde se deberá instalar el cliente faltante. Actualmente se encuentran 7 clientes no instalados, se registraron para mitigación en la SR996365 con fecha de finalización provisoria 07/04/2017*
2. *Clientes Inactivos: A través de la RES SSC 267-2015 - Manual de Reglas Gestión Seguridad Informática, Pagina 45 "Administración de Cuentas de equipo en Sistema Operativo de Red, Punto C de la narrativa se define Inactividad. Las cuentas de equipos qua presenten un periodo de Inactividad mayor a 45 (cuarenta y cinco) días deberán ser dadas de baja.*

   Considerando dicha definición se modificara la configuración del cliente de SCCM para contabilizar los equipos inactivos como aquellos que no responden pasados los 45 días. A partir de este momento dichos equipos se darán de baja en Active Directory siguiendo la normativa indicada.

Fecha de Cumplimiento: 28/04/2017

Opinión UAI

De acuerdo con la respuesta brindada, el área se encuentra desarrollando acciones a efectos de regularizar la observación. Su efectivo cumplimiento y los resultados que se obtengan serán verificados en próximas tareas de auditoría.

Unidad Auditoría Interna MTEySS

2. Observación

De acuerdo a la información relevada con el SCCM y a una calificación realizada por la CSI, surge que existen 106 aplicaciones. En el **Anexo A** se expone la nómina de tales aplicaciones instaladas que podrían poner en riesgo la seguridad, integridad y confidencialidad de la información y red del Organismo.

Recomendación

La DGIIT, por intermedio de las áreas que intervienen en la autorización y control de los usuarios Administradores de PC's, debe evaluar los casos críticos y, en los casos que corresponda, proceder a su desinstalación previa comunicación a los respectivos usuarios.

Respuesta del Sector Auditado

La CSI analizará las aplicaciones detalladas en el Anexo A e identificará los casos más críticos.

Luego realizará una comunicación formal, a través de la DGIIT, a los usuarios afectados y a sus responsables para informar los riesgos asociados.

Finalizada la comunicación, la CSI aportará un listado a la DOyS con el detalle del software que debe ser desinstalado.

Fecha de Cumplimiento: 30/06/2017

Opinión UAI

De acuerdo con la respuesta del Sector Auditado, se receptó favorablemente la observación efectuada y ha iniciado acciones tendientes a sanearla. Su efectiva aplicación será objeto de verificaciones en próximas tareas de control.

B.- Registros y Procedimientos establecidos para la Gestión de Administración Local de Puestos de Trabajo

Descripción

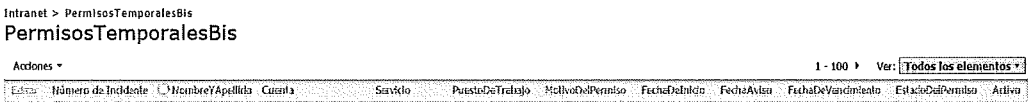
La DGIIT posee dentro del área de Intranet y Soporte Funcional de Aplicativos (IySFA) un sector denominado "Administración de Cuentas y Recursos" (ACyR), que se encarga del ABM de solicitudes de Administrador de PC's derivadas desde el área de Mesa de Ayuda (SR). En el **Anexo B** se detalla el circuito administrativo relevado.

Unidad Auditoría Interna MTEySS

El sector ACyR mantiene dos registros en su sitio de intranet, bajo el siguiente esquema:

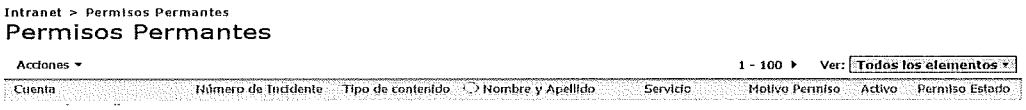
- Registros Temporales

  http://intranet/Lists/PermisosTemporalesBis/AllItems.aspx



- Registros Permanentes

  http://intranet/Lists/PermisosPermantes/AllItems.aspx



3. Observación

Del relevamiento realizado sobre el circuito administrativo utilizado en el alta de los Usuarios Administradores de Pc's, surge que la CSI no interviene en el mismo.

Recomendación

La DGIIT debe evaluar el circuito administrativo descripto en el **Anexo B** y contemplar la intervención de la CSI en forma activa, realizando tareas de control o verificación sobre el usuario y su equipo en forma previa, establecer contacto a modo informativo con el usuario solicitante y comunicarle sus responsabilidades y los riesgos que involucra este tipo de permisos.

Respuesta del Sector Auditado

La CSI gestionará, ante la DOyS, la inclusión de una nueva actividad en el circuito administrativo de alta para evaluar la pertinencia de cada solicitud.

La CSI contactara a los usuarios solicitantes e intervendrá el formulario electrónico de solicitud.

Cada nueva solicitud será derivada a la CSI mediante formulario electrónico de sharepoint.

Fecha de Cumplimiento: 28/04/2017

Opinión UAI

El Sector Auditado receptó favorablemente la recomendación efectuada. La efectiva aplicación de las acciones propuestas será objeto de verificaciones en futuras tareas de control.

Unidad Auditoría Interna MTEySS

4. Observación

Del cotejo entre los agentes que integran el Registro Temporal del área de ACyR y el detalle obtenido de la herramienta SCCM, surgen las siguientes diferencias:

TIPO	CANTIDAD
Usuarios registrados sin información en SCCM	**18**
Usuarios identificados por el SCCM que no poseen registro temporal	**16**

Respuesta del Sector Auditado

Se analizarán estos casos para poder determinar la situación de cada uno.

5. Observación

Se han detectado dos usuarios que acceden en condición de Administradores de PC a más de un equipo y no han cumplimentado las solicitudes correspondientes:

ETIQUETAS DE FILA	JPOCOVI	VMARUCHNIAK
PC05587	Sin SR	
PC05594	SR861567	
PC05604		Sin SR
PC3132		SR915931

Recomendación

La Dirección de Operaciones y Servicios (DOyS), en particular el área de ACyR, deberá automatizar este tipo de controles y proceder a la baja de aquellos usuarios que no consten en sus registros.

Respuesta del Sector Auditado

- *PC05587 - JPOCOVI --> Se quitó el acceso mediante IR804167.*
- *PC05594 - JPOCOVI --> SR861567 registro valido y actualmente vigente.*
- *PC05604 - VMARUCHNIAK --> Se normalizó mediante SR928835.*
- *PC3132 - VMARUCHNIAK --> SR91931 registrado valido y actualmente vigente. Este acceso fue otorgado para el usuario instale el software necesario para sus tareas diarias.*

Se agregó como rutina la verificación diaria de los registros temporales vs OU de Administradores. Se gestionará con Soporte Técnico el acceso al reporte de Administradores de PC para realizar los crucen necesarios de información para validar las bajas de usuarios administradores.

Unidad Auditoría Interna MTEySS

Opinión UAI

De acuerdo con la respuesta del Sector Auditado, la Observación Nº 4 está en proceso de regularización y la Observación Nº 5 ya fue regularizada.

6. Observación

Se han detectado dos usuarios locales que no se encuentran registrados por él área de ACyR en su portal colaborativo:

EQUIPO	GRUPO	CUENTA	TIPO	DOMINIO	TIPO DE DOMINIO
NOT00126	Administradores	usuario	UserAccount	NOT00126	Local
PC06290	Administradores	admincaut	UserAccount	PC06290	Local

Recomendación

La DGIIT debe verificar la existencia de los casos detallados y proceder a la regularización o baja de los mismos.

Respuesta del Sector Auditado

- *NOT00126 se deshabilitó la cuenta del equipo mediante IR804167.*
- *PC06290 se quitó al usuario JLARA y por lo tanto la PC se movió a una OU de no administradores, mediante IR804167. Por lo tanto el usuario admincaut pierde también los privilegios de Administrador.*

La CSI aportará a la DOyS un listado actualizado con los hallazgos del PGV.

Opinión UAI

De acuerdo con la respuesta del Sector Auditado, receptó favorablemente la recomendación efectuada. La observación fue regularizada.

7. Observación

Se ha detectado un usuario administrador local cuya denominación es genérica, no posee formulario de solicitud y no se han cumplido los pasos correspondientes para su aprobación.

NÚMERO DE INCIDENTE	USUARIO	TIPO DE CONTENIDO
SR900172	USERWALLASCENSORES	Solicitud de Permiso Permanente

Unidad Auditoría Interna MTEySS

Respuesta del Sector Auditado

Se generaron los formularios electrónicos.

La CSI recomienda que el administrador de la cuenta "USERWALL ASCENSORES" o un responsable de la DOyS cargue el formulario.

8. Observación

Se ha detectado un usuario administrador local inactivo que no posee formulario de gestión de permiso permanente al servicio de administración de PC.

NÚMERO DE INCIDENTE	SERVICIO	TIPO DE CONTENIDO	MOTIVO PERMISO	ACTIVO
SR522444	Administrador de PC	Permiso Permanente	Accesos para Autoridades	No

Recomendación

La DGIIT por intermedio de las áreas que corresponda debe establecer controles periódicos sobre aquellos usuarios que no hayan cumplimentado los pasos previstos para la gestión de solicitudes y accesos a servicios.

Por otra parte, debe evaluar la vigencia y pertinencia de los accesos otorgados en los 2 casos detallados y proceder en consecuencia.

Respuesta del Sector Auditado

1. *El registro de permisos temporales del caso informado se encuentra finalizado el 06/01/2017. Este acceso fue autorizado por Microinformática. La pc fue deshabilitada por inactividad el día 14/11/2016.*
2. *Se agregó como rutina la verificación diaria de los registros temporales vs OU de Administradores. Se gestionará con Soporte Técnico el acceso al reporte de Administradores de PC para realizar los crucen necesarios de información para validar las bajas de usuarios administradores.*

Opinión UAI

Habiéndose receptado favorablemente la recomendación de esta Unidad de Control, las Observaciones Nros. 7 y 8 fueron regularizadas.

Unidad Auditoría Interna MTEySS

9. Observación

Se han detectado usuarios administradores locales registrados por el área ACyR cuyos permisos temporales exceden los 12 meses de vigencia que establece la Regla de "Gestión de Usuarios con Privilegios Avanzados en Puestos de Trabajo" (SSC-POI-DGIIT-14.08.01):

Número de Incidente	Puesto de Trabajo	Fecha del Inicio	Fecha Aviso	Fecha de Vencimiento	Cantidad Días	Estado del Permiso	Activo
SR905050	PC04724	02/01/2017	17/01/2018	01/02/2018	395	Vigente	Si
SR787831	PC06289	02/09/2016	29/08/2017	13/09/2017	376	Vigente	Si
SR563875	PC05590	28/01/2016	13/01/2017	28/01/2017	366	Vigente	Si

Recomendación

La DGIIT debe evaluar y revisar los casos detallados y proceder a su corrección de acuerdo a las reglas vigentes. Resulta oportuno resaltar la necesidad de controles en los formularios de carga de datos respecto de las fechas de inicio y fin del servicio.

Respuesta del Sector Auditado

Analizando los casos entendemos que los tiempos de permanencia de los permisos se excedieron debido a la demora en la firma por parte del responsable y por ende la carga y ejecución del requerimiento.

Se propuso a la CSI que intervenga en el formulario electrónico registrando la fecha de caducidad del permiso, lo cual facilitará y clarificará la fecha de fin de los permisos sin tener en cuenta la demora en el circuito.

Opinión UAI

De acuerdo con la respuesta del Sector Auditado, se receptó favorablemente la recomendación efectuada. En futuras actividades de seguimiento se examinará la implementación de las medidas propuestas.

C.- Actividades de Control y Monitoreo

Descripción

En el marco del Proceso de Gestión de Vulnerabilidades, aprobado por Disposición DGIIT Nº 2/2015, la Coordinación de Seguridad Informática ejecuta periódicamente dos verificaciones sobre los usuarios administradores en puestos de trabajo:

1º. Identifica qué usuarios administradores carecen de registro en la lista de permisos temporales.

2º. Identifica qué usuarios administradores tienen permisos vencidos, evaluando la fecha de finalización registrada por Administración de Cuentas y Recursos en la lista de permisos temporales.

Para llevar a cabo tales verificaciones, en el marco de su cronograma de actividades, la CSI consulta el relevamiento de usuarios efectuado por la herramienta SCCM y cruza

Unidad Auditoría Interna MTEySS

esta información con la lista de permisos temporales a cargo del área Administración de Cuentas y Recursos.

Del análisis de la información provista por la CSI sobre los hallazgos detectados en las verificaciones realizadas entre febrero del 2016 y enero del 2017, surgen los siguientes resultados:

ESTADO	FEB/2016	ABR/2016	JUN/2016	SEPT/2016	ENE/2017
Detectados (Hallazgos)	149	163	177	51	55
Pendientes (Hallazgos)	121	140	38	32	3
Remediación (Promedio en días)	89	119	153	257	154

La periodicidad de los controles denota una reducción en la cantidad de detecciones, como así también una disminución de los hallazgos pendientes de remediación;

10. Observación

Se verifican demoras significativas en el proceso de remediación de los hallazgos detectados por la CSI en sus actividades de monitoreo. Esta situación incrementa el nivel del riesgo de control.

Recomendación

La DOyS junto con la CSI deben evaluar el procedimiento establecido como resultante del Monitoreo de Usuarios Administradores, establecer un cronograma para las acciones de monitoreo y reducir el tiempo insumido hasta la remediación de los hallazgos.

Respuesta del Sector Auditado

La CSI utiliza un cronograma de monitoreo aprobado por la DGIIT en el marco del Proceso de Gestión de Vulnerabilidades. Se adjunta.

Se agregó como rutina la verificación diaria de los registros temporales vs OU de Administradores. Se gestionará con Soporte Técnico el acceso al reporte de Administradores de PC para realizar los crucen necesarios de información para validar las bajas de usuarios administradores.

Los tiempos de remediación los administra la DOyS.

Opinión UAI

De acuerdo con la respuesta del Sector Auditado, se receptó favorablemente la observación efectuada. La CSI está impulsando acciones tendientes a su regularización, las cuales serán verificadas en futuras actividades de seguimiento.

Unidad Auditoría Interna MTE/SS

11. Observación

El detalle de las responsabilidades de la DGIIT y del usuario expuesto en el formulario "Gestión de Privilegios Avanzados Sobre Equipos" **(Anexo C)**, no se encuentra referenciado con las Políticas de Seguridad de la Información del Ministerio (Res. MTEySS N° 1012/2014), lo cual se estima necesario atento que en ciertos casos no existe una correspondencia con éstas últimas.

Recomendación

La DGIIT debe, para un mejor entendimiento de las responsabilidades de las partes, precisar para cada ítem del formulario la referencia normativa en que se sustenta.

Respuesta del Sector Auditado

La CSI gestionará la actualización del contenido del formulario de "Gestión de Privilegios Avanzados sobre Equipos" para que este contenga la referencia a las Políticas de Seguridad de la Información aprobadas por Res. MTEySS 1012/14.

La CSI enviará un GDE a la DOyS con el nuevo contenido del formulario para su actualización.

Fecha de Cumplimiento: 28/04/2017

Opinión UAI

Las acciones enunciadas se consideran pertinentes. Su efectiva implementación, será objeto de evaluación por parte de esta Unidad de Control mediante el desarrollo de tareas de seguimiento.

Resumen General de Observaciones

En el **Anexo D** se enumeran las observaciones descriptas precedentemente con el detalle para cada una de ellas de la siguiente información: a) Área y sub-área/s temática/s a las que se encuentran referidas; b) Calificación de impacto; c) Estado de situación; y d) Área/s Responsable/s que deben impulsar las acciones correctivas.

Resumen

Observaciones según su estado de situación				
Regularizada	**En Trámite**	**Sin Acción Correctiva**	**No Compartida**	**No Regularizable**
4	7	0	0	0
Total: 11 Observaciones				

Unidad Auditoría Interna MTEySS

VI) CONCLUSIÓN

Sobre la base de las tareas desarrolladas, conforme al objeto y al alcance de las mismas, esta Unidad de Control estima que el procedimiento y las medidas de control adoptadas para la asignación de derechos de "Administrador de PC's" resultan adecuados.

De la respuesta brindada al Informe Preliminar se desprende el reconocimiento de los hallazgos formulados y la adopción de acciones correctivas que permitirán reducir el nivel de riesgo en aspectos vinculados a la seguridad, integridad y confidencialidad de la información y red del Organismo.

Buenos Aires, 3 de abril de 2017

Lic. Maximiliano Antonio IORGI Supervisor de Auditoría de Tecnología de la Información	Dr. CP José Norberto DE NARDO Auditor Adjunto de Gestión de Recursos y Procesos de Apoyo	Lic. Ariel Ernesto DILEVA Auditor Interno Titular

ANEXOS

ANEXO A

Software Instalado que presenta un Nivel de Riesgo Significativo

NIVEL DE RIESGO ALTO			
NRO.	SOFTWARE	AREA	DETALLE
1	Advertising Center	Security Threat	Software con contenido malicioso (AdWare)
2	Claro Internet	Device Drivers, Configuration, and Utilities	Driver para conectividad mediante Claro.
3	EnCase v6.8	Security	Software especifico de Seguridad Informatica
4	eye perform	Security Threat	Software con contenido malicioso (AdWare)
5	FortiClient	Security	Software especifico de Seguridad Informatica
6	Its Results Hub	Security Threat	Software con contenido malicioso (AdWare)
7	Microsoft Application Virtualization (App-V) Client	Virtualization Software	Software de Virtualizacion en estacion de trabajo.
8	Microsoft Application Virtualization (App-V) Client x64	Virtualization Software	Software de Virtualizacion en estacion de trabajo.
9	Microsoft Application Virtualization (App-V) Client x86	Virtualization Software	Software de Virtualizacion en estacion de trabajo.
10	Microsoft Application Virtualization Desktop Client	Application and Collaboration Servers	Software de Virtualizacion en estacion de trabajo.
11	Microsoft Virtual PC 2007 SP1	Virtualization Software	Software de Virtualizacion en estacion de trabajo.
12	Movistar 3.5G	Device Drivers, Configuration, and Utilities	Driver para conectividad mediante Movistar.
13	Oracle VM VirtualBox 4.2.18	Information and Data Management	Software de Virtualizacion en estacion de trabajo.
14	Oracle VM VirtualBox 4.3.10	Information and Data Management	Software de Virtualizacion en estacion de trabajo.
15	Oracle VM VirtualBox 4.3.20	Information and Data Management	Software de Virtualizacion en estacion de trabajo.
16	Oracle VM VirtualBox 4.3.6	Information and Data Management	Software de Virtualizacion en estacion de trabajo.
17	Oracle VM VirtualBox 5.0.14	Information and Data Management	Software de Virtualizacion en estacion de trabajo.
18	Oracle VM VirtualBox 5.0.16	Information and Data Management	Software de Virtualizacion en estacion de trabajo.
19	Oracle VM VirtualBox 5.1.6	Unidentified	Software de Virtualizacion en estacion de trabajo.
20	Oracle VM VirtualBox 5.1.8	Unidentified	Software de Virtualizacion en estacion de trabajo.
21	Personal Internet	Unidentified	Driver para conectividad mediante Personal.

Unidad Auditoría Interna MTEySS

NIVEL DE RIESGO ALTO			
NRO.	SOFTWARE	AREA	DETALLE
22	Proxy Master	Unidentified	Software de acceso remoto
23	Python 2.7 (64-bit)	Frameworks and Support	Desarrollo en Python.
24	Python 2.7.12 (64-bit)	Frameworks and Support	Desarrollo en Python.
25	Python 2.7.8 (64-bit)	Frameworks and Support	Desarrollo en Python.
26	Python 3.5.0 Core Interpreter (32-bit)	Development Resources	Desarrollo en Python.
27	Python 3.5.0 Development Libraries (32-bit)	Development Resources	Desarrollo en Python.
28	Python 3.5.0 Documentation (32-bit)	Development Resources	Desarrollo en Python.
29	Python 3.5.0 Executables (32-bit)	Development Resources	Desarrollo en Python.
30	Python 3.5.0 Launcher (32-bit)	Development Resources	Desarrollo en Python.
31	Python 3.5.0 pip Bootstrap (32-bit)	Development Resources	Desarrollo en Python.
32	Python 3.5.0 Standard Library (32-bit)	Development Resources	Desarrollo en Python.
33	Python 3.5.0 Tcl/Tk Support (32-bit)	Development Resources	Desarrollo en Python.
34	Python 3.5.0 Test Suite (32-bit)	Development Resources	Desarrollo en Python.
35	Python 3.5.0 Utility Scripts (32-bit)	Development Resources	Desarrollo en Python.
36	Python Tools Redirection Template	Development Resources	Desarrollo en Python.
37	VMware Player	Virtualization Software	Software de Virtualizacion en estacion de trabajo.
38	VMware Player	Development Tools	Software de Virtualizacion en estacion de trabajo.
39	WibuKey Setup (WibuKey Remove)	Security	Software especifico de Seguridad Informatica
40	WinPcap 4.1.2	Networking Software	Software para lectura de trafico de red.
41	WinPcap 4.1.3	Networking Software	Software para lectura de trafico de red.
42	Wireshark 1.12.7 (64-bit)	Networking Software	Software de monitoreo de conexiones
43	Wireshark 2.0.7 (64-bit)	Networking Software	Software de monitoreo de conexiones
44	Yahoo Search Set	Security Threat	Software con contenido malicioso (AdWare)

NIVEL DE RIESGO MEDIO			
NRO.	SOFTWARE	AREA	DETALLE
45	Apache Tomcat 8.0.15	Application and Collaboration Servers	Servidor web en estacion de trabajo.
46	aTube Catcher versión 3.8	System Utilities	Descarga multimedia
47	BOARD 9 Server	Unidentified	Software para admin./soluciones de empresas.

Unidad Auditoría Interna MTEySS

NIVEL DE RIESGO MEDIO			
NRO.	SOFTWARE	AREA	DETALLE
48	Dropbox	System Utilities	Software para almacenamiento en la nube.
49	Dropbox Update Helper	System Utilities	Software para almacenamiento en la nube.
50	Fiddler	Development Tools	Analizador de Web Proxys.
51	Free YouTube Downloader 4.1.559	Internet Utilities and Applications	Descarga multimedia
52	GlassFish Server Open Source Edition 4.1.1	Unidentified	Servidor/Plataforma de aplicaciones
53	Google Drive	Storage, Archive, Backup, and Retrieval	Software para almacenamiento en la nube.
54	IIS 10.0 Express	Application and Collaboration Servers	Servidor web en estacion de trabajo.
55	IIS 8.0 Express	Application and Collaboration Servers	Servidor web en estacion de trabajo.
56	IIS Express Application Compatibility Database for x64	Web Design and Development	Servidor web en estacion de trabajo.
57	IIS Express Application Compatibility Database for x86	Web Design and Development	Servidor web en estacion de trabajo.
58	IIS URL Rewrite Module 2	Development Tools	Servidor web en estacion de trabajo.
59	LWS YouTube Plugin	Device Drivers, Configuration, and Utilities	Descarga multimedia
60	Microsoft ASP.NET Core Module for IIS Express	Development Resources	Servidor web en estacion de trabajo.
61	Microsoft Exchange Server 2007	Application and Collaboration Servers	Servidor de correos en estacion de trabajo.
62	Microsoft Exchange Web Services Managed API 2.0	Application and Collaboration Servers	Servidor de correos en estacion de trabajo.
63	Microsoft Exchange Web Services Managed API 2.1	Application and Collaboration Servers	Servidor de correos en estacion de trabajo.
64	Microsoft SQL Server 2000	Information and Data Management	Servidor de base de datos en estacion de trabajo.
65	Microsoft SQL Server 2005 Compact Edition [ENU]	Information and Data Management	Servidor de base de datos en estacion de trabajo.
66	Microsoft SQL Server 2005 Express Edition	Information and Data Management	Servidor de base de datos en estacion de trabajo.
67	Microsoft SQL Server 2005 Express Edition - Express Edition	Information and Data Management	Servidor de base de datos en estacion de trabajo.
68	Microsoft SQL Server 2008	Information and Data Management	Servidor de base de datos en estacion de trabajo.
69	Microsoft SQL Server 2008 (64-bit)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
70	Microsoft SQL Server 2008 Database Engine Services	Information and Data Management	Servidor de base de datos en estacion de trabajo.
71	Microsoft SQL Server 2008 Database Engine Services - Enterprise Edition (64-bit)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
72	Microsoft SQL Server 2008	Information and Data	Servidor de base de datos en

Unidad Auditoría Interna MTEySS

NIVEL DE RIESGO MEDIO			
NRO.	SOFTWARE	AREA	DETALLE
	Database Engine Services - Express Edition	Management	estacion de trabajo.
73	Microsoft SQL Server 2008 Database Engine Services - Express Edition (64-bit)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
74	Microsoft SQL Server 2008 Database Engine Shared	Information and Data Management	Servidor de base de datos en estacion de trabajo.
75	Microsoft SQL Server 2008 Database Engine Shared	Information and Data Management	Servidor de base de datos en estacion de trabajo.
76	Microsoft SQL Server 2008 R2	Information and Data Management	Servidor de base de datos en estacion de trabajo.
77	Microsoft SQL Server 2012	Information and Data Management	Servidor de base de datos en estacion de trabajo.
78	Microsoft SQL Server 2012 (64-bit)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
79	Microsoft SQL Server 2012 Express LocalDB	Information and Data Management	Servidor de base de datos en estacion de trabajo.
80	Microsoft SQL Server 2012 Setup (English)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
81	Microsoft SQL Server 2012 Setup (English)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
82	Microsoft SQL Server 2014	Information and Data Management	Servidor de base de datos en estacion de trabajo.
83	Microsoft SQL Server 2014 (64-bit)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
84	Microsoft SQL Server 2014 Setup (English)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
85	Microsoft SQL Server 2014 Setup (English)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
86	Microsoft SQL Server 2016	Information and Data Management	Servidor de base de datos en estacion de trabajo.
87	Microsoft SQL Server 2016 LocalDB	Information and Data Management	Servidor de base de datos en estacion de trabajo.
88	Microsoft SQL Server 2016 Setup (English)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
89	MongoDB 3.2.0 2008R2Plus SSL (64 bit)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
90	MySQL Installer	Information and Data Management	Servidor de base de datos en estacion de trabajo.
91	MySQL Installer - Community	Information Access and Delivery	Servidor de base de datos en estacion de trabajo.
92	PostgreSQL 9.4 (x86)	Unidentified	Servidor de base de datos en estacion de trabajo.
93	SQL Server 2008 R2 Database Engine Services	Information and Data Management	Servidor de base de datos en estacion de trabajo.
94	SQL Server 2008 R2 Database Engine Shared	Information and Data Management	Servidor de base de datos en estacion de trabajo.
95	SQL Server 2008 R2 SP1 Database Engine Services	Information and Data Management	Servidor de base de datos en estacion de trabajo.
96	SQL Server 2008 R2 SP1 Database Engine Services - Express Edition (64-bit)	Information and Data Management	Servidor de base de datos en estacion de trabajo.

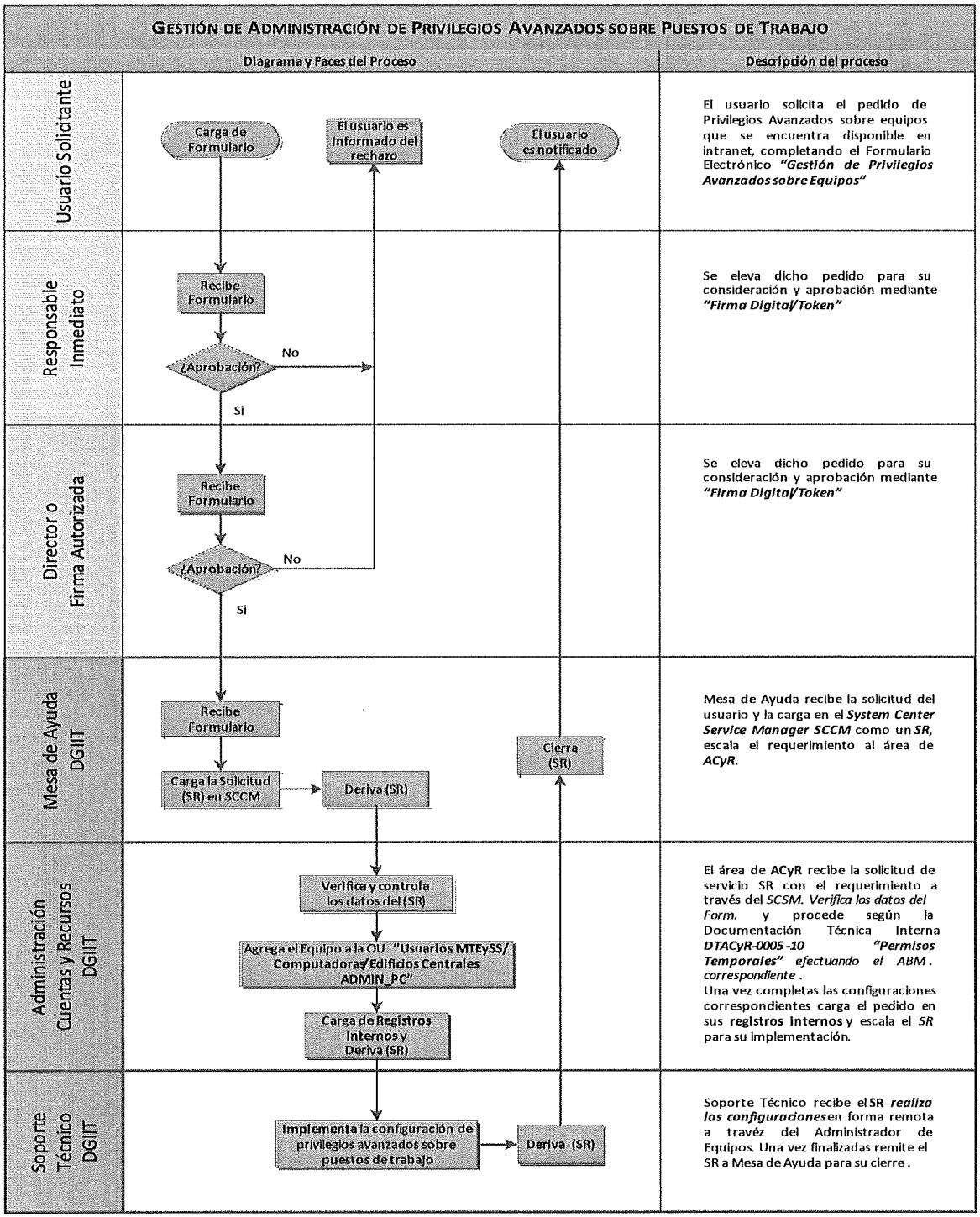
Unidad Auditoría Interna MTEySS

NIVEL DE RIESGO MEDIO			
NRO.	SOFTWARE	AREA	DETALLE
97	SQL Server 2008 R2 SP1 Database Engine Shared	Information and Data Management	Servidor de base de datos en estacion de trabajo.
98	SQL Server 2008 R2 SP2 Database Engine Services	Information and Data Management	Servidor de base de datos en estacion de trabajo.
99	SQL Server 2008 R2 SP2 Database Engine Services - Express Edition with Advanced Services	Information and Data Management	Servidor de base de datos en estacion de trabajo.
100	SQL Server 2008 R2 SP2 Database Engine Shared	Information and Data Management	Servidor de base de datos en estacion de trabajo.
101	SQL Server 2012 Database Engine Services	Information and Data Management	Servidor de base de datos en estacion de trabajo.
102	SQL Server 2012 Database Engine Services - Enterprise Edition (64-bit)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
103	SQL Server 2012 Database Engine Services - Express Edition (64-bit)	Information and Data Management	Servidor de base de datos en estacion de trabajo.
104	SQL Server 2014 Database Engine Services	Information and Data Management	Servidor de base de datos en estacion de trabajo.
105	SQL Server 2014 Database Engine Shared	Information and Data Management	Servidor de base de datos en estacion de trabajo.
106	WampServer 2.2	Application and Collaboration Servers	Servidor web en estacion de trabajo.

Unidad Auditoría Interna MTEySS

ANEXO B

CIRCUITO ADMINISTRATIVO



Unidad Auditoría Interna MTEySS

ANEXO C

DETALLE DE RESPONSABILIDADES

De acuerdo a las Políticas de Seguridad de la Información vigentes, la Dirección General de Informática e Innovación Tecnológica (DGIIT) es responsable de:

- Brindar garantía de funcionamiento correcto y seguro de los procesos de información.
- Asegurar la correcta operación de los puestos de trabajo.
- Dar soporte a nivel hardware de todos los equipos que sean propiedad y/o activos del MTEySS.
- Asegurar la Instalación de software homologado.
- Realizar auditorías y remitir copia a los responsables. (ésta Dirección podrá efectuar auditorías periódicas sobre el equipo, sea por reinstalación del Sistema Operativo, por detectar irregularidades o por rutina de control).
- Quitar y/o modificar cualquier configuración del equipo que viole las políticas de seguridad vigentes.
- Dar la baja proactiva de los usuarios con privilegios avanzados en el caso de detectar irregularidades o bien si se provee una solución para que el usuario pueda ejecutar el software sin estos privilegios.
- Llevar registro identificando al usuario, puesto de trabajo, privilegio otorgado y vigencia.
- Asignar privilegios avanzados debidamente autorizados.

El usuario solicitante asume la responsabilidad de:

- Instalación software: Informar a la DGIIT toda necesidad de instalación de software a efectuarse sobre el puesto de trabajo. El mismo deberá tener licencia autorizante y estar homologado por la DGIIT, evitando así la instalación de software no autorizado, malicioso o vulnerado. El usuario se hará responsable del software que pudiere instalar sin consentimiento de esta Dirección y por los daños que estos pudiesen ocasionar.
- Mecanismos de protección y seguridad: El usuario no podrá modificar los mecanismos, políticas y definiciones de seguridad vigentes. (Ej. Firewall, Antivirus, Auditorías de Seguridad, Modificación de Eventos de Seguridad).
- Política de Puestos de Trabajo: Los equipos son configurados inicialmente de acuerdo a la Política de Puestos de Trabajo vigente al momento de realizar la instalación y puesta a punto del equipo. El usuario no podrá infringir esta política en ningún momento. (Ej. Modificar la IP, el nombre del equipo; eliminar componentes de hardware; modificar el cliente de inventario o de soporte remoto; quitar los permisos de administración de esta Dirección; etc.).
- Asignar privilegios avanzados a otros usuarios: El usuario no podrá asignar a otros usuarios privilegios avanzados sobre el puesto de trabajo. (Ej. Agregar a otro usuario como administrador; etc.).
- Recursos Compartidos: el usuario no podrá compartir recursos locales de la PC con otros puestos de trabajo, ya que las Políticas de Seguridad de la Información propugnan el almacenamiento de información laboral en los servidores propios de este Ministerio.

Unidad Auditoría Interna MTEySS

Anexo D

RESUMEN GENERAL DE OBSERVACIONES [1]

Nº de Orden	Área Temática	Sub-Área Temática	Calificación de Impacto			Estado de Situación [2]					Área/s Responsable/s[3]
			Alto	Medio	Bajo	R	ET	SAC	NC	NR	
1	Proceso de apoyo	Sistemas			X		X				DGIIT
2	Proceso de apoyo	Sistemas	X				X				DGIIT
3	Proceso de apoyo	Sistemas		X			X				DGIIT
4	Proceso de apoyo	Sistemas			X		X				DGIIT
5	Proceso de apoyo	Sistemas			X	X					DGIIT
6	Proceso de apoyo	Sistemas			X	X					DGIIT
7	Proceso de apoyo	Sistemas			X	X					DGIIT
8	Proceso de apoyo	Sistemas			X	X					DGIIT
9	Proceso de apoyo	Sistemas			X		X				DGIIT
10	Proceso de apoyo	Sistemas		X			X				DGIIT
11	Proceso de apoyo	Sistemas			X		X				DGIIT

Unidad Auditoría Interna MTEySS

[1] Incorporadas en el Sistema de Seguimiento de Informes y Observaciones (SISIO).
[2] Referencias: (R) Regularizada / (ET) En Trámite / (SAC) Sin Acción Correctiva / (NC) No Compartida / (NR) No Regularizable.
[3] Unidades Organizativas que deben impulsar acciones correctivas respecto de la observación formulada. Referencia: (DGIIT) Dirección General de Informática e Innovación Tecnológica.

Unidad de Auditoría Interna

Avenida Leandro N. Alem 650, piso 3º
(1001AAO), Ciudad Autónoma de Buenos Aires
Tel. 4310-6175
E-mail: uauditor@trabajo.gob.ar

Ministerio de
Trabajo, Empleo
y Seguridad Social