EVALUACION REALIZADA AL PROCESO CITACION - CI
SISTEMAS PRISMA E ICFES-INTERACTIVO

Objetivos

- Evaluar el grado de soporte tecnológico que tiene el sistema Icfes Interactivo para su funcionalidad como herramienta de apoyo a la Gestión de Citación.

- Verificar el estado, operatividad y ambiente de control interno del módulo de Citación PRISMA con el fin de identificar oportunidades de mejora para que se implementen planes de acción que mitiguen los riesgos observados.

- Determinar la consistencia de la información de las aplicaciones de pruebas que ingresan al módulo de Citación Prisma y se desactivan del sistema Icfes – Interactivo.

Alcance

La evaluación del módulo Citación se realiza a los sistemas que apoyan el proceso, instalados en el ambiente de producción (Prisma e Icfes-Interactivo), de acuerdo con las mejores prácticas, y teniendo en cuenta los aspectos señalados en el plan de trabajo de auditoria de aplicaciones.

Metodología

La evaluación al módulo de Citación – PRISMA e ICFES-Interactivo se desarrolla bajo las mejores prácticas de Auditoria de Sistemas y Seguridad de Información existentes (Metodología General Interna Proyecto Misional, Modelo COBIT, Programa de Aseguramiento para Auditoria de Aplicaciones ISACA, Sistema de Gestión de Seguridad de la Información ISO 27001:2013)

Resultados

El proceso de información de Citación se apoya en las plataformas tecnológicas internas Prisma e Icfes Interactivo. A fecha de revisión, la plataforma PRISMA soporta la aplicación de pruebas Saber 11 (Presaber 11, Validante y Saber 11 que se ha realizado para calendario A 2014 y calendario B 2015) en su quinta liberación (reléase); el resto de pruebas (Saber Pro, Saber 3ero, 5to y 9nvo, Docentes, Policía,

Terce, Pisa, Inglés, entre otras) aún se procesan en el sistema Icfes Interactivo, las cuales se inactivan en la medida en que se trasladan al sistema Prisma.

La evaluación al módulo de Citación se realizó con base en las reuniones y entrevistas efectuadas a los funcionarios de la Subdirección de Aplicación de Instrumentos (señora: Martha Vasquez y señor Holman Herrera), Subdirección de Estadísticas (señor: Cristian Montaño), Oficina de Atención al Ciudadano (señora: Edna Paez) y Subdirección de Desarrollo de Aplicaciones responsable del proyecto de Tecnología Prisma (Señor: Camilo Velandia, señora Adriana Arboleda y señora Maribel Hernández) y de otra parte, se tuvo en cuenta la documentación física y digital suministrada y ubicada en el repositorio "Subversion".

(Se solicitó al Gerente del Proyecto de Tecnología Prisma acceso al ambiente de pruebas para validar la funcionalidad del módulo, el cual no estuvo disponible en razón a que el ambiente está dispuesto para el equipo de desarrolladores de pruebas. Esta situación impide realizar una revisión detallada de la funcionalidad del sistema).

Oportunidades de mejora

De la evaluación adelantada al módulo Citación del sistema ICFES-Interactivo, se observó que:

Control de Procesamiento ICFES-Interactivo

1. Presenta alta dependencia del recurso humano técnico para la ejecución y operación del proceso citación, pues no es el área usuaria coordinadora de la información quien opera en su totalidad el sistema (Subdirección de Aplicación de Instrumentos). La Subdirección de Desarrollo de Tecnología hace la configuración de los parámetros, los cuales se incluyen en el mismo programa de software, para ejecutar el procedimiento que genera el archivo de los datos de citación del inscrito (reporte de citación). Esta función no debe ser competencia de tecnología por el principio de protección a la información y por ser conocimiento y responsabilidad del área que realiza el procedimiento.

2. No es oportuna y exige alto recurso técnico la atención de necesidades y requerimientos que demanda el proceso en esta plataforma tecnológica (Icfes-Interactivo), debido a que el instituto no cuenta con personal entrenado totalmente en este software y no se tiene documentación técnica que permita reconocer la organización de los datos, flujos, programas y procedimientos de software que utiliza el sistema. falta de documentación en la configuración tecnológica y a la ausencia de conocimiento.

3. El sistema interactivo presenta un grado de obsolescencia importante debido a que el diseño tecnológico del software es poco parametrizable por la mezcla que hace de datos y software, lo cual genera carga operativa y limita el mantenimiento por el diseño particular que se debe suministrar a cada aplicación (Saber Pro, Saber 5, 9, 11, Policía, Sena, Cambrige, etc.).

   Recomendación

   Es importante agilizar el desarrollo del software en Prisma y se implementen las aplicaciones pendientes (Saber Pro, Saber 3, 5 y 9, Docentes, Policía y Pruebas internacionales -Terce, Pisa, y Cambrige).
   (ISO 27001, Anexo A-14.2 Seguridad en los procesos de desarrollo y de soporte, COBIT proceso DSS03 Manejo de Problemas, DSS06 Administración de los proceso de control del negocio).

En la evaluación adelantada al módulo citación del sistema PRISMA, se observó que:

Control de acceso Prisma

4. De la revisión a la lista de usuarios que acceden directamente los archivos (tablas) de la base de datos de producción PRISMA, se evidenció que los siguientes usuarios de la Dirección de Tecnología tienen permisos en la base de datos para hacer borrado, inserción, selección y actualización de registros en el módulo Citación, lo cual afecta principios de protección de la información y segregación de función por las actividades de gestión de seguridad y de desarrollo de tecnología de software que realizan:

Usuario	Función/Area	Permisos	Archivos que Acceden
JCASTELLANOS – Jefferson Castellanos	Analista de Datos - Subdirección de Información	Borrado Inserción Selección Actualización	PARA_TEXTO, PARA_TEXTOAPLICACION, CITA_AGRUPADORPOBLACION CITA_CITACIONSESILO2 CITA_CITACIONSESILOGIS CITA_DETALLEPROCESO CITA_EXCEPCIONCITA CITA_GRUPOSESION CITA_GRUPOSESIONSELO CITA_MARCADOR CITA_PROCESO CITA_SALONSESION CITA_SALOSESIDISC CITA_SESIONLOGISTICA CITA_SESISELO CITA_SITIOAPLICACION CITA_SORDOS18OCT CITA_SS20140218
DGARZON – Danny Garzon	Seguridad de Información - Subdirección de Información		
NBARAHONA – Nydia E Barahona	Analista de Datos - Subdirección de Información		
EVILLAMIZAR – Erika Villamizar	Seguridad de Información - Subdirección de Información		
NBENAVIDES – Natalia Benavides	Analista de Datos - Subdirección de Información		
DLOPEZ – Daniel Lopez	Analista de Datos - Subdirección de Información		
DRINCON Darío Rincon	Analista de Datos - Subdirección de Información		
CROJAS - Camilo Rojas	Analista de Datos - Subdirección de Información		
JBARRERA Joan Sebastián Barrera	Analista de Datos - Subdirección de Información		
JDIAZ Jenny Diaz	Analista de Datos - Subdirección de Información		

<u>Recomendación</u>

Revisar las lista de usuarios que interactúan con las tablas del módulo de citación en la base de datos con el fin evaluar junto con el propietario responsable de los datos, los usuarios a los cuales se les asignarán permisos para acceder a la información, teniendo en cuenta la función que desempeña en el área y sistema.

De otra parte, evaluar que el procedimiento de borrado, modificado o ingreso de información a la base de datos sea controlado por un comité de seguridad que valide el impacto y determine la acción a seguir, a través de un funcionario encargado de dicha labor, hasta tanto no se implemente el proceso automático que permita realizar los cambios de datos directamente en el aplicativo por el usuario responsable de la operación. (Por ejemplo: los requerimientos que provienen de la oficina de atención al cliente, los cuales son atendidos por el área de tecnología).

Como mecanismo de apoyo se puede utilizar la matriz de asignación de responsabilidades (RACI), la cual permite relacionar actividades con los recursos (personas y equipos) para asegurar que los componentes estén controlados.

Las Subdirecciones de Tecnología por su nivel de conocimiento que tienen de los sistemas y por su labor de producción y construcción de software no deben realizar simultáneamente tareas de operación y producción de la información, pues se afecta la segregación de función de estas áreas.

(ISO 27001, Anexo A-9.2 Gestión de acceso de usuarios, A-9.4 Control de acceso a sistemas y aplicaciones, COBIT proceso APO13 Administración de Seguridad, DSS05 Administración de la seguridad del servicio).

5. Si bien se cuenta con log activado que preserva el registro de trazabilidad de los permisos (cambios, inserciones y borrados de datos) y privilegios (Drop, alter de tablas, etc.) de la información sensible que se accede directamente a la base de datos Prisma, se evidencia que no se genera reporte del registro de pistas de auditoria (informe de operaciones y privilegios) de las tablas que se utilizan en el módulo. Además, no se tiene responsable asignado para la revisión de esta información.

   <u>Recomendación</u>

   Previa evaluación de las tablas y datos sensibles a auditar, se requiere formalizar la generación del reporte de la información del log de pistas de auditoria de Citación y determinar el responsable de efectuar el control y supervisión de permisos y privilegios.

   (ISO 27001, Anexo A-9.2 Gestión de acceso de usuarios, COBIT proceso APO13 Administración de Seguridad).

6. Se evidenció que aún no está dispuesta la definición de usuarios finales que acceden el módulo en el ambiente de Producción. Actualmente, el área de tecnología se encuentra determinando la estructura de controles de acceso a los usuarios internos del instituto que utilizan las diferentes opciones (ítems) de menú en el aplicativo.

   <u>Recomendación</u>
   Es importante revisar junto con el responsable de los datos, la lista de usuarios autorizados para acceder la información del módulo, determinando los permisos (ingreso, modificación, borrado y consulta) que tendrán para acceder las diferentes opciones (items) del menú.
   (Entre otros items para acceder en módulo de citación: 23-Parametrizar reglas, 24-Cargar marcadores a inscritos, 221-Cargar marcadores a salones, 26-Parametrizar textos de formato citación por examen aplicación, 641-Crear Editar Marcas, 28-Publicar citación, 30-Realizar citación manual, 33-Modificar citación individual 32-Trasladar citados por sitio aplicación, 365-Reportes Citación, 29-Ejecutar procesos, 281-Consultar procesos, 282-Eliminar procesos masivos).
   Como mecanismo de apoyo se puede utilizar la matriz de asignación de responsabilidades (RACI), la cual permite relacionar actividades con los recursos (personas y equipos, y asegurar que los componentes estén controlados.
   (ISO 27001, Anexo A-9.2 Gestión de acceso de usuarios, A-9.4 Control de acceso a sistemas y aplicaciones, COBIT proceso APO13 Administración de Seguridad, DSS05 Administración de la seguridad del servicio).

7. Aunque se tiene pista de auditoria (del ingreso, modificación, borrado y actualización de información) en el aplicativo de Citación, no se hace trazabilidad de las Consultas que se realizan a los datos sensibles y de propiedad del inscrito o proveedor, por lo que no se dispone de los mecanismos necesarios para atender lo establecido en materia de “Protección de datos Personales”.

   <u>Recomendación</u>
   Implementar los mecanismos necesarios que propendan por seguridad y trazabilidad de los datos de inscritos, proveedores y terceros que se conservan en los archivos del módulo, en cumplimiento de lo establecido para la protección de datos personales.
   (ISO 27001, Anexo A-9.2 Gestión de acceso de usuarios, COBIT proceso APO13 Administración de Seguridad, Ley Estatutaria 1266 de 2008 Disposiciones generales del habeas data y manejo de información contenida en base de datos personales, Ley 1581 de 2012 Protección de los datos

Personales, Decreto 1377 de 2013 y Resolución interna 000633 de 12 septiembre de 2014).

Control de Procesamiento Prisma

8. El área de investigación realizó una encuesta para los inscritos de la prueba Saber 11 calendario B 2015, la cual fue incorporada al sistema, para que el inscrito respondiera a un grupo de preguntas antes de conocer la información de su citación, no obstante, esta situación generó retraso y queja por la obligatoriedad de su diligenciamiento. Igualmente, la oficina de atención al cliente no fue informada ni entrenada oportunamente sobre este nuevo procedimiento en el sistema.

   Recomendación
   Es necesario que todo cambio o alteración en la secuencia del proceso, en especial los que impactan al inscrito, sea informada oportunamente a las áreas involucradas, entre otras Tecnología y Atención al cliente, con el propósito de que se prevea con tiempo: el desarrollo del software, las pruebas al sistema y la capacitación, campaña y divulgación para que se ofrezca mejor prestación de servicio al usuario.
   (ISO 27001, Anexo A-14.2 Seguridad en los procesos de desarrollo y soporte, COBIT proceso DSS06 Administración de los proceso de control del negocio).

9. No se produce automáticamente desde el módulo, el reporte de citación que tiene la información del inscrito y el sitio de presentación de la aplicación (Saber 11). El área de tecnología genera desde la base de datos del sistema Prisma un archivo Excel que es entregado a la Subdirección de Aplicación de Instrumentos (área usuaria) para que sea clasificado y distribuido a los profesionales responsables en cada regional. Este proceso que es manual, genera carga operativa a las áreas que intervienen.

   Recomendación
   Propender por el desarrollo de la generación automática del reporte de citación, de tal manera que los usuarios finales, entre otros, la Subdirección de Aplicación de Instrumentos, ingresen desde sus cuentas de usuario y obtengan el reporte sin intervención de la Dirección de Tecnología.
   (ISO 27001, Anexo A-14.2 seguridad en los procesos de desarrollo y soporte, COBIT proceso DSS06 Administración de los proceso de control del negocio

Control de Salida Prisma

10. La metodología interna que define los criterios a seguir en el proyecto de desarrollo de software, establece unos elementos o artefactos de entrada y salida (entre otros: casos de uso, caso de prueba, diseño, arquitectura y prueba unitarias) que son necesarios cumplir en las diferentes disciplinas o etapas planteadas en el proyecto.
De la revisión a la información dispuesta en el repositorio “Subversión” del módulo Citación Prisma, se observó que no todos los Casos de Uso (en total 24) contienen la información requerida.

Por ejemplo:

Caso de Uso “”	Descripción Proceso	Inconsistencia
CI_CUS_002	Realizar Citación Manual	No se encontraron pruebas unitarias, documento arquitectura y diseño
CI_CUS_004	Modificar Citación Individual	No se encontraron pruebas unitarias, documento arquitectura y diseño
CI_CUS_006	Crear editar Marcas	No se encontró casos de prueba
CI_CUS_011	Consultar citaciones por programa Académico	No se encontró casos de prueba
CI_CUS_015	Parametrizar textos formato citación	No se encontró casos de prueba
CI_CUS_031	Ejecutar ordenamiento masivo	No se encontró pruebas unitarias
CI_CUS_032	Cargar material	No se encontró pruebas unitarias y casos de prueba
CI_CUS_033	Activar e inactivar material	No se encontró casos de prueba
CI_CUS_034	Asociar secuencias aplicación	No se encontró pruebas unitarias y casos de prueba
CI_CUS_035	Aprobar secuencias	No se encontró casos de prueba
CI_CUS_036	Ejecutar asignación combos	No se encontró pruebas unitarias y casos de prueba
CI_CUS_037	Ejecutar numeración combos	No se encontró pruebas unitarias y casos de prueba

Ruta de la Información: (“http://192.168.147.76/svn/misional/aplicacion_pruebas/citacion/trunk/...”)
Pruebas unitarias: (“…/Pruebas/Pruebas Unitarias/“); Documentos arquitectura y diseño: (…“/Diseno/Documentos/”)
Casos de prueba: (“…/Pruebas/Casos de Pruebas/”); Casos de Uso (“…/Requerimientos/Casos de uso/)

De otra parte, el proceso “Consultar inscrito vs pupitres” carece de “Casos de uso”, “Pruebas unitarias” y “Documento de arquitectura”, a pesar de contar con: caso de prueba (”Diseño CI_CUS_007”) y documento de diseño (“CI_DD_007”).

Recomendación
Es importante evaluar la información que se mantiene en el repositorio “Subversión”, de tal manera que se cumpla los requisitos establecidos en las disciplinas o etapas que establece el ciclo de desarrollo de software del proyecto Prisma, los cuales están definidos en la metodología interna.
(ISO 27001, Anexo A-14.2.5 Principios de construcción de los sistemas seguros, A-12.1.1 Procedimientos de operación documentados COBIT proceso DSS06 Administración de los proceso de control del negocio).

11. Los documentos de definición de la arquitectura de datos que se conservan en el repositorio “Subversión” se encuentran desactualizados (“20140204ParametriazacionCitacion.png” y “20131230_citacion.png”), ya que estos relacionan archivos que no existen en la base de datos de producción Prisma (entre otras tablas: “cita_parametrodefault”, “cita_reglaparametro”, “cita_textoaplicacion”, “cita_texto”, “cita_reglaconfigurada”, “cita_parametro”, “cita_filtroregla”, “cita_reglacitacion”, “cita_tipofiltro”).

    Igualmente, la documentación del modelo entidad relación de la base de datos Prisma, suministrada por la arquitecta de datos, no incluye todas las tablas que existen en el ambiente de producción. Entre otras, las utilizadas para el manejo y control de usuarios en el módulo citación (tablas no reportadas: “USUA_GRUPOUSUAROL”, “USUA_GRUPOUSUARIO” y “USUA_GRUPOACCESO”).

    <u>Recomendación</u>
    Es necesario realizar actualización de la documentación que se mantiene en el repositorio “Subversión”, de tal manera que represente los datos, recursos y procesos que componen el sistema Prisma en producción.
    (ISO 27001, Anexo A-14.2.5 Principios de construcción de los sistemas seguros, A-12.1.1 Procedimientos de operación documentados COBIT proceso DSS06 Administración de los proceso de control del negocio).

12. Aunque se solicitó, no se obtuvo información documentada de la estructura de datos Prisma (diccionario de datos). Esta situación no permite precisar el detalle y descripción del flujo, almacén y proceso de datos que componen el sistema.

    <u>Recomendación</u>
    Como herramienta para el diseño y desarrollo de software es importante contar con la estructura de datos actualizada, con el fin de identificar las características (fortalezas y debilidades) que conforman el sistema.
    (ISO 27001, Anexo A-14.2.5 Principios de construcción de los sistemas seguros, COBIT proceso DSS06 Administración de los proceso de control del negocio).

13. El manual de Proceso de Citación se limita y circunscribe a una breve descripción que forma parte de otro manual de Procesos, llamado: “Gestionar Material – Asignación de Combos de Material CUN04” numeral 3.4, el cual no detalla las características operativas y funcionales que involucra los subprocesos del módulo (como son: creación marcas, parametrización

reglas, marcadores a inscritos, a salones, parametrizar textos de formato de citación, publicar citación, realizar citación manual, trasladar citados por sitio aplicación, modificar citación individual, eliminar citación masiva, ejecutar procesos, consultar procesos y reportes).

Recomendación
Se requiere documento específico para el Proceso de Citación que detalle los diferentes subprocesos que componen el módulo, tanto en la operación como en el aplicativo.
(ISO 27001, Anexo Anexo A-12.1.1 Procedimientos de operación documentados, COBIT proceso DSS06 Administración de los proceso de control del negocio).

14. El Manual del usuario del módulo citación: "¿Cómo realizar la Citación?" hace una presentación muy general de las opciones de menú del sistema sin precisar la funcionalidad que tiene cada una de ellas (Por ejemplo: en la opción creación de una regla no se detalla si el proceso corresponde a definir una regla adicional a las referenciadas en la tabla uno (1) o a incorporar una regla predefina en una aplicación; en la definición del filtro de inscrito y/o salón no se define la relación del filtro con la regla a utilizar en cada filtro y en la agregación de filtros no obligatorios no se especifica los criterios a tener en cuenta para definir variables, condiciones y valores, entre otros aspectos).

Recomendación
Se requiere que el Manual del Usuario de Citación incluya una descripción precisa que oriente y guíe al usuario final en la operación y funcionalidad de las diferentes opciones de menú que componen el módulo.
Además, Independientemente a la documentación que se hace de los casos de uso, especificaciones suplementarias, diseño, arquitectura, pruebas, modelo diseño y prototipos, los cuales son necesarios para el cumplimiento de la metodología, se requiere un Manual Técnico que integre, compendie los documentos anteriores sin repetir información, y describa la tecnología de software que conforma el módulo.
(ISO 27001, Anexo A-12.1.1 Procedimientos de operación documentados, COBIT proceso DSS06 Administración de los proceso de control del negocio).

Control de Cambios Prisma

15. Aunque se tiene definido un procedimiento para la "Gestión de Control de Cambios" que describe las actividades que se deben seguir para atender, evaluar y autorizar las peticiones de cambio de un proceso por efecto de innovación, mejora de servicios o cumplimiento de nuevas normativas

legales que generalmente requieren cambio en la infraestructura tecnológica del software Prisma, se evidencia que para su manejo y control se utiliza la herramienta de uso manual como es la hoja Excel (“Listado Controles de Cambio Citación), la cual no permite controlar automáticamente el software de cambio autorizado que ingresa efectivamente al ambiente de producción. (Por ejemplo, en el caso de citación, se reportan solamente cuatro controles de cambio de cinco liberaciones -reléase- que ha tenido el módulo, ellos son: 42-adicionar discapacidades, 43-ordenamiento carga, 44-no diferenciar mayúscula y minúscula en materiales y 45-cargar mismo material para diferentes combos).

De otra parte, no se cuenta con procedimiento que determine las actividades y recursos tecnológicos utilizados para el control y registro de las unidades de software que se ingresan, modifican o borran en el ambiente computacional de producción Prisma.

<u>Recomendación</u>

Se requiere contar con un mecanismo automático (software) que permita controlar (detalle fecha de ingreso, usuario, característica del software y sitio de instalación en el sistema, entre otros) el software que ingresa al ambiente de producción, no solamente por efecto de cambio sino que incluya todo nuevo producto que se instala en la plataforma y se mantenga registro y trazabilidad del proceso de transporte de programas.

La Coordinación del proyecto manifestó que la Dirección de Tecnología se encuentra evaluando la compra de un software que permita controlar el software que se traslada y mantiene en el ambiente Prisma.

(ISO 27001, Anexo A-12.1.2 Gestión de Cambios, A.14.2.4 Restricciones en los cambios a los paquetes de software, BAI06 Administración de cambios).

16. El área de tecnología realizó el 25 de enero de 2015 una revisión a lista de usuarios con conexión a la base de datos (Analista de seguridad), del cual se han reportado unos comentarios en el: “*Informe de usuarios de las bases de datos Productivas y Planeación de la configuración de Políticas de Bloqueo sobre las aplicaciones con conexión a estas bases de datos*”.

<u>Recomendación</u>

Es necesario evaluar lo indicado en el informe con el fin de establecer formalmente un plan de trabajo que procure la seguridad del sistema.

(ISO 27001, Anexo A-18.2 Revisiones de seguridad de la Información, MEA01 Monitoreo, evaluación y valoración de desempeño y conformidad).

Conclusión

1. Si bien se realiza el proceso de citación de pruebas saber 11 en el ambiente de producción Prisma (con el mayor número de inscritos con respecto a las otras pruebas), aún se encuentra pendiente de instalar las pruebas: Saber Pro, Saber 3ero, 5to y 9nvo, Docentes, Policía, Terce, Pisa, Inglés, entre otras, las cuales se encuentran en el sistema Icfes Interactivo que genera carga operativa y presenta deficiencias de seguridad de la información.

2. El desarrollo e implementación de los módulos Prisma, en el cual se procesa las pruebas Saber 11, atiende a la necesidad principal de la operación en un ambiente que presenta deficiencias en la administración de seguridad de datos. Además, el módulo Citación no cuenta con reportes de trazabilidad que permitan ejercer supervisión y control de las operaciones que se realizan en el sistema.

3. A fecha de revisión, no se ha entregado formalmente la funcionalidad operativa del módulo de citación Prisma implementada en producción (aplicación de pruebas Saber 11) a los usuarios y áreas responsables de la operación del sistema, lo que afecta principios de responsabilidad y segregación de la función y tareas por que se comparten responsabilidades en el manejo de la información.