AUDITORIA INTERNA
Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050
San Pedro de Montes de Oca

UNIVERSIDAD ESTATAL A DISTANCIA
Institución Benemérita de la Educación y la Cultura

UNIVERSIDAD ESTATAL A DISTANCIA

AUDITORÍA INTERNA

EVALUACIÓN DE LOS PROCEDIMIENTOS ESTABLECIDOS POR LA UNED PARA EL CONTROL Y LA ADMINISTRACIÓN DE USUARIOS, PERFILES Y CONTRASEÑAS DE ACCESO PARA FUNCIONARIOS QUE OPERAN LOS SISTEMAS INFORMÁTICOS INSTITUCIONALES: SAE, FINANCIERO-CONTABLE Y DE PRESUPUESTO.

INFORME FINAL DTIC-2012-01

2012

AUDITORIA INTERNA
Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050
San Pedro de Montes de Oca

UNIVERSIDAD ESTATAL A DISTANCIA
Institución Benemérita de la Educación y la Cultura

Índice

1. Introducción..... 1
1.1 Origen del estudio..... 1
1.2 Objetivos. 1
1.3 Alcance. 2
1.4 Limitaciones. 2
1.5 Antecedentes. 2
1.6 Deberes en el trámite de informes y plazos que se deben observar. 2
2. Resultados. 4
2.1 Sobre la solicitud para trámite referente a usuarios de los sistemas objeto de estudio. 5
2.2 Sobre la definición, clasificación y control de usuarios, sus perfiles y niveles de privilegios (opciones habilitadas) para funcionarios que operan los sistemas informáticos objeto de estudio. 12
2.2.1 Sobre la gestión para la definición y clasificación de usuarios o grupos de usuarios, sus perfiles y niveles de privilegios (opciones habilitadas). 12
2.2.2 Sobre el control y mantenimiento de usuarios creados para funcionarios que operan los sistemas objeto de estudio. 14
2.3 Sobre el personal, tanto de la DTIC como de las instancias usuarias, que gestionan acciones referentes a la creación de usuarios, perfiles y claves de acceso para los sistemas objeto de estudio 22
2.3.1 Sobre el personal de la DTIC 22
2.3.2 Sobre el personal usuario de las dependencias que administran los sistemas objeto de estudio 28
2.4 Controles de acceso y bitácoras inmersas en las estructuras de los sistemas objeto de estudio 31
2.4.1 Sobre los controles de acceso desarrollados en las estructuras de los sistemas. 31
2.4.2 Sobre la existencia y control de bitácoras inmersas en los sistemas objeto de estudio. 32
2.5 Sobre las gestiones para las claves de acceso para usuarios de los sistemas objeto de estudio. 36
2.6 Sobre la valoración de Riesgos. 40
2.7 Sobre capacitación al personal para operar los sistemas objeto de estudio. 45
2.8 Sobre conformación y resguardo de la documentación referente a las gestiones realizadas. 48
3. Conclusiones. 51
4. Recomendaciones. 54

AUDITORIA INTERNA
Tel: 2527 2276
Telefax: 2224 9684
Apdo. 474-2050
San Pedro de Montes de Oca

UNIVERSIDAD ESTATAL A DISTANCIA
Institución Benemérita de la Educación y la Cultura

INFORME FINAL Nº DTIC-2012-01
(Al contestar refiérase a este número)

EVALUACIÓN DE LOS PROCEDIMIENTOS ESTABLECIDOS POR LA UNED PARA EL CONTROL Y LA ADMINISTRACIÓN DE USUARIOS, PERFILES Y CONTRASEÑAS DE ACCESO PARA FUNCIONARIOS QUE OPERAN LOS SISTEMAS INFORMÁTICOS INSTITUCIONALES: SAE, FINANCIERO-CONTABLE Y DE PRESUPUESTO.

1. Introducción.

1.1 Origen del estudio.

El presente Estudio se originó en atención al Plan Anual de Trabajo de la Auditoría Interna de la UNED para el año 2012, específicamente en el Área de Auditoría en Tecnología de la Información.

1.2 Objetivos.

Objetivos generales.

Evaluar la validez, suficiencia y cumplimiento del control interno en cuanto al acceso y opciones habilitadas a usuarios de los sistemas informáticos institucionales: SAE, Financiero-Contable y de Presupuesto.

Objetivos específicos.

Verificar que el acceso a las opciones habilitadas a usuarios de dichos sistemas, están debidamente aprobadas, autorizadas y afines a la necesidad funcional de las actividades del cargo que desempeñan.

Evaluar el control interno en cuanto a las actividades de control que regulan el registro e inactivación de usuarios, la asignación de derechos de acceso, la asignación, el control y uso de privilegios, el proceso de administración de contraseñas, la revisión periódica de los derechos de acceso y la documentación generada.

Verificar el cumplimiento de la normativa aplicable, tanto interna como externa que regula el proceso objeto de examen.

1.3 Alcance.

El período objeto de estudio comprende el año 2011 (17/01/2011 al 16/12/2011), ampliándose en los casos en que se consideró necesario.

1.4 Limitaciones.

La DTIC no cuenta con reporte o lista actualizada de todos los usuarios que utilizan los sistemas objeto de estudio; tampoco se tiene identificado por sistema, el perfil (acceso) autorizado a cada funcionario que lo opera.

1.5 Antecedentes.

Se analizó el Informe X-24-2011-02 denominado “Estudio sobre la seguridad física y lógica del Data Center de la UNED”, entregado a la Rectoría con Oficio AI-047-2012 fechado 28/03/2012, en el cual se plasmaron situaciones que debilitan el control en actividades referentes a la creación e inhabilitación de usuarios en los sistemas de información institucional y en el correo electrónico, así también sobre los controles de acceso lógico a las bases de datos y la administración de cuentas y claves de usuarios para los sistemas informáticos institucionales.

Estas situaciones al tener una relación directa con esta investigación, se harán referencia de las mismas en el desarrollo de este informe.

1.6 Deberes en el trámite de informes y plazos que se deben observar.

Artículo 36.—Informes dirigidos a los titulares subordinados.

Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:

a. El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.
b. Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.
c. El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.

ARTÍCULO 38. — Planteamiento de conflictos ante la Contraloría General de la República.

Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.

> La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994.
>
> ARTÍCULO 39. — Causales de responsabilidad administrativa.
>
> (…) El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios.
>
> El jerarca, los titulares subordinados y los demás funcionarios públicos incurrirán en responsabilidad administrativa, cuando debiliten con sus acciones el sistema de control interno u omitan las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo, según la normativa técnica aplicable.
> …
>
> Igualmente, cabrá responsabilidad administrativa contra los funcionarios públicos que injustificadamente incumplan los deberes y las funciones que en materia de control interno les asigne el jerarca o el titular subordinado, incluso las acciones para instaurar las recomendaciones emitidas por la auditoría interna, sin perjuicio de las responsabilidades que les puedan ser imputadas civil y penalmente…

2. Resultados.

En la evaluación realizada al proceso que enmarca las actividades correspondientes a la creación e inactivación de usuarios, sus respectivas claves de acceso, los perfiles y niveles de privilegios (habilitación de opciones) para los sistemas informáticos institucionales: SAE, Financiero-Contable y de Presupuesto, se determinaron situaciones de control interno que evidencian que las mismas no están debidamente administradas y controladas, estas a continuación se detallan:

2.1 Sobre la solicitud para trámite referente a usuarios de los sistemas objeto de estudio.

Para el trámite correspondiente a la solicitud de creación, activación, modificación o inactivación de usuarios y sus perfiles (opciones habilitadas en el sistema), así como de las claves de acceso para funcionarios que operan los sistemas objeto de estudio, se determinó que la gestión carece de lineamientos o procedimientos debidamente formalizados y avalados por el Consejo de Rectoría que coadyuven a:

- Guiar el ¿cómo? debe proceder la instancia solicitante y los requisitos que debe cumplir en el trámite de la solicitud y la estandarización de la gestión mediante instrumentos tales como: solicitud, formulario, orden de servicio u otro, ya sean en formato impreso o digital.
- Unificar y oficializar el medio para la comunicación y coordinación de la gestión entre las instancias usuarias y la Dirección de Tecnología, Información y Comunicaciones (en adelante DTIC).
- La aprobación formal de los trámites realizados.

Sobre la situación, el Director de la DTIC, Mag. Francisco Durán Montoya manifestó lo siguiente:

> (…) El administrador del Sistema determina el nivel de acceso que se debería crear, y posterior es responsable de tramitar la solicitud ante esta Dirección, ya sea mediante oficio o correo electrónico.
>
> Este procedimiento no está documentado."
>
> …, las solicitudes se tramitan por medio de correo electrónico, otras mediante oficio.
> …
> No se cuenta con un instrumento que estandarice el trámite de las solicitudes y el comunicado del cumplimiento de las mismas.
> …
> No se cuenta con formularios tanto para la solicitud como para la prestación del servicio, donde se plasme el cumplimiento de lo solicitado y el aval por parte del solicitante.
> ...

> Actualmente se tienen diferentes canales para estas gestiones (oficio, nota, correo electrónico). No se cuenta con un canal único y estandarizado para estas gestiones, tanto por esta Dirección como por la (sic) Unidades Usuarias. (Entrevista aplicada el 14/05/2012, respuestas a los ítems 2, 3, 6, 15).

También cabe transcribir las respuestas dadas por personal encargado de instancias usuarias de los sistemas objeto de estudio:

Licda. Susana Saborío Álvarez, Jefa de la Oficina de Registro y Administración Estudiantil:

> (…) La labor esta a la libre, aunque se ha tratado de formalizar y controlar no se ha logrado.
>
> Varios usuarios de los que fueron creados para la utilización del Sistema SAE, no medió control alguno.
> …
> "Se les ha comunicado vía correo electrónico a las escuelas y centros universitarios de que la solicitud referente a estas gestiones solo la puede realizar el Director. No guardo copia del correo electrónico enviado.
> …
> "No se tiene establecido formalmente instrumento alguno para estas gestiones, estas se llevan a cabo vía correo electrónico o por medio de nota u oficio, además no se resguarda la documentación que se generó de las acciones realizadas. (Entrevista aplicada el 14/05/2012, ítems 2, 3, 4).

Mag. Mabel León Blanco, Jefa de la Oficina de Presupuesto

> (…) Sí, se tiene definido un formulario y la nota que se le dirige a la DTIC, en la cual se aprueba las gestiones para usuarios externos.
>
> Para el personal de esta oficina no se cuenta con documentación alguna, ya que el proceder en relación a estas actividades es la comunicación verbal.
> …

> La solicitud se nos comunica vía correo electrónico, se les comunica de igual forma, que debe llenar el formulario, el cual se encuentra en las carpetas públicas de esta oficina. Realizadas las gestiones por parte del solicitante se procede a analizar la solicitud y de aprobarse se tramita ante la DTIC. (Entrevista aplicada el 14/06/2012, ítems 2, 4).

Licda. Ana Cristina Pereira Gamboa, Jefa de la Oficina de Tesorería.

> (…) Se cuenta para estas actividades con un protocolo que elaboró la DTIC, en él se plasma el proceder y los requerimientos para estas actividades.
>
> *Este documento se comunicó vía correo electrónico.*
>
> …, lo que se procede es cumplir con lo que se plasmó en el protocolo, y se canaliza actualmente vía correo electrónico ya que anteriormente se realizaba mediante nota u oficio. (Entrevista aplicada el 05/06/2012, ítems 2, 4).

El protocolo al que se refiere la funcionaria Pereira, corresponde a la plantilla en formato Excel, remitida vía correo electrónico por parte de la funcionaria María Luisa Molina Mendez con el cargo de "Líder de Proyectos de la DTIC"; en la siguiente figura se muestra la estructura y el encabezado de dicha plantilla:

Figura Nº 1

Plantilla comunicada vía correo electrónico para tramitar solicitud de usuario y su perfil para los sistemas Administrativo Financiero y Presupuesto

Tiene Usuario AS/400	Código Usuario AS/400	Nombre Funcionario	Nombre del Sistema al que requiere acceso	Se conserva el acceso Actual	Perfil de Usuario a heredar
			Detallar opciones (puede adjuntar pantallas)	N	

Fuente: Plantilla remitida por la funcionaria María Luisa Molina Mendez de la DTIC, mediante correo electrónico, fechado 29/05/2012, hora 14:05.

Sobre esta plantilla cabe hacer la observación de que su estructura carece de espacios donde se incorpore información referente al Nº consecutivo de la plantilla, Nº de identificación del funcionario (cédula, permiso u otro), dependencia donde presta servicio, observaciones por parte de la DTIC (estas dirigidas a determinar el estado de la misma, como por ejemplo: en valoración, rechazada, proceso, finalizado), donde se plasme el visto bueno por la instancia solicitante de conformidad con lo solicitado.

Además, recalcar que la acción de implementarla fue dirigida solo a los usuarios administradores de los sistemas Financiero Contable y Presupuesto, sistemas que a la fecha lidera la funcionaria Molina, quién ante consulta hecha por esta Auditoría Interna manifestó:

> (…) El año pasado (18 noviembre del 2011) les remití a los administradores un comunicado (mediante correo electrónico) de cómo proceder la parte usuaria respecto a la creación de usuarios, utilizando como estándar una plantilla en formato Excel.
>
> Este comunicado fue una decisión e iniciativa propia, lo anterior, por la ausencia de un procedimiento lo cual provocaba desorden en las gestiones.
> …
> La plantilla a completar que les trasladé vía correo electrónico (18 noviembre del 2011), la cual, hasta la fecha solo es utilizada por la Oficina de Presupuesto mediante un oficio y en el caso de la Oficina de Tesorería están iniciando su uso y el envío es mediante correo electrónico. (Entrevista aplicada el 01/06/2012, ítems 2, 4).

Las situaciones expuestas van en contraposición de lo estipulado en el documento N-2-2007-CO-DFOE denominada “Normas técnicas para la gestión y el control de las Tecnologías de Información” (en adelante Normas de TI), aprobado por la Contraloría General de la República mediante resolución R-CO-26-2007, fechada 07/06/2007 y publicada en La Gaceta Nro.119 del 21/06/2007, dicho documento establece lo siguiente:

Capítulo III “Implementación de tecnologías de información”, su norma 3.1 denominada “Consideraciones generales de la implementación de TI”, la cual detalla lo siguiente:

> (…) La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe:
>
> a. Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.
> …
> c. Garantizar la participación activa de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas.

También lo indicado en el capítulo IV "Prestación de servicios y mantenimiento su norma 4.1 "Definición y administración de acuerdos de servicios", misma que se transcribe:

> (…) La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades.
>
> El jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben:

a. Tener una comprensión común sobre: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.
b. Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio.
c. Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.
d. Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.
e. Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.

f. Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros.

Resaltar de la Ley Nº 8292 “Ley General de Control Interno” su Artículo 2º inciso g) el cual define Actividades de control como: “(…) políticas y procedimientos que permitan obtener la seguridad de que se llevan a cabo las disposiciones emitidas por la Contraloría General de la República, por los jerarcas y los titulares subordinados para la consecución de los objetivos del sistema de control interno.

También el artículo 8º, en el cual se define control interno como:

(…) Serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:

a) Proteger y conservar el patrimonio contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal.

b) Exigir confiabilidad y oportunidad de la información.

c) Garantizar eficiencia y eficacia de las operaciones.

d) Cumplir con el ordenamiento jurídico y técnico.

Y del Artículo 15. — “Actividades de Control”, lo siguiente:

(…) Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:

a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.

b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:

> i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la Institución…

Del documento denominado "Normas de control interno para el Sector Público" (N-2-2009-CO-DFOE) Publicadas en "La Gaceta" Nº 26 del 6 de febrero, 2009, de su norma 4.2 "Requisitos de las actividades de control", lo siguiente:

> (…)
>
> e. Documentación. Las actividades de control deben documentarse mediante su incorporación en los manuales de procedimientos, en las descripciones de puestos y procesos, o en documentos de naturaleza similar. Esa documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación.
>
> f. Divulgación. Las actividades de control deben ser de conocimiento general, y comunicarse a los funcionarios que deben aplicarlas en el desempeño de sus cargos.
> Dicha comunicación debe darse preferiblemente por escrito, en términos claros y específicos.
>
> 4.4.2 Formularios uniformes
>
> El jerarca y los titulares subordinados, según sus competencias, deben disponer lo pertinente para la emisión, la administración, el uso y la custodia, por los medios atinentes, de formularios uniformes para la documentación, el procesamiento y el registro de las transacciones que se efectúen en la institución. Asimismo, deben prever las seguridades para garantizar razonablemente el uso correcto de tales formularios.

La ausencia de planificación y control aunado al incumplimiento de la normativa anterior, son posibles causas de que la administración activa, no cuente con procedimientos ni acuerdos debidamente formalizados, avalados y autorizados por el Consejo de Rectoría o Consejo Universitario, diseñados para asegurar la adecuada gestión y control de la prestación del servicio para actividades referentes a solicitud de: creación, activación, modificación e inactivación de usuarios, sus perfiles (opciones habilitadas en el sistema) y claves de acceso de los funcionarios que operan los sistemas objeto de estudio.

Además reseñar que mediante el referido Informe X-24-2011-02 denominado “Seguridad física y lógica del Data Center de al UNED” en su punto 2.3, punto número 1”Administración de cuentas y claves de usuarios” y punto 2“ Inhabilitación de usuarios”, se hizo del conocimiento de la Administración Activa de la ausencia de un procedimiento debidamente aprobado, divulgado y actualizado, que regule las actividades relacionadas con la creación e inhabilitación de usuarios, el control y su mantenimiento, así como para la reasignación de contraseñas.

2.2 Sobre la definición, clasificación y control de usuarios, sus perfiles y niveles de privilegios (opciones habilitadas) para funcionarios que operan los sistemas informáticos objeto de estudio.

2.2.1 Sobre la gestión para la definición y clasificación de usuarios o grupos de usuarios, sus perfiles y niveles de privilegios (opciones habilitadas).

El establecimiento de privilegios o perfil de acceso a los sistemas informáticos asociados a usuarios o grupos de usuarios, permite controlar qué tipo de acciones podrán ser realizadas por el usuario desde el acceso al recurso o aplicación.

Sobre la gestión para la definición y clasificación de usuarios o grupos de usuarios, sus perfiles y niveles de privilegios (opciones habilitadas) para los sistemas objeto de estudio, no se localizó ni se aportó documentación que plasme la identificación y detalle de los procesos de estos sistemas automatizados que operan las diferentes instancias usuarias, siendo esta información insumo primordial para la definición y clasificación de usuarios o grupos de usuarios, situación que a la vez da paso a que tampoco se cuente con la documentación correspondiente a la definición, clasificación de usuarios o grupos de usuarios y sus perfiles (accesos); éstos bajo el esquema del proceso o procesos de cada sistema, alineados también a los cargos o puestos de cada instancia usuaria.

Sobre esta situación, el Mag. Francisco Durán Montoya indicó a esta Auditoría Interna que no se cuenta con la documentación, además adicionó: “(…), esta actividad a mi parecer debe realizarse de forma conjunta y debidamente coordinada con los administradores de los sistemas, más aún que estos sistemas (AS 400) son muy viejos.”. (Entrevista aplicada el 14/05/2012, ítem 4).

La ausencia de la documentación es reafirmada por los líderes de los sistemas objeto de estudio, ante consulta realizada, indicaron lo siguiente:

María Luisa Molina Méndez, líder de los sistemas Financiero Contable y Presupuesto, manifestó: (…) No se encuentran identificados ni documentado. (Entrevista aplicada 01/06/2012, ítem 5).

Randall Gutiérrez López, lidera el Sistema SAE indicó que de todas las aplicaciones que conforman dicho sistema, las desarrolladas en plataforma de software AS 400 (SNAP) carecen de esta documentación (entrevista aplicada 08/11/2012, ítem 5) y mediante correo electrónico de fecha 08/02/2013, puntualizó las aplicaciones que conforman dicho sistema y que a la fecha no cuentan con la documentación, a continuación detalle:

- Administración de Cobro de Matrícula
- Admisión y Matrícula de Estudiantes
- Apelaciones
- Asignación de Tiempos Académicos
- Graduaciones
- Notas Parciales
- Notas Finales
- Módulo de Becas
- Administración de Planes de Estudio
- Entorno Estudiantil
- Estadísticas de Matricula
- Programa Apoyo Didáctico a Distancia

También aquellas que cuentan con la documentación, a saber:

- Notas Parciales
- Reconocimiento de Estudios (En proceso de creación)
- Admisión y empadronamiento Web (En proceso de creación)

Además informo que de la totalidad de las aplicaciones, solo “Apelaciones”, “Asignación de Tiempos Académicos” y “Administración de Planes de Estudio” cuentan con el Manual de Usuario Final.

También las Jefaturas de instancias usuarias de los sistemas objeto de estudio, armonizaron en no contar con dicha documentación; a continuación en refuerzo de lo exteriorizado se transcriben las manifestaciones:

Licda. Susana Saborío Álvarez, Jefa de la Oficina de Registro y Administración Estudiantil:

> (…) No se cuenta con un documento donde se plasmen los procesos que abarca el Sistema SAE, tanto de esta Oficina como de otras instancias que lo utilizan, en el que se definan los diferentes grupos de usuarios de acuerdo a los procesos que ejecutan y sus accesos a los menús de los módulos que lo conforman. (Entrevista aplicada el 14/05/2012, ítem 5).

Licda. Ana Cristina Pereira Gamboa, Jefa de la Oficina de Tesorería:

> (…) No. La definición de los accesos a los sistemas se define según las actividades que le asigna la jefatura al funcionario, de los módulos o procesos que ejecutará en el sistema automatizado.
>
> Se define a cuales opciones se le debe dar acceso y se le comunica a la DTIC para que finalice el trámite". (Entrevista aplicada 05/06/2012, ítem 5).

2.2.2 Sobre el control y mantenimiento de usuarios creados para funcionarios que operan los sistemas objeto de estudio.

Se determinó que los sistemas objeto de estudio cuyos desarrollos fueron llevados a cabo en software denominado SNAP, no cuentan en sus estructuras con un módulo o proceso para el registro y control de los usuarios según clasificación y definición de privilegios autorizados y creados para operar el mismo, situación que es reafirmada por los líderes de proyectos María Luisa Molina Méndez y Randall Gutiérrez López; además ambos funcionarios coinciden en que implementar un sistema de accesos y sus roles para cada sistema técnicamente es posible.

Actualmente la definición, creación y registro de los perfiles para los usuarios se lleva a cabo mediante la programación y desarrollo del menú o menús,

según lo solicitado y autorizado por la parte usuaria. El menú contempla las diferentes opciones a las que tendría acceso el funcionario y se desarrollan en el ambiente AS 400, ambiente donde residen otros sistemas. Estas actividades son llevadas a cabo por las siguientes unidades de la DTIC:

- Unidad Estratégica de Sistemas de Información (en adelante UESI), le corresponde la programación y desarrollo del menú o menús.

- Unidad Estratégica de Operaciones (en delante UEO), incorpora y ejecuta a nivel de producción en el ambiente AS 400 los menús y los liga o asigna al respectivo usuario, al cual también debe crearle su cuenta y clave para validación de acceso.

Sobre las gestiones realizadas por estas unidades se determinaron las siguientes situaciones:

1. No se tiene un adecuado control para el mantenimiento de usuarios, ya que se detectaron casos de exfuncionarios de la UNED, a quienes se les mantiene activo su usuario para el acceso al AS 400 y en algunos casos se comprobó que la situación también se da para el servicio de correo electrónico.

2. No se cuenta con una estandarización para la inclusión e identificación de usuarios; existen casos en los cuales el nombre de la persona a la que se le creó el usuario carece del segundo apellido; en otros, refleja tanto el detalle completo o parte del nombre, así como el de la instancia física donde se le ubicó, además cabe recalcar la ausencia de campo donde se registre el número de identificación (cédula, pasaporte o permiso de trabajo), así como de opción de consulta por este dato. El no registro de este dato siendo este único, no permite tener la certeza de que el usuario creado, corresponde efectivamente al funcionario autorizado.

3. La opción de “Suprimir” usuarios, se mantiene activa a nivel de administración del ambiente AS 400, lo cual permite realizar acciones de eliminación de usuarios, aunado a esta condición se da la ausencia de bitácora, donde se registren las pistas o registros que permitan identificar el o los usuarios a nivel técnico (DTIC), que realizó o realizaron las acciones y fecha, siendo esta información clave para sentar las responsabilidades ante supuestas anomalías.

Cabe indicar que las situaciones arriba citadas, así como los casos encontrados, se hicieron del conocimiento a la Administración Activa mediante Oficio de Advertencia AI-136-2012, fechado 31/08/2012; y mediante Oficio DTIC-2012-182 fechado 14/09/2012, la Dirección de Tecnología de Información y Comunicaciones informa a esta Auditoría Interna de acciones tomadas y otras a realizar en relación a las situaciones y casos señaladas.

4. Se requiere mayor tiempo para ejecutar las acciones, ya que para cada usuario se debe programar y desarrollar un menú, este proceder es conocido en la DTIC como perfiles de acceso personalizado.

En alusión a este punto se transcribe el siguiente comentario emitido por la funcionaria de la DTIC María Luisa Molina Méndez, ubicada en la UESI y con el cargo de líder de proyectos: "(…) lo que se procede es rastrear en el sistema las opciones que corresponda, revisando en la mayoría de los casos, el programa que utiliza el usuario y determinando de ésta forma las opciones que tiene definidas los diferentes menús". (Entrevista aplicada el 01/06/2012, ítem 5).

Este actuar no permite tener un adecuado control de todos los registros de usuarios creados e incorporados por sistema, generando en algunos casos desconocimiento de los permisos creados a los usuarios o listas de usuarios; sobre esta situación se transcribe el siguiente comentario aportado por el funcionario Rolando Rojas Coto, funcionario de la DTIC y encargado de la UEO:

> (…) También se incorpora el usuario al grupo de usuario o lista de distribución, lo anterior dependiendo del sistema.
>
> Actualmente se cuenta con una cantidad aproximada a 70 grupos, hago la observación que varios de estos grupos no tienen relacionado o asignado ningún usuario. También que no se nos ha comunicado cual es la diferencia entre un grupo o una lista de distribución para estos sistemas, la falta de documentación es una limitante para nosotros sobre este aspecto y otros que se relacionan con las actividades que ejecutamos. (Entrevista aplicada el día 30/07/2012, Ítem Nº 6).

5. Se carece de opciones automatizadas en el ambiente AS 400 para el procesamiento y emisión de reportes de usuarios por cada sistema, debidamente estandarizados según opciones definidas de búsqueda y selección, que permitan obtener tanto por un único usuario como por grupos pertenecientes al sistema, ya

que actualmente solo permite obtener el reporte de forma unitaria por medio del nombre del funcionario o el usuario creado.

6. Tanto la DTIC como las instancias usuarias de los sistemas objeto de estudio, carecen de un procedimiento o control estandarizado que implique la revisión periódica de los usuarios creados, el cual tenga como fin el determinar si los usuarios cuentan con la correcta asignación de roles y privilegios autorizados; y que corresponden a funcionarios activos.

Se hace la observación que la jefatura de la Oficina de Presupuesto, aportó lista de usuarios autorizados para operar el sistema, pero con la limitante de que ésta solo contiene a los usuarios de otras dependencias, careciendo del detalle del personal de dicha Oficina que ejecuta acciones en el sistema, aparte la información que contiene dicha lista es mínima por cuanto solo muestra detalle de la Unidad Presupuestaria y el nombre del funcionario autorizado.

También la Oficina de Registro remite a esta Auditoría Interna mediante Oficio OR-169-2012, fechado 14/06/2012, lista digital aportada por la DTIC de los usuarios activos a mayo del 2012, creados para operar el sistema SAE, y a la vez informa que existen anomalías en dicha lista, al encontrar pensionados o difuntos, desconociendo si existe coordinación con la Oficina de Recursos Humanos para estos efectos.

En relación al punto anterior, sobre las anomalías informadas; esta Auditoría Interna en coordinación con el funcionario Rolando Rojas Coto, Encargado de la Unidad Estratégica de Operaciones de la DTIC, realizó pruebas de verificación de los estados de usuarios con las condición de: Difunto (a), Pensionado (a), “Contrato Vencido” y un caso relacionado a “Matritel” el cual correspondía a matricula vía telefónica, y misma que no aplica desde hace dos años. Se verificaron 16 casos en su totalidad, de éstos, 10 correspondieron a la condición de “Pensionado (a)”, 3 a la de “Difunto (a)”, 2 a “Contrato Vencido” y 1 a “Matritel”; a continuación se detallan los pormenores:

- De la totalidad de casos se determinó que 11 casos a la fecha los usuarios están habilitados en producción. En la siguiente tabla se muestra el detalle:

USUARIO	MENU	DESCRIPCION	Instancia donde laboró	Situación según Registro

AMONTOYA	AMMNU109	Ana Maria Montoya - Registro	REGISTRO	Difunta
EFRODRIGUE	AMMNU22	Efrain Rodriguez Mena-San Jose-certificaciones'	CEU 01	Difunto
REPINES	AMMNU61	Matritel	N/I	
DOBANDO	ESMMNU04	Encargado Catedra-Dinorah Obando	ESCUELAS	Pensionada
LBARQUERO	ESMMNU04	Encargado Catedra-Leda Barquero	ESCUELAS	Pensionada
MALOPEZ	ESMMNU04	Encargado Catedra-Manuel Lopez	ESCUELAS	Pensionado
RAMEN	ESMMNU04	Encargado Catedra-Rosa Amen Chen	ESCUELAS	Pensionada
PVENEGAS	POMMNU02	Pedro Venegas Jimenez-grppo03-posgrados-pommnu02'	SEP	Pensionado
SVILLALOBO	AMMNU127	Sandra Villalobos Barquero-Extension AMMNU203	EXTENSION	Pensionada
MCORDOBAC	RMMNU06	Michael Cordoba Chaves	REGISTRO	Contrato vencido
PRODRIGUE1	AMMNU20	Pablo Rodriguez Matricula	CEU	Contrato vencido

N/I: no indica

- Dos casos su usuario de correo electrónico a la fecha está habilitado, en la siguiente tabla el detalle:

USUARIO	MENU	DESCRIPCION	Instancia donde laboró	Situación según Registro
MCORDOBAC	RMMNU06	Michael Cordoba Chaves	REGISTRO	Contrato vencido
CBARQUERO	ESMMNU00	Carmen Barquero Sandoval-secretaria escuela social	ESCUELAS	Difunta

Todas estas situaciones, constituyeron ser limitantes para la aplicación de las pruebas que planeó realizar esta Auditoría Interna; además es preocupante que estos sistemas siendo ejes fundamentales de la Universidad Estatal a Distancia y que las situaciones detalladas son del claro conocimiento de la DTIC; a la fecha no se hayan gestionado medidas para su solución, justificando esa dependencia técnica dicho proceder en que estos sistemas informáticos son muy viejos, o aunque técnicamente es posible implementarlos, no se cuenta con los recursos y tiempo para llevarlos a cabo, afirmaciones ausentes del debido estudio de factibilidad.

Las situaciones supra citadas se contraponen al siguiente ordenamiento jurídico y técnico:

Ley General de Control Interno N° 8292, publicada en la Gaceta N°169 del 4 de Setiembre de 2002 los siguientes artículos:

Artículo 12. —"Deberes del jerarca y de los titulares subordinados en el sistema de control interno" del cual se transcribe lo siguiente:

> (…) En materia de control interno, al jerarca y los titulares subordinados les corresponderá cumplir, entre otros, los siguientes deberes:
>
> a) Velar por el adecuado desarrollo de la actividad del ente o del órgano a su cargo.
> b) Tomar de inmediato las medidas correctivas, ante cualquier evidencia de desviaciones o irregularidades…"

Artículo 14. — "Valoración del Riesgo", en lo que nos interesa se recalca:

> (…) d) Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar".

Artículo 15. — "Actividades de Control", que exterioriza:

> (…) Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:
>
> a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.
>
> b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:
>
> i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la Institución…

> iii. El diseño y uso de documentos y registros que coadyuven en la anotación adecuada de las transacciones y los hechos significativos que se realicen en la Institución. Los documentos y registros deberán ser administrados y mantenidos apropiadamente.
>
> iv. La conciliación periódica de registros, para verificar su exactitud y determinar y enmendar errores u omisiones que puedan haberse cometido".
>
> v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación".

De las Normas de TI las siguientes:

La norma: 1.4 "Gestión de la seguridad de la Información"; en lo que nos interesa, se extrae lo siguiente:

> (…) La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales:
>
> -La implementación de un marco de seguridad de la información…
>
> -La seguridad en las operaciones y comunicaciones
>
> -El control de acceso…"

La norma 1.4.1 "Implementación de un marco de seguridad de la información" su inciso b; detalla:

> (…) La organización debe implementar un marco de seguridad de la información, para lo cual debe:
>
> …
> b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.

La norma 1.4.5 “Control de acceso”, reza lo siguiente:

> (…) La organización debe proteger la información de accesos no autorizados.
>
> Para dicho propósito debe:
>
> a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y la aplicación, a las bases de datos y a las terminales y otros recursos de comunicación…
>
> d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI”.
>
> e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitantes o restricciones.
>
> f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.
> …
> j. Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI…

La norma 4.3 “Administración de datos”, detalla: “(…) La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma

completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura".

También recalcar del Manual de Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) de la Contraloría General de la República la norma 4.5.1 Supervisión constate, que reza: "(…) El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos".

Del documento denominado "Uso de correo electrónico", aprobado por el Consejo de Rectoría en Sesión N°1605 Artículo IV, inciso 2), celebrada el 26 de agosto de 2009, que hace referencia a la "Gestión y control del servicio de correo electrónico" y en su punto No. 1, establece: (…) " Indicar a la Oficina de Recursos Humanos la responsabilidad de informar a la Dirección de Tecnología, Información y Comunicaciones (DTIC) cuando un funcionario deja de laborar para la institución, con el fin de eliminar la correspondiente cuenta de correo electrónico".

La inapropiada planificación además de la falta de control y supervisión, aparte del incumplimiento de normativa que regula y guía la adecuada gestión de las actividades que nos ocupan, son posibles causas de que a la fecha la administración activa arrastre las situaciones detalladas.

2.3 Sobre el personal, tanto de la DTIC como de las instancias usuarias, que gestionan acciones referentes a la creación de usuarios, perfiles y claves de acceso para los sistemas objeto de estudio.

2.3.1 Sobre el personal de la DTIC.

Antes de entrar en detalle, cabe citar el nombre del personal de esta Dirección que participa en la administración y mantenimiento de dichos sistemas:

Por Unidad Estratégica de Sistemas de Información (en adelante UESI).

Sistema Financiero Contable y Presupuesto.

Líder: María Luisa Molina Mendez.

Analistas: Sylvia Umaña Ávila, Sergio Calvo Mata, Carmen María Gutiérrez Yglesias.

Sistema SAE

Líder: Randall Gutiérrez López.

Analistas: Fernando Lara Campos, Luis Gerardo González Pérez, Marino Alberto Sánchez Ramírez. Alejando Olivares Salazar, Verónica Sánchez Elizondo.

Administración de base de datos:

Gonzalo Rodríguez Benavidez

Por la Unidad Estratégica de Operaciones, en adelante (UEO):

Encargado: Rolando Rojas Coto.

Personal de apoyo: Octavio Araya Córdoba, Esteban Artavia Herrera y Andrés Céspedes Monge

Por la Unidad Estratégica de Seguridad Digital, en adelante UESD:

Encargado: Johnny Saborío Álvarez

Sobre la designación de tareas y funciones a este personal, se determinó lo siguiente:

Informalidad en las gestiones para la designación del recurso humano, de las actividades y de la responsabilidad referente al cargo o papel que desempeñan los funcionarios según acciones referentes a la administración y mantenimiento de los sistemas objeto de estudio, lo que involucra la creación de usuarios, sus perfiles (menús de usuarios), claves de acceso para los funcionarios que los operan, por cuanto no se localizó prueba documental de la asignación por parte de la jefatura.

Sobre esta situación el Director de la DTIC Mag. Francisco Durán Montoya, manifestó: "(…) La designación se dió de forma verbal." (Entrevista aplicada14/05/2012, ítem Nº 14).

Lo exteriorizado por el Mag. Durán, es reafirmado por los siguientes funcionarios:

María Luisa Molina Méndez: "(…) En lo que realiza la Unidad Estratégica de Sistemas de Información (UESI), es establecer el menú que se debe asociar en la creación del usuario. Esta actividad fue asignada de forma verbal por la jefatura de la DTIC". (Entrevista aplicada 01/06/2012, ítem Nº 15).

Randall Gutiérrez López: "(…) Por la parte nuestra sí se tiene definido el personal para las labores, pero no existe asignación formal por parte de la jefatura de las mismas y de la responsabilidad". (Entrevista aplicada el 08/11/2012, ítem Nº 11).

Rolando Rojas Coto: "(…) Formalmente no se tiene asignado el personal, por ser éstas actividades propias de la UEO, solo personal ubicado en dicha unidad tienen autorización para realizar estos trámites, estos cuentan con el usuario denominado "Operador""… (Entrevista aplicada 30/07/2012, ítem Nº 14).

La asignación de usuario y creación de su perfil al funcionario, sin que medie definición y justificación bajo el principio "de necesidad de saber o menor privilegio", principio que busca en la asignación de perfiles, que al usuario se le asignen, por defecto, únicamente los permisos estrictamente necesarios para la realización de sus labores, se justifica este actuar por el desconocimiento de cómo delimitar las opciones del usuario, por lo tanto proceden a autorizar y asignar a todo el personal de la unidad UEO el usuario "Operador".

Dicho proceder es reafirmado por Rolando Rojas Coto, encargado de dicha instancia; quien ante consulta sobre la situación manifestó:

> (…) Esto se debe al usuario autorizado denominado "Operador", este usuario engloba varios permisos para diferentes actividades que gestiona la Unidad.

> Hemos tratado de delimitarlo para así contar con diferentes perfiles, pero al tratar de delimitarlo nos ha ocasionado problemas para realizar las gestiones, ya que al inactivar opciones automáticamente no nos permite ejecutar otras, por lo tanto se ha tomado la decisión, de que todo el personal de la unidad que tengo a mi cargo, cuente con la autorización de dicho usuario". (Entrevista aplicada 30/07/2012, ítem 22).

A esta situación se une el caso del funcionario Johnny Saborío Alvarez, encargado de la UESD, quien ostenta también el usuario de "Operador", usuario que según lo manifestado por el encargado de la UEO es exclusivo solo para funcionarios a su cargo; esta autorización y designación no manifiesta una clara independencia de funciones, tampoco una adecuada coordinación y comunicación con otras dependencias internas de la DTIC, por cuanto, la jefatura de la DTIC justifica la autorización en que es el encargado de seguridad y por lo tanto está autorizado para tener el perfil para realizar las gestiones, además de que le corresponde realizar la supervisión y verificación de las actividades hechas por los otros funcionarios de la UEO. (Entrevista aplicada a Francisco ítem Nº 20), justificación que no es congruente con el rol que ejerce el encargado de la UEO, cargo que actualmente ostenta el funcionario Rolando Rojas Coto, quién manifestó lo siguiente: "(…), cabe recalcar que este funcionario no pertenece a la UEO, es funcionario de la Unidad Estratégica de Seguridad Digital y ostenta el cargo de Encargado de la Unidad, desconozco el motivo por el cual se le autorizó ese perfil." (Entrevista aplicada 30/07/2012, ítem 14).

Al mismo tiempo este proceder no se ajusta a las actividades correspondientes a la UESD, plasmadas en la página Web de la Universidad, las cuales se transcriben:

> (…) Evaluar el desempeño de los sistemas informáticos, la granja de servidores y las redes de comunicaciones para proporcionar los controles necesarios que permitan la confiabilidad de la Información así como un elevado nivel de seguridad.
>
> Evaluar los controles establecidos para proteger los bienes institucionales, referente al manejo de hardware, software y comunicaciones.
>
> El área de Seguridad Digital deberá realizar las actividades correspondientes a la verificación de los controles internos establecidos en el área de Sistemas, así como estudios de seguridad física y lógica; análisis de los riesgos a que está

> expuesta la información y los equipos y la elaboración de la documentación necesaria.
>
> Además deberá constatar que se sigan procedimientos que aseguren la confidencialidad, confiabilidad y disponibilidad de los datos, garanticen la seguridad de la información y prevean las posibles contingencias en cuanto a la seguridad de la información que se maneja en la Institución, misma que por definición es muy delicada, asimismo que regule la gestión de la infraestructura y que en general se dedique a guiar el desarrollo y correcto funcionamiento del área de sistemas de esta Institución." (Fuente: Internet, dirección: estatico.uned.ac.cr/dtic/seguridad.shtml).

A las situaciones expuestas se asocia la ausencia de controles automatizados, en este caso de bitácora, donde se incorporen registros claves que sirvan de pistas de auditoría, que permitan identificar al usuario por la DTIC y determinar la acción o acciones realizadas, situación ya expuesta en el punto 3 del resultado 2.2 de este informe.

Sobre la ausencia de estas bitácoras el funcionario Rolando Rojas Coto, indicó que aparte de no contar con ellas; desconoce cómo obtenerlas del AS 400 (entrevista aplicada 30/07/2012, ítem 21).

La situación también es reafirmada por el Director de la DTIC Mag. Durán, quién a la vez informó que la situación también se extiende a las bases de datos, además adicionó lo siguiente: "(…) Con respecto a estas actividades, la DTIC no cuenta con procedimiento de control que permita validar el cumplimiento de la labor ejercida por el encargado de seguridad, así como por el resto del personal de la Unidad Estratégica de Operaciones en cumplimiento de dichas actividades. (Entrevista aplicada el 14/05/2012, ítem Nº 12 y Nº 20). Lo adicionado por el Director de la DTIC demuestra que la función supervisora llevada a cabo no se ha ejercido de la manera más adecuada.

Estas situaciones contravienen de las Normas de TI lo siguiente:

> (…) Capítulo I "Normas de aplicación general"
>
> Norma 1.4.1 "Implementación de un marco de seguridad de la información", su inciso c) el cual reza lo siguiente:

"(…) Documentar y mantener actualizadas las responsabilidades tanto del personal de la organización como de terceros relacionados.

Recalcar nuevamente la Norma 1.4.5 Control de acceso, en lo que nos interesa, lo siguiente:

La organización debe proteger la información de accesos no autorizados.

Para dicho propósito debe:

d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.

e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.

Capítulo III Implementación de tecnologías de información.

Norma 3.1 Consideraciones generales de la implementación de TI, lo siguiente:
(…) c. Garantizar la participación activa de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas.

d. Instaurar líderes de proyecto con una asignación clara, detallada y documentada de su autoridad y responsabilidad.

La Norma 3.2 "Implementación de software" su inciso c), el cual describe:"(…) Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software"

Capítulo V, la norma 5.1 "Seguimiento de los procesos de TI", la cual indica:

> (…) La organización debe asegurar el logro de los objetivos propuestos como parte de la gestión de TI, para lo cual debe establecer un marco de referencia y un proceso de seguimiento en los que defina el alcance, la metodología y los mecanismos para vigilar la gestión de TI. Asimismo, debe determinar las responsabilidades del personal a cargo de dicho proceso.

2.3.2 Sobre el personal usuario de las dependencias que administran los sistemas objeto de estudio.

En cuanto al personal de instancias usuarias, se determinó que en las oficinas de "Registro y Administración estudiantil" y "Tesorería", las acciones referentes a solicitud de creación de usuarios y sus perfiles, aparte de las jefaturas, son realizadas por otros funcionarios, a saber:

- Teddy Chang Amen, Encargado de Admisión y Matrícula.
- Tatiana Bermúdez Vargas, Encargada de Graduación, Certificación y Actas.

  Ambos por la Oficina de Registro y Administración Estudiantil.

- Magaly Moya Lacayo, Encargada de la Unidad de Cuentas por Pagar de la Oficina de Tesorería

No se localizó documento que evidencie la designación, la autorización y la responsabilidad por la ejecución de las actividades encomendadas a los funcionarios anteriormente indicados. Sobre el particular se transcriben los comentarios dados por las jefaturas de ambas oficinas ante consulta realizada por esta Auditoría Interna:

Licda. Susana Saborío Álvarez: "(…) La designación se realizó vía correo electrónico, por motivo de cambio de computadora no cuento con copia de los emitidos, ya que no se realizó respaldo de la información. (Entrevista aplicada14/05/2012, ítem 15)

Licda. Ana Cristina Pereira Gamboa: "(…) en el caso de Magaly Moya, se le comunicó de la labor vía correo electrónico. No se cuenta con el correo electrónico." (Entrevista aplicada 05/06/2012, ítem 15)

Para las situaciones indicadas tanto del personal de la DTIC, como el de las instancias usuarias, se resalta la siguiente normativa que regula el accionar de la Universidad:

Del Estatuto de Personal de la UNED, de su Capítulo III-Deberes y Prohibiciones, su Artículo 33: Obligaciones de la UNED o sus representantes, en lo que nos interesa, lo siguiente: "(…) Sin perjuicio de las consignadas en otras normas aplicables, son obligaciones de la UNED respecto a sus funcionarios, las siguientes: a) Darles instrucciones claras sobre sus deberes y responsabilidades, competencia y ámbito de acción".

De las Normas de CI (N-2-2009-CO-DFOE) su norma 4.5.1 "Supervisión constante", la cual detalla: "(…) El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI (Sistema de Control Interno), así como emprender las acciones necesarias para la consecución de los objetivos.

Además resaltar del Artículo 12 "Deberes del Jerarca y de los titulares subordinados en el sistema de control Interno" de la Ley General de Control Interno, establece lo siguiente:

> (…) En materia de control interno, al jerarca y los titulares subordinados les corresponderá cumplir, entre otros, los siguientes deberes:
>
> a) Velar por el adecuado desarrollo de la actividad del ente o del órgano a su cargo.
>
> b) Tomar de inmediato las medidas correctivas, ante cualquier evidencia de desviación o irregularidades.

Así también del documento denominado "Normas de control interno para el Sector Público" (N-2-2009-CO-DFOE) Publicadas en "La Gaceta" Nº 26 del 6 de febrero, 2009, lo sucesivo:

> (…) 2.5.1 Delegación de funciones

El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que la delegación de funciones se realice de conformidad con el bloque de legalidad, y de que conlleve la exigencia de la responsabilidad correspondiente y la asignación de la autoridad necesaria para que los funcionarios respectivos puedan tomar las decisiones y emprender las acciones pertinentes.

2.5.2 Autorización y aprobación

La ejecución de los procesos, operaciones y transacciones institucionales debe contar con la autorización y la aprobación respectivas de parte de los funcionarios con potestad para concederlas, que sean necesarias a la luz de los riesgos inherentes, los requerimientos normativos y las disposiciones institucionales.

2.5.3 Separación de funciones incompatibles y del procesamiento de transacciones

El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que las funciones incompatibles, se separen y distribuyan entre los diferentes puestos; así también, que las fases de autorización, aprobación, ejecución y registro de una transacción, y la custodia de activos, estén distribuidas entre las unidades de la institución, de modo tal que una sola persona o unidad no tenga el control por la totalidad de ese conjunto de labores.

Cuando por situaciones excepcionales, por disponibilidad de recursos, la separación y distribución de funciones no sea posible debe fundamentarse la causa del impedimento. En todo caso, deben implantarse los controles alternativos que aseguren razonablemente el adecuado desempeño de los responsables.

El incumplimiento a lo normado aunado a la ausencia de procedimientos formales tanto por la DTIC como por las instancias usuarias en relación con la asignación de las actividades y de la responsabilidad al recurso humano, da paso a no contar con documentación que respalde las funciones administrativas, técnicas, de dirección, de coordinación, control y responsabilidades para los funcionarios que ejecutan actualmente la labor, siendo esto limitante para sentar eventuales responsabilidades en caso de detectarse incumplimiento de las instrucciones encomendadas.

2.4 Controles de acceso y bitácoras inmersas en las estructuras de los sistemas objeto de estudio.

2.4.1 Sobre los controles de acceso desarrollados en las estructuras de los sistemas.

En revisión realizada por esta Auditoría Interna de los controles desarrollados en las estructuras de los sistemas objeto de estudio los cuales residen en el AS 400, y pruebas de verificación realizadas en coordinación con el funcionario Rolando Rojas Coto, Encargado de la Unidad Estratégica Operaciones de la DTIC, se determinó lo siguiente:

- Ausencia de control, específicamente que no permita cuando se dé un cambio de clave, la aceptación de claves anteriormente utilizadas.

- Ausencia de control que tenga como fin la inactivación del acceso del usuario, cuando se dé el caso de un margen de intentos de acceso fallidos, al tratar de ingresar con una clave (contraseña) incorrecta.

- El control de bloqueo de la sesión del usuario en el sistema actualmente se encuentra inactivo; éste tiene como fin que en caso de un lapso de tiempo definido de no utilización del sistema obliga al usuario a autenticar nuevamente sus credenciales.

Sobre la inactivación de este control el Director de la DTIC Mag. Durán, indicó:

> "(…) lo que sucede es que por motivo de que se deben correr procesos de contabilidad y de planillas que requieren tiempos muy amplios, se tomó la decisión de inactivar este control, ya que impedía que se concluyeran.
>
> Esta situación se presentó con el equipo AS 400, el cual fue remplazado por el ISERIES.

> A la fecha no se han realizado las pruebas para verificar que con este nuevo equipo estos procesos se ejecutan en tiempo menor en su ejecución y poder activar nuevamente este control.
>
> La inactivación del control fue tomada a nivel de la DTIC, no se coordinó ni comunicó a los administradores por la parte usuaria de los sistemas SAE, Financiero-Contable y de Presupuesto." (Entrevista aplicada 14/05/2012, ítem Nº 11)

Sobre el último párrafo del comentario aportado por el Mag. Durán se transcribe lo señalado por la Licda. Susana Saborío Álvarez, Jefa de la Oficina de Registro y Administración Estudiantil, Oficina usuaria y administradora del sistema SAE sobre dicho control:

> (…) El Sistema SAE sí lo tenía, he verificado y hoy día este control de seguridad no está activo.
>
> La eliminación o suspensión de este control no se coordinó con mi persona, a la fecha desconozco la justificación o los motivos que asumió la DTIC, para detener su ejecución" (Entrevista aplicada 14/05/2012, ítem Nº 12)

Lo anterior es muestra clara de una inadecuada coordinación y comunicación por parte de la DTIC, con las instancias usuarias de las aplicaciones objeto de estudio. Además no cumple con la norma 2.4 Independencia y recurso humano de la Función de TI de las Normas de TI, la cual detalla: "(…) El jerarca debe asegurar la independencia de la Función de TI respecto de las áreas usuarias **y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas.** (El resaltado es nuestro)

Y del capítulo III "Implementación de tecnologías de información", su norma 3.1 "Consideraciones generales de la implementación de TI", su inciso c), el cual se transcribe: "(…) Garantizar la participación activa de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas.

2.4.2 Sobre la existencia y control de bitácoras inmersas en los sistemas objeto de estudio.

En relación con las bitácoras, se determinó que los sistemas “Financiero Contable y Presupuesto” sus estructuras carecen de estos sitios de alojamiento (bitácoras) donde se almacene información de eventos relacionados con el uso del sistema, en cuanto a eliminación o modificación de información o dato alguno sensible, de los principales procesos que ejecuta cada una de las instancias usuarias, esta información es el equivalente a pistas, las cuales tienen como fin ser la evidencia que permita determinar, identificar y responsabilizar los movimientos realizados.

Sobre la situación el Mag. Durán indicó que los sistemas no cuentan con bitácoras de movimientos realizados por usuarios autorizados, tampoco con las de movimientos realizados a nivel de bases de datos; que se cuenta con la referente al histórico del cambio de clave a nivel de aplicación pero, por cambio de servidor, no se encuentra activa, por lo tanto no se cuenta con la información. (Entrevista aplicada el 14/05/2012, ítem 10 y 12).

También cabe hacer la observación del desconocimiento por la parte usuaria, en cuanto a la existencia de bitácoras para los procesos esenciales que ejecutan en los sistemas que operan; sobre esta situación las jefaturas de las oficinas de Tesorería y Presupuesto, en su orden manifestaron:

Lcda. Ana cristina Pereira Gamboa

> (…) Lo desconozco, a la fecha no se ha requerido reporte alguno.
>
> A mi parecer todo sistema con que cuenta esta institución, debe estar contemplado por la DTIC la creación de las bitácoras, en las cuales se registren datos claves de movimientos realizados por usuarios. (Entrevista aplicada 05/06/2012, ítem Nº 13)

Mag. Mabel León Blanco

> (…) Sinceramente, desconozco si el sistema cuenta con bitácoras para el registro de esa información. Esta consulta la puede aclarar la DTIC. (Entrevista aplicada el 14/06/2012, ítem Nº 13)

En el caso del sistema SAE, aunque cuenta con bitácoras para procesos sensibles como por ejemplo: cambio de notas, matrícula, reconocimiento, ingreso y acreditación de estudiantes, éstas no son sujetas de mecanismo o procedimiento alguno para su revisión periódica.

Las debilidades relacionadas a los controles de acceso y las bitácoras, contravienen de lo regulado en las Normas de TI, lo siguiente:

> Del Capítulo I Normas de aplicación general las siguientes normas:
>
> (…) 1.4.5 Control de acceso, en lo que nos interesa lo siguiente:
>
> La organización debe proteger la información de accesos no autorizados.
>
> Para dicho propósito debe:
>
> …
>
> f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.
>
> i. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.
>
> j. Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.

De la norma 1.4.6 “Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica”, su inciso c, el cual reza lo siguiente:

> (…) La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.
>
> Para ello debe:
>
> …
>
> c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.

Además del Capítulo III Implementación de tecnologías de información, de la norma 3.1 Consideraciones generales de la implementación de TI, su inciso f) el cual señala lo siguiente: "(…) Contar con una definición clara, completa y oportuna de los requerimientos, como parte de los cuales debe incorporar aspectos de control, seguridad y auditoría bajo un contexto de costo – beneficio.

También destacar del documento denominado "Normas de control interno para el Sector Público" (N-2-2009-CO-DFOE) Publicadas en "La Gaceta" Nº 26 del 6 de febrero, 2009, lo siguiente:

> (…) 5.8 Control de sistemas de información
>
> El jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter.
>
> 5.9 Tecnologías de información
>
> El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. Para ello deben observar la normativa relacionada con las tecnologías de información, emitida por la

CGR. En todo caso, deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información

La ausencia de un marco metodológico para el desarrollo y control de proyectos de sistemas computarizados, situación ya hecha del conocimiento de la administración activa mediante informe "Evaluación del Proyecto Sistema de Gestión y Desarrollo de Personal (SGDP) de la Oficina de Recursos Humanos", informe Nº X-24-2011-04, en su resultado 2.1.3.; la ausencia de procedimientos tanto por la DTIC como por las instancias usuarias, que tengan como fin la valoración periódica de la seguridad de los sistemas, son posibles causas de las situaciones denotadas dando paso a que las aplicaciones adolezcan de mecanismos automatizados en sus estructuras que minimicen el riesgo de accesos o cambios no autorizados a información contenida en los sistemas en estudio, así como de las bitácoras de los procesos automatizados sensibles, en las cuales se resguarde información que permita determinar incidentes de seguridad, entre otros, con el fin de identificar, resolver y sentar la responsabilidad del caso.

2.5 Sobre las gestiones para las claves de acceso para usuarios de los sistemas objeto de estudio.

Al ser las claves (contraseñas) el mecanismo utilizado por la UNED, para el acceso a los sistemas, debe adoptar e implantar procedimientos para una adecuada gestión, fijando controles que garanticen la confidencialidad e integridad de las mismas.

Sobre las gestiones para la creación, control, comunicación y resguardo de las claves de acceso (password o contraseña), para los usuarios de los sistemas informáticos de la UNED, se determinó que la DTIC no cuenta con un procedimiento debidamente formalizado para llevar a cabo las actividades, el cual enmarque como mínimo lo siguiente:

- Las instrucciones o lineamientos estandarizados para la definición de la clave, su longitud, su composición (si se conforma de solo letras, caracteres o números; o mediante la combinación de los tres), así como de alguna otra consideración que coadyuve a los usuarios a la definición y creación de clave acceso robusta.

- Mecanismos que garanticen la autenticidad del funcionario, la debida entrega, la recepción y la confidencialidad de la clave. Lo anterior por cuanto no se tiene definidas las instrucciones y delimitado el canal o medio por el cual se lleve a cabo la actividad, ya que aparte de oficio o nota, también se gestiona por correo electrónico o vía teléfono; en relación a esta última actualmente la práctica es la siguiente:

Ante la solicitud de reactivación o cambio de clave por motivo de bloqueo u olvido por parte del usuario, el funcionario de la DTIC que atiende la solicitud procede a realizar la gestión cambiando la clave anterior por "UNED 2012", e indicarle la misma al solicitante para que ingrese al sistema, además al ingresar, la aplicación le exigirá cambiar la clave dada. Las acciones anteriores las realiza sin que medie mecanismo o instrucción alguna, que le asegure y confirme que el solicitante vía teléfono es quién dice ser y que está autorizado a utilizar el sistema o módulo.

Lo supra citado es reafirmado tanto por el Director de la DTIC como por el encargado de la Unidad Estratégica de Operaciones, Unidad que lleva a cabo estas gestiones, quienes en su orden manifestaron lo siguiente:

Mag. Francisco Durán Montoya.

> (…) No se cuenta con instrumentos (formularios, orden de servicio, etc.) para la tramitación de gestiones referentes a la activación, renovación, y comunicación de clave de acceso para usuarios de los sistemas automatizados SAE, Financiero Contable y de Presupuesto, además adicionó que tampoco se cuenta con un instrumento que estandarice el trámite de las solicitudes y el comunicado del cumplimiento de las mismas." (Entrevista aplicada14/05/2012, ítem 3).

Rolando Rojas Coto.

> (…) No se cuenta con documentación alguna referente a la definición de las claves de acceso (contraseñas) donde se enmarque la longitud mínima y lineamientos a considerar para la creación y definición de claves robustas". (Entrevista aplicada 30/07/2012, ítem 4).

Todo lo anterior se contrapone a la siguiente normativa:

De las Normas de TI del Capítulo I, las siguientes normas:

1.4.4 Seguridad en las operaciones y comunicaciones

La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información.

Para ello debe:

(…) a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.

Nuevamente recalcar la Norma 1.4.5 Control de acceso, en lo que nos interesa, lo siguiente:

La organización debe proteger la información de accesos no autorizados.

Para dicho propósito debe:

…

f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.

Del documento denominado “Normas de control interno para el Sector Público” (N-2-2009-CO-DFOE) Publicadas en “La Gaceta” Nº 26 del 6 de febrero, 2009, lo siguiente:

5.7 Calidad de la comunicación

El jerarca y los titulares subordinados, según sus competencias, deben establecer los procesos necesarios para asegurar razonablemente que la comunicación de la información se da a las instancias pertinentes y en el tiempo propicio, de acuerdo con las necesidades de los usuarios, según los asuntos que se encuentran y son necesarios en su esfera de acción. Dichos procesos deben estar basados en un enfoque de efectividad y mejoramiento continuo.

5.7.1 Canales y medios de comunicación

Deben establecerse y funcionar adecuados canales y medios de comunicación, que permitan trasladar la información de manera transparente, ágil, segura, correcta y oportuna, a los destinatarios idóneos dentro y fuera de la institución.

5.7.2 Destinatarios

La información debe comunicarse a las instancias competentes, dentro y fuera de la institución, para actuar con base en ella en el logro de los objetivos institucionales.

5.7.3 Oportunidad

La información debe comunicarse al destinatario con la prontitud adecuada y en el momento en que se requiere, para el cumplimiento de sus responsabilidades.

5.7.4 Seguridad

Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección

> apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran.

Las situaciones supra citadas son muestra que la gestión carece de una adecuada administración, por ende ausente de procedimientos o lineamientos debidamente formalizados y avalados por la instancia respectiva, cuyo fin sea el asegurar la adecuada administración, seguridad, confiabilidad y control de las actividades referentes a la creación, comunicación, recibido y resguardo de la clave de acceso.

2.6 Sobre la valoración de Riesgos.

En la investigación realizada se determinó que la DTIC no cuenta con la identificación y evaluación de riesgos según clasificación y criticidad de los recursos de TI, por lo tanto se carece de la definición y valoración de riesgos que pueden afectar directa o indirectamente las actividades referentes a la creación de usuarios, perfiles y claves de acceso para usuarios que operan los sistemas con que cuenta la UNED

En cuanto a esta situación, el Director de la DTIC, Mag. Durán, indicó que actualmente se trabaja en el mapeo de los riesgos, que como antecedente existe una valoración de riesgos a modo general que se realizó aproximadamente hace un año y medio. Dicho funcionario se comprometió a remitir la documentación tanto de la valoración como del mapeo, pero a la fecha no cumplió dicha acción, lo cual impidió evidenciar lo expuesto.

Esta situación también se presenta en las instancias usuarias de los sistemas objeto de estudio, ya que al igual que en la DTIC, no cuentan con la definición y valoración de los riesgos que pueden incidir en las gestiones o procesos que ejecutan en las aplicaciones automatizadas objeto de estudio; a continuación cabe transcribir los comentarios aportados por las jefaturas:

Mag. Mabel León Blanco, Jefa de la Oficina de Presupuesto.

> (…) Este tema solo se ha tratado de forma verbal con el analista de la DTIC, se han tomado medidas a nivel de la aplicación, entre

> esas mediadas puedo mencionar que solo el personal de esta oficina está autorizado para incluir, modificar y borrar información. (Entrevista aplicada 14/06/2012, ítem Nº 6).

Licda. Susana Saborio Álvarez, Jefa de la Oficina de Registro y Administración Estudiantil.

> (…)Aparte de conformar el equipo de trabajo y realizar las gestiones de capacitación en control interno, la cual solo ha sido recibida por Karolina Sánchez y mi persona, no se ha realizado ninguna otra, por lo tanto las situaciones expuestas en la valoración a la fecha se mantienen, así también la ausencia de un plan para mitigar las mismas. (Entrevista aplicada el 14/05/2012, ítem Nº 29)

Además aporta a esta Auditoría Interna copia de documentación referente a la elaboración del informe del proceso de Autoevaluación del Control Interno de la oficina a su cargo, en ésta se muestran los riesgos definidos en ese momento para dicha oficina y fue trasladado mediante oficio O.R.-311-2008, fechado 27/10/2008 al MBA. Carlos Montoya R, Encargado de la Unidad de Control; cabe hacer la observación que la documentación aportada carece del recibido por dicha unidad.

Licda. Ana Cristina Pereira Gamboa, Jefa de la Oficina de Tesorería.

> (…) El estudio fue elaborado por PROVAGARI. Esta Oficina no cuenta con el documento, tampoco se cuenta con el plan de medidas para la mitigación de los riesgos.
>
> Entre las medidas que ha tomado esta oficina, está la revisión de la documentación que se genera con estos sistemas (reportes), contra la documentación recibida y autorizada para ejecutar los movimientos. (Entrevista aplicada 05/06/2012, ítem Nº 6)

Sobre la “Gestión de Riegos” las Normas de TI, señala lo siguiente:

Capítulo I Normas de aplicación general:

(…)1.3 Gestión de riesgos: La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de Tecnologías de Información, mediante una gestión continua de riesgos que está integrada al sistema específico de valoración institucional y considere el marco normativo que le resulte aplicable.

…

1.4.1 Implementación de un marco de seguridad de la información:

La organización debe implementar un marco de seguridad de la información, para lo cual debe:

a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.

b. Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.

1.4.3 Seguridad física y ambiental

La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos.

Como parte de esa protección debe considerar:

…

d. El debido control de los servicios de mantenimiento.

Sobre este tema también la Ley General de Control Interno exterioriza lo siguiente:

Artículo 14

(…) Valoración del riesgo. En relación con la valoración del riesgo, serán deberes del jerarca y los titulares subordinados, entre otros, los siguientes:

a. Identificar y analizar los riesgos relevantes asociados al logro de los objetivos y las metas institucionales, definidos tanto en los planes anuales operativos como en los planes de mediano y de largo plazos.

b. Analizar el efecto posible de los riesgos identificados, su importancia y la probabilidad de que ocurran, y decidir las acciones que se tomarán para administrarlos.

c. Adoptar las medidas necesarias para el funcionamiento adecuado del sistema de valoración del riesgo y para ubicarse por lo menos en un nivel de riesgo organizacional aceptable.

d. Establecer los mecanismos operativos que minimicen el riesgo en las acciones por ejecutar.

Artículo 18.

(…) Sistema específico de valoración del riesgo institucional. Todo ente u órgano deberá contar con un sistema específico de valoración del riesgo institucional por áreas, sectores, actividades o tarea que, de conformidad con sus particularidades, permita identificar el nivel de riesgo institucional y adoptar los métodos de uso continuo y sistemático, a fin de analizar y administrar el nivel de dicho riesgo.

La Contraloría General de la República establecerá los criterios y las directrices generales que servirán de base para el establecimiento y funcionamiento del sistema en los entes y órganos seleccionados, criterios y directrices que serán obligatorios y prevalecerán sobre los que se les opongan, sin menoscabo de la obligación del jerarca y titulares subordinados referida en el artículo 14 de esta Ley.

Artículo 19.

> Responsabilidad por el funcionamiento del sistema. El jerarca y los respectivos titulares subordinados de los entes y órganos sujetos a esta Ley, en los que la Contraloría General de la República disponga que debe implantarse el Sistema Específico de Valoración de Riesgo Institucional, adoptarán las medidas necesarias para el adecuado funcionamiento del Sistema y para ubicarse al menos en un nivel de riesgo institucional aceptable.

Así también de las "Directrices generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI)" (D-3-2005-CO-DFOE), aprobadas mediante resolución R-CO-64-2005 del 1º de julio de 2005, y publicadas en el Diario Oficial "La Gaceta" Nº 134 del 12 de julio de 2005, su directriz 2.1, la cual fue modificada mediante el documento N-2-2009-CO-DFOE, para que se lea de la siguiente manera:

> (…) "2.1 Ámbito de aplicación. Toda institución pública deberá establecer y mantener en funcionamiento un Sistema Específico de Valoración del Riesgo Institucional (SEVRI) por áreas, sectores, actividades o tareas, de acuerdo, como mínimo, con lo establecido en estas directrices generales que serán de acatamiento obligatorio. Se exceptúa de su aplicación a las instituciones de menor tamaño, entendidas como aquellas que dispongan de un total de recursos que ascienda a un monto igual o inferior a seiscientas mil unidades de desarrollo y que cuenten con menos de treinta funcionarios, incluyendo al jerarca, los titulares subordinados, y todo su personal, quienes deberán observar lo que al efecto establecen las "Normas de control interno para el sector público".

Ausencia de supervisión y seguimiento a la gestión de riesgos conlleva al incumplimiento de normativa que establece y regula el instaurar y mantener en funcionamiento un Sistema Específico de Valoración del Riesgo Institucional (SEVRI), lo cual da paso a no contar con la clasificación y definición de los posibles riesgos que puedan incidir en las actividades referentes a la creación de usuarios, perfiles y claves de acceso para usuarios que operan los sistemas con que cuenta la UNED, así como para los procesos automatizados que ejecutan las instancias usuarias, además del plan de mejoras para mitigar su impacto y los mecanismos para su evaluación periódica.

2.7 Sobre capacitación al personal para operar los sistemas objeto de estudio.

La capacitación debe dirigirse tanto a nuevos usuarios como aquellos que operaran el sistema y que por variación o asignación de otras tareas se requiere que utilicen otras opciones de la aplicación; para la adecuada gestión se debe contar con lineamientos formalizados que permitan determinar: su objetivo, a ¿quién (es)? se capacitará y ¿quién (es)? los capacitará, así como los métodos aplicados.

Sobre la formalización de lineamientos o procedimientos para gestionar y evaluar la actividad, se determinó que estos están ausentes, tanto a nivel de la DTIC como de instancias usuarias, además que por parte de estas instancias cuando corresponde dar capacitación, esta se imparte en funcionamiento real del sistema o sea en producción, sin que medie un ambiente de pruebas.

Sobre esta situación el Mag. Francisco Durán Montoya, Director de la DTIC, manifestó que no se cuenta con procedimientos o actividades para capacitar a funcionarios de nuevo ingreso en cuanto al uso de opciones de los sistemas: SAE, Financiero-Contable y de Presupuesto, así como para validar su aplicación, además adicionó a su respuesta lo siguiente:

> (…) A mi parecer esta actividad es muy importante, hay usuarios que desconocen todas las funciones y procesos de las aplicaciones, en otros casos solo una persona es la que conoce todas las funciones del sistema en cuanto al proceso que realiza, lo que da paso a que se cree dependencia de ese funcionario, ya que ningún otro de la unidad u oficina ha sido capacitado.
>
> Por parte de la DTIC no se cuenta con el personal para encomendarle esta labor. (Entrevista aplicada14/05/2012, ítem 7)

Por otro lado las jefaturas de instancias usuarias de las aplicaciones manifestaron lo siguiente:

Mag. Mabel León Blanco, Jefa de la Oficina de Presupuesto.

(…) Por parte de esta Oficina la capacitación es dada en la marcha de las actividades según rol asignado en el sistema. No se cuenta con mecanismos internos, ni se tiene costumbre de documentar estas acciones, además la rotación del personal de esta oficina es mínima. (Entrevista aplicada 14/06/2012, ítem Nº 8).

Licda. Ana cristina Pereira Gamboa, Jefa de la Oficina de Tesorería.

(…) En el caso de los funcionarios de esta Oficina la capacitación se da sobre la marcha (en producción) y no se emite documentación alguna que valide su aplicación, por ejemplo:

Caja Chica

Fondo de trabajo

Fondos de importes.

En estos casos tenemos procesos de revisión de la información para validar que no se haya incorporado información errónea, Ejemplo revisión de los reportes referentes al cierre de caja, revisión de ordenes de emisión de pagos. (Entrevista aplicada 05/06/2012, ítem Nº 8)

Licda. Susana Saborio Álvarez, Jefa de la Oficina de Registro y Administración Estudiantil.

(…) Efectivamente esos son las tres formas:

1. Son en el lugar de trabajo cuando así lo solicita, directamente con el usuario y con el trabajo que debe realizar el Encargado en real.

2. Son masivas o videoconferencia cuando hay algo nuevo para todos, por medio de diapositivas que contienen imágenes de lo que van a ver y que también se encuentran en el Manual.

3. Son por medio de manuales cuando los usuarios nuevos son asignados, y si consideran que requieren más, solicitan y aplicamos el punto No.1. (correo electrónico fechado 10/12/2012, hora 10:32 AM.

La norma 1.4 de las Normas de TI la cual la describe como gestión de la seguridad de la información y en la cual destaca como uno de los aspectos a considerar en la implementación de una política de seguridad el compromiso del personal con la seguridad de la información (norma 1.4.2) de la cual se recoge lo siguiente:

> (…) El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI.
>
> Para ello, el jerarca, debe:
>
> a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.
>
> b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.

La ausencia de un procedimiento que plasme los lineamientos o pasos a seguir y cumplir, para capacitar usuarios en el uso de las aplicaciones automatizadas, tanto por la DTIC como de las instancias usuarias, da lugar a las situaciones descritas anteriormente, lo cual es muestra de que la gestión no se realiza y se controla de forma adecuada, lo anterior pone en alto riesgo la veracidad, confiabilidad y seguridad de la información, además de no poder determinar, contar y controlar lo siguiente:

- Posibles instructores internos que se encuentran familiarizados con la aplicación según las diferentes áreas funcionales que utilizan.

- Los métodos, los temas a desarrollar, los documentos y materiales diseñados para impartir la capacitación.

- Lugar o lugares convenientes para impartir la capacitación, así como el ambiente pruebas para ejecutar la aplicación sin que medie riesgo alguno que pueda afectar la información.

- Los mecanismos de control y gestión que respalden la evaluación de la capacidad del aprendizaje adquirido por el usuario, que permita asegurar que ha sido instruido adecuadamente para operar el sistema, sumado a esto también lo referente al debido resguardo de la documentación generada.

2.8 Sobre conformación y resguardo de la documentación referente a las gestiones realizadas.

Se determinó que la DTIC no cuenta con instrucciones o lineamientos debidamente formalizados y establecidos, para el resguardo de la documentación e información generada de las actividades y tareas referentes a la creación, activación o inhabilitación de usuarios, perfiles y niveles de privilegios (opciones habilitadas) para los sistemas objeto de estudio. Sobre la situación el Mag. Durán exteriorizó lo siguiente: "(…) La Dirección no cuenta ni ha emitido instrucción alguna referente al resguardo de información que respalde estas gestiones". (Entrevista aplicada el 14/05/2012, ítem 16).

La situación es reafirmada por los líderes de proyectos María Luisa Molina Méndez (entrevista aplicada 01/06/2012, ítem 17) y Randall Gutiérrez López (entrevista aplicada 08/11/2012, ítem 13), ambos ubicados en la Unidad Estratégica de Sistemas (UESI), unidad que recibe la solicitud para crear y programar el menú que se le debe asociar al usuario, además de coordinar con la Unidad Estratégica de Operaciones (UEO) las demás gestiones y finalmente es la que comunica a la instancia usuaria el cumplimiento de lo solicitado.

Caso contrario, lo manifestado por el funcionario Rolando Rojas Coto, Encargado de la Unidad UEO ; en entrevista realizada el día 30/07/2012, pues afirmó la existencia de instrucciones o lineamientos dirigidos al resguardo de la documentación relacionada a dichas actividades, pero en la información y documentación (formato digital) remitida por el Sr. Rojas el día 08/08/2012 a esta Auditoría Interna, no se localizó alguna que evidencie y confirme lo manifestado; aparte, tampoco la documentación en orden cronológico de las diferentes solicitudes recibidas y tramitadas por la unidad bajo su cargo en el año 2011, lo cual impidió verificar y determinar la cantidad de trámites llevados a cabo en ese año.

La ausencia de instrucciones o lineamientos debidamente formalizados y establecidos, para el resguardo de la documentación ya sea esta en formato físico o digital, también se extiende a las instancias usuarias de estos sistemas, a continuación como complemento de la situación, se detallan las manifestaciones aportadas por las jefaturas:

Licda. Susana Saborio Álvarez, Jefa de la Oficina de Registro y Administración Estudiantil: "(…) No se cuenta con instrucciones o lineamientos para el resguardo de la documentación generada de las acciones realizadas, ya que la mayoría de las solicitudes se tramitan vía correo electrónico." (Entrevista aplicada 14/05/2012, ítem 17).

Licda. Ana cristina Pereira Gamboa, Jefa de la Oficina de Tesorería: "(…) He emitido instrucciones para la creación de usuarios y claves, pero no para el resguardo de la documentación generada de esas acciones." (Entrevista aplicada 05/06/2012, ítem 17).

Mag. Mabel León Blanco, Jefa de la Oficina de Presupuesto.

> (…) Por costumbre si se archiva la documentación, pero el año pasado por problemas de goteras, mucha documentación se daño, entre esta la de estas gestiones.
>
> Verbalmente he hecho el recordatorio de resguardar la documentación generada de estas acciones." (Entrevista aplicada 14/06/20012, ítem 17)

En el Capítulo 1 de las Normas de TI, su norma 1.4 la cual la describe como "Gestión de la seguridad de la información" y en la que destaca como uno de los aspectos a considerar en la implementación de una política de seguridad el tener presente las medidas de seguridad relacionadas con el manejo de la documentación, el establecimiento de estas medidas debe ser en una proporción razonable entre su costo y los riesgos asociados.

Así también rescatar del Capítulo III, de la norma 3.1 Consideraciones generales de la implementación de TI su inciso a) el cual detalla: "(…) Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.

Del documento denominado “Normas de control interno para el Sector Público” (N-2-2009-CO-DFOE) Publicadas en “La Gaceta” Nº 26 del 6 de febrero, 2009 lo siguiente:

> 5.4 Gestión documental
>
> El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información propicien una debida gestión documental institucional, mediante la que se ejerza control, se almacene y se recupere la información en la organización, de manera oportuna y eficiente, y de conformidad con las necesidades institucionales.
>
> 5.5 Archivo institucional
>
> El jerarca y los titulares subordinados, según sus competencias, deben implantar, comunicar, vigilar la aplicación y perfeccionar políticas y procedimientos de archivo apropiados para la preservación de los documentos e información que la institución deba conservar en virtud de su utilidad o por requerimiento técnico o jurídico. En todo caso, deben aplicarse las regulaciones de acatamiento obligatorio atinentes al Sistema Nacional de Archivos.
>
> Lo anterior incluye lo relativo a las políticas y procedimientos para la creación, organización, utilización, disponibilidad, acceso, confidencialidad, autenticidad, migración, respaldo periódico y conservación de los documentos en soporte electrónico, así como otras condiciones pertinentes.

La usencia de lineamientos o instrucciones debidamente formalizadas; referentes al resguardo de la documentación, así como la informalidad y la falta de estandarización en la gestión de trámites referentes a usuarios y sus accesos da paso a no contar con documentación o información ordenada y resguardada, que evidencie y asegure que las acciones realizadas fueron avaladas y autorizadas.

Cabe hacer la observación que dicha situación fue limitante para realizar pruebas de verificación por parte de esta Auditoría Interna.

3. Conclusiones.

La inadecuada administración y gestión de la calidad dirigida a la eficiencia y mejoramiento continuo del software, ligado a la ausencia de una Política de Seguridad de la Información, en cumplimiento a normativa y buenas prácticas, en la cual se defina y formalicen los procedimientos, lineamientos y reglas correspondientes a los aspectos relacionados con el control de acceso para asegurar y proteger la información de la organización, conlleva a que la administración adolezca entre otras cosas de:

3.1. Procedimientos, lineamientos o acuerdos debidamente formalizados y avalados por el Consejo de Rectoría o Consejo Universitario según corresponda, para el trámite para la creación, activación, modificación o inactivación de usuarios y sus perfiles (opciones habilitadas en el sistema), así como de las claves de acceso para funcionarios que operan los sistemas objeto de estudio. (Ver resultado 2.1).

3.2. Documentación en la que se plasme la identificación y detalle de los procesos de los sistemas automatizados “Financiero Contable”, “Presupuesto” y “SAE”, a lo que se suma también la correspondiente a la definición y clasificación de usuarios o grupos de usuarios, sus perfiles (accesos); estos bajo el esquema del proceso o procesos de cada sistema e instancia usuaria, alineados también a los cargos o puestos de cada una de estas. (Ver Resultado 2.2.1).

3.3. Aparte de la ausencia de esta información o documentación se agrega la carencia de la automatización en cada sistema del proceso para el registro y control de los usuarios según clasificación y definición de privilegios autorizados y creados para operar el mismo, dando paso estas situaciones a las subsiguientes:

- No se tiene un adecuado control para el mantenimiento de usuarios creados para operar las aplicaciones objeto de estudio.

- No se cuenta con una debida estandarización para la inclusión e identificación de usuarios.

- La opción de “Suprimir” usuarios, se mantiene activa a nivel de administración del ambiente AS 400, lo cual permite realizar acciones de eliminación de usuarios sin existir ningún control, aunado a esta condición se da la ausencia

de una bitácora en el sistema o ambiente donde se registren las pistas o registros que permitan identificar cual usuario (s) a nivel técnico (DTIC), realizó o realizaron las acciones.

- El método actual que utiliza la DTIC para crear un menú para un usuario del sistema no permite tener un adecuado control de todos los registros de usuarios creados e incorporados por sistema, generando en algunos casos desconocimiento de los permisos dados a grupos de usuarios o listas de usuarios.

- Se carece de opciones automatizadas a nivel del ambiente AS 400 para el procesamiento y emisión de reportes de usuarios por cada sistema, así como de otros debidamente estandarizados según opciones o parámetros definidos como por ejemplo: estado (inactivo(s) o activo (s), por grupos pertenecientes al sistema u otros.

- Ausencia de un procedimiento o control estandarizado que implique la revisión periódica de los usuarios creados, el cual tenga como fin determinar si los usuarios cuentan con la correcta asignación de roles y privilegios autorizados; y que correspondan a funcionarios activos. (Ver resultado 2.2.2).

3.4. Informalidad en la designación de las actividades a ejecutar y en la definición de responsabilidad al llevar a cabo las mismas, tanto de la DTIC como de las instancias usuarias de los sistemas objeto de estudio. (Ver resultado 2.3).

3.5. Ausencia de programación y desarrollo de controles de acceso, tanto en las estructuras de los sistemas objeto de estudio como del AS 400. Además controles desarrollados actualmente están inactivos sin que medie estudio y justificación de dicho proceder. (Ver resultado 2.4.1).

A lo anterior se une la usencia de la programación y desarrollo de bitácoras o sitios de alojamiento, donde se almacenen registros en orden cronológico para identificar al usuario que realizó cambio o registro alguno a información o datos sensibles de los principales procesos que ejecuta cada una de las instancias, estos registros son el equivalente a pistas, las cuales tienen como fin ser la información que permita determinar y responsabilizar los movimientos realizados. (Ver resultado 2.4.2).

3.6 Ausente de procedimientos o lineamientos debidamente formalizados y avalados por la instancia respectiva, cuyo fin sea el asegurar la adecuada administración, seguridad, confiabilidad y control de las actividades referentes a la creación, comunicación, recibido y resguardo de la clave de acceso. (Ver resultado 2.5).

3.6. Ausencia de supervisión, de un plan de acción y seguimiento a la gestión de riesgos, pues se carece de la definición y valoración de los riesgos que pueden afectar directa o indirectamente las actividades referentes a la creación de usuarios, sus perfiles, claves de acceso, así como de los procesos automatizados que se ejecutan en las aplicaciones objeto de estudio por parte de las instancias usuarias. (Ver resultado 2.6).

3.7. Ausencia de lineamientos o procedimientos debidamente autorizados y avalados, para capacitar usuarios en el uso de las aplicaciones automatizadas objeto de estudio. (Ver Resultado 2.7).

3.8. Se carece de instrucciones o lineamientos debidamente formalizados y establecidos, para el resguardo de la documentación e información que se genera de las actividades y tareas referentes a la creación, activación o inhabilitación de usuarios, perfiles y niveles de privilegios (opciones habilitadas) para los sistemas objeto de estudio. (Ver resultado 2.8).

Siendo la seguridad un tema que está inmerso en el desarrollo de los sistemas informáticos, por cuanto, minimiza los riesgos y controla aspectos que pueden afectar los datos y el sistema en sí, ya que dicho tema, busca la implementación de mecanismos eficientes y efectivos para prevenir al máximo intrusiones no permitidas tanto de personas ajenas, como de aquellas internas que lo operan, así como del manejo seguro de dichos datos y de la información que se procesa; es de gran preocupación para esta Auditoría Interna, que siendo la plataforma de IBM–AS/400, la más antigua y que en ella se concentra entre otros, los sistemas institucionales “Sistema Financiero Contable, Sistema de Administración de Estudiantes y Sistema de Presupuesto”; y siendo estos sistemas ejes fundamentales del quehacer diario de la UNED, a la fecha se arrastren situaciones que afectan la adecuada administración y control de la seguridad.

Las situaciones expuestas van en contra de las Normas Técnicas para la Gestión y el Control de las Tecnologías de información emitidas mediante

Resolución de la Contralora General de la República, Nro. R-CO-26-2007 del 7 de junio, 2007. Publicada en La Gaceta Nro. 119 del 21 de junio, 2007, normas que tienen como fin lograr eficiencia y eficacia en la gestión de las tecnologías de la información, dicha normativa contempla la seguridad en las operaciones de tecnologías de la información, con el fin de salvaguardar la integridad, disponibilidad y confidencialidad, tanto de los recursos de tecnología de la información como de la información.

Cabe resaltar que la ausencia de aplicación y cumplimiento de dichas normas, fue comunicado a la Administración Activa por esta Auditoría Interna en el Informe S-2010-01 denominado "Estudio sobre el cumplimiento de la implementación de la Normativa 2-2007-CO-DFOE, Normas Técnicas para la Gestión y el Control de las Tecnologías de información en la Universidad Estatal a Distancia", mediante Oficio AI-003-2011 de fecha 27/01/2011.

4. Recomendaciones.

4.1. Al Sr. Rector.

Girar las instrucciones a la Dirección de Tecnología de Información y Comunicaciones para que proceda a:

Elaborar, documentar y formalizar un procedimiento dirigido a las gestiones de la prestación del servicio para la creación e inactivación de: usuarios, perfiles (niveles de privilegios) y claves de acceso para operar los sistemas informáticos institucionales.

En su contenido como mínimo lo siguiente:

- Establecer claramente las actividades, tareas y responsabilidades tanto de la parte técnica como usuaria en el cumplimiento del trámite.
- Establecer la responsabilidad de la parte usuaria en cuanto a la obligatoriedad de comunicar a la DTIC la inactivación del usuario que por motivo justificado debe denegarse el acceso al sistema.
- El o los instrumentos estandarizados (formulario, orden de servicio u otro) para gestionar la solicitud, así como para el recibido a satisfacción del servicio prestado.

- Definir el canal o medio oficial por el cual se tramita y coordina el servicio, así como los mecanismos que aseguren la confiabilidad y oportunidad de la información en la prestación del servicio.

Someter el procedimiento a conocimiento y aprobación por parte del Consejo de Rectoría, para su aplicación y comunicación a toda la Comunidad Universitaria, además de velar por su debida actualización. (Ver Resultado 2.1).

Esta recomendación debe implementarse en concordancia con la recomendación 4.8 del informe X-24-2011-02 la cual se transcribe: "Formular un procedimiento que regule las actividades de creación, mantenimiento e inhabilitación de usuarios a nivel de sistemas de información en la red de datos. Posteriormente, someterlo a la aprobación del Consejo de Rectoría, implementarlo y velar por su adecuada divulgación. (Resultado 2.3.1).

4.2. Al Sr. Rector.

Girar las instrucciones a la Dirección de Tecnología, Información y Comunicaciones para que en coordinación con las Jefaturas de las Oficinas de "Registro y Administración Estudiantil", "Tesorería", "Presupuesto", y "Recursos Humanos" que opera alguno de los módulos que estructuran los sistemas objeto de estudio procedan a:

Elaborar y documentar los diseños o esquemas en los cuales se enmarquen los diferentes procesos y opciones que tienen los módulos que conforman los sistemas objeto de estudio y que utilizan para ejecutar las actividades o tareas encomendadas a cada instancia; y a la vez definan y clasifiquen los posibles usuarios o grupos de usuarios y sus perfiles (habilitación de opciones), estos alineados con las actividad de los puestos o roles que desempeñan.

Clasificar, estandarizar y mantener los usuarios o grupos de usuarios y sus perfiles o roles por sistema, con base a la información y documentación generada del punto anterior. (Ver resultado 2.2.1).

4.3. Al Sr. Rector:

Girar las instrucciones a la Dirección de Tecnología, Información y Comunicaciones para que proceda a:

Fortalecer el control actual del registro de usuarios de los sistemas automatizados que residen en el ambiente AS 400 implementando lo siguiente:

a. Campo para el registro del número de identificación del funcionario al que se le asoció el usuario (Nº cédula, permiso de trabajo, pasaporte u otro). Este dato como atributo único e irrepetible; debe permitir la consulta o búsqueda del usuario al que se le asocia.

b. Campo para el registro de la fecha de inclusión del usuario, y campo para la fecha de inactivación como usuario del sistema.

c. Campo o cambio del texto del campo denominado "Texto descriptivo" por "Nombre del funcionario" y que se estandarice el registro del nombre completo del funcionario al que se asocia el usuario.

d. Campo donde se registre únicamente el nombre de la (dependencia) donde presta los servicios el funcionario al que se le asocia el usuario.

e. Implementar las medidas que tengan como fin el no permitir la eliminación de usuarios que en un momento dado fueron creados y activados a funcionarios usuarios de los sistemas objeto de estudio; esta recomendación se haga extensiva hacia todos los sistemas institucionales.

f. Crear y desarrollar opciones de emisión de reportes de la información contenida en el registro de usuarios de los sistema objeto de estudio, y como mínimo se establezcan los siguientes: Reporte de todos los usuarios creados por sistema, Reporte por grupos o clase de usuario por sistema, Reporte por estado (activo, inactivo u otro) de los usuarios por sistema, Reporte de usuarios por dependencia usuaria del sistema; y en estos se refleje información según parámetros definidos del contenido de todo el registro.

g. Coordinar, con las instancias usuarias, la incorporación de la debida información y a la vez la revisión de los usuarios y sus privilegios (opciones habilitadas en el sistema), con el fin de asegurar que efectivamente corresponden

a funcionarios que conforman el nivel ocupacional institucional y que actualmente están autorizados para ejecutar acciones en las aplicaciones, de lo contrario se tomen las medidas para proceder a su inactivación.

h. Respaldar y conjuntar toda la documentación, correos electrónicos u otra instrucción que se generen de las diferentes acciones realizadas para dar cumplimiento a las actividades supra citadas, está debidamente organizada por cada sistema automatizado objeto de estudio. (Ver resultado 2.2.2).

4.4. Al Sr. Rector:

Girar las instrucciones a las Jefaturas de las Oficinas de "Tesorería", "Registro y Administración Estudiantil" y de "Presupuesto" para que procedan a:

Documentar, formalizar e Implementar los controles que aseguren la revisión y el mantenimiento periódico de los diferentes usuarios y perfiles autorizados a funcionarios para operar los sistemas o módulos bajo su cargo, con la finalidad de mantener una adecuada administración de la identidad y los privilegios otorgados a funcionarios usuarios (internos, externos y temporales) que operan los sistemas informáticos institucionales objeto de estudio y que residen en el ambiente AS 400. (Ver resultado 2.2.2).

4.5. Al Sr. Rector:

Girar las instrucciones a la Dirección de Tecnología, Información y Comunicaciones para que proceda a:

Valorar el desarrollar para los sistemas objeto de estudio, un proceso automatizado independiente, el cual tenga como objetivo el control y administración de usuarios que lo operan. (Ver resultado 2.2.2).

Esta recomendación no pretende limitar en modo alguno a la Administración Activa, para que, si lo considera conveniente, proceda a valorar la contratación externa de asesoría o realizar estudios de productos externos que permitan el adecuado control y gestión de usuarios; como parte de la evaluación de escenarios que puedan ser factibles de implementarse, y así determinar con mayor criterio su desarrollo.

4.6. Al Sr. Rector

Girar las instrucciones a la Dirección de Tecnología, Información y Comunicaciones para que proceda a:

a. Asignar formalmente las actividades y responsabilidades del personal que desempeña acciones referentes a liderar y prestar servicio de mantenimiento de los sistemas objeto de estudio, lo que involucra la creación de usuarios, sus perfiles (menús de usuarios) y claves de acceso, además el implementar y formalizar los mecanismos de supervisión de la labor encomendada. (Ver resultado 2.3.1).

b. Realizar un análisis de las opciones que engloba actualmente el usuario "OPERADOR" y proceda a delimitar o crear otro u otros usuarios y perfiles; y se realice una nueva asignación bajo el principio "de necesidad de saber o menor privilegio", hacia el personal de la Unidad Estratégica de Operaciones (UEO) y el caso específico del funcionario Johnny Saborío Álvarez Encargado de la Unidad Estratégica Seguridad Digital (UESD). Aunado a esto deben implementarse los mecanismos de supervisión y control de la labor asignada. (Ver resultado 2.3.1).

c. Implementar la o las bitácoras a nivel del ambiente AS 400 para los usuarios de la DTIC, incorporar en ellas registros claves que sirvan de pistas de auditoría para identificar al funcionario que realizó la acción, a que recurso acceso (sistema), la acción o acciones realizadas (inclusión, modificación, eliminación) y fecha. Además establecer el mecanismo o procedimiento para su revisión periódica. (Ver Resultado 2.3.1).

4.7. Al Sr. Rector

Girar las instrucciones a las Jefaturas de las Oficinas de "Registro y Administración Estudiantil" y de "Tesorería" para que procedan a:

Asignar formalmente las actividades y responsabilidades al personal bajo su cargo que también gestiona ante la DTIC, solicitud de servicios referentes a la creación e inactivación de usuarios, perfiles y claves para funcionarios que operan u operarían los sistemas o módulos que administran; y a la vez informar de la designación a la DTIC. (Resultados 2.3.2).

4.8 Al Sr. Rector

Girar las instrucciones a la Dirección de Tecnología, Información y Comunicaciones para que proceda a:

a. Desarrollar e implementar los controles automatizados que coadyuven a fortalecer la seguridad y acceso a los sistemas objeto de estudio en cuanto a:

- No permitir, cuando se realice cambio de clave (contraseña), la utilización de claves (contraseñas) utilizadas anteriormente.

- Inactivación del acceso al sistema cuando se registre un número definido de intentos fallidos, al tratar de ingresar con un usuario o una clave (contraseña) incorrecta.

- Realizar las pruebas que tengan como fin determinar que se debe mantener inactivo el control de bloqueo de la sesión del usuario en los diferentes sistemas objeto de estudio; de tomarse la medida de continuar con la inactivación de dicho control, deberá implementarse la o las medidas alternas.

Para todo lo anterior debe realizar la debida coordinación y comunicación con las jefaturas de instancias usuarias. (Ver resultado 2.4.1).

b. Formalizar e implementar los mecanismos que aseguren y mantengan la debida coordinación, comunicación y participación con los responsables de administrar los sistemas institucionales por la parte usuaria, ante cambios o acción alguna que se relacione con la funcionalidad y seguridad de los mismos. (Ver resultado 2.4.1).

c. Coordinar con las áreas usuarias de los sistemas objeto de estudio la implementación de bitácoras que almacenen las pistas de auditoría, para identificar el usuario, la acción y fecha del movimiento realizado; estas dirigidas a los principales procesos que ejecuta cada dependencia.

En complemento, se deben definir y desarrollar los respectivos reportes, así como los mecanismos para el monitoreo periódico de las mismas. (Ver resultado 2.4.2).

4.9. Al Sr. Rector

Girar las instrucciones a la Dirección de Tecnología, Información y Comunicaciones para que proceda a:

Formalizar e implementar los procedimientos y mecanismos que aseguren la adecuada administración, seguridad, confiabilidad y control de las tareas referentes a la creación, comunicación, recibido y resguardo de la clave de acceso a los sistemas objeto de estudio (contraseña). Además hacer del conocimiento del funcionario la responsabilidad en cuanto al uso de la misma. (Ver resultado 2.5).

4.10. Al Sr. Rector

Girar las instrucciones a las Jefaturas de la "Dirección de Tecnología, Información y Comunicaciones", "Oficina de Registro y Administración Estudiantil", "Oficina de Tesorería" y de la "Oficina de Presupuesto", para que en coordinación con el Programa de Valoración de la Gestión Administrativa y del Riesgo Institucional (PROVAGARI) procedan a:

Implementar y ejecutar las acciones para dar cumplimiento a la valoración de riesgos (SEVRI) por cada área a su cargo y que dicha valoración incluya las actividades referentes a los trámites y la prestación de servicios para la creación de usuarios, perfiles y claves de acceso para operadores del o de los sistemas bajo su cargo, así como de los procesos automatizados que se ejecutan. (Ver resultado 2.6).

4.11. Al Sr. Rector

Girar las instrucciones a las Jefaturas de la "Dirección de Tecnología, Información y Comunicaciones", "Oficina de Registro y Administración Estudiantil", "Oficina de Tesorería" y de la "Oficina de Presupuesto", para que procedan a:

a. Implementar y formalizar un procedimiento para capacitar al personal en el uso de los sistemas objeto de estudio, que asegure que la actividad se lleva a cabo en un ambiente controlado (ambiente de pruebas). (Ver resultado 2.7).

b. Formalizar e implementar lineamientos dirigidos al resguardo y conservación de la documentación, sea esta en soporte físico o electrónico, que se genera de los trámites relacionados con la creación, modificación e inactivación de usuarios, perfiles y claves para funcionarios que operan los sistemas objeto de estudio. (Ver resultado 2.8).