CONTENIDO

1. OBJETIVO

Evaluar la eficacia, eficiencia y cumplimiento normativo del diseño y ejecución de los controles del proceso de Tecnologías de la información y las Comunicaciones del Instituto Distrital de Gestión del Riesgo y Cambio Climático.

2. ALCANCE

Incluye la verificación de la gestión de riesgos de tecnología de la información y seguridad de la información, así como la ejecución de los controles asociados a los procesos y procedimientos de la Oficina de tecnologías de la Información y las Comunicaciones del IDIGER.

3. DURACIÓN DE LA AUDITORÍA

De 06 de septiembre a 5 de diciembre de 2022

4. CRITERIOS

- Ley 1712 de 2014 o de Transparencia y del Derecho de Acceso
- Resolución MinTIC 1519 del 2020 Directrices de accesibilidad web
- Plan de seguridad y privacidad de la información
- Norma técnica Colombiana NTC/IOS 27001:2013 Sistemas de Gestión de Seguridad de la Información (SGSI)
- Guía de implementación de la política seguridad digital
- Decreto Único Reglamentario 1078 de 2015
- Decreto 1008 de 2018
- Resolución 500 Anexo 1 Nuevo MSPI
- Modelo de Seguridad y Privacidad de la Información (MSPI)
- Norma NTC5854 y Demás normatividad asociada con la Política y Manual de Gobierno Digital identificadas en el transcurso de la auditoría.
- página web, contenidos, datos abiertos, seguridad, confiabilidad e integridad de la información, normas vigentes para accesibilidad WEB, procedimientos del proceso
- PETI.
- y Demás normatividad asociada al alcance

5. ACTIVIDADES DESARROLLADAS

5.1. CONOCIMIENTO DE LA UNIDAD AUDITABLE

El Decreto 648 de 2017 redefinió los roles sobre los cuales la Oficinas o Unidades de Control Interno desarrollaran su labor: 1) "Evaluación de la Gestión del Riesgo" y 2) "Evaluación y Seguimiento"; para cumplir con los roles referidos, en el ejercicio de Auditoría se deben incluir lineamientos que permitan:

i. Conocimiento de la Unidad Auditable
ii. Identificar actividades críticas en la unidad auditable y sus puntos de control.
iii. Asociar estas actividades críticas con los riesgos del proceso y los controles implementados
iv. Validar si estos controles mitigan los riesgos identificados.
v. Efectuar pruebas para verificar que los controles están operando.

El desarrollo de las actividades da respuesta al objetivo general de la presente Auditoría: Evaluar la eficacia, eficiencia y cumplimiento normativo del diseño y ejecución de los controles para la implementación de la Política y manual de Gobierno Digital, así como los tres habilitadores transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, con enfoque de auditoría basados en riesgos".

Con base en lo anterior, el equipo auditor utilizó una serie de instrumentos para auditar los procedimientos asociados al alcance de la auditoría como se presenta a continuación:

5.1.1 ENTREVISTAS

Se realizaron 8 entrevistas a los dueños de los procesos con el fin de verificar e identificar los controles identificados en los procedimientos que conforman el proceso de Tecnologías de la Información y las Comunicaciones:

PROCEDIMIENTO	ENTREVISTADO
TC-PD-15 Atención mesa de servicios	Iván Bautista Combita
Entrevista - Seguridad de la Información - Se01	Carmenza González
TICS-PD-09 Mantenimiento de redes de monitoreo	Jorge Luis Vargas
Entrevista - Seguridad de la Información - Se01	Andrés Daza
TICS-PD-12 Ingeniería de Software	Luis Fernando Sánchez
TICS-PD-13 Administración de servicios de Información	Jesús Alfredo Sanabria Mejía
TICS-PD-07 Administración de Infraestructura	Jon Jairo García

Tecnológica	
TICS-PD-13 Administración de servicios de Información	Jesús Alfredo Sanabria Mejía

5.1.2 SOLICITUD DE INFORMACIÓN

1. Solicitud de información con número de radicado 2022IE3036 del 26072022, dirigida a la Oficina TICS.
2. Solicitud de información con número de radicado 2022IE3234 del 09082022, dirigida a la Oficina TICS.
3. Solicitud de información con número de radicado 2022IE3586 del 02092022, dirigida a Oficina asesora de jurídica.

5.1.3 MUESTRA DE USUARIOS BASE DIRECTORIO ACTIVO

Se tomó una muestra no estadística aleatoria de 16 formatos de usuarios activos e inactivos extraídos de los 400 Formatos en Físico denominados creación del usuario TC-FT-31 con el fin de comparar la información contenida en los formatos vs la información de la base de datos del directorio activo de la entidad:

ID	NOMBRE DEL ACTIVO	USUARIO ACTIVO
1	ANDRES AUGUSTO ROJAS ARDILA	SI
2	ERNEY BELEÑO FLOREZ	S
3	LAURA ANGELA GONZALEZ ORTIZ	SI
4	OSCAR EDUARDO ROMERO	SI
5	DIEGO ALEXANDER BELTRAN MORENO	SI
6	GLORIA INES SANCHEZ	SI
7	DELIA PATRICIA ZAPATA YEPES	NO
8	JOSE DEMETRIO BARBOSA	NO
9	ANDRES AUGUSTO ROJAS ARDILA	NO
10	ANDREY MAURICIO LOPEZ PIÑEROS	NO
11	LAURA ANGELA GONZALEZ ORTIZ	NO
12	DIEGO ALEXANDER	NO

ID	NOMBRE DEL ACTIVO	USUARIO ACTIVO
	BELTRAN MORENO	
13	DANIEL RICARDO OLMOS MUÑOZ	NO
14	PILAR BELTRAN MORA	NO
15	CAMILA TORRES HERNANDEZ	NO
16	KAREN ANDREA VILLAREAL	NO

5.2 IDENTIFICACIÓN DE RIESGOS Y CONTROLES

En esta etapa de acuerdo con el Marco Internacional para la Práctica Profesional de la Auditoría Interna se establecen aquellos riesgos más relevantes, para la evaluación de sus respectivos controles en el alcance de la auditoría.

Entiéndase riesgo como posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos, es decir, una situación potencial que puede afectar el cumplimiento de lo dispuesto estratégica u operativamente por la entidad.

Esta fase es requerida para identificar posteriormente los controles desarrollados por la entidad para mitigar la materialización de estos riesgos.

5.3 PRUEBAS DE RECORRIDO

Conforme al procedimiento de auditoria interna se realizó un conjunto de técnicas o procedimientos para recopilar y evaluar la información en el proceso de auditoría, para obtener evidencia suficiente y objetiva que sustente los resultados de la auditoria, y se diligenciaron los papeles de trabajo que sustentan las pruebas de recorrido.

5.4 RESULTADOS DE LAS PRUEBAS DE RECORRIDO Y VALORACIÓN DE CONTROLES

En el marco del alcance y riesgos identificados, se evidenciaron controles clave para diseñar y efectuar las pruebas de auditoría y recorrido para el proceso auditado, las cuales se presentan a continuación:

5.4.1 Prueba de Auditoría: Verificar la elaboración del Inventario de Activos de Información, actualización, publicación de acuerdo a la Guía para la Gestión y

Clasificación de Activos de Información de la política de gobierno digital.

Frente al riesgo identificado por el proceso Tecnologías de la Información y las Comunicaciones en el Mapa de Riesgos Institucional relacionado con: "*Posibilidad de afectación económica o presupuestal, por debilidades en la revisión de los productos entregados por los contratistas de prestación de servicios, debido a la falta de lineamientos y herramientas institucionalizados para una adecuada trasferencia de conocimiento*", se realizó la presente prueba de auditoría:

El equipo auditor verificó la elaboración y publicación del Inventario de Activos de Información 2022 arrojando los siguientes resultados:

CONFORMIDAD 1

Elaboración y publicación del Inventario de Activos de Información 2022 en la página web de la entidad, dando cumplimiento a a la Guía para la Gestión y Clasificación de Activos de Información de la política de gobierno digital.

REGISTRO DE ACTIVOS DE INFORMACIÓN: Corresponde al inventario de la información pública del Idiger que Incluye la información que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico o almacenada en equipos de cómputo, incluyendo datos contenidos en registros, archivos, bases de datos, videos e imágenes. Se encontro publicado en la página en el siguiente enlace **Activos de información.**

CONDICIÓN: Se verificó la elaboración y publicación del Inventario de Activos de Información mediante solicitud de informacion 2022IE3036 del 26072022, y en la página web de la entidad.

CRITERIO: Ley 1712 de 2014 Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, que regula el derecho de acceso a la información pública, los procedimientos para el ejercicio, la garantía del derecho y las excepciones a la publicidad de información, Articulo 11. información mínima obligatoria respecto a servicios, procedimientos y funcionamiento del sujeto obligado. Todo sujeto obligado deberá publicar la siguiente información mínima obligatoria de manera proactiva: j) Un registro de publicaciones que contenga los documentos publicados de conformidad con la presente ley y automáticamente disponibles, así como un Registro de Activos de Información.

CAUSA: La causa obedece a que los controles identificados por el equipo auditor son efectivos y su implementación por parte de la Oficina Tecnologías de la Información y las Comunicaciones.

CONSECUENCIA: Lo que genera esta situación es que evita la materialización del riesgo e incumplimientos que generen hallazgos por parte de los entes externos según la Ley 1712 de 2014 de Transparencia y del Derecho de Acceso a la Información.

5.4.2 Prueba de auditoría: verificación de la existencia de Políticas de Seguridad de la información.

Frente al riesgo identificado por el proceso Tecnologías de la Información y las Comunicaciones en el Mapa de Riesgos Institucional relacionado con: "*Posibilidad de afectación económica, reputacional y de perdida de integridad por la instalación de software malicioso en los equipos de computo personales, cuando se realiza trabajo en casa o teletrabajo, debido al desconocimiento por parte de los procesos, de los riesgos de ciber seguridad.*", se realizó la presente prueba de auditoría al siguiente control documentado en la norma ISO 27001 objetivo de control 4 la Organización y su contexto:

CICLO DEL PROCESO	REQUISITO/ CONTROL A VERIFICAR	DESCRIPCIÓN	RESULTADO		
			cumplimiento	no conformidad	observación
PLANEAR	4	Contexto de la organización	x		
	4.1	Entendiendo la entidad y su contexto	X		
	4.2	Entendiendo las necesidades y expectativas de las partes interesadas	X		
	4.3	Determinando el alcance del sistema de gestión de seguridad	X		
	4.4	Sistema de Gestión de la Seguridad de la Información.	X		

CONFORMIDAD 2

Elaboración y publicación de la política de Seguridad de la Información del IDIGER.

CONDICIÓN: Se verificó la elaboración y publicación en la página web de la

entidad de la Política Seguridad de la Información del IDIGER.

CRITERIO: Cumplimiento norma ISO 27001 objetivo de control 4 la Organización y su contexto.

CAUSA: El proceso de TICS cuenta con políticas establecidas para mitigar el riesgo de "*Posibilidad de afectación económica, reputaciones y de perdida de integridad por la instalación de software malicioso en los equipos de cómputo personales, cuando se realiza trabajo en casa o teletrabajo, debido al desconocimiento por parte de los procesos, de los riesgos de ciber seguridad.*

CONSECUENCIA: El IDIGER tiene determinado el contexto al que se enfrenta el sector con el fin emprender acciones y genera lineamientos para la gestión del riesgo de desastres y la adaptación al cambio climático, pieza fundamental para mitigar los aspectos externos e internos que pueden afectar el adecuado direccionamiento del sector y poner en riesgo el cumplimiento de los objetivos estratégicos, así como el logro del propósito superior planteado para la el distrito. Es así como el IDIGER considera los aspectos fundamentales que deben ser tenidos en cuenta en el sector y en la operación del Sistema Integrado de Gestión - SIG, en el marco de lo planteado en el Modelo Integrado de Planeación y Gestión – MIPG; específicamente, con el modelo referencial del sistema de gestión de seguridad de la información.

El IDIGER a través de la resolución 214 del 23 de abril de 2019, definió que el SGSI recoge los lineamientos del Ministerio de las TIC para el desarrollo de seguridad digital de MIPG, buscando gestionar adecuadamente la seguridad y privacidad de los activos de información, en el marco de la estrategia de Gobierno Digital, establecido en el Decreto 1078 de 2015.

5.4.3 Prueba de auditoria: Verificación de Usuarios activos en el Directorio Activo vs Usuarios Diligenciados en Formato para la creación del usuario TC-FT-31

Frente al riesgo identificado por el proceso Tecnologías de la Información y las Comunicaciones en el Mapa de Riesgos Institucional relacionado con: "*Posibilidad de Afectación reputacional por Acceso no autorizado a los Sistemas de Información Debido a posibles ataques ciberneticos Y/o Falta de seguimiento efectivo a la cancelación de los usuarios que ya no laboran en la entidad*", se verifico la ejecución de los siguientes controles establecidos en el procedimiento TICS-PD-07 Administración de Infraestructura Tecnológica.

- "Formato para la creación del usuario TC-FT-31"
- "Formato "Expedición de certificado"
- "Formato "Administración de Backups y recuperación de datos"

El equipo auditor verificó la eficacia y eficiencia de la implementación de los controles arrojando los siguientes resultados:

Formato	Observaciones
Formato para la creación del usuario TC-FT-31"	El Formato TC-FT-31 no es muy entendible y posee deficiencias en los permisos hacia la NAS a nivel de Escritura, Lectura y Ejecución. Los formatos TC-FT-31 no están en digitalizados.
Formato "Expedición de certificado"	Este formato no se está siendo utilizado en el procedimiento.
Formato "Administración de Backups y recuperación de datos"	Este formato no se está siendo utilizado en el procedimiento.
Formato "Actualización "Hoja de vida de servidores."	Este formato se está utilizando de manera parcial ya que no existen registros de mantenimiento preventivos para la vigencia 2022.

Se comparó la base de datos del directorio activo vs los formatos físicos para la creación del usuario TC-FT-31", la oficina de TICS remitió 400 formatos de los cuales se realizó una muestra aleatoria no estadística de 16 formatos en el periodo comprendido entre el 1 de enero del 2022 al 31 de agosto de 2022.

De los 16 usuarios escogidos como muestra aleatoria 6 cumplieron y 10 no cumplieron con la desactivación del acceso como se evidencia a continuación:

NOMBRE DEL ACTIVO	FUERON ACTIVADOS LOS SERVICIOS SOLICITADOS EN EL FORMATO	FUERON DESACTIVADOS EL ACCESO A LOS SERVICIOS	CONTRA SEÑA/ SEGURO	OBSERVACIONES
ANDRES AUGUSTO ROJAS ARDILA	SI	SI	SI	
ERNEY BELEÑO FLOREZ	SI	SI	SI	
LAURA ANGELA GONZALEZ ORTIZ	SI	SI	SI	
OSCAR EDUARDO ROMERO	SI	SI	SI	
DIEGO ALEXANDER	SI	SI	SI	

BELTRAN MORENO				
GLORIA INES SANCHEZ	SI	SI	SI	
DELIA PATRICIA ZAPATA YEPES	PARCIALMENTE	NO	NO	El formato no especifica que permisos deberían aplicarle
JOSE DEMETRIO BARBOSA	PARCIALMENTE	NO	NO	El formato no especifica que permisos deberían aplicarle
ANDRES AUGUSTO ROJAS ARDILA	PARCIALMENTE	NO	NO	El formato no especifica que permisos deberían aplicarle
ANDREY MAURICIO LOPEZ PIÑEROS	PARCIALMENTE	NO	NO	El formato no especifica que permisos deberían aplicarle
LAURA ANGELA GONZALEZ ORTIZ	PARCIALMENTE	NO	NO	El formato no especifica que permisos deberían aplicarle
DIEGO ALEXANDER BELTRAN MORENO	PARCIALMENTE	NO	NO	El formato no especifica que permisos deberían aplicarle
DANIEL RICARDO OLMOS MUÑOZ	PARCIALMENTE	NO	NO	El formato no especifica que permisos deberían aplicarle
PILAR BELTRAN MORA	PARCIALMENTE	NO	NO	El formato no especifica que permisos deberían aplicarle
CAMILA TORRES HERNANDEZ	PARCIALMENTE	NO	NO	El formato no especifica que permisos deberían aplicarle
KAREN ANDREA VILLAREAL	PARCIALMENTE	NO	NO	El formato no especifica que permisos deberían aplicarle

5.4.4 Prueba de auditoria: Verificar el Formato "Expedición de certificado vs verificación Directorio Activo

Frente al riesgo identificado por el proceso Tecnologías de la Información y las Comunicaciones en el Mapa de Riesgos Institucional relacionado con: "Posibilidad de afectación económica, reputacional y perdida de la confidencialidad de la información almacenada en las carpetas compartidas de cada proceso, debido a las debilidades en la solicitud oportuna para la actualización de los permisos de la carpetas compartidas.", se realizó la presente prueba de auditoría al siguiente control documentado:

Para realizar la prueba recorrido se escogieron 16 usuarios como muestra aleatoria evidenciando que para el periodo de evaluación de la auditoria correspondiente al 01 de enero al 31 de agosto de 2022 el 100% de la muestra no gestiona los controles del procedimiento TICS-PD-07 Administración de Infraestructura Tecnológica, correspondientes a los formatos de la actividad No. 2 Formato "Expedición de certificado", actividad 6.4 Formato "Administración de Backups y recuperación de datos Procedimiento TICS-PD-07 Administración de Infraestructura Tecnológica.

NOMBRE DEL ACTIVO	POSEE EXPEDICION DE CERTIFICADO	OBSERVACIONES
ANDRES AUGUSTO ROJAS ARDILA	NO	Se encuentra aun activo en el directorio activo
ERNEY BELEÑO FLOREZ	NO	
LAURA ANGELA GONZALEZ ORTIZ	NO	Se encuentra aun activo en el directorio activo
OSCAR EDUARDO ROMERO	NO	
DIEGO ALEXANDER BELTRAN MORENO	NO	Se encuentra el usuario activo al momento de la revision
GLORIA INES SANCHEZ	NO	
DELIA PATRICIA ZAPATA YEPES	NO	
JOSE DEMETRIO BARBOSA	NO	
ANDRES AUGUSTO ROJAS ARDILA	NO	
ANDREY MAURICIO LOPEZ PIÑEROS	NO	Se encuentra aún activo en el directorio activo
LAURA ANGELA GONZALEZ ORTIZ	NO	
DIEGO ALEXANDER BELTRAN MORENO	NO	
DANIEL RICARDO OLMOS MUÑOZ	NO	
PILAR BELTRAN MORA	NO	
CAMILA TORRES HERNANDEZ	NO	Se encuentra aun activo en el directorio activo
KAREN ANDREA VILLAREAL	NO	

NOMBRE DEL ACTIVO	USUARIO ACTIVO	POSEE FORMATO DE BACKUPS	TIEMPOS DE RETENCIÖN
ANDRES AUGUSTO ROJAS ARDILA	SI	NO	NO
ERNEY BELEÑO FLOREZ	S	NO	NO
LAURA ANGELA GONZALEZ ORTIZ	SI	NO	NO
OSCAR EDUARDO ROMERO	SI	NO	NO
DIEGO ALEXANDER BELTRAN MORENO	SI	NO	NO
GLORIA INES SANCHEZ	SI	NO	NO
DELIA PATRICIA ZAPATA YEPES	NO	NO	NO
JOSE DEMETRIO BARBOSA	NO	NO	NO
ANDRES AUGUSTO ROJAS ARDILA	NO	NO	NO
ANDREY MAURICIO LOPEZ PIÑEROS	NO	NO	NO
LAURA ANGELA GONZALEZ ORTIZ	NO	NO	NO
DIEGO ALEXANDER BELTRAN MORENO	NO	NO	NO
DANIEL RICARDO OLMOS MUÑOZ	NO	NO	NO
PILAR BELTRAN MORA	NO	NO	NO
CAMILA TORRES HERNANDEZ	NO	NO	NO
KAREN ANDREA VILLAREAL	NO	NO	NO

OBSERVACIÓN 1

Cumplimiento parcial al Procedimiento TICS-PD-07 Administración de Infraestructura Tecnológica para desactivar y/o anular un usuario y lograr mitigar el riesgo. Actividad 2, Formato "Expedición de certificado" y ACTIVIDAD 6.4 Formato "Administración de Backups y recuperación de datos

CONDICIÓN: Se encontraron deficiencias en la desactivación y/o anulación de registro de usuarios que ya no se encuentran vinculados A la entidad.

CRITERIO: actividad 2, Formato "Expedición de certificado" y 6.4 del Procedimiento Formato "Administración de Backups y recuperación de datos Procedimiento TICS-PD-07 Administración de Infraestructura Tecnológica generando deficiencia en el objetivo de control A.9.2.1 Registro de usuarios y anulación de registro de la norma

ISO27001.

CAUSA: Ausencia de Control en la desactivación y/o anulación de registro de usuarios de la entidad por la ausencia del registro de Formato "Expedición de certificado" y ACTIVIDAD 6.4 Formato "Administración de Backups y recuperación de datos

Ausencia de Control de Copias de Respaldo de la información, software y sistemas de la entidad.

CONSECUENCIA: Posible materialización del riesgo "Posibilidad de afectación económica, reputacional y perdida de la confidencialidad de la información almacenada en las carpetas compartidas de cada proceso, debido a las debilidades en la solicitud oportuna para la actualización de los permisos de la carpetas compartidas", por Accesos no autorizados a sistemas de información que puedan afectar la disponibilidad, confidencialidad e integridad.

5.4.5 Prueba de auditoria: Verificar el cumplimiento de la GUÍA MARCO REFERENCIA PARA LA GESTIÓN DEL RIESGO DEL INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO

En este contexto se analizaron las siguientes fuentes de identificación de riesgos, aplicables a este ejercicio:

● DE-FT-13 Mapa de Riesgos Institucional, riesgos identificados por los responsables de los procesos.

Análisis de equipo auditor frente a los objetivos los procesos y procedimientos auditadosrelacionado con el alcance de la auditoría. Como resultado de este análisis seidentificaron y compilaron los riesgos y controles a revisar en la auditoría, en el formato EI- FT-55-PROGRAMA ESPECÍFICO DE TRABAJO DE AUDITORÍA del 15 septiembre de 2022.

Teniendo en cuenta el ejercicio de identificación de riesgos efectuado por el equipo auditor, se evaluó la gestión de controles de 10 riesgos relacionados con el objetivo de la auditoría, identificados por el responsable del proceso de Tecnologías de la Información y las Comunicaciones.

ID	RIESGOS	CONTROLES MAPA DE RIESGOS
1	Posibilidad de Afectación reputacional por Acceso no autorizado a los Sistemas de Información Debido a posibles ataques cibernéticos Y/o Falta de seguimiento efectivo a la cancelación de los usuarios que ya no laboran en la entidad.	1. Formato "Usuarios en tecnología y SI", se diligencia formato para tener claro fecha de inicio y fecha de finalización de contrato. 2. Formato "Expedición de certificado". 3. Formato "Administración de Backups y recuperación de datos". 4. Formato Actualización "Hoja de vida de servidores.".
2	Posibilidad de afectación económica, reputacional y perdida de la confidencialidad de la información almacenada en las carpetas compartidas de cada proceso, debido a las debilidades en la solicitud oportuna para la actualización de los permisos de las carpetas compartidas.	El subdirector, Jefe o personal delegado Solicita a través de la mesa de servicio y cuando sea necesario. el acceso a las carpetas compartidas, para el personal que considere pertinente.
3	Posibilidad de afectación económica y/o reputacional y perdida de disponibilidad de los servicios de TI por el Incumplimiento de buenas practicas en el manejo de usuarios de altos privilegios para administrar la infraestructura y servicios de TI debido a la ausencia de lineamientos para la adecuada gestión de los usuarios de altos privilegios.	**SIN CONTROL IDENTIFICADO POR EL PROCESO TICS**
4	Posibilidad de afectación económica o presupuestal, por la alta rotación de personal de planta, debido a la falta de lineamientos y herramientas institucionalizados para una adecuada transferencia de conocimiento.	El Jefe Inmediato verifica el acta de entrega de puesto de trabajo con sus respectivos soportes, remitida por el funcionario al momento de una desvinculación o traslado laboral.

ID	RIESGOS	CONTROLES MAPA DE RIESGOS
		El funcionario realiza el informe o charla en la que transfiere el conocimiento adquirido, producto de una capacitación brindada por el IDIGER mediante su Plan Institucional de Capacitación.
5	Posibilidad de afectación económica o presupuestal, por debilidades en la revisión de los productos entregados por los contratistas de prestación de servicios, debido a la falta de lineamientos y herramientas institucionalizados para una adecuada trasferencia de conocimiento.	El Supervisor del contrato verifica el informe de actividades y soportes entregados por el Contratista de prestación de servicios, de manera mensual.
6	Posibilidad de afectación reputacional por falencias en desarrollos y soluciones tecnológicas debido a Falta de control y seguimiento durante el ciclo de vida del sistema de información, No hay personal especializado en pruebas de software, Falta monitoreo automatizado de soluciones, Pruebas de seguridad antes de salir a producción, perdidas de conexión de las bases de datos por falla en la infraestructura tecnológica.	Profesional 12 de desarrollo Tecnológico Seguimiento al cargue de requerimientos desde el área funcional de requerimientos en Gitlab: Software libre de control y gerencia de desarrollos tecnológicos, con respecto a las funcionalidades a ajustar, seguimiento a las labores de los desarrolladores de acuerdo con las necesidades de las áreas, validación de pruebas para paso a producción.
7	Posibilidad de afectación económica y/o reputacional y perdida de disponibilidad por fallas en la prestación de los servicios de TI debido a la inadecuada gestión de cambios en los ambientes productivos de la entidad.	**SIN CONTROL IDENTIFICADO POR EL PROCESO TICS**
8	Posibilidad de afectación reputacional por perdida de disponibilidad del servicio SIRE debido a fallas tecnológicas causando perdidas reputacionales	Profesional especializado 23 administración SIRE Seguimiento al funcionamiento y disponibilidad del Sistema de

ID	RIESGOS	CONTROLES MAPA DE RIESGOS
	debido a Fallas de funcionamiento de servidor, Fallas o intermitencias en la conexión de la base de datos, Fallas en la conectividad.	información, Reinicio del servidor de aplicación.
9	Posibilidad de afectación económica, reputacional y de perdida de integridad por la instalación de software malicioso en los equipos de computo personales, cuando se realiza trabajo en casa o teletrabajo, debido al desconocimiento por parte de los procesos, de los riesgos de ciberseguridad.	**SIN CONTROL IDENTIFICADO POR EL PROCESO TICS**
10	Posibilidad de afectación reputacional por falencias en la operatividad de la infraestructura tecnológica debido a Falta de operatividad de la infraestructura (Servidores, pc, aires acondicionados, UPS,etc) por problemas de obsolescencia tecnológica, software desactualizado o, con fallas o, terminación de vida útil de componentes. Problemas con el fluido eléctrico en términos de falta del mismo, sobrecargas y problemas en la red eléctrica. Falta de conectividad de red o problemas con infraestructura de red de comunicaciones (LAN / WAN)"	Profesional especializado 23 de infra estructura tecnológica, contratistas de redes de conectividad Plan de Actualización tecnológica, elaboración de procesos, adjudicación de contratos y ejecución contractual. Contratista de seguridad de la información Elaboración del Mapa de riesgos Infraestructura Tecnológica

OBSERVACIÓN 2

Cumplimiento parcial de la GUÍA MARCO REFERENCIA PARA LA GESTIÓN DEL RIESGO DEL INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO, numeral 8.2.2 Valoración de controles.

CONDICIÓN: Tras el conocimiento de la unidad auditable se evidencio ausencia de controles asociados a la gestión de los siguientes riesgos institucionales, identificados por el proceso de Tecnologías de la Información y las Comunicaciones:

- Posibilidad de afectación económica y/o reputacional y perdida de disponibilidad de los servicios de TI por el Incumplimiento de buenas prácticas en el manejo de usuarios de altos privilegios para administrar la infraestructura y servicios de TI debido a la ausencia de lineamientos para la adecuada gestión de los usuarios de altos privilegios.
- Posibilidad de afectación económica y/o reputacional y pérdida de disponibilidad por fallas en la prestación de los servicios de TI debido a la inadecuada gestión de cambios en los ambientes productivos de la entidad.
- Posibilidad de afectación económica, reputacional y de perdida de integridad por la instalación de software malicioso en los equipos de cómputo personales, cuando se realiza trabajo en casa o teletrabajo, debido al desconocimiento por parte de los procesos, de los riesgos de ciberseguridad.

CRITERIO: Esta circunstancia desconoce los lineamientos para la valoración de controles contenida en el numeral 8.2.2 de la Guía Marco Referencia para la Gestión del Riesgo del Instituto Distrital de Gestión de Riesgos y Cambio Climático, Código: DE-GU-01, versión 11.

CAUSA: Debilidades por parte de la Oficina TICS en identificar controles que permitan mitigar los riesgos de su proceso.

CONSECUENCIA: Si los riesgos identificado por la Oficina TICS no tienen controles que lo mitiguen existe una alta probabilidad de materialización del riesgo.

5.4.6 Prueba de auditoria: verificación de mantenimiento preventivo y correctivo de los servidores de la entidad.

Frente al riesgo identificado por el proceso Tecnologías de la Información y las Comunicaciones en el Mapa de Riesgos Institucional relacionado con: "*Posibilidad de afectación reputacional por falencias en la operatividad de la infraestructura tecnológica debido a Falta de operatividad de la infraestructura (Servidores, pc, aires acondicionados, UPS,etc) por problemas de obsolescencia tecnológica, software desactualizado o, con fallas o, terminación de vida útil de componentes. Problemas con el fluido eléctrico en términos de falta del mismo, sobrecargas y problemas en la red eléctrica. Falta de conectividad de red o problemas con infraestructura de red de comunicaciones (LAN / WAN)*", se realizó la presente prueba de auditoría al siguiente control documentado:

Para la prueba de auditoria se verifico el mantenimiento de los servidores de la entidad a través del diligenciamiento del formato denominado "Formatos Actualización "Hoja de vida de servidores."

Se solicitaron los Formatos de Actualización "Hoja de vida de servidores", identificados en

la actividad 8.7 del procedimiento TICS-PD-07 Administración de Infraestructura Tecnológica con el fin de verificar el mantenimiento preventivo/y o correctivo que se le están realizando a los equipos para identificar si el control que se encuentra documentado está siendo efectivo y eficaz permitiendo estar al día en actualizaciones de software para prevenir afectación en la disponibilidad, confidencialidad, e integridad de la información que se aloja en la infraestructura que administra la oficina de TICS de la entidad.

Para realizar la prueba recorrido se escogieron 11 servidores como muestra aleatoria en donde el 100% no cumple con el mantenimiento preventivo anual según las buenas prácticas de seguridad contempladas en la norma ISO27001.

EQUIPO / REFERENCIA / MODELO	FECHA DEL MANTENIMIENTO PREVENTIVO Y/O CORRECTIVO	OBSERVACIONES
JICA	27/02/2021	
RHB2	27/2/2021	
LOKI	27/2/2021	
ZYRUMA	27/2/2021	
SRVMON	27/2/2021	
SRVSTORAGE1	27/2/2021	
SRVSTORAGE2	19/9/2018	
JUPITER	27/2/2021	
SIRE	27/2/2021	
COMPELLENT SC200	NO TIENE	
COMPELLENT SC4020	NO TIENE	

INCIDENTES DE SEGURIDAD DE LA APLICACIÓN SIRE

Con el fin de evidenciar la materialización del riesgo de falencias en la operatividad de la infraestructura tecnológica debido a Falta de operatividad de la infraestructura (Servidores, se solicitaron los reportes de incidentes de seguridad de los sistemas de información de la entidad, evidenciando incidentes en la operación debido a desconexión de las bases de datos, saturación de recursos de los servidores, ´problemas de acceso a los sistemas de información

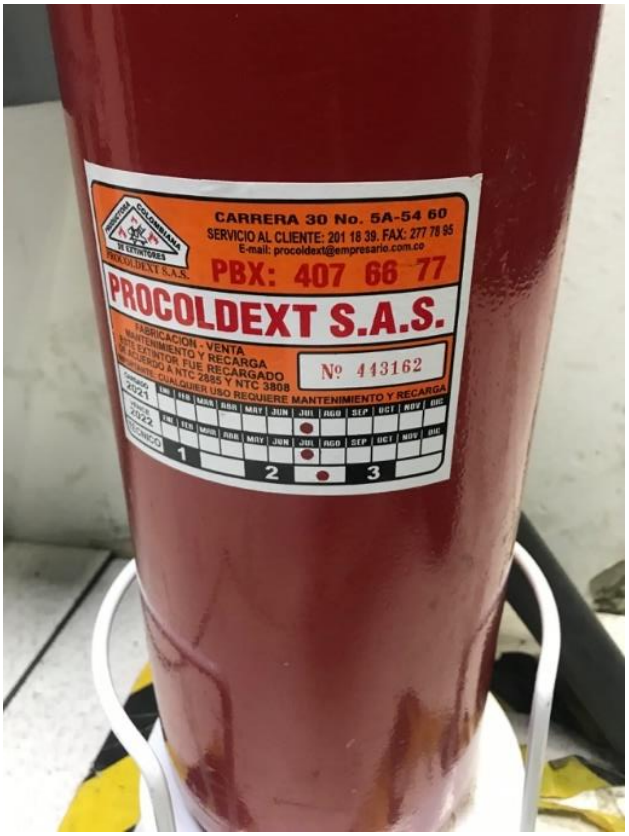
Como evidencia se anexa formato de soporte de incidentes SIRE en formato Excel.

ENERO 2022						
Fecha	Descripcion	Usuario Confirmado	Medio Contacto	Categoria	Origen	Atendido por
3/01/22 8:50	Desde C4 solicitan a modificación de la localidad y barrio del evento sire 5389654 ya que nos aparece como localidad de USME y el evento es en la localidad de SAN CRISTÓBAL, la dirección es la correcta barrio juan rey	C4 CITEL	Correo	Actualización de Datos en BD y Roles	SIRE	JSANABRIA
3/01/22 10:50	Usuarios C4 reportan problemas de acceso a sSIRE, se observa perdida de conexion a base de datos, se reporta y escala el caso	C4 CITEL	WhatsApp	novedades de Acceso	NO RELACIONADA	JSANABRIA
3/01/22 20:14	Usuario C4 CITEL reporta que aplicativo SIRE no funciona, se constata y existe una novedad en el acceso a las redes de IDIGER, se escala el caso y se constata el acceso una vez se reporta solucionado.	C4 CITEL	WhatsApp	Lentitud de Navegación en el Aplicativo	SIRE	MCABRERA
4/01/22 7:27	Usuario C4 CITEL reporta que aplicativo SIRE no funciona, se constata y está caido. Se realiza el reinicio de la instancia y queda funcionando	C4 CITEL	WhatsApp	Lentitud de Navegación en el Aplicativo	SIRE	JGARCIA
5/01/22 9:43	Usuario C4 CITEL reporta que aplicativo SIRE no funciona, se constata y está caido. Se realiza el reinicio de la instancia y queda funcionando	C4 CITEL	WhatsApp	Lentitud de Navegación en el Aplicativo	SIRE	MCABRERA
5/01/22 12:34	Usuario de C$ envia error reportando un fallo en la fecha del formulario, se dan indicaciones para que valide la informacion ingresada o pruebe desde incognito, se evidencia funcionando	C4 CITEL	WhatsApp	Lentitud de Navegación en el Aplicativo	SIRE	MCABRERA
5/01/22 14:25	Usuario C4 CITEL reporta que aplicativo SIRE no funciona, se constata y está caido. Se realiza el reinicio de la instancia y queda funcionando	C4 CITEL	WhatsApp	Lentitud de Navegación en el Aplicativo	SIRE	MCABRERA
8/01/22 15:41	Usuario C4 CITEL reporta que aplicativo SIRE no funciona, se constata y se pide al Usuario limpiar el cache del navegador, se reporta funcionando	C4 CITEL	WhatsApp	Lentitud de Navegación en el Aplicativo	SIRE	MCABRERA
10/01/22 10:59	Usuario C4 CITEL reporta que aplicativo SIRE no funciona, se constata y está caido. Se realiza el reinicio de la instancia y queda funcionando	C4 CITEL	WhatsApp	novedades de Acceso	NO RELACIONADO	JSANABRIA
11/01/22 7:52	Usuario Edwin Edinson Gomez solicita confirmar el usuario de ingreso del ADMINISTRADOR del SURE, se confirma que el usuario requerido es "verificadoridiger" el usuario valida y puede ingresar normalmente	EDWIN EDINSON GOMEZ LOMBANA	Correo / Chat	Novedades de Acceso	NO RELACIONADA	JSANABRIA
12/01/22 12:09	Se da respues a requerimiento de Servicio No 16669 trata de novedades al actualziar el estado de un requerimiento en CORDIS ,el caso es solucionado por Nancy Gomez	BERTHA LUCIA RODRIGUEZ VELASQUEZ	ARANDA	Actualización de Datos en BD y Roles	NO RELACIONADA	JSANABRIA
14/01/22 10:18	Se efectua la regeracion del caso bitacora 5389931, se restaiuran acciones y observaciones y se envia correo para que puedan verificar	DIANA CAROLINA GARZON GALEANO	Correo	Actualización de Datos en BD y Roles	SIRE	JSANABRIA

5.4.7 Prueba de auditoria visita de campo al centro de datos del Instituto Distrital de Gestión del Riesgo y Cambio Climático con el fin de observar, verificar y analizar mediante una prueba de recorrido las fortalezas y deficiencias en temas de gestión de la seguridad de la información

DATACENTER

1. Dispositivos y señales de acceso y seguridad. El DATACENTER cuenta con instrumentos de seguridad de acceso al medio no obstante se evidencio que el extintor que se encuentra dentro del DATACENTER se encuentra vencido con fecha de caducidad de julio de 2022



2. Seguridad de los equipos (Equipos sin anclaje al rack). Se evidencia inadecuada disposición de equipos servidores los cuales se encuentran dispuestos fuera del DATACENTER.

3. Seguridad de los equipos (Aires Acondicionados sin uncionar). Se evidencia que uno de los aires acondicionados del DATANCER está fuera de servicio

-4. Cableado estructurado: El cableado estructurado del DATACENTER no cuenta con los estándares de SEGURIDAD COMO etiquetas en ambos extremos y desorganización y rack de comunicaciones que no cumple con las características de maquillado y organización de cables.

NO CONFORMIDAD 1

Materialización del riesgo Posibilidad de afectación reputacional por falencias en la operatividad de la infraestructura tecnológica debido a Falta de operatividad de la infraestructura (Servidores, pc, aires acondicionados, UPS,etc) por problemas de obsolescencia tecnológica, software desactualizado o, con fallas o, terminación de vida útil de componentes. Problemas con el fluido eléctrico en términos de falta del mismo, sobrecargas y problemas en la red eléctrica. Falta de conectividad de red o problemas con infraestructura de red de comunicaciones".

CONDICIÓN:

Se evidencia falta de mantenimiento preventivo y o correctivo de los servidores a cargo de la oficina TICS para la vigencia de la auditoria 2022 de los equipos de TI.

Se evidencia debilidades en el tratamiento de las medidas técnicas y de seguridad de la infraestructura del DATACETER.

CRITERIO: Ley Estatutaria 1581 DE 2012 Por la cual se dictan disposiciones generales para la protección de datos personales. Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

CAUSA: Ausencia de tratamiento para asegurar controles que ayuden a gestiones y manejar las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;

CONSECUENCIA: materialización del riesgo identificado, como Posibilidad de afectación reputacional por falencias en la operatividad de la infraestructura tecnológica debido a Falta de operatividad de la infraestructura (Servidores, pc, aires acondicionados, UPS,etc) por problemas de obsolescencia tecnológica, software desactualizado o, con fallas o, terminación de vida útil de componentes. Problemas con el fluido eléctrico en términos de falta del mismo, sobrecargas y problemas en la red eléctrica. Falta de conectividad de red o problemas con infraestructura de red de comunicaciones (LAN / WAN)".

5.4.8 Prueba de auditoria: Verificación del estado actual de los documentos que hacen parte del sistema de gestión del proceso de Tecnologías de la Información y las Comunicaciones del IDIGER

El proceso auditor identifico el riesgo correspondiente a posible incumplimiento en la implementación de la política y Manual de gobierno digital por desactualización normativa y falta de controles en los procedimientos asociados al proceso de Tecnologías de la información y las comunicaciones del IDIGER.

Se verificó la información correspondiente a versión, idioma, medios de soporte número de referencia autor y fecha con el fin de determinar el cumplimiento normativo de los procedimientos asociados al proceso TICS, evidenciando que estos no permiten dar cumplimiento a lo establecido en el manual de gobierno digital Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 (Compilado en el Decreto 1078 de

2015, capítulo 1, título 9, parte 2, libro 2)

Lineamiento Guías y estándares Guía 8 Controles de Seguridad y Privacidad de la Información **SIEMPRE se deben mencionar los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001**

Plan Institucional De Seguridad Y Privacidad De La Información 2022: 2.RESULTADOS AUTODIAGNOSTICO Se realiza una actualización al diagnóstico al Modelo de Seguridad y Privacidad de la Información (MSPI) durante el mes de diciembre de 2021, la herramienta contempla los 114 controles de los 14 dominios que componen la **Norma ISO 27001:2013.**

PROCEDIMIENTO	OBSERVACIONES
Desarrollo de Software para la gestión de Información geográfica y alfanumérica en riesgos. ADM-PD-12 Versión 2 10-03-2015 Actualización del Procedimiento por ajuste Institucional	El procedimiento no tiene actividades ni controles ni políticas de operación relacionadas con pruebas unitarias del desarrollo de software establecido en la norma ISO 27001. Objetivo de control A.14.2.8. Se deberían realizar pruebas de funcionalidad durante las etapas del desarrollo Ausencia de actividades de controles de cambios con el fin de contar con criterios de calidad establecido en la norma ISO 27001. Objetivo de control A.12.1.2. Los procesos de cambio pueden conllevar riesgos asociados para la seguridad de la información. Es por ello que la norma nos propone controles para que analicemos los procesos de cambio tanto: Comerciales, Instalaciones o infraestructuras (Equipos y Software), Sistemas de procesamiento de información
Atención Mesa De Servicios TC-PD-15 Versión 1. 24/12/2019 Creación del procedimiento de "Atención mesa de servicios"	El procedimiento no tiene actividades ni controles ni políticas de operación relacionadas con Acuerdos de Niveles de Servicio norma ISO 27001 A.14.2.7, A.15.2.1 **Soporte, mantenimiento y régimen de cobertura** Todo sistema, servicio y equipamiento crítico del centro de datos debe contar con soporte de mantenimiento y recambio de partes o, en su defecto, con un plan acción en caso de falla. Se debe establecer el régimen de cobertura para los servicios críticos de acuerdo a las necesidades de la organización. La administración de infraestructura del centro de datos requiere atención en modalidad 7x24 (o la

PROCEDIMIENTO	OBSERVACIONES
	que mejor se adapte a las necesidades del negocio). **Acuerdos de nivel de servicio** Muchas veces las organizaciones no tienen la capacidad operativa para cubrir este servicio por lo que delegan o comparten la operación del centro de datos a proveedores. Es importante firmar con los proveedores acuerdos de niveles de servicio que pauten el cumplimiento de tiempos de respuesta, estipulados según las necesidades de negocio, así como el aseguramiento de la disponibilidad comprometida de los servicios del centro de datos. **Tiempos de respuesta** También es necesario tener acuerdos que aseguren los tiempos de respuesta para aquellos componentes que por su complejidad no puedan ser redundantes pero que, por su criticidad, su falla pueda provocar disrupción de servicios u otros daños.
Soporte y Mantenimiento ERP, Si Capital ADM-PD-34 Versión 1. 13-01-14 Creación del procedimiento	El procedimiento no tiene actividades ni controles ni políticas de operación relacionadas con ambiente de desarrollo seguro norma ISO 27001 A.14. Adquisición, Desarrollo y mantenimiento del sistema Controles para garantizar que se tienen en cuenta las necesidades de la seguridad de la información en los entornos de desarrollo de sistemas de información.

NO CONFORMIDAD 2

Materialización del riesgo identificado por el proceso auditor correspondiente a "Posible incumplimiento normativo debido a la ausencia de controles y desactualización de los procedimientos que aseguren el cumplimiento de los objetivos estratégicos del proceso de Tecnologías de la información y las comunicaciones del IDIGER."

CONDICION

Se verificó la información correspondiente a versión, idioma, medios de soporte número de referencia autor y fecha con el fin de determinar el cumplimiento normativo de los procedimientos asociados al proceso TICS, evidenciando que estos no permiten dar cumplimiento a lo establecido en el manual de gobierno digital Implementación de la Política de Gobierno Digital Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2)

Lineamiento Guías y estándares Guía 8 Controles de Seguridad y Privacidad de la Información **SIEMPRE se deben mencionar los controles correspondientes al Anexo A de la norma NTC: ISO/IEC 27001**

CRITERIO
Riesgo identificado por el proceso auditor *posible incumplimiento en la implementación de la política y Manual de gobierno digital por desactualización normativa y falta de controles en los procedimientos asociados al proceso de Tecnologías de la información y las comunicaciones del IDIGER.*

CAUSA
Posible ausencia de controles que aseguren el cumplimiento normativo del proceso de Tecnologías de la Información y las Comunicaciones del IDIGER.

CONSECUENCIA
Materialización del riesgo identificado por el proceso auditor correspondiente a posible incumplimiento en la implementación de la política y Manual de gobierno digital por desactualización normativa y falta de controles en los procedimientos asociados al proceso de Tecnologías de la información y las comunicaciones del IDIGER.

6. RESULTADOS

6.1. CONCLUSIÓN GENERAL

Se llevó a cabo el cumplimiento del objetivo general de la auditoría con la respectiva valoración de los riesgos, diseño y ejecución de controles del procedimiento auditado, los resultados del presente informe se refieren a la información remitida por la Subdirección de Tecnologías de la Información y las Comunicaciones no se hacen extensivas a otros soportes o información adicional.

Se observó que el Sistema de Control Interno relacionado con los procedimientos asociados al procedo de Tecnologías de la información y las Comunicaciones, por parte de la primera línea de defensa, es adecuado, sin embargo, es susceptible de mejora y correcciones inmediatas de acuerdo con las situaciones evidenciadas en el presente informe.

A continuación, se resumen las principales fortalezas:

FORTALEZA 1. COMPROMISO CON LA AUDITORIA INTERNA

Se evidenció el compromiso por parte de la oficina TICS en el transcurso de la ejecución de la auditoría.

FORTALEZA 2. COMPROMISO CON EL CONTEXTO DE LA ENTIDAD

El IDIGER tiene determinado el contexto al que se enfrenta la entidad, pieza fundamental para mitigar los aspectos externos e internos que pueden afectar el adecuado direccionamiento del sector y poner en riesgo el cumplimiento de los objetivos estratégicos.

FORTALEZA 3. COMPROMISO CON EL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

El IDIGER a través de la resolución 214 del 23 de abril de 2019, definió que el SGSI recoge los lineamientos del Ministerio de las TIC para el desarrollo de seguridad digital de MIPG, buscando gestionar adecuadamente la seguridad y privacidad de los activos de información, en el marco de la estrategia de Gobierno Digital, establecido en el Decreto 1078 de 2015.

6.2. HALLAZGOS – OBSERVACIONES

TIPO DE HALLAZGO	Página
CUMPLIMIENTO	
5.4.1 Prueba de Auditoría: Verificar la elaboración del Inventario de Activos de Información, actualización, publicación de acuerdo a la Guía para la Gestión y Clasificación de Activos de Información de la política de gobierno digital.	7
CONFORMIDAD 1 **Elaboración y publicación del Inventario de Activos de Información 2022 en la página web de la entidad, dando cumplimiento a la Guía para la Gestión y Clasificación de Activos de Información de la política de gobierno digital.**	
5.4.2. Prueba de auditoría: verificación de la existencia de Políticas de Seguridad de la información.	8
CONFORMIDAD 2 **Elaboración y publicación de la política de Seguridad de la Información del IDIGER**	
OBSERVACIONES	
5.4.3 Prueba de auditoria: Verificación de Usuarios activos en el Directorio Activo vs Usuarios Diligenciados en Formato para la creación del usuario TC-FT-31	9
5.4.4 Prueba de auditoria: Verificar el Formato "Expedición de certificado vs verificación Directorio Activo	12
OBSERVACION 1 **Cumplimiento parcial al Procedimiento TICS-PD-07 Administración de Infraestructura Tecnológica para desactivar y/o anular un usuario y lograr**	

mitigar el riesgo. Actividad 2, Formato "Expedición de certificado" y ACTIVIDAD 6.4 Formato "Administración de Backups y recuperación de datos	
5.4.5 Prueba de auditoria: Verificar el cumplimiento de la GUÍA MARCO REFERENCIA PARA LA GESTIÓN DEL RIESGO DEL INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO	14
OBSERVACION 2 **Cumplimiento parcial de la GUÍA MARCO REFERENCIA PARA LA GESTIÓN DEL RIESGO DEL INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO, numeral 8.2.2 Valoración de controles.**	
NO CONFORMIDAD	
5.4.6 Prueba de auditoria: verificación de mantenimiento preventivo y correctivo de los servidores de la entidad.	18
5.4.7 Prueba de auditoria visita de campo al centro de datos del Instituto Distrital de Gestión del Riesgo y Cambio Climático con el fin de observar, verificar y analizar mediante una prueba de recorrido las fortalezas y deficiencias en temas de gestión de la seguridad de la información.	20
NO CONFORMIDAD 1 **Materialización del riesgo Posibilidad de afectación reputacional por falencias en la operatividad de la infraestructura tecnológica debido a Falta de operatividad de la infraestructura (Servidores, pc, aires acondicionados, UPS,etc) por problemas de obsolescencia tecnológica, software desactualizado o, con fallas o, terminación de vida útil de componentes. Problemas con el fluido eléctrico en términos de falta del mismo, sobrecargas y problemas en la red eléctrica. Falta de conectividad de red o problemas con infraestructura de red de comunicaciones".**	
5.4.8 Prueba de auditoria: Verificación del estado actual de los documentos que hacen parte del sistema de gestión del proceso de Tecnologías de la Información y las Comunicaciones del IDIGER	25
NO CONFORMIDAD 2 **Materialización del riesgo identificado por el proceso auditor correspondiente a "Posible incumplimiento normativo debido a la ausencia de controles y desactualización de los procedimientos que aseguren el cumplimiento de los objetivos estratégicos del proceso de Tecnologías de la información y las comunicaciones del IDIGER."**	

7. RECOMENDACIONES

- De acuerdo con el contexto de la entidad se recomienda a la Oficina de Tecnologías de la información y la comunicación implementar un procedimiento para incidentes de seguridad, con la finalidad de gestionar oportunamente las vulnerabilidades que se generan en los sistemas de la entidad.

- Teniendo en cuenta que la entidad está en proceso de actualizar la NAS se recomienda generar los planos de arquitectura de la red con el fin de establecer una Zona desmilitarizada protegiendo servidores que se encuentran publicados hacia internet.

- Se recomienda diseñar un plan maestro en Seguridad de la Información con el fin verificar la medición de los indicadores que genera cada proceso del Sistema de Gestión de la Seguridad de la Información.

- Teniendo en cuenta que la mayoría de los ataques a la seguridad de la información son causados por la falta de conocimiento, se recomienda formar a los responsables del proceso TICS en seguridad de la información.

- Las cuentas de usuario con privilegios de administrador deberían estar restringidas, solo se debe proveer acceso a las personas que estén autorizadas para este cometido. Si estas cuentas caen en manos de ciber delincuentes podrían causarles graves daños a los sistemas e incluso afectar el funcionamiento de la entidad.

- Establecer y comunicar una política que indique los usos permitidos y no permitidos, y las medidas de seguridad que deben activar o contemplar (mantenimiento, actualización o sincronización) en caso de utilizar dispositivos móviles personales para uso profesional.

- Actualizar los manuales funcionales y de usuarios de la mesa de servicio como Aranda con el fin de generar uso y apropiación dentro de la entidad en la utilización de las herramientas tecnológicas.

- Se recomienda mejorar la efectividad de los controles establecidos y/o diseñar otros, con el propósito de planear una mejora continua en los objetivos de control de la seguridad de la información permitiendo mitigar riesgos residuales de los procedimientos establecidos.

- Gestionar los riesgos identificados por el proceso de Tecnologías de la Información y Comunicaciones en el mapa de riesgos de la entidad e identificar controles monitoreando su ejecución con el fin de mitigar su materialización y por ende el incumplimiento de los objetivos estratégicos del proceso.

Nota: El análisis de este informe, se fundamentó en las evidencias remitidas frente a las solicitudes de información, desarrollo de las pruebas de recorrido y auditoría, información publicada, página WEB del IDIGER, (aquí describir las fuentes) asociada con el alcance de la auditoría y no se hace extensible a otros soportes.

Nombre y firma del del Equipo Auditor:	**Nombre y firma del Jefe de Control Interno:**
 **Jorge Beduit Torres Sanchez** **Contratista**	 **Ana Lucia Bacares Toledo** Jefe Oficina de Control Interno
Fecha: 23/11/2022	**Fecha:** 23/11/2022