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.