Radicado No: 202130002474
Fecha Radicación: 2021/12/31

COMUNICACIÓN INTERNA

PARA: **MÓNICA PATRICIA OSPINA LONDOÑO**
Directora General

COMITÉ INSTITUCIONAL DE CONTROL INTERNO

DIRECTORES, SUBDIRECTORES, JEFES DE OFICINA Y ASESORES

DE: **ADRIANA BELLO CORTÉS**
Jefe Oficina de Control Interno

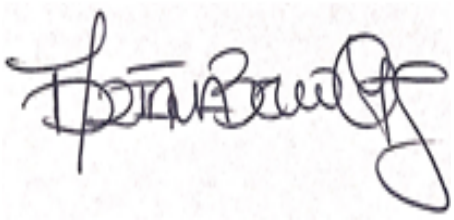
ASUNTO: ***Informe de Auditoría Interna al Sistema de Gestión de Seguridad de la Información 2021***

Respetados líderes:

De manera atenta les informo que en cumplimiento al Plan Anual de Auditoría y de acuerdo con el procedimiento de Auditoría Interna, se remite el Informe de la Auditoría practicada al Sistema de Gestión de Seguridad de la Información. Este contiene los hallazgos evidenciados por el Ingeniero Oscar Fernando Ramos Benavides, así como las recomendaciones para fortalecer el Sistema.

Es procedente que los resultados se socialicen con los responsables del sistema evaluado y en cumplimiento al Procedimiento de Gestión Planes de Mejoramiento (PDE-PR008), se formule el Plan de Mejoramiento pertinente para atender las situaciones observadas dentro de los quince (15) días hábiles siguientes a la notificación del cargue en el aplicativo Daruma.

Cordialmente,



ADRIANA BELLO CORTÉS
Jefe Oficina de Control Interno

Anexo: Informe en ocho (8) folios

icfes mejor saber	**INFORME DE AUDITORIA**	**Código: CSE-FT004**
	CONTROL Y SEGUIMIENTO	**Versión: 001**
CLASIFICACIÓN DE LA INFORMACIÓN	☐ **Pública** ■ **Clasificada** ☐ **Reservada**	

Informe Preliminar:								**Informe Final:**	x										
Fecha de emisión:						**30/12/2021**													
Reunión de Apertura						**Ejecución de la Auditoría**								**Reunión de Cierre**					
Día	10	**Mes**	12	**Año**	2021	**Desde**	01/12/2021 D / M / A	**Hasta**	31/12/2021 D / M / A	**Día**	30	**Mes**	12	**Año**	2021				

Proceso / Programa / Proyecto auditado:	**PDE**-Planeación y Direccionamiento Estratégico., **AYD** Análisis y Difusión., **API** Aplicación de instrumentos de evaluación., **AGI** Atención de grupos de interés. **CIE** Construcción de instrumentos de evaluación., **CDI** Control Disciplinario., **CSE** Control de Seguimiento., **DFI** Desarrollo y Fomento de la Investigación., **DES** Direccionamiento Estratégico., **DYC** Divulgación y Comunicación., **GEC** Gestión Comercial., **GAB** Gestión de Abastecimiento., **GEP** Gestión de Proyectos., **GTH** Gestión de Talento Humano., **GTI** Gestión de Tecnología e Información., **GCI** Gestión de Conocimiento y la innovación., **GDO** Gestión documental., **GFI** Gestión Financiera., **GJU** Gestión Jurídica., **PYC**
Objetivo de la Auditoría:	A continuación, se relacionan los Objetivos de la auditoría interna: • Determinar la conformidad del sistema de gestión con los requisitos de la norma de sistema de gestión. • Determinar la capacidad del sistema de gestión para asegurar que la organización cumple los requisitos legales, reglamentarios y contractuales aplicables al alcance del sistema de gestión y a la norma de requisitos de gestión. • Determinar la eficacia del sistema de gestión para asegurar que la organización puede tener expectativas razonables con relación al cumplimiento de los objetivos especificados. • Identificar áreas de mejora potencial del sistema de gestión.
Alcance de la Auditoría:	El SGSI y la presente Política de seguridad y privacidad de la información aplican a todos los procesos del Instituto Colombiano para la Evaluación de la Educación – ICFES, y de obligatorio complimiento para los funcionarios, contratistas, practicantes y terceros que tengan vínculos laborales o contractuales con este. Dentro de los controles de ISO/IEC 27001:2013 Anexo A No Aplicables: A.11.1.6 Áreas de despacho y carga
Criterios de la Auditoría:	• Norma Técnica Colombiana **NTC/IEC 27001:2013** • Políticas de seguridad y privacidad de la información-**GTI-PT001.** • Manual de políticas de seguridad y privacidad de la información-**GTI-MN001.**

- Mapa de riesgos de seguridad de la información (vigente).
- Modelo de seguridad y privacidad de la información - MSPI
- Instrumento de evaluación MSPI – ICFES 30072020
- Plan anual de auditoria/año anterior (2021).
- Normatividad SGSI_Icfes 2021.
- Ley 1581 de 2012.
- **Caracterizaciones de procesos:**
  - ✓ Análisis y Difusión AYD -CR001
  - ✓ Aplicación de instrumentos de evaluación API -CR001
  - ✓ Atención a grupos de interés AGI -CR001
  - ✓ Construcción de instrumentos de evaluación CIE -CR001
  - ✓ Control Disciplinario CDI -CR001
  - ✓ Control y seguimiento CSE -CR001
  - ✓ Desarrollo y fomento de la investigación DFI -CR001
  - ✓ Direccionamiento Estratégico DES -CR001
  - ✓ Diseño de instrumentos de evaluación DIE -CR001
  - ✓ Divulgación y comunicaciones DYC -CR001
  - ✓ Gestión Comercial GEC -CR001
  - ✓ Gestión de abastecimiento GAB -CR001
  - ✓ Gestión de proyectos GEP -CR001
  - ✓ Gestión de talento humano GTH -CR001
  - ✓ Gestión de tecnología e información GTI -CR001
  - ✓ Gestión del conocimiento y la innovación GCI -CR001
  - ✓ Gestión documental GDO -CR001
  - ✓ Gestión financiera GFI -CR001
  - ✓ Gestión Jurídica GJU -CR001
  - ✓ Procesamiento y calificación PYC -CR001

METODOLOGÍA Y PROCEDIMIENTO DE LA AUDITORÍA

En la auditoría interna se asegurará el cumplimiento de los lineamientos definidos en el procedimiento **CSE-PR001** de auditoría interna del Icfes y la norma de directrices para la auditoría de sistemas de gestión **ISO 19011:2018;** la auditoría será realizada a través de métodos de auditoría aprobados tales como, entrevistas, observación y análisis de la documentación y recolección de evidencia correspondiente, la cuál será validada a través de muestreos aleatorios con el fin de evaluar el cumplimiento del criterio que se esté evaluando, a continuación, se detallan las actividades a ejecutar:

1. **PLANEACIÓN AUDITORIA INTERNA**:

a. **Definición el sistema de gestión a auditar:** Sistema de gestión de seguridad de la información bajo el marco de la norma internacional ISO/IEC 27001:2013.
b. **Definición del plan de auditoria:** para la definición del plan de auditoría interna, se han determinado los siguientes criterios:
   - Procesos por auditar
   - Objetivo de la auditoria
   - Alcance
   - Criterios, marco regulatorio y fuentes de información
   - Agenda de ejecución de la auditoría interna.
c. **Reunión con el equipo auditor:** Esta reunión se realiza con el fin de coordinar y dar los lineamientos sobre la ejecución de las sesiones de auditorías internas.
d. **Preparar documentos de trabajo:** Solicitud y análisis de la documentación de cada proceso, y elaboración de las listas de verificación (chequeo), por parte del equipo auditor previo a la realización de la auditoría interna.
e. **Enviar el plan de auditoria:** el equipo auditor enviará el plan de auditoría a las partes interesadas para su revisión, aprobación y formalización mediante comunicación a los responsables de atender cada una de las sesiones de auditoría. Este plan de auditoria contendrá el itinerario detallado por proceso.

2. **EJECUCIÓN AUDITORIA INTERNA:**

a. Realizar reunión de apertura: se realizará la reunión con las partes interesadas con el fin de socializar el detalle del plan de auditoria aquí referenciado incluyendo el itinerario, así mismo se analizará en caso de aplicar los ajustes que sean solicitados.

b. Ejecución de auditoria por proceso:

✓ Se realizará la auditoría interna a través de entrevistas con los responsables de los procesos y equipo de trabajo, momento en el cual se solicitará y recolectará información clave que permita evidenciar el cumplimiento de los requisitos definidos en la norma ISO/IEC 27001:2013 y los de la organización. Lo anterior con el fin de evaluar el correcto desempeño y eficacia del sistema de gestión de seguridad de la información.

✓ Verificación del cumplimiento de: Roles y responsabilidades, toma de conciencia, documentación de cada proceso (evidencias), implementación y seguimiento de actividades definidas en el manual de sistemas de gestión **PDE-MN001**, de políticas de seguridad y privacidad de la información **GTI-PT001** y caracterizaciones entre otros.

✓ Valoración y cierre de acciones correctivas, preventivas o de mejora, incluyendo análisis, seguimiento y ejecución por proceso o preventivas dentro de plan de acción, aquellas que se encuentren en estado “100% finalizada”.

Nota: se contará con la asistencia de un auditor observador de la oficina de control interno y de la oficina de planeación en la ejecución de auditoría de cada proceso.

c. Reuniones de pre cierre de auditoria: antes de finalizar el ejercicio de auditoría interna por proceso, el equipo auditor compartirá de manera general los hallazgos de la auditoría (fortalezas, aspectos de

cumplimiento, oportunidades de mejora, observaciones, y posibles no conformidades, tanto de los requisitos y controles de la norma ISO/IEC 27001:2013.

d. **Preparación de informe de auditoría:** El equipo auditor preparará el informe de cierre en el formato cse-ft004_informe_de_auditoria__v1 informando el resultado de la auditoria al responsable del sistema de gestión de seguridad de la información.

e. **Reunión de cierre:** Se realizará reunión de cierre con los responsables de los líderes de procesos en donde se formalizarán los hallazgos de fortalezas, oportunidades de mejora o no conformidades determinadas y que se hayan identificado durante el ejercicio de la auditoría interna, en caso de presentarse alguna solicitud de revisión esta misma será evaluada y gestionada según aplique.

f. **Envío de informe final:** El auditor líder enviará el informe final a las partes interesadas durante los cinco (5) días siguientes a la reunión de cierre.

LIMITACIONES

Ninguna.

RESULTADO DE LA AUDITORÍA

FORTALEZAS

1. El alto compromiso evidenciado por parte de la alta dirección en la medida que asigna los recursos necesarios para mantener el sistema de gestión.
2. El grado de apropiación y conocimiento de los propósitos de seguridad de la información por parte de los líderes de los procesos, en la medida que asegura el cumplimiento de los objetivos de protección de la información y demás activos de la organización.
3. Los gestores de desempeño institucional como enlaces entre el sistema de gestión de seguridad de la información y los procesos aseguran la implementación de las prácticas del SGSI.
4. La generación de campañas de comunicación y socialización de los propósitos del sistema de gestión de seguridad de la información (tips o cápsulas de conocimiento), por lo que refuerzan la cultura de seguridad de la información al interior de la Entidad.
5. El uso de la herramienta DARUMA en la medida que permite el registro, seguimiento y control tanto de los inventarios de activos de información como de la valoración de los riesgos de seguridad de la información.
6. Una clara definición de la estructura documental asociada para los propósitos del SGSI por lo que permiten el registro y consulta de la información de acuerdo con su nivel y propósito para consulta de los interesados.
7. Un modelo de control estricto con respecto a las actividades del proyecto y sistema de gestión de seguridad de la información, permiten asegurar y/o alcanzar los propósitos del SGSI.
8. La estricta aplicación y recolección de los acuerdos de confidencialidad y no divulgación de información confidencial con todos aquellos quienes mantienen una relación bien laboral o de servicios con la entidad, por tanto, asegura el conocimiento, responsabilidad y su aceptación.

9. El establecimiento de cláusulas de propiedad intelectual, confidencialidad y tratamiento de datos personales en minutas contractuales, por lo que clarifica las responsabilidades y acuerdos entre las partes.
10. La identificación de la información de errores o incidentes de seguridad de la información en repositorio central, por tanto, aporta una base de conocimiento para atender situaciones similares y de manera oportuna.
11. La identificación y registro centralizado de los requisitos de legislación y normativos asociados a seguridad de la información (normograma), por tanto, asegura la identificación de estrategias o planes para su estricto cumplimiento.
12. El tratamiento de los aspectos de seguridad de la información a través de los comités primarios, permiten una retroalimentación directa con los usuarios y/o colaboradores de la Entidad.
13. Seguridad perimetral basado en Firewall, Switches, logs en Access Point, seguridad en cuanto a portal y equipos de seguridad., IDS propio del firewall, por lo que mitiga ataques de ciberseguridad en la organización.
14. La implementación de seguridad para accesos de usuarios a aplicaciones y sistemas de información de ICFES a tra conexión remota segura bajo VPN.

NO CONFORMIDADES

DESCRIPCION DE LA NO CONFORMIDAD
1. Herramientas Plan View y Mercurio no cumplen con los lineamientos de seguridad en cuanto a longitud mínima de caracteres para la construcción de la contraseña de acuerdo con lo definido por la política de acceso (mínimo 10).
2. El sistema de información o módulo para el acceso y control de información de inventario y activos fijos no exige el cambio de la contraseña con periodicidad definida.
3. Exposición de información datos privados en sistema APEX a usuarios no autorizados

NO CONFORMIDADES RECURRENTES IDENTIFICADOS DURANTE AUDITORÍA AÑO 2021

1. Usuarios que pre-almacenan o predeterminan contraseñas para acceso a sistema de información mercurio.
2. No se evidenció el total diligenciamiento de la información de gestión de la capacidad de los componentes ERP, PLEXI y Saber 311, información que permita la toma de decisiones.
3. Accesos a sitios en internet que no se encuentran permitidos por política interna, entre ellos sitios para almacenamiento gratuito de información en nubes públicas DROPBOX, ICLOUD, MEGA, también acceso a NETFLIX.
4. Incumplimiento de la política de escritorio y pantalla limpios, dado que se identificaron equipos de cómputo de usuarios con alojamiento o exposición de información y accesos directos a información desde la carpeta “escritorio” de sus equipos.
5. No se identifica evidencia de los resultados de las pruebas de restauración de información de respaldo, software e imágenes del sistema, que permitan establecer el nivel de funcionalidad de los medios en los cuales se almacena la información.
6. No se ha realizado la ejecución de los análisis de vulnerabilidades técnicas de activos de la plataforma tecnológica, redes y comunicaciones para los años 2019, 2020 como tampoco para el año 2021, que permita evaluar la exposición de Icfes con respecto a potenciales vulnerabilidades, de esta manera, se tomen las medidas correspondientes para remediar y mantener un nivel de riesgo bajo.

7. El sitio web de Icfes www.interactivo.icfes.gov.co se registra como sitio no seguro (desde navegación externa), en cuanto a que registra certificado digital no válido, por tanto, se podrían presentar ataques de accesos no autorizados y/o interrupción del servicio de información.
8. Aunque el proceso de Gestión Tecnológica y de Información ha definido la estrategia de DRP (Disaster Recovery Plan) con la identificación de valores para RTO (Recovery Time Objective) y RPO (Recovery Point Objective), no se han realizado las pruebas de recuperación de plataforma tecnológica y servicios, de modo tal, permitan identificar su grado de funcionalidad y adherencia.

OPORTUNIDADES DE MEJORA

1. Formalizar el esquema de control y evaluación de actividades dentro del plan de seguridad y privacidad de información.
2. Identificar los medios de evaluación de cada uno de los planes que son definidos para el logro de los objetivos de SGSI.
3. Incluir en el sistema de gestión documental la declaración de aplicabilidad, donde se asigne código al documento, fecha de aprobación, aprobador, al igual que el control sobre el contenido y su versionamiento.
4. Incluir el riesgo asociado el no tratamiento y protección de datos personales para el proceso de divulgación y comunicaciones.
5. Realizar el match entre las lecciones aprendidas de incidentes de seguridad de la información y aquellas de la gestión de innovación y conocimiento.
6. Considerar la disgregación de los activos de información en el inventario de Gestión de Tecnología a Información, de modo tal se identifique la critidad de cada uno de ellos, de igual manera se identifique valoración de riesgos de manera individual.
7. Fortalecer los requisitos de seguridad de la información en cuanto a la módulo de seguridad de usuarios, condifuración de usuarios, contraseñas, parametrización, reduciendo el tiempo de expiración de contraseña a 30 días ó máximo 45 días; además reducir a 3 los intentos no válidos de contraseña.
8. Revisar e incluir como práctica de organización el el modelo de OWASP (Opern Web Application Security Project), de manera aporte y agregue valor a la calidad y seguridad de la información sobre los propósitos de desarrollo de software.
9. Realizar actividades de capacitación y socialización de los lineamientos de desarrollo seguro para los desarrolladores, de modo tal sean ellos quienes apliquen o implementen las buenas prácticas en su diario desarrollo de software.
10. Evitar el uso firmas digitalizadas pero si, certficados de firmas, de modo tal se eviten usos no autorizados.
11. Incluir en los inventarios de activos de información aquellos servicios contratados a terceros, de manera tal se realice su valoración en cuanto a disponibilidad y/o integridad de estos ejemplo (Avance – proveedor de actualización de normograma).
12. Definir y asignar la responsablidad para desarrollar las actividades tendientes a definir e implementar un plan de continuidad de continuidad de negocio.

13. Identificar los costos de impactos de imagen, económicos, operativos y de recuperación posterior a la atención y solución de los incidentes de seguridad de la información.
14. Fortalecer los lineamentos de control de configuración de seguridad en equipos de cómputo de terceros que son de uso al interior de la Entidad.
15. Aunque se ha identificado y definido estrategias de continuidad de negocio se recomienda identificar la criticidad de cada uno de los procesos de negocio, en la medida que se identifique la estrategia necesaria para su recuperación ente situaciones que conlleven a su interrupción.

SEGUIMIENTO A PLANES DE MEJORAMIENTO

Evaluación planes de mejoramiento sobre hallazgos de auditorías previas

Descripción	Total
Número total de hallazgos presentados para evaluación en la auditoría	71
Número total de hallazgos evaluados y en estado cumplimiento total para su cierre	60
Número total hallazgos que posterior a evaluación de la auditoría, se establece que no pueden ser cerrados bajo el entendimiento que, existen planes de acción, aún proceso de ejecución.	11

NOTA: Los detalles de los resultados de evaluación y concepto de auditoría para el cierre de los hallazgos de auditoría previas y otros incluidos en informes previos, se adjunta al presente informe en documento formato Excel.

CONCLUSIONES

Bajo en entendimiento de los objetivos de la auditoría, se concluye que:

- El sistema de gestión viene de buena manera evidenciando avance en cuanto a la adopción e implementación de acciones en cumplimiento de los requisitos y controles de la norma ISO/IEC 27001:2013.
- Se denota el alto compromiso y apropiación de seguridad de la información por parte de los líderes de procesos de la entidad y sus equipos de trabajo.
- Adecuada identificación de información de activos de información y de la valoración de los riesgos de seguridad de la información.
- El SGSI es adecuado en cuanto a que la implementación de prácticas aporta para el cumplimiento de los objetivos del sistema de gestión.
- Es conveniente dado a que demuestra el cumplimiento y apoyo a la entidad y el apoyo para el logro de los objetivos estratégicos de esta, al igual que, a todos los requisitos aplicables.
- El SGSI se determina eficaz en la medida que, aunque se han presentado incidentes de seguridad de información, estos no han generado alto impacto y han sido atendidos con oportunidad en términos de control o reducción de los impactos de confidencialidad, integridad y disponibilidad de los activos de información.
- Icfes demuestra la capacidad de atender las necesidades de protección de la información como requisito interno de la Entidad, dar respuesta a las necesidades y expectativas de las partes interesadas.

El ICFES ha evidenciado para la auditoría en año 2021 un importante nivel de mejora y avance en cuanto al cumplimiento de requisitos y controles de seguridad de a información presentado por la norma ISO/IEC 27001:2013, por tanto, esfuerzos adicionales, pondrán a la Entidad en el camino a lograr obtener el certificado internacional como gestores de seguridad de la información otorgada por entidad certificadora.

RECOMENDACIONES

Tener en cuenta los escenarios de oportunidad de mejora propuesta identificados en el presente informe y aplicar planes de acción en atención de las No Conformidades, de manera tal, fortalezca los propósitos y enfoque de mejora del sistema de gestión de seguridad de la información en general.

Para los propósitos de lograr una certificación internacional en ISO/IEC 27001:2013 se deberá asignar esfuerzos con prioridad para continuar y finalizar la implementación de controles relevantes tales como:

- Aplicación de BIA (Business Impact Analysis) para cada uno de los procesos de negocio, de esta manera, el proceso de Gestión de Tecnología e Información definirá el soporte tecnológico de contingencia para satisfacer dichas necesidades de continuidad de procesos.
- Planeación, implementación y pruebas de plan de continuidad de negocio con la vinculación de controles de seguridad de la información en la continuidad de negocio.
- Evaluación de vulnerabilidades técnicas.

EQUIPO AUDITOR

Auditor Líder:	OSCAR FERNANDO RAMOS BENAVIDES	**Cargo:**	AUDITOR INTERNO
Auditores:	N/A	**Cargo:**	N/A