UNIVERSIDAD NACIONAL DE COLOMBIA

OFICINA NACIONAL DE CONTROL INTERNO

INFORME FINAL

EVALUACIÓN AL MACROPROCESO GESTIÓN DE LA INFORMACIÓN – PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC)

Elaboró:
Mario Robayo Higuera
Luisa Fernanda Ríos Giraldo

Revisó:
Carlos Manuel Llano Alzate
Jefe ONCI

Bogotá, julio de 2014

TABLA DE CONTENIDO

CONSOLIDADO DE TABLAS

EVALUACIÓN AL MACROPROCESO GESTIÓN DE LA INFORMACIÓN PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC)

1. ANTECEDENTES

En el Plan de Actividades para la vigencia 2014 la ONCI incluyó la actividad *Evaluación Sistemas de Información,* teniendo en cuenta el nivel de riesgo presente en la ejecución de las actividades encaminadas a administrar el acceso lógico de los usuarios autorizados en el controlador de dominio y en los sistemas de información de la Universidad.

2. ALCANCE

Esta evaluación estuvo orientada a la identificación de riesgos y controles asociados a los accesos lógicos en los sistemas de información QUIPU, SIA – UNIVERSITAS XXI, SARA y en el controlador de dominio de la Universidad.

3. OBJETIVOS

3.1 Objetivo general

Evaluar la existencia y funcionamiento de los mecanismos de control asociados al Macroproceso Gestión de la Información, particularmente al proceso Gestión de Tecnologías de la Información y las Comunicaciones (TIC) en lo asociado al acceso lógico del controlador de dominio y en algunos sistemas de información, mediante técnicas de auditoría, con el fin identificar riesgos y controles, con lo cual se contribuya al mejoramiento de la gestión administrativa de la Universidad.

3.2 Objetivos específicos

- Evaluar los riesgos y controles en las actividades relacionadas con la administración del acceso lógico en los sistemas de información QUIPU, SIA – UNIVERSITAS XXI y SARA.

- Evaluar los riesgos y controles en las actividades relacionadas con la administración del acceso lógico en el controlador de dominio de la Universidad.

4. NORMATIVIDAD

- ISO 27001 *"Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la Información – Requerimientos"*.
- ISO 27002 *"Código de prácticas para la gestión de seguridad de la información"*.
- COBIT *"Objetivos de Control para la Información y Tecnologías Relacionadas"*.

5. METODOLOGÍA

- Se llevarán a cabo las entrevistas que sean requeridas a los líderes funcionales de los sistemas de información QUIPU, SIA – UNIVERSITAS XXI, SARA y al funcionario responsable del controlador de dominio en la Oficina de Tecnologías OTIC – Sede Bogotá.

- Verificación documental y análisis de datos.

- Verificación en bases de datos de los usuarios con accesos a los sistemas de información y tipo de vinculación con la Universidad.

6. RESULTADOS OBTENIDOS

6.1 Políticas y procedimientos establecidos para el control de acceso lógico

De acuerdo a lo establecido por las normas y estándares internacionales para la seguridad de la información y específicamente atendiendo a lo definido en la norma ISO 27001 e ISO 27002 y al conjunto de mejores prácticas para el manejo de la información COBIT, en la presente evaluación se analizaron aspectos relacionados con políticas y administración del acceso lógico de los sistemas de información QUIPU, SARA y SIA-UNIVERSITAS, al igual que el controlador de dominio de la Universidad. Lo anterior, mediante análisis de datos y entrevistas realizadas, conforme a lo indicado inicialmente en la Guía de Evaluación.

La OTIC mediante oficio @TICS-BOG:539-14 del 9 de julio de 2014, presentó la siguiente observación: "*La Universidad Nacional no tiene una directriz aprobada para cumplir: ISO27001, ISO27002 y COBIT (Normas referenciadas en el informe)*". La ONCI no comparte la observación, dado que a pesar de que la Universidad aún no cuenta con un sistema de seguridad de la información, las normas mencionadas apuntan a las buenas prácticas al interior de una organización a fin de establecer implementar y hacer seguimiento a la seguridad de la información.

Así las cosas, se pudo identificar lo siguiente:

- Respecto a políticas relacionadas con el control de accesos lógicos a los sistemas de información y al controlador de dominio.

Observación No.1

Por medio de la verificación documental y las entrevistas realizadas a los líderes funcionales de los tres sistemas de información[1] y al administrador del controlador de dominio, se pudo evidenciar que la Universidad Nacional de Colombia no cuenta con una política definida para el control de accesos lógicos.

Recomendaciones:

Se recomienda a la Dirección Nacional de Tecnologías de la Información y Comunicaciones DNTIC, elaborar políticas y/o directrices que permitan establecer controles de acceso lógico, al igual que la clasificación de la información[2] en la Universidad, de manera que se asegure el acceso a los sistemas de información, a los programas, red y datos por usuarios autorizados.

Se sugiere a la DNTIC, una vez formuladas y adoptadas las directrices para el control de acceso lógico, definir mecanismos para la concientización de los usuarios sobre "sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular en relación al uso de contraseñas y a la seguridad del equipo de cómputo"[3], teniendo en cuenta que la cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad.

[1] QUIPU, SARA Y SIA-UNIVERSITAS.
[2] Por ejemplo información clasificada como reservada, o no pública.
[3] ISO 27002, numeral 11.

La OTIC mediante oficio @TICS-BOG:539-14 del 9 de julio de 2014, presentó la siguiente observación: "*Se recomienda al auditor del proceso (ONCI), incluir la importancia de la clasificación de la información en la UNAL. Los controles de acceso lógico a la información se le aplican a la información clasificada como reservada, o no pública*".

La ONCI acepta la observación y la reincorpora en la recomendación.

- En cuanto al Procedimiento establecido para la comunicación por parte de la Dirección Nacional de Personal Académico y Administrativo DNPAA y/u otras instancias para la solicitud de emisión e inactivación de las cuentas de usuario en los sistemas de información y en el controlador de dominio.

Respecto al registro y cancelación de usuarios, la norma ISO 27001 en el *Anexo A11* e ISO 27002 en el *Dominio 11 Control de Acceso*, mediante uno de los requisitos de la norma establece:

"*Para el registro y cancelación de usuarios para acceder a los diferentes sistemas y servicios de información multiusuarios de la Organización debe definirse y establecerse un procedimiento de registro y desactivación de usuarios, el cual debe incluir:*

- *Identificador único para cada usuario.*
- *Comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema o servicio de información.*
- *Verificación del nivel de acceso asignado.*
- *Entrega a usuario de relación escrita de sus derechos de acceso.*
- *Mantenimiento de un registro formalizado.*
- *Eliminación inmediata de autorizaciones de acceso a usuarios que dejan la organización".* (Subrayado de la ONCI).

Frente a este tema, cada uno de los funcionarios entrevistados manifestó que actualmente se maneja un procedimiento informal por medio del cual, mediante correo electrónico, formato o por oficio proyectado por el jefe inmediato del solicitante, se efectúa la solicitud de la activación o inactivación del usuario.

Por su parte el líder funcional de QUIPU mediante entrevista[4] expresó: *"(…) no nos hablamos entre los sistemas para la creación e inactivación de los usuarios. (…) para crear un usuario, se tiene definido un formato que debe diligenciar el usuario y avalado por el jefe inmediato del usuario en donde se le asignan las funcionalidades y las sedes de las operaciones que se le están autorizando (…) el jefe es finalmente el que autoriza al*

[4] Registro de entrevista 26 de mayo de 2014.

usuario, pero existen unos límites que están demarcados. Con este formato se le autoriza y se envía por correo el usuario y contraseña y las indicaciones para que ingrese y cambie la clave".

De igual forma, el líder funcional de SARA manifestó[5]: *"(…) No existe un procedimiento. En realidad considero que debería establecerse porque nos hemos dado cuenta que (sic) usuarios que se retiran y uno no se entera. (…) la creación siempre está asociada a una solicitud del jefe donde se encuentra ubicado el usuario. Este debe tener la justificación y los permisos que debe tener (…) se hace a través de la cuenta institucional y nosotros respondemos a esa cuenta y con copia al correo personal del jefe del funcionario que hace la solicitud".*

De cara al procedimiento, el funcionario responsable del controlador de dominio señaló[6]: *"En su momento se crearon estándares con periodicidad para que las instancias notificaran novedades pero a veces no se aplica el procedimiento por algunas áreas. (…) El procedimiento establece que cada fuente debe crearlo. Nosotros no creamos usuarios es decir el dueño es el que pide crearlo. El procedimiento establece que una persona administrativa o docente efectúa la solicitud a la mesa de ayuda".*

Por su parte el líder funcional de UNIVERSITAS XXI mediante entrevista[7] expresó: *"(…) acá se maneja SIA y UNIVERSITAS XXI que manejan usuarios diferentes. Para el caso de acceso de usuarios esta última tiene un procedimiento definido de manera que las dependencias, facultades y demás puedan hacer la solicitud correspondiente(…) Las cuentas del SIA están ligadas al LDAP y las de UNIVERSITAS XXI están ligadas a la consulta de UNIVERSITAS XXI y estas son las que nosotros administramos."*

Al consultar sobre el procedimiento relacionado con la emisión y suspensión de cuentas de usuario, indicó: *"(…) está establecido un formato por medio del cual se define la creación, bajo reasignación o modificación de perfiles (…) Las facultades son las que notifican el cambio de estado pero ellas son recelosas en eso, dado que cuando se envía el reporte para que lo remitan, algunas son muy juiciosas pero otras no lo reportan oportunamente (…)".*

Observación No.2

Se evidencia que no existe un procedimiento unificado y formalmente adoptado que describa actividades y controles relacionados con la comunicación por medio de la cual la DNPAA y/o las instancias pertinentes, informen tanto a los líderes funcionales como al responsable del controlador de dominio sobre las acciones relacionadas con la emisión y suspensión de las cuentas de usuario de acuerdo con las novedades que se puedan presentar en la comunidad universitaria.

[5] Ibídem
[6] Registro de entrevista 27 de mayo de 2014.
[7] Registro de entrevista 29 de mayo de 2014.

Recomendación:

Se recomienda a la DNTIC en conjunto con la DNPAA generar un procedimiento que asegure las acciones relacionadas con la activación o suspensión de las cuentas de usuario en los sistemas de información y en el controlador de dominio. Lo anterior, por medio de la comunicación oportuna de las novedades de los usuarios desde la DNPPA o las dependencias, facultades y/o demás instancias solicitantes a los funcionarios responsables de las actividades de activación o suspensión según el caso, lo cual aportaría en gran medida a la seguridad de la red, sistemas y datos de la Universidad Nacional de Colombia.

6.2 Riesgos y controles en la administración del acceso lógico del controlador de dominio y los sistemas de información

- Creación e inactivación de usuarios en el controlador de dominio de la Universidad Nacional de Colombia

De acuerdo a las entrevistas efectuadas y al análisis de datos de la información entregada por la OTIC Sede Bogotá, la ONCI pudo identificar que: *"(…) a nivel de controlador no se efectúa ningún movimiento en el controlador de dominio, no se maneja el tema de creación o eliminación de cuentas, únicamente cuando se requiere soporte en el cambio de contraseñas (…) en el controlador de dominio no se desactiva, se hace a nivel del LDAP, lo cual por su sincronización se efectúa automáticamente".*

En ese orden de ideas, la ONCI solicitó a la OTIC Sede Bogotá, instancia encargada de la administración del controlador de dominio y el LDAP[8], el reporte de la totalidad de las cuentas de usuario creadas en el controlador de dominio al mes de mayo de 2014.

En respuesta a la solicitud, la OTIC Sede Bogotá remitió la información correspondiente a 146.707 cuentas de usuario activas del dominio. Esta instancia por su parte consideró importante anexar a esta solicitud, el total de los usuarios creados en el LDAP, reportando un total de 244.198[9] cuyo resumen se puede observar en el Tabla No. 1.

[8] LDAP (**L**ightweight **D**irectory **A**ccess **P**rotocol) Protocolo Ligero de Acceso a Directorios: protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. Fundación Wikimedia, Inc. (27 de 12 de 2013). *Wikipedia*. Recuperado el 28 de 05 de 2014, de http://es.wikipedia.org/wiki/LDAP

[9] Dato que incluye las Sedes de Arauca, Bogotá, Leticia, Manizales, Medellín, Pacifico, Palmira y San Andrés, al igual que

Tabla 1 Número de usuarios creados en LDAP por tipo de vinculación y Sede

Sede	Tipo de vinculación									Total
	Adtvo	Contratis.	Dependencia	Docente	Egresado	Estudiante	Institucional	Pensionado	Exter.	
Orinoquia	9	76	16	90	9	1054	32			1286
Bogotá	2481	3315	593	5004	20854	113360	2917	256		148780
Amazonia	12	42	2	75	1	1148	56			1336
Manizales	257	261	88	841	4398	17166	246	138		23395
Medellín	1140	404	196	1282	2498	44287	1220	45		51072
Tumaco							2			2
Palmira	255	49		406	1420	10019	247	1		12397
Caribe	6	45	6	71		489	41			658
Externos									5272	5272
	4160	4192	901	7769	29180	187523	4761	440	5272	244198

Fuente: OT Sede Bogotá – Tabla elaborada por la ONCI.

Frente al tema y con el ánimo de identificar aspectos relacionados con el control de las cuentas de usuario tanto en el LDAP como en el controlador de dominio, se solicitó a la DNPAA y a la Dirección de Talento Humano Sede Bogotá, la base de datos del personal activo y retirado del Nivel Nacional y Sede Bogotá de la Universidad Nacional de Colombia desde la vigencia 2010 hasta el 14 de mayo de 2014[10]. La ONCI utilizó como muestra para el análisis de datos en el presente informe, dada su complejidad, la información reportada en la base de datos del personal activo y retirado de la Sede Bogotá, para algunas consultas se verificó con personal del nivel nacional.

De acuerdo al análisis efectuado, se pudieron identificar las siguientes situaciones de la base de datos del controlador de dominio:

i) 11 cuentas de usuario tienen asignación simultánea, las cuales cuentan con igual user name e igual nombre de usuario, ver Anexo 1. Hoja Dominio duplicados por User-No.

ii) 2.301 cuentas de usuario tienen asignación simultánea, las cuales cuentan con igual nombre de usuario y diferente user name, ver Anexo 1. Hoja Dominio Dupli-tri.

[10] Solicitud efectuada mediante comunicaciones internas ONCI 359 y ONCI 360 del 14 de mayo de 2014.

iii) 28 usuarios tienen asignada más de dos cuentas de usuario, las cuales cuentan con igual nombre de usuario y diferente user name, ver Anexo 1. Hoja Dominio Dupli-tri.

iv) 416 cuentas de usuario corresponden a cuentas genéricas denominadas: cuenta provisional, unidad administrativa, decanatura académica, decanatura, rectoría y sedes ONCI[11].

v) 10 cuentas de usuario no tienen nombre de usuario y sus user name corresponden a: tecnicoPC1, tecnicoPC5, tecnicoPC9, tecnicoPC4, tecnicoPC10, tecnicoPC6, tecnicoPC3, tecnicoPC7, tecnicoPC2 y tecnicoPC8, ver Anexo 1. Hoja Dominio sin nombre usuario.

Observación No.3

La base de datos del controlador de dominio no se encuentra debidamente depurada ni cuenta con los suficientes controles que eviten, entre otros: i) duplicidad en la información; ii) asignación de más de un User Name a una misma persona y iii) asignación de cuentas genéricas. Igualmente, no se cuenta con una política de asignación de cuentas que evite la creación de usuarios que no requieren de este servicio.

Recomendación

Se recomienda a la OTIC Bogotá, instancia encargada de la administración del controlador de dominio y el LDAP, realizar una depuración de los mismos, con el visto bueno de las instancias de la Universidad que corresponda, según la situación que se encuentre.

La OTIC mediante oficio @TICS-BOG:539-14 del 9 de julio de 2014, presentó la siguientes observaciones:

"*... OTIC no administra la información de cuentas de usuario, solo opera la infraestructura tecnológica. OTIC, solo es responsable por mantener la máquina y el software en operación. La OTIC ejecuta la creación de cuentas y borrado por mandato de las áreas funcionales. Los responsables de depurar la información son las áreas funcionales*".

La ONCI acepta la observación y modifica la recomendación en el siguiente sentido: *Se recomienda a las áreas funcionales (DNPAA y a la Dirección de*

[11] En el análisis no se tuvieron en cuenta las cuentas de usuario de Administrador.

Talento Humano Sede Bogotá) en coordinación con la OTIC Bogotá, realizar una depuración de los mismos, según la situación que se encuentre.

"Respecto a los indicadores de inconsistencias de nombres duplicados con muchas repeticiones podemos anotar: Muchos registros (usuarios) en el LDAP, para personas que están contratadas con ODS están creados con el campo responsable diligenciado con el nombre del Interventor. Muchos usuarios están creados con muchos roles porque fueron estudiantes, después fueron egresados, después ODS y algunos se han convertido en profesores. Muchos usuarios de tipo institucionales como oficina, vicerrectorías, etc., han sido directores asignadas a los responsables de área con el nombre del director y tendrá conflicto con su usuario personal dentro de la Universidad."

La ONCI acepta parcialmente la observación en cuanto no se anexa soporte sobre los "*muchos*" casos indicados por la OTIC, el cual podría evidenciar el control de los casos identificados, de otro lado no se cuenta con una política definida para el tratamiento de estos casos especiales.

- Con respecto a la inactivación de usuarios retirados

De igual forma, durante la revisión de las cuentas activas del dominio con respecto a la base de datos entregada por la Dirección de Talento Humano DTH Sede Bogotá, se pudo identificar:

i) El controlador de dominio reporta 715 cuentas de usuario activas de funcionarios que se encuentran retirados de la Universidad, Ver Anexo No. 2, Hoja Activos Dominio vs Retirados.

ii) 12 funcionarios retirados no contaron con cuentas de usuario en el controlador de dominio. Lo anterior, llama la atención teniendo presente que ocuparon cargos que necesitan contar con su respectiva cuenta para ingresar a la red de la Universidad. Estos son: cajero, secretaria ejecutiva, profesor asociado, profesor auxiliar, profesional universitario, educador de enseñanza básica y media licenciado, técnico operativo y técnico administrativo, Ver Anexo No. 2, Hoja Retirados sin dominio.

Observación No.4

La base de datos del controlador de dominio no está siendo actualizada oportunamente, como ya se mencionó la DNPAA y/o las instancias pertinentes no están informando tanto a los líderes funcionales como al responsable del

controlador de dominio sobre las acciones relacionadas con la emisión y suspensión de las cuentas de usuario de acuerdo con las novedades que se puedan presentar en la comunidad universitaria.

Recomendación:

Se recomienda a la DNTIC en conjunto con la DNPAA incorporar en el procedimiento ya recomendado mediante la Observación No. 2 del presente informe, acciones y controles relacionados con la suspensión de las cuentas de usuario en el controlador de dominio.

- Control de accesos no autorizados

De cara a lo establecido en el objetivo de control número 4 de la norma ISO 27001 y 27002, denominado *Control de acceso a las Redes,* se define:

"Objetivo: evitar el acceso no autorizado a los servicios en red. Es recomendable controlar el acceso a los servicios en red, tanto internos como externos. El acceso de los usuarios a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que:

1. *existen interfaces apropiadas entre la red de la organización y las redes que pertenecen a otras organizaciones y las redes públicas:*
2. *se aplican mecanismos adecuados de autenticación para los usuarios y los equipos.*
3. *se exige control de acceso de los usuarios a los servicios de información".* (Subrayado de la ONCI).

El equipo evaluador de la ONCI atendiendo a lo mencionado en el objetivo de control, efectuó el análisis de la información proporcionada por la OTIC Sede Bogotá con respecto al control de accesos de usuarios no autorizados. De lo anterior, se pudo identificar que de las 715 cuentas de usuario de funcionarios que se encuentran retirados, 140 han presentado accesos a la red después de su retiro de la Universidad, tal y como se observa en el Anexo No. 2, Hoja Accesos de Retirados.

Observación No.5

Como ya se indicó mediante la Observación No. 2 del presente informe, no se cuenta con una política sobre el control de accesos lógicos, ni con un mecanismo de bloqueo a los usuarios retirados de la Universidad, lo cual está permitiendo

ingresos[12] *a la red de la Universidad de exfuncionarios, sin que adicional a este ingreso, se conozca el tipo de acciones realizadas en los mismos.*

Recomendaciones:

Se recomienda a la Dirección Nacional de Tecnologías de la Información y Comunicaciones DNTIC, elaborar políticas y/o directrices que permitan establecer controles de acceso lógico que aseguren el acceso a los sistemas de información, a los programas, red y datos por usuarios autorizados.

Se recomienda a la DNTIC en conjunto con la DNPAA generar un procedimiento que asegure las acciones relacionadas con la suspensión de las cuentas de usuario en los sistemas de información y en el controlador de dominio. Lo anterior, por medio de la comunicación oportuna de las novedades de los usuarios desde la DNPPA o las dependencias, facultades y/o demás instancias solicitantes a los funcionarios responsables de las actividades de suspensión según el caso, lo cual aportaría en gran medida a la seguridad de la red, sistemas y datos de la Universidad Nacional de Colombia.

- Seguridad de sistemas

El marco de mejores prácticas de Tecnología COBIT, define en su dominio *Ds5 Garantizar la seguridad de sistemas* y como objetivo*: "(…) salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados y toma en consideración: Autorización, autenticación y el acceso lógico junto con el uso de los recursos de TI deberá restringirse a través de la instrumentación de mecanismos de autenticación de usuarios identificados y recursos asociados con las reglas de acceso (…)"* (Subrayado de la ONCI).

Para la verificación de lo anteriormente mencionado, se efectuó el análisis de información a las bases de datos de usuarios de los sistemas de información (UNIVERSITAS XXI, SARA y QUIPU) y al controlador de dominio y al LDAP. No se tomó en cuenta la base de datos de cuentas de usuario del sistema de información SIA, dado que no fue entregada la información a la ONCI por el líder funcional. Del análisis se pudo identificar que:

[12] Los casos detectados por la ONCI, son sobre una base de funcionarios retirados en el periodo 2010 a mayo de 2014, lo cual hace posible que el número de personas que ingresan a la red y sistemas de información de la Universidad sea mayor, más aun teniendo en cuenta que la muestra tomada no abarca exfuncionarios del 2010 hacia atrás, contratistas y personal externo que se le ha asignado cuentas (p.e. grupo auditor de la Contraloría General de la República).

A. LDAP vs controlador de dominio.

El total de usuarios reportados en el LDAP es de 146.707. Se verificaron los funcionarios activos, respecto a las cuentas de usuario en el dominio, encontrándose 19 casos con diferencias. Sin embargo, realizada la consulta por nombre se observó que solo un caso no tiene login, los otros 18 casos si existen con otro User Name en el dominio, ver Anexo No.03, Hoja Activos sin dominio.

Respecto a lo anterior, llama la atención lo mencionado por el funcionario responsable de la administración del controlador del dominio mediante entrevista realizada el 27 de mayo de 2014, en donde manifiesta "*...a nivel de controlador no se efectúa ningún movimiento en el controlador de dominio, no se maneja el tema de creación o elaboración de cuentas, únicamente cuando se requiere soporte en el cambio de contraseñas*"

Accesos Cero En Dominio: De la base de datos entregada por la DTH Sede Bogotá filtrando los funcionarios activos, se encontró que 1.641 funcionarios nunca han ingresado al dominio, en esta relación se encuentran funcionarios administrativos y docentes que por su cargo, se podría decir, que es casi que indispensable haber ingresado al mismo[13], no obstante, tienen registrado en el campo "Ultimo Ingreso al Sistema" el valor cero (0) en el archivo, que al parecer corresponde a "nunca haber ingresado", ver Anexo No.03, Hoja Acceso cero en Dominio. Del total de los 146.707 usuarios activos en el dominio, se identificaron 91.608 usuarios que tienen registrado en el campo "Ultimo Ingreso al Sistema" el valor cero, ver Anexo No.03, Hoja Total Acceso cero.

El total de usuarios reportados en el LDAP es de 244.198, incluye todas las sedes de la Universidad y los tipos de vinculación (docentes, externos, contratistas, administrativos, dependencias, estudiantes, egresados, institucional y pensionados). Para esta evaluación y en el ejercicio del cruce con el dominio se tuvieron en cuenta las cuentas asignadas a la Sede Bogotá, un total de 14.780.

De los cruces de información realizados entre las cuentas del LDAP y las del Dominio para cada grupo[14] se encontró:

[13] p.e. Alba Lucía Marín Zuluaga Directora Talento Humano Sede Bogotá. Victor Julio Flórez Roncancio Decano Facultad de Agronomía

[14] Administrativos, Contratistas, Docentes, Dependencias y Externos. No se realizó para Estudiantes , egresados y pensionados por no ser parte del alcance de la evaluación.

- *Administrativos*: De un total de 2.481 registros, 2.480 registros coinciden en las dos bases, salvo la cuenta *user_ldap* que corresponde a un "*Usuario de Consulta LDAP*"
- *Contratistas:* De un total de 3.315 registros, 3.311 coinciden y 4 no coinciden en las dos bases. ver Anexo No.03, Hoja Contratistas vs Dominio.
- *Dependencias:* de un total de 593 registros, 578 no coinciden (lo cual es correcto) y 15 coinciden en las dos bases, estos últimos cuentan con el User Name en el controlador de dominio, lo cual no es lo recomendable dado que estos deben tener asignadas personas y no oficinas o dependencias, ver Anexo No.03, Hoja Dependencias vs Dominio.
- *Docentes:* De 5.004 registros, 5.001 coinciden y 3 no coinciden (dos de estas cuentas, corresponden a cuentas adicionales de dos docentes), ver Anexo No.03, Hoja Docentes vs Dominio.
- *Externos:* Del total de 5.272 registros, ninguno coincide, lo cual es lo adecuado dado que ninguna persona externa a la Universidad debe tener el permiso de ingreso a la red interna.

Observación No.6

La ONCI evidenció que se encuentran creadas cuentas de usuario en el controlador de dominio, de personal que de acuerdo a su cargo y sus funciones no debería ser necesario tener acceso a recursos compartidos o a una máquina de la red de la Universidad. De igual forma, se identificaron funcionarios que en el controlador de dominio tienen perfiles que en algún momento de su vida laboral han requerido autenticarse en el dominio y no lo han efectuado.

Recomendación

Se recomienda a la DNTIC, incorporar en las directrices de control de acceso lógico recomendado en la Observación No. 1 del presente informe, un lineamiento por medio del cual se definan los funcionarios que de acuerdo a su cargo, deben tener cuenta de usuario tanto en el LDAP como en el controlador de dominio, de manera que no se creen cuentas de usuarios innecesarias, lo cual podría atentar contra la seguridad de la red de la Universidad.

En el evento que las políticas incluyan a todos los funcionarios de la Universidad, se recomienda a la DNTIC y OTIC de las sedes realizar una capacitación al personal que no hace uso de este servicio para dar a conocer sus beneficios y procurar el uso del mismo, así esto se haga únicamente como medio de recibo de información institucional.

B. QUIPU NACIONAL

Total de usuarios reportados a nivel Nacional: 10.215 registros de estos registros 852 tienen el perfil "BASURA", que corresponde a personas retiradas de la Universidad, de las cuales se ha reportado por las áreas el retiro, sin embargo, en el Quipu no se cuenta con un parámetro para inactivarlos.

Se identificaron a nivel de duplicados:

1. 2 cuentas de usuario tienen asignación simultánea, las cuales cuentan con igual user name e igual nombre de usuario, Ver Anexo No.04, Hoja Quipu Nal Duplicados por User.
2. 1944 registros duplicados por nombre de usuario, ver Anexo No.04, Hoja Quipu Nal Duplicados por Nombre así: i) 936 cuentas de usuario tienen asignación simultánea, las cuales cuentan con igual nombre de usuario y diferente user name; ii) 22 funcionarios tienen más de una cuenta de usuario asignada. Estas cuentas tienen igual nombre de usuario y diferente user name; y iii) 3 son registros vacios y 3 son registros con información genérica.

De otra parte, en la base de datos de Quipu-Nal se identificaron 1.200 usuarios que tiene como logín un registro numérico el cual "al parecer" corresponde al número de identificación, ver anexo 4. Hoja Login Numérico Nal. Al respecto la norma ISO 27002, indica "*Control: Todos los usuarios tienen un identificador único (ID de usuario) para su uso personal, y se debiera escoger una técnica de autenticación adecuada para sustanciar la identidad de un usuario*", en ese sentido se observa que no se está empleando una técnica de autenticación adecuada, utilizando el número de identidad como login.

C. QUIPU BOGOTA

Total de usuarios reportados a nivel Nacional: 12.075 registros, de estos 1.591 tienen el perfil "BASURA", que corresponde a personas retiradas de la Universidad, de las cuales se ha reportado por las áreas el retiro, sin embargo, en el Quipu no se cuenta con un parámetro para inactivarlos.

Se identificaron a nivel de duplicados:

1. 2 cuentas de usuario tienen asignación simultánea, las cuales cuentan con igual user name e igual nombre de usuario, ver Anexo No.04, Hoja Quipu Bogotá Duplicados por User.

2. 2428 registros duplicados por nombre de usuario, ver Anexo No.04, Hoja Quipu Bogotá Duplicados por Nombre así: i) 1.161 cuentas de usuario tienen asignación simultánea, las cuales cuentan con igual nombre de usuario y diferente user name; ii) 34 funcionarios tienen más de una cuenta de usuario asignada, estas cuentas tienen igual nombre de usuario y diferente user name; y iii) 2 registros vacios y 2 registros con información genérica.

En la base de datos de Quipu-Bogotá se identificaron 1.440 usuarios que tiene como logín un registro numérico el cual "al parecer" corresponde al número de identificación, ver anexo 4. Hoja Login Numérico Bta.

D. SARA NIVEL NACIONAL Y BOGOTÁ

El ingreso al sistema de información SARA, se realiza a través de dos arquitecturas: bajo el modelo cliente servidor y vía web, por lo tanto la creación de los usuarios tiene alguno de esos dos orígenes. La información remitida por la DNPAA se hizo en un archivo USUARIOS_CLIENTE_SERVIDOR_WEB.

Total de usuarios reportados: 7.064. De los cuales 6.193 están registrados en la Sede Bogotá, 803 en el Nivel Nacional y 68 registros "*SIN IDENTIFICACION…* " en el campo SEDE.

A nivel de duplicados de la base por origen usuario WEB (6.656 registros) se identificaron:

- 4 registros, 2 funcionarios tienen asignación simultánea, las cuales cuentan con igual NOMBRE DE USUARIO, ver Anexo No.05, Hoja SARA-WEB duplicados por Nombre.
- No hay registros con asignación simultánea, con igual USER NAME.

A nivel de duplicados de la base por origen usuario cliente_servidor (408 registros), no se encontraron duplicados por USER NAME ni por NOMBRE USUARIO.

El líder funcional de SARA mediante correo electrónico del 23 de julio de 2014, presentó la siguiente observación: "*En el literal D del ítem "Seguridad de Sistemas" se mencionan dos usuarios con cuentas duplicadas en web. En este momento ya se corrigió la información y se dejo una sola cuenta para estas personas.*"

E. UNIVERSITAS XXI

Total de usuarios reportados a nivel Nacional: 1.188.

En la consulta duplicados por el campo USUARIO, no se encontraron duplicados. Se observa que en general los usuarios creados en UNIVERSITAS XXI están asociados a un área o a un cargo y no tienen vínculo con el nombre de un usuario.

En el campo OBSERVACIONES se indica la persona que figura como responsable del usuario. Sin embargo, esta forma de registro no permite realizar un control efectivo sobre la validez y actualización de la información respecto a otras bases de datos, dado que la persona que figura como responsable puede estar asignada a otra área[15] o se encuentre desvinculada de la Universidad.

Frente al tema, en entrevista realizada con los ingenieros de soporte del sistema de información SIA[16] y el Jefe de la División y Registro de la Sede Bogotá, manifestaron: *"(…) En UNIVERSITAS XXI no se tiene la posibilidad de mediante campos definir la fecha de inicio y finalización de la activación de usuarios, ejemplo los contratistas (…) no se cuenta con el pero si se cuenta con el campo de observación mencionado. Se efectuó el requerimiento pero no se ha efectuado en el sistema, sería muy bueno que se contara con esta posibilidad de manera que se defina que cuando se termina el contrato de un funcionario el sistema bloquee automáticamente".* El campo de observaciones permite registrar las novedades y datos de las personas que utilizarían el usuario.

De igual forma señalaron: *"(…) no hay un control de que equipos puede tener UNIVERSITAS XXI a nivel de la Universidad, sería bueno que fuera a nivel de ips. Nosotros no tenemos un control de este tipo, considero que este control lo debería hacer la OTIC que es el encargado de la infraestructura (…)".*

La División de Registro mediante los soportes a la entrevista, pudo evidenciar la necesidad actual de que el sistema de información cuente con un módulo de auditoría de usuarios, el cual *"(…) permita tener un histórico de cada uno de los usuarios, es decir, en este momento el aplicativo solo cuenta con un campo de observaciones (…) se debería tener una opción de auditoría la cual permita llevar un histórico de todos los funcionarios que han utilizado un determinado usuario UXXI, es decir debe haber un check el cual permita desactivar o dar continuidad de un usuario como también registre las actividades realizadas por este"*

[15] Por ejemplo: figura con el usuario SEC_SEDE1, como "..PERSONA RESPONSABLE DEL USUARIO CARMEN MARÍA ROMERO ISAZA C.C. 41509961 SECRETARIA DE SEDE", a la fecha la profesora Carmen María Romero Isaza ya no cumple funciones como Secretaria de Sede, sin embargo el usuario tiene status de OPEN.

[16] Registro de entrevista del 29 de mayo de 2014.

Esta instancia realizó una propuesta para la creación del módulo de auditoría, por medio de la cual se define la incorporación de campos específicos para la creación del usuario, al igual que una fecha de vinculación[17], una fecha de inicio y terminación del contrato del servidor público con el propósito de *"(…) garantizar que cada jefe de sección reporte estos cambios de personal o continuidad del mismo a la dependencia que se encarga de la administración de usuarios para actualizar los datos"*[18]. Del mismo modo se incluyen temas relacionados con mantenimiento y definición de parámetros y controles de acceso en la aplicación[19].

Observación No. 7

Se evidenció que en el sistema de información UNIVERSITAS XXI, las cuentas de usuario no se encuentran asociadas a un único funcionario, estas se encuentran creadas a nivel de dependencias de manera genérica, es así como la administración de los usuarios se efectúa por medio de un campo de texto en el cual se reportan datos como: nombre, dependencia y novedades de las personas que están utilizando la cuenta de usuario. Lo anterior, representa un posible riesgo en la seguridad y confiabilidad de la información, al igual que en la falta de controles que permitan en caso necesario efectuar la auditoria de los movimientos en el sistema de un usuario especifico.

Recomendación:

Se recomienda a la Dirección Nacional del SIA, continuar con la gestión necesaria para efectuar los ajustes en el sistema de información UNIVERSITAS XXI que apunten a garantizar la seguridad y confiabilidad de la información.

F. BD Personal Bogotá retirados vs SARA

De la verificación realizada entre la base de datos de funcionarios retirados de la Universidad-Sede Bogotá respecto al sistema de información SARA, se encontró que 4 personas retiradas aún figuran en SARA (opción cliente-servidor) como Activos, ver Anexo 6 Hoja Retirados Bta – Activos SARA-C. Igualmente se encontraron 679 personas retiradas que aún figuran en SARA (opción WEB) como activos, ver Anexo 6 Hoja Retirados Bta – Activos SARA-W.

[17] Para el manejo de los funcionarios de planta, provisión y contratista
[18] Registro de entrevista del 29 de mayo de 2014.
[19] Manejo de perfiles, usuarios y módulos.

G. Personal Nivel Nacional retirados vs SARA

De la verificación realizada entre la base de datos de funcionarios retirados de la Universidad-Nivel Nacional respecto al sistema de información SARA, se encontró que 6 personas retiradas aún figuran en SARA (opción cliente-servidor) como Activos, ver Anexo 6 Hoja Retirados Nal – Activos SARA-C. Igualmente se encontraron 202 personas retiradas que aún figuran en SARA (opción WEB) como activos, ver Anexo 6 Hoja Retirados Nal – Activos SARA-W.

El líder funcional de SARA mediante correo electrónico del 23 de julio de 2014, presentó las siguientes observaciones:

"*En los literales F y G del ítem "Seguridad de Sistemas" se mencionan usuarios retirados que aun tienen cuenta activa en SARA cliente/servidor, sin embargo no es claro de donde se tomaron esos datos dado que al consultar a estas personas se evidencia que a la fecha son empleados activos y no retirados. Sugiero hacer una verificación conjunta de la forma en que se hicieron los cruces para determinar que genero esta diferencia.*"

La ONCI no acepta la observación, pues revisada nuevamente las bases de datos de funcionarios activos y retirados del nivel nacional y de la Sede Bogotá, remitidas por la Dirección Nacional de Personal Académico y Administrativo y la Dirección de Talento Humano Sede Bogotá y los respectivos cruces efectuados por la ONCI, se ratifica que los casos reportados figuran como personas retiradas de la Universidad.

"En los literales F y G del ítem "Seguridad de Sistemas" se mencionan también usuarios retirados que aun tienen cuenta activa en SARA WEB. En este sentido debo aclarar que a la fecha una persona retirada mantiene el acceso a los datos propios de SU hoja de vida para efectos de las actualizaciones que considere pertinentes, actualizaciones que son avaladas por las áreas de talento humano correspondientes según los soportes aportados por el exfuncionario, sin embargo se debería definir entonces si se quitan incluso esos accesos después del retiro del funcionario."

La ONCI considera que se debe analizar por parte del líder funcional, la Dirección de Personal en conjunto con la Oficina Nacional de Gestión y Patrimonio Documental los procedimientos orientados al tratamiento de este tipo de información, de manera que se apliquen los lineamientos para el manejo de los soportes y medios de registro digitales tal y como lo establece el Archivo General de la Nación mediante el artículo 2 del Decreto 2609 de 2012.

H. Personal Bogotá Retirado vs QUIPU

De la verificación realizada entre la base de datos de funcionarios retirados de la Universidad-Sede Bogotá respecto al sistema de información QUIPU, se encontró que 694 personas retiradas aún figuran en QUIPU como Activos, ver Anexo 7 Hoja Retirados Bta-Activos Quipu Bta.

I. Personal Nivel Nacional Retirado vs QUIPU

De la verificación realizada entre la base de datos de funcionarios retirados de la Universidad-Nivel Nacional respecto al sistema de información QUIPU, se encontró que 238 personas retiradas aún figuran en QUIPU como Activos, ver Anexo 7 Hoja Retirados Nal-Activos Quipu Nal.

Observación No. 8

Se evidenció que en los sistemas de información SARA y QUIPU, no son retiradas o inactivadas de las bases de datos, todas las personas que se retiran de la Universidad, en QUIPÚ para algunos de los retirados se les asigna un perfil que los identifica, sin embargo, a la fecha aún están registrados como activos un alto número de exfuncionarios.

Recomendaciones

Se recomienda a la DNTIC en conjunto con la DNPAA generar un procedimiento que asegure las acciones relacionadas con la suspensión de las cuentas de usuario en los sistemas de información SARA y Quipu de las personas que pierdan la vinculación con la Universidad. Lo anterior, por medio de la comunicación oportuna de las novedades de los usuarios desde la DNPPA, lo cual aportaría en gran medida a la seguridad de la red, sistemas y datos de la Universidad Nacional de Colombia.

Se recomienda a los administradores de las bases de datos de QUIPU y SARA, realizar una depuración a la base de tal manera que inactive el acceso a personas ya retiradas de la Universidad.

- Parámetros de seguridad lógica aplicados en el controlador de dominio

Con respecto a los parámetros de seguridad lógica como lo son: i) parámetro para determinar la longitud mínima de claves de acceso; ii) parámetro para establecer

la vigencia máxima de las contraseñas; iii) aplicación del parámetro para bloquear una cuenta después de un número determinado de intentos fallidos; iv) aplicación de conteo en tiempos de intentos inválidos de acceso a windows, el funcionario encargado de la administración del controlador de dominio manifestó: *"No están definidas políticas de password y actualmente se está trabajando en esa articulación dado que está obsoleta la tecnología para integrar (la tecnología a nivel de software es de hace trece años). (…) la Universidad con respecto al manejo de la identidad se encuentra atrasado 10 años. Se debe contar con un buen presupuesto para lograr el manejo óptimo que es bien necesario".*

De igual forma señaló: *"Se necesita un cambio a nivel tecnológico y el manejo de integración de las personas a nivel cultural (política y cultura). Ya la DNTIC sabe y estamos trabajando en el tema".*

Observación No.9

La ONCI evidenció que actualmente no se cuenta con la definición y aplicación de parámetros de seguridad lógica en el controlador de dominio de la Universidad Nacional de Colombia, parte de su causa radica en la tecnología obsoleta, que según lo señalado por la OTIC Sede Bogotá es de hace más de 13 años y en manejo de identidad de aproximadamente 10 años.

Recomendación

La ONCI recomienda a la OTIC Sede Bogotá y a la DNTIC, continuar con las gestiones necesarias para efectuar la actualización de este tipo de tecnología al igual que la definición de políticas que permitan establecer los parámetros necesarios para garantizar, en gran medida, a nivel de seguridad lógica lo necesario para la Universidad Nacional de Colombia.

7. CONCLUSIONES

- De acuerdo a lo definido por las normas internacionales, la seguridad de la información se logra con la implementación de controles establecidos por medio de políticas, procesos y procedimientos. En consecuencia, por su nivel de importancia, la Universidad Nacional de Colombia debe contar con lineamientos definidos para la protección de la información, mitigando riesgos que atenten contra esta, considerada como uno de los activos más importantes, la cual necesita estar eficazmente protegida.

- Desde la DNTIC, con la colaboración de las Oficinas de Tecnología de las Sedes y los líderes funcionales de los sistemas de información, se deben definir controles a implementarse en los procedimientos tendientes a dar solución a las situaciones encontradas, relacionadas con el control de los accesos lógicos. De igual forma, estas instancias deben vigilar la posible asignación de los derechos de acceso privilegiados, tal y como lo definen las normas, teniendo en cuenta que este tipo de accesos permiten a los usuarios superar los controles aplicados.