202330003355
Fecha Radicado: 2023-08-03 16:01:24.837

Radicado No: 202330003355

COMUNICACIÓN INTERNA

PARA: **ELIZABETH BLANDÓN BERMÚDEZ**
Directora General

COMITÉ INSTITUCIONAL DE COORDINACIÓN DE CONTROL INTERNO
SERGIO ANDRÉS SOLER ROJAS
Director de Tecnología e Información
CARLOS ALBERTO DURÁN PÉREZ
Subdirector de Información
ARMANDO ALFONSO LEYTON GONZÁLEZ
Subdirector de Desarrollo de Aplicaciones

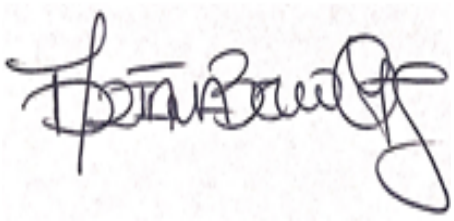
DE: **JEFE OFICINA DE CONTROL INTERNO**

ASUNTO: **Informe de asesoría en el proceso de Gestión de Tecnología e Información (GTI), frente al incidente reportado en el aplicativo PLEXI durante la realización de la prueba Saber PRO y T&T primer semestre 2023.**

Respetados líderes:

De manera atenta les informo que en cumplimiento al Plan Anual de Auditoría y de acuerdo con el procedimiento de Asesoría Control Interno CSE-PR009 se remite el informe del asunto para su conocimiento y fines pertinentes.

Cordialmente,



ADRIANA BELLO CORTÉS
Jefe Oficina de Control Interno

Anexo: Informe en dos (2) folios

icfes	**INFORME DE ASESORÍA CONTROL INTERNO**			**Código: CSE -FT010**
	Control y Seguimiento			**Versión: 001**
Clasificación de la información	[X] PÚBLICA	[ ] CLASIFICADA	[ ] RESERVADA	

Fecha de Solicitud de la Asesoría	16/06/2023	**Fecha de la Asesoría**	28/06/2023	29/07/2023

PROCESO / PROGRAMA / PROYECTO ASESORADO	**Gestión de Tecnología e Información (GTI)**		
Dependencia	Dirección de Tecnología e Información Subdirección de Información Subdirección de Desarrollo de Aplicaciones	**Equipo OCI asignado**	Adriana Bello Cortes Marco Ramiro Marín Buitrago
Nombre del solicitante de la asesoría	Andrés Molano Flechas Luisa Fernanda Trujillo Bernal Evelyn Julio Estrada	**Cargo del solicitante de la asesoría**	Director General Secretaria General Jefe Oficina Asesora Jurídica
Tema Objeto de Asesoría	Asesoría Plexi frente al incidente del 27 de mayo de 2023	**Origen de la asesoría**	Incidente de seguridad registrado el 27 de mayo de 2023 en el marco de la pruebas saber Pro y T&T.
Criterios de la Asesoría	Procedimiento CSE-PR009 “Asesoría Control Interno", estándar ISO 27001:2013 y Política de Seguridad y Privacidad de la Información del Instituto.		
Objetivo	Prestar asesoría en el proceso de Gestión de Tecnología e Información (GTI), frente al incidente reportado en el aplicativo PLEXI durante la realización de la prueba Saber PRO y T&T primer semestre 2023.		
Alcance	Efectuar la revisión a las causas y mejoras planteados al sistema de información PLEXI y sus componentes, consecuencia del incidente de seguridad que se registró el 27 de mayo de 2023 en el marco de la pruebas saber Pro y T&T.		

CONTEXTO QUE ANTECEDE EL PROCESO DE ASESORÍA

El 27 de mayo de 2023, durante la aplicación de las pruebas Saber Pro y Saber T&T, se registró un incidente de seguridad relacionado con el software de Evaluación del Instituto (PLEXI) y los componentes que lo conforman, llevando a suspender y a reprogramar la aplicación de las pruebas Saber Pro y T&T del primer semestre. La Alta Dirección del Instituto solicitó hacer una revisión contextualizada del incidente, las causas que lo originaron y las posibles recomendaciones para que, situaciones similares no se repitan.

Durante el desarrollo de la asesoría, se revisó la documentación de los cambios y mejoras realizados a PLEXI entre octubre de 2022 y mayo de 2023, se efectuaron socializaciones a los equipos de trabajo de la Dirección de Tecnología e Información - DTI y a los líderes de los procesos misionales de la Dirección de Producción de Operaciones - DPO y de la Dirección de Evaluación - DE, con el propósito de contar con diversas opiniones y sugerencias de las partes interesadas en el desarrollo de las pruebas Saber Pro y T&T.

De igual manera, se revisó la documentación relacionada con el incidente de seguridad registrado el 27 de mayo de 2023, así como, de las actividades que fueron desplegadas por la Dirección de Tecnología - DTI para mitigarlo y para identificar la causa inmediata del mismo.

Sobre el particular se evidenció lo siguiente:

a) Durante el incidente de seguridad, el equipo de la Dirección de Tecnología e Información activó el "plan de contingencia" descrito en el documento "Documento DRP_PruebaElectronica_2023"; sin embargo, estas actividades no fueron suficientes para subsanar la crisis.

b) Las actividades que fueron desarrolladas por la DTI posteriores al incidente, evidenciaron que los "reingresos" a PLEXI realizados por algunos evaluandos durante la aplicación de las pruebas Saber Pro y T&T, fueron la causa inmediata de la "indisponibilidad" de la base de datos del software de Evaluación. De igual manera, en ese análisis se evidenció, que los "reingresos" fueron originados por la pérdida de conexión de internet en algunos sitios de aplicación, originando que la aplicación PLEXI en sitio (QUIOSCO) no cargara la totalidad de las preguntas de los evaluandos, generando errores inesperados y llevando a reiniciar la aplicación como solución inmediata para continuar con la prueba.

RECOMENDACIONES

1. Fortalecer las actividades descritas en el procedimiento denominado "Gestión de Cambios de TI", cuando se realicen cambios significativos al software de Evaluación (PLEXI) del Instituto y a sus componentes asociados. Entre octubre de 2022 y mayo de 2023, la Dirección de Tecnología de Información - DTI y sus subdirecciones, realizaron cambios significativos en la aplicación PLEXI y a sus componentes que la soportan, esto es, a la base de datos y al QUIOSCO, que fueron necesarios para soportar las nuevas cargas de trabajo que se presentarían durante la aplicación de las pruebas Saber Pro y T&T del primer semestre de 2023.

Estas actividades fueron desarrolladas por los equipos de trabajo de la DTI utilizando los procedimientos del Instituto denominados "Gestión de Cambios" y "Desarrollo de Soluciones Informáticas"; sin embargo, cuando existan estas actualizaciones en PLEXI, se sugiere que:

a) Las nuevas funcionalidades y configuraciones deberían probarse en escenarios "reales", esto es, teniendo en cuenta las condiciones, situaciones, comportamientos u otros originados por parte del usuario del aplicativo, que no pueden ser simuladas con los software de carga y estrés; Las causas de los "reingresos" a PLEXI podrían ocurrir en diversas situaciones, por ejemplo, es posible que se produjeran por una "errónea" manipulación del usuario final durante la aplicación de la prueba o que, el computador donde fue instalada la aplicación fallara o que, el sitio de aplicación tuviera caídas de energía; eventos, que generarían la necesidad de reiniciar PLEXI para continuar con el examen.

b) Las nuevas funcionalidades implementadas en PLEXI deberían ser validadas de manera independiente e imparcial por un tercero o "par" que no haya participado en el desarrollo de la aplicación o en la implementación de estas. Con esta actividad se busca fortalecer la confianza en PLEXI, los requisitos del sistema de gestión en el numeral "8.3 diseño y desarrollo" del estándar ISO 9001:2015 y las capacidades operativas del mismo como software de Evaluación en el Instituto.

2. Implementar un módulo de auditoría que registre :

a) los eventos e incidentes de los principales componentes de PLEXI y su funcionamiento, de tal manera, que se cuente con insumos suficientes para determinar con mayor precisión los "errores" o fallas durante la aplicación de la prueba; si bien es cierto que, durante la asesoría se evidenciaron soportes de registros, éstos deberían ser parte de la documentación del módulo de auditoría;

b) Los eventos asociados a los evaluandos y las principales actividades que estos realizan durante la aplicación como: registro del número de veces que el usuario ingresó a la aplicación; registro del diligenciamiento o no de los campos en las preguntas (con el propósito de evidenciar si los campos vacío del string obedecen a errores técnicos de plexi o por el ocntrario porque el estudiante decidió no responder la pregunta); asímismo, el registro del envío efectivo de las cadenas de respuesta; entre otras. Lo anterior con el fin de contar con evidencia técnica y objetiva sobre los posibles cuestionamientos que se puedan originar en torno a la aplicación de la prueba.

3. Fortalecer la gestión de riesgos cuando se realicen cambios significativos en el software de Evaluación (PLEXI) y sus componentes; sobre el particular se recomienda lo siguiente:

a) Como proceso de Gestión de Tecnología e Información, se sugiere identificar y evaluar los nuevos escenarios de riesgos como consecuencia de las nuevas configuraciones y funcionalidades que fueron implementadas en PLEXI, para soportar las cargas de trabajo durante la aplicación de las pruebas Saber Pro y T&T, de esta manera, se pueden implementar nuevos controles (técnicos, documentales o humanos) que minimicen la ocurrencia o materialización de estos.

b) Como parte de la cadena de valor del Instituto, se sugiere fortalecer los escenarios de riesgos propuestos en el documento denominado "continuidad de negocio" relacionado con el desarrollo de las pruebas Saber Pro y T&T, en el cual se recomienda que los procesos de "Gestión de Tecnología e Información", "Aplicación de Instrumentos de Evaluación" y "Procesamiento y Calificación" participen de manera activa e integral, debido a que, las actividades que se encuentran descritas en estos procesos y que rodean la aplicación y calificación de las pruebas Saber Pro y T&T son dependientes entre sí, al fallar alguno de estos los demás de manera directa o indirecta se verán afectados; por ejemplo, la materialización del riesgo de "disponibilidad" en la aplicación PLEXI ocurrida el 27 de mayo, afectó de manera directa a los demás procesos y estos no contaban con los suficientes controles para mitigarlo.

4. Fortalecer el documento denominado "Esquema líneas de defensa en el Icfes". El incidente de seguridad del 27 de mayo evidenció que la gestión de riesgos y el monitoreo de estos no se realizan de manera eficaz, por tal motivo se recomienda:

a) Asignar el Área de Seguridad y Privacidad de la Información del Instituto que actualmente se encuentra bajo la responsabilidad de la Dirección de Tecnología e Información - DTI, como parte de la segunda línea de defensa del Icfes y cercano a la Dirección, con las funciones de gestionar y monitorizar los riesgos de seguridad de la información y los de ciberseguridad de manera objetiva y transversal al Instituto, esto, de acuerdo con lo propuesto en los numerales “3.2.1.4. Política de seguridad digital” del manual operativo de MIPG y del numeral “7.2.3 Roles y responsabilidades” del documento Maestro del Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de Tecnologías de la Información y Comunicaciones - MINTIC en el que se indica “*se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la entidad, el cual debe pertenecer a un área transversal que haga parte de la Alta Dirección* ” y de ser posible cuente con voz en los comités que se realicen.

b) Fortalecer y hacer seguimiento a la "mesa técnica de riesgos" que se encuentra liderada desde la Oficina Asesora de Planeación (OAP). Los riesgos relacionados con las pruebas de Estado (Saber Pro, T&T y las demás) deberían ser revisados y analizados de manera contextual, de tal manera, que, en la cadena de valor se evidencien los riesgos que en común pueden afectar a más de un proceso y de esta manera determinar responsabilidades compartidas sobre controles.

COMENTARIOS Y OBSERVACIONES GENERALES

1. Continuar con los desarrollos y las mejoras propuestas al software de Evaluación (PLEXI) construido al interior del Icfes. Los procesos de maduración del software de Evaluación se verán reflejados a medida que sea utilizado en escenarios "reales" y puesto a prueba durante la aplicación de los exámenes de Estado, con incremento de usuarios de manera escalonada, que permita tener mayor control de la prueba.

2. Como parte de los procesos de "continuidad de negocio", sería prudente contar con alternativas que minimice los riesgos de "integridad", "confidencialidad" y "disponibilidad" de la aplicación PLEXI durante la aplicación de una prueba. Los procesos de maduración de PLEXI deberán indicar las capacidades del software de evaluación en cuanto a cantidad de usuarios soportados, pero, los procesos de "negocio" deberán contar con contingencia en caso de que falle el primero.

3. En la actualidad las mejoras a PLEXI propuestas por la Dirección de Tecnología e Información - DTI, producto del incidente objeto del presente análisis, son coherentes y oportunas que ayudaran a minimizar los riesgos de "disponibilidad" durante la aplicación de las pruebas Saber Pro y T&T; sin embargo, evidenciamos que los nuevos cambios son significativos, por lo que, sugerimos realizar la gestión de riesgos como proceso de GTI y de manera contextual con los otros procesos que interactúa, así mismo, estos cambios, deberían ser probados en escenarios "reales" para validar su funcionalidad y operación.

CONCLUSIONES

Las mejoras efectuadas a la aplicación PLEXI (Quiosco y base de datos) por la Dirección de Tecnología e Información - DTI entre octubre de 2022 y mayo de 2023, se enmarcaron y cumplieron las actividades descritas en los procedimientos "Gestión de Cambios" y "Desarrollo de Soluciones Informáticas", se encontraron documentadas las etapas de desarrollo, pre-producción y producción. De igual manera, se evidenció documentado el incidente de seguridad, donde se analizaron las "causas" que lo originaron, logrando simular el escenario del incidente en un ambiente de control. Sin embargo, pese a haber cumplido con cada uno de los requerimientos que el Instituto exige para este tipo de desarrollos, no fueron suficientes, por lo que, se sugiere abarcar cada una de las recomendaciones descritas en este documento para minimizar eventuales incidentes de seguridad relacionados con el software de Evaluación del Instituto.