

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 1 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

## INFORMACIÓN GENERAL

- **Tipo de auditoría:** Auditoría de Gestión
- **Unidad auditable:** Sistema de Gestión de Seguridad de la Información y Política de Gobierno Digital
- **Líder del proceso / Jefe de dependencia:** Aura Herminda López Salazar, Subdirectora Gestión Corporativa
- **Responsable operativo:** Mary Elizabeth Rojas, Gestión de Sistemas y Tecnología de la información.
- **Objetivo de la auditoría:** Prestar servicios profesionales al Instituto Distrital de Patrimonio Cultural, apoyando en la ejecución de la Auditoría al Modelo de Seguridad y Privacidad de la Información, así como a la política de Gobierno Digital
- **Alcance de la auditoría:** Auditar el cumplimiento del sistema de gestión de la información para las diferentes plataformas tecnológicas del Instituto Distrital de Patrimonio Cultural y la Política de Gobierno Digital, para el periodo 1 de enero a 31 de diciembre de 2023.
- **Criterios de la auditoría:** Los criterios de auditoría, están determinados por la regulación externa e interna descritos a continuación:
  1. Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales"
  2. Decreto 1078 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"
  3. Decreto 1008 de 2018, "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"
  4. Manual de Gobierno Digital – MinTIC.
  5. Guía sobre el tratamiento de datos personales en las entidades estatales – Superintendencia de Industria y Comercio.
  6. Sistema de Gestión de Seguridad de la Información (SGSI).
  7. Sistema de Gestión de la Calidad (SGC).
  8. Norma ISO-27001
  9. Directrices Gobierno Digital
- **Pruebas de auditoría utilizadas:** Inspección, prueba de recorrido y observación
- **Métodos de muestreo:** Guía de tamaño de muestra dado por el IDPC y procesos aleatorios.

## RESPONSABLES

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 2 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

- **Asesor de Control Interno:** Eleana Marcela Páez Urrego
- **Auditor Líder:** José Guillermo Benavides González
- **Equipo auditor:** José Guillermo Benavides González

## RESULTADOS DE LA AUDITORÍA

### Hallazgos

- **Fortalezas / Conformidades / Cumplimientos:**


No.	Descripción Fortaleza / Conformidad / Cumplimiento
<b>Sistema de Gestión de Seguridad de la Información</b>	
1	El nivel de cumplimiento es de <u>79.27%</u> el cual debe ser mejorado con el fin de obtener la certificación de la norma ISO.27001 por parte de una entidad certificadora.
2	Existe un gran compromiso del Área de Tecnología en cumplir con todos los controles que cubre la norma ISO-27001. Durante la Auditoria se pudo evidenciar que los recursos humanos están muy ajustados, pero aun así su desempeño es bueno.
3	Existe un gran compromiso de todas las áreas, y en general de todo el personal de planta y contratistas para cumplir con los controles de Seguridad de la Información, con el fin de lograr los tres objetivos fundamentales de la norma como son: <u>Integridad, confidencialidad y disponibilidad</u>
<b>Política de Gobierno Digital</b>	
4	El nivel de cumplimiento es de <u>70.42%</u> el cual debe ser mejorado con el acompañamiento y asesoría del equipo técnico responsable del programa de Gobierno Digital del Ministerio de Tecnologías de la Información y Comunicaciones de Colombia
5	Existe un gran compromiso del Área de Tecnología en cumplir con todos los controles del programa de Gobierno Digital. Durante la Auditoria se pudo evidenciar que los recursos técnicos, humanos y financieros están muy ajustados, pero aun así su desempeño es bueno.
6	Se evidenció un compromiso de todas las áreas, y en general de todo el personal de planta y contratistas para cumplir con los controles de la Política

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 3 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

No.	Descripción Fortaleza / Conformidad / Cumplimiento
	de Gobierno Digital para prestar más y mejores servicios a la comunidad.

**- Observaciones / Cumplimientos parciales:**

No.	Descripción Observación / Cumplimiento parcial
<b>Sistema de Gestión de Seguridad de la Información</b>	
<b>A6 Organización de la SI</b>	
1	<ol style="list-style-type: none"> <li>1. Protocolos para teletrabajo</li> <li>2. Plan y cronograma para las capacitaciones de concientización para el uso adecuado de los dispositivos móviles (Backup)</li> </ol>
<b>A8-Gestión de activos</b>	
2	Procedimiento de Backup de los medios removibles-Gestión de medios extraíbles.
<b>A9-Control de acceso</b>	
3	<ol style="list-style-type: none"> <li>1. Reglas de contraseñas</li> <li>2. Uso de privilegios en los sistemas de información (derechos de administrador)</li> <li>3. Procedimiento y que controles tienen para restringir el acceso al código fuente.</li> <li>4. Registro de eventos de intentos exitosos y fallidos de los usuarios, en las aplicaciones (LOG)</li> </ol>
<b>A10-Cifrado</b>	
4	Controles y protocolos de cifrado deben ser estar más detallados.
<b>A12-Seguridad de las operaciones</b>	
5	<ol style="list-style-type: none"> <li>1. Registros y logs de auditoría</li> <li>2. Estrategia de retroceso (Rollback) antes de implementar los cambios.</li> <li>3. Política de Control de Cambios</li> <li>4. Análisis de la Gestión de capacidad de procesamiento</li> </ol>
<b>A13-Seguridad de las comunicaciones</b>	
6	Políticas y protocolos de comercio electrónico con terceras partes.
7	<b>A14-Adquisición, desarrollo y mantenimiento del sistema</b>

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 4 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

No.	Descripción Observación / Cumplimiento parcial
	<ol style="list-style-type: none"> <li>1. Protocolos o metodologías de desarrollo de software seguro en la organización.</li> <li>2. Información para las pruebas deben estar seleccionadas, protegidas y gestionadas adecuadamente.</li> <li>3. Procedimiento riguroso para realización de modificaciones en los paquetes de software.</li> <li>4. Procedimiento formal de borrado seguro de los datos de prueba.</li> <li>5. Políticas y protocolos para el manejo de información involucrada en transacciones en línea</li> </ol>
<b>8</b>	<b>A16-Gestión e incidentes de SI</b> <ol style="list-style-type: none"> <li>1. Seguimiento de incidentes de seguridad que implican una acción legal</li> <li>2. Procedimientos internos desarrollados para recolectar y presentar evidencia para propósitos disciplinarios dentro de la organización.</li> </ol>
<b>9</b>	<b>A17-Aspectos de la SI en la gestión de la continuidad de la actividad</b> <ol style="list-style-type: none"> <li>1. Procesos y procedimientos para la continuidad de operaciones en IDPC.</li> <li>2. Responsables de activar el plan de contingencia.</li> </ol>
<b>Política de Gobierno Digital</b>	
<b>10</b>	<b>A7-Ejecución</b> Funciones del área de control interno para el desarrollo de acciones, métodos y procedimientos de control y de gestión del riesgo en la implementación de la política de Gobierno Digital


**- No conformidades / Incumplimientos:**

No.	Descripción No conformidad / Incumplimiento
<b>Sistema de Gestión de Seguridad de la Información</b>	
<b>1</b>	<b>A9-Control de acceso</b> <ol style="list-style-type: none"> <li>1. Perfiles de acceso para los administradores y usuarios con privilegios en los Sistemas Operativos, Base de Datos, Correo y demás SI.</li> <li>2. Pistas de auditoría</li> </ol>
<b>2</b>	<b>A11-Seguridad física y medioambiental</b> Control de activos fuera de las instalaciones de la organización.
<b>3</b>	<b>A12-Seguridad de las operaciones</b>

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 5 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

No.	Descripción No conformidad / Incumplimiento
	Política de Gestión de Cambios
4	<b>A14-Adquisición, desarrollo y mantenimiento del sistema</b> 1. Política de Gestión de Cambios.
5	<b>17-Aspectos de la SI en la gestión de la continuidad de la actividad</b> 1. Falta elaboración del BCP 2. Falta de evidencias de las pruebas del DRP 3. Redundancia suficiente para asegurar la disponibilidad del servicio
<b>Política de Gobierno Digital</b>	
6	<b>A1-Definición Roles</b> No hay líder del Gobierno Digital
7	<b>A3-Priorización Temas</b> No están definidos los perfiles de las personas que están asignadas al equipo de Gobierno Digital.
8	<b>A4-Estudio</b> No se han tomado los cursos y entrenamientos dictados por MinTIC.
9	<b>A7-Ejecución</b> 1. No se recibido ni solicitado la asesoría, acompañamiento ni retroalimentación del MinTIC. 2. No se tiene un concepto técnico sobre la aplicabilidad de los lineamientos de la Política de Gobierno Digital por parte del MinTIC. 3. No Se ha hecho un análisis de riesgo de la implementación de la política de Gobierno Digital
10	<b>A8-Cumplimiento</b> 1. No se ha revisado el estado de implementación del Marco de Referencia de Arquitectura Empresarial. 2. Se ha aplicado el formato de autodiagnóstico disponible en el sitio web del Modelo Integrado de Planeación y Gestión - MIPG7. 3. No se ha recibido el acompañamiento o asesoría del MinTIC.

### Detalle de auditoría

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 6 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

Las actividades desarrolladas hasta la fecha de elaboración de este informe son las siguientes:

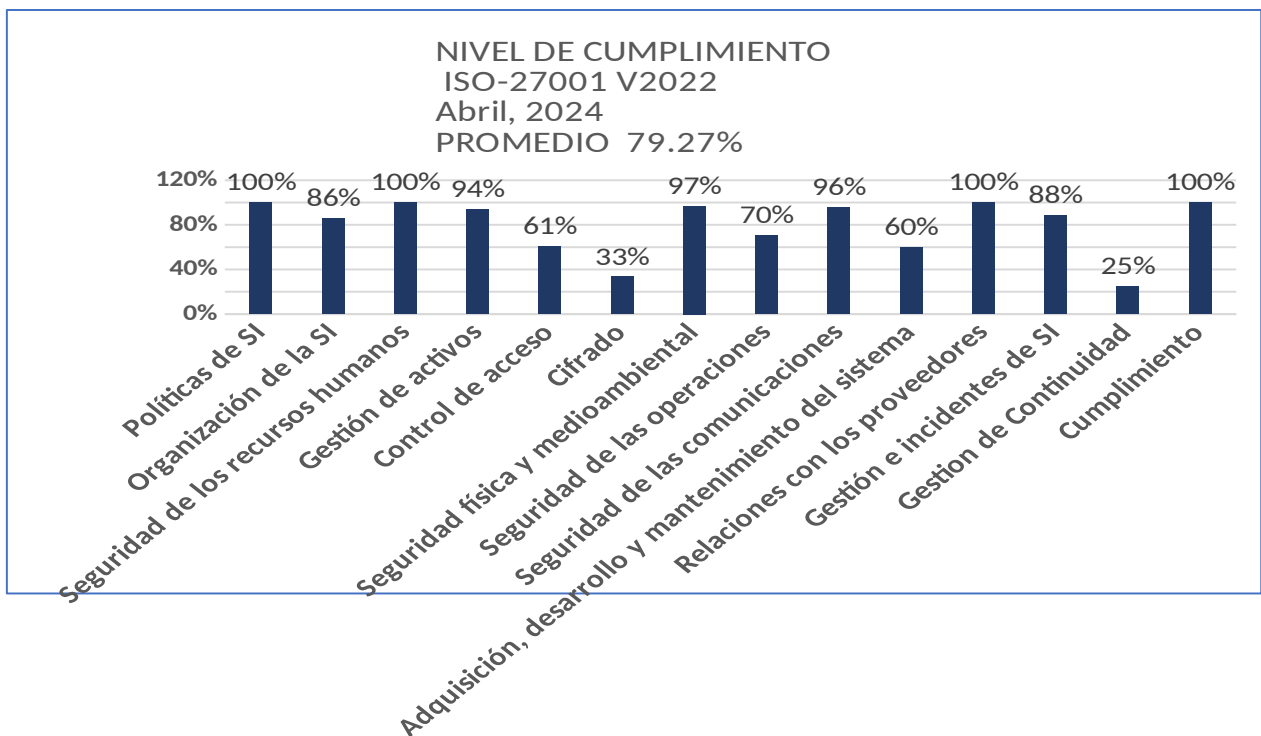
- Reunión de Apertura
- Entrevistas con los usuarios claves o dueños del proceso para diligenciar el cuestionario de la SGSI de la información.
- Solicitud de envío de las evidencias que sustenten las respuestas dadas en el punto anterior
- Las evidencias recibidas hasta la fecha corresponden a los procesos de:
  - a. Políticas de SI
  - b. Organización de la SI
  - c. Seguridad de los recursos humanos
  - d. Gestión de activos
  - e. Control de acceso
  - f. Cifrado
  - g. Seguridad física y medioambiental
- Se presentó informe de avance el 11 de abril de 2024 a la Coordinadora de Control Interno como parte del seguimiento que hace dicha área en forma mensual.
- Se evaluaron las evidencias recibidas con corte a abril 30, 2024.
- Todas las evidencias fueron revisadas, analizadas y almacenadas en Google Drive debidamente ordenadas y clasificadas.
- Se asistió a todas las reuniones programadas
  - a. Se programaron 8 reuniones virtuales para hacer pruebas de recorrido con los usuarios expertos en el manejo de los diferentes aplicativos que utiliza el IDPC
  - b. Se hizo reunión para presentar los resultados preliminares de las evidencias evaluados con corte 30 de abril de 2024.
- Se revisó la matriz de Riesgos de seguridad digital. Se recomienda que se incluya que todos los sistemas operativos, bases de datos, aplicaciones tengan PISTAS DE AUDITORIA (LOGS) para realizar labores de monitoreo, revisión e investigación en caso de que se presente algún evento que comprometa la seguridad de la información del IDPC.
- Entrega del Informe preliminar de la auditoría sobre la seguridad de la información y la Política de Gobierno Digital.

## **1. SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION -SGSI DEL IDPC**

La Auditoría se hizo bajo el marco de referencia de la norma ISO-27001 V2002. Se revisaron 250 archivos de evidencias para comprobar que los controles existen y son eficaces. Se hizo una cuantificación de los controles de la siguiente forma:

1. Verificar que el control exista y sea efectivo puntaje 1
2. Si el control no existe el puntaje es 0
3. Si el control existe, pero no es efectivo 0
4. La escala es 1 a 100

De acuerdo con la cuantificación que se hizo, el nivel de cumplimiento es 79.27%, cuya grafica se muestra a continuación:



El detalle de las evidencias analizadas, se detallan a continuación:

- 203 evidencias son satisfactorias, es decir los controles están funcionando adecuadamente
- 15 hallazgos, lo cual significa que los controles no mitigan el riesgo asociado a cada control.
- 32 evidencias que **Cumplen Parcialmente**, por lo tanto, se clasificaron como **Oportunidades de Mejora**. Es decir que el control existe, pero no está funcionando en forma eficaz y por tanto requiere un ajuste o mejora para mitigar el riesgo asociado y lograr el funcionamiento de eficacia que se requiere.

No.	Proceso	Total		CONTROL EXISTE	CONTROL NO EXISTE	SI EXISTE PERO NO ES EFECTIVO
		Evidencias Recibidas	% Analizado			
A5	Políticas de SI	8	100%	8	0	0
A6	Organización de la SI	21	100%	18	0	3
A7	Seguridad de los recursos humanos	14	100%	14	0	0
A8	Gestión de activos	16	100%	15	0	1
A9	Control de acceso	23	100%	14	3	6
A10	Cifrado	6	100%	2	0	4
A11	Seguridad física y medioambiental	33	100%	32	1	0
A12	Seguridad de las operaciones	37	100%	26	6	5
A13	Seguridad de las comunicaciones	23	100%	22	0	1
A14	Adquisición, desarrollo y mantenimiento del sistema	21	100%	12	1	8
A15	Relaciones con los proveedores	11	100%	11	0	0
A16	Gestión e incidentes de SI	17	100%	15	0	2
A17	Gestión de Continuidad	8	100%	2	4	2
A18	Cumplimiento	12	100%	12	0	0
<b>TOTAL</b>		<b>250</b>	<b>100%</b>	<b>203</b>	<b>15</b>	<b>32</b>
				EFFECTIVAS	HALLAZGOS	OPORTUNIDAD DE MEJORA

Durante el desarrollo de la auditoría y al revisar cada una de las 203 evidencias entregadas, se encontró el cumplimiento parcial de la ejecución de algunos controles, por lo cual se recomienda desarrollar las siguientes **Oportunidades de Mejora** para lograr la efectividad de los controles.

### 1.1. Detalle de los cumplimientos parciales

Durante el desarrollo de la auditoría y al revisar cada una de las 203 evidencias entregadas, se encontró el cumplimiento parcial de la ejecución de algunos controles, por lo cual se recomienda desarrollar las siguientes OPORTUNIDADES DE MEJORA para lograr la efectividad de los controles.



#### 1.1.1. A6 Organización de la SI:

Descripción: A6-6.7-14- Protocolos que utiliza la entidad para la seguridad en las comunicaciones para el teletrabajo.

Observación: Es necesario definir en un anexo técnico adicional en forma detallada los protocolos de seguridad de la información que garanticen conexiones seguras. Se recomienda detallar más los siguientes temas:

1. Definir factores de autenticación doble (cuando sea posible)
2. Utilizar solo por protocolos seguros (HTTPS)
3. Limitar los accesos remotos únicamente a los servicios permitidos y a zonas aisladas en la red



	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 9 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

4. Validar la actualización de software de defensa como antivirus, antimalware, etc.
5. Configurar las capacidades de borrado y bloqueo remoto en los equipos.
6. Instalar software de cifrado en los discos duros de los equipos
7. Realizar copia de seguridad de la información crítica.
8. Monitoreo de los intentos autenticación fallidos, Acceso con un mismo usuario desde múltiples direcciones IP, tráfico de red sospechoso, conexiones desde ubicaciones anómalas o inusuales.

Cumplimiento Parcial: La evidencia suministrada cumple PARCIALMENTE porque faltan detalles más técnicos y protocolos que ayuden a precisar la forma del teletrabajo.

Descripción: A6-8.1-19 - Plan y cronograma para las capacitaciones de concientización para el uso adecuado de los dispositivos móviles. Debido a que se debe adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos

Observación: Desarrollar un programa de capacitación de concientización para el uso adecuado de dispositivos móviles.

Cumplimiento Parcial: La evidencia cumple PARCIALMENTE porque NO define aspectos de seguridad relacionados con copias de respaldo y capacitación en el uso de dispositivos móviles.



Descripción: A6-8.1-20 – Proceso para el Backup de la información de los dispositivos móviles.

Observación: Actualizar MANUAL: POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN para incluir el procedimiento relacionado con las copias de respaldo para dispositivos móviles.

Cumplimiento Parcial: La evidencia cumple PARCIALMENTE porque no define aspectos de seguridad relacionados con copias de respaldo y capacitación en el uso de dispositivos móviles.

### **1.1.2. A8-Gestión de activos**

Descripción: A8-7.1-10- \_Procedimiento de Backup de los medios removibles-Gestión de medios extraíbles.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 10 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

**Observación:** Se debe actualizar PROCEDIMIENTO: BACKUP Y RESTAURACIÓN DE LA INFORMACIÓN, PROCESO: GESTIÓN DE SISTEMAS DE INFORMACIÓN Y TECNOLOGÍA, Versión: 3 del 29 de diciembre de 2023, para incorporar el procedimiento de realización de copias de seguridad en los dispositivos removibles.

**Cumplimiento Parcial:** La evidencia suministrada cumple parcialmente porque El PROCEDIMIENTO: BACKUP Y RESTAURACIÓN DE LA INFORMACIÓN, no describe ni define el procedimiento para la copia de respaldo de los dispositivos removibles. Debe ser analizado y evaluado para verificar que se aplique el numeral 7.10:

-Establecer una política específica de un tema sobre la administración de medios de almacenamiento extraíbles y comunicar dicha política a cualquier persona que utilice o gestione medios de almacenamiento extraíbles.

### **1.1.3. A9-Control de acceso**

**Descripción:** A9-5.17-10- Definición y configuración de las reglas de las contraseñas para todos los aplicativos para garantizar que sean seguras, robustas y confiables.



**Observación:** Los siguientes aplicativos no tienen aún definidas las reglas de contraseñas:

1. SISBIC: Dado que los perfiles de acceso y roles aún están en desarrollo, aún no se cuenta con reglas de validación de contraseña.
2. Koha: no se tiene definido las reglas de contraseña porque el software no está operando.
3. A un Clic del Patrimonio: No hay caducidad, lo cual no es satisfactorio porque debe tenerse un control de la caducidad de las contraseñas.

**Cumplimiento Parcial:** La evidencia cumple parcialmente porque no se tienen definidas las reglas de contraseña para todos los aplicativos que utiliza el IDPC.

**Descripción:** A9-8.2-14-Procedimiento que se realiza para el uso de privilegios en los sistemas de información (derechos de administrador) y como se restringen y controlan dichos privilegios.

**Observación:** Se requiere hacer la supervisión de las actividades de los empleados y contratistas que trabajaban en actividades de desarrollo, mantenimiento, administración de los Sistemas Operativos, Bases de Datos y Aplicativos del IDP. Todas sus actividades deben estar registradas en los LOGS respectivos para tener una trazabilidad de todo el trabajo desarrollado.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 11 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

Cumplimiento Parcial: Las evidencias son parcialmente satisfactorias porque la supervisión se hace en forma manual sobre los informes escritos que presentan mensualmente los contratistas y empleados, pero no hay registros en los LOGS del sistema o monitoreo sobre las actividades desarrolladas directamente en las plataformas tecnológicas del IDPC.

Descripción: - A9-8.2-15. Quien es la persona responsable de gestionar/autorizar los privilegios a los sistemas de información (derechos de administrador).

Observación: Se requiere hacer la supervisión de las actividades de los empleados y contratistas que trabajaban en actividades de desarrollo, mantenimiento, administración de los Sistemas Operativos, Bases de Datos y Aplicativos del IDP. Todas sus actividades deben estar registradas en los LOGS respectivos para tener una trazabilidad de todo el trabajo desarrollado.

Cumplimiento Parcial: Las evidencias son parcialmente satisfactorias porque la supervisión se hace en forma manual sobre los informes escritos que presentan mensualmente los contratistas, pero no hay registros en los LOGS del sistema o monitoreo sobre las actividades desarrolladas directamente en las plataformas tecnológicas del IDPC.

Descripción: A9-8.2-16\_ Seguimiento o monitoreo que se realiza a los usuarios con los privilegios (derechos de administrador) específicos a los sistemas de información.

Observación: Se requiere hacer la supervisión de las actividades de los empleados y contratistas que trabajaban en actividades de desarrollo, mantenimiento, administración de los Sistemas Operativos, Bases de Datos y Aplicativos del IDP. Todas sus actividades deben estar registradas en los LOGS respectivos para tener una trazabilidad de todo el trabajo desarrollado.

Cumplimiento Parcial: Las evidencias son parcialmente satisfactorias porque la supervisión se hace en forma manual sobre los informes escritos que presentan mensualmente los contratistas, pero no hay registros en los LOGS del sistema o monitoreo sobre las actividades desarrolladas directamente en las plataformas tecnológicas del IDPC.

Observación: A9-8.5-19\_Como es procedimiento y que controles tienen para restringir el acceso al código fuente.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 12 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

**Observación:** Se deben crear los perfiles de acceso de los desarrolladores de código, las cuales deben ser monitoreados por La Profesional Especializada de Gestión de Sistemas y Tecnologías de la Información.

**Cumplimiento Parcial:** La evidencia es parcialmente satisfactoria porque NO muestra como está restringido a las librerías o repositorios del código fuente de los aplicativos sobre los cuales el IDPC tiene control y manejo.

**Descripción:** A9-8.5-22-Registro de eventos de intentos exitosos y fallidos de los usuarios (LOG), en todas las aplicaciones que utiliza el IDPC.

**Observación:** Se deben activar los LOGS para todos los aplicativos, Sistemas Operacionales y Base de Datos para que quede registrado toda actividad de cualquier usuario.

**Cumplimiento Parcial:** La evidencia cumple parcialmente porque NO muestra información clara y estructurada, de acuerdo con las mejores prácticas del manejo de LOGS, de los registros de auditoria para ser utilizados en caso de una investigación.

Igualmente, se requiere registros de auditoria para cada uno de los aplicativos siguientes aplicativos: Koha, SISBIC., ORFEO, “A un clic del Patrimonio”.



#### **1.1.4. A10-Cifrado**

**Descripción:** A10-8.24-3-La información confidencial y/o privilegiada se debe transmitir con controles de cifrado o protocolos seguros (HTTPS/TLS v1.2 o superior, FTPS usando TLS v 1.2 o superior, SFTP, AES y 3DES.).

**Observación.** Se debe detallar en el numeral 6.4 Política de criptografía del Manual: políticas de seguridad y privacidad de la información, proceso: gestión de sistemas de información y tecnología, Versión: 3 del 28 de abril de 2023, los controles de cifrado o protocolos seguros tales como (HTTPS/TLS v1.2 o superior, FTPS usando TLS v 1.2 o superior, SFTP, AES y 3DES.)

**Cumplimiento Parcial:** La evidencia cumple parcialmente, lo exigido por la norma ISO-27001 V2022, Numeral 8.24. Uso de cifrado. Se debe complementar el procedimiento con los siguientes temas:

1. Detalle de los protocolos o controles de cifrado para la protección y seguridad de la información confidencial.
2. Describir los mecanismos aleatorios o semialeatorios para la generación de llaves de cifrado.

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 13 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

3. Como se protegen los equipos utilizados para generar o almacenar claves de cifrado.
4. Como se protege la información confidencial tanto en reposo como en tránsito con protocolos de cifrado.

Descripción: A10-8.24-4 - A10-8.24-5 - A10-8.24-6-



1. Las llaves de cifrado deben ser generadas con mecanismos aleatorios o semialeatorios y en ninguna circunstancia de forma manual con parámetros introducidos por colaboradores o terceros.
2. Los equipos utilizados para generar o almacenar claves, están físicamente protegidos
3. La información confidencial y/o bajo cumplimiento normativo o legal, debe ser cifrada tanto en reposo como en tránsito y debe permanecer de esta forma en los medios de respaldo.

Observación: Se debe actualizar la política de cifrado, incluyendo más detalle sobre estos temas:

1. Detalle de los protocolos o controles de cifrado para la protección y seguridad de la información confidencial
2. Describir los mecanismos aleatorios o semi aleatorios para la generación de llaves de cifrado
3. Como se protegen los equipos utilizados para generar o almacenar claves de cifrado.
4. Como se protege la información confidencial tanto en reposo como en tránsito con protocolos de cifrado.

Cumplimiento Parcial: La evidencia cumple parcialmente porque no se tiene una descripción detallada sobre estos temas:

1. Detalle de los protocolos o controles de cifrado para la protección y seguridad de la información confidencial
2. Describir los mecanismos aleatorios o semi aleatorios para la generación de llaves de cifrado
3. Como se protegen los equipos utilizados para generar o almacenar claves de cifrado.
4. Como se protege la información confidencial tanto en reposo como en tránsito con protocolos de cifrado.

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 14 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

### 1.1.5. A12-Seguridad de las operaciones

Descripción: A12-8.15-12-Los equipos que contienen los registros y logs de auditoría deben estar bien protegidos contra posibles manipulaciones y acceso no autorizado.

Observación: Se debe implementar el control de acceso a los equipos que contienen los registros y logs de auditoría para que se encuentran bien protegidos contra posibles manipulaciones y acceso no autorizado. Es decir, se debe definir claramente que usuarios (Administradores o Usuarios con Privilegios) son los que pueden ingresar a estos equipos y se debe guardar el LOG de las actividades que realicen estos usuarios.

Cumplimiento Parcial: La evidencia cumple parcialmente porque no se puede comprobar que los equipos donde están los registros de auditoría están protegidos contra posibles manipulaciones y acceso no autorizado.

Se debe restringir el acceso a los equipos donde están almacenados los registros de auditoría para lo cual solo debe existir una persona con acceso a dichos equipos (y una persona de respaldo) que al ingresar a realizar alguna actividad en estos equipos deben autenticarse y los registros de las actividades que desarrolle deben quedar registrados en los LOGS del equipo o del aplicativo.



Descripción: A12-8.19-19-Se debe tener implementada una estrategia de retroceso (Rollback) antes de implementar los cambios.

Observación: Se recomienda incluir en el manual de POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IDPC, una estrategia de reversión (rollback) antes de implementar la actualización o parcheo de programas, sistemas operativos, bases de datos, aplicativos licenciados; que puedan resultar fallidos o que pueda afectar a otros sistemas.

Cumplimiento Parcial: La evidencia cumple parcialmente porque no hay evidencia de procesos de Rollback en caso de que la actualización de software resulte fallida y se pueda volver al estado anterior para no afectar el desarrollo de las actividades del IDPC.

Descripción: A12-8.32-26-Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de información deben estar adecuadamente controlados.

Observación: Redactar formalmente una Política de Control de Cambios de acuerdo con las guías dadas por la norma ISO-SO/IEC 27002, la cual debe contener los siguientes ítems de acuerdo con la mencionada norma y las mejores metodologías:

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 15 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

1. Diligenciar el formato de solicitud de cambios donde se detalle la identificación y registro de los cambios significativos.
2. Análisis de la evaluación de los impactos potenciales, incluyendo los impactos en la seguridad de la información de dichos cambios.
3. Realizar la planificación, escritura o generación del código de software necesario.
4. Realizar las pruebas por parte del usuario; documentación de las pruebas.
5. Verificar que los requisitos de seguridad de la información se cumplen.
6. Comunicación de los detalles de los cambios a todas las personas correspondientes.
7. Procedimientos de vuelta atrás, incluyendo los procedimientos y responsabilidades para abortar y recuperar los cambios infructuosos y los eventos imprevistos.
8. Procedimiento de aprobación formal de los cambios propuestos por parte del dueño del proceso o del Comité de Cambios.
9. Disposición de un proceso de cambio de emergencia que habilite la implantación rápida y controlada de los cambios necesarios para resolver un incidente.
10. Guardar toda la documentación de los cambios realizados para tener las memorias y constituir una base de datos de conocimiento y lecciones aprendidas.



Cumplimiento Parcial: La evidencia cumple parcialmente porque no se tiene detallado y consolidado todo el proceso de control de cambios, con todas y cada una de las fases que comprende este proceso.

Descripción: A12-8.6-30-Análisis y mediciones de la capacidad de procesamiento de los sistemas debe ser monitoreada con base en la demanda y con proyección basada en requerimientos futuros, de modo que se asegure que la capacidad de proceso y almacenamiento estén disponibles Ejemplo: Monitoreo de espacio en disco, Memoria RAM, CPU en los servidores críticos, ancho de banda para Internet.

Observación: Se recomienda formalizar los análisis de gestión de capacidad con el software que el IDPC pueda adquirir para realizar mediciones y cuantificaciones sobre los recursos necesarios relacionados con Monitoreo de espacio en disco, Memoria RAM, CPU en los servidores críticos, ancho de banda para Internet.

Cumplimiento Parcial: La evidencia es parcialmente satisfactoria porque no hay evidencia de estudios sobre la capacidad de procesamiento de los sistemas con base en



	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 16 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

la demanda y con proyección basada en requerimientos futuros. Igualmente, en el Informe de Auditoría de 2020 se deja constancia de que no existe "Procedimiento de Gestión de Capacidad".

Descripción: A12-8.6-31-El procedimiento de Gestión de la Capacidad debe estar formalmente documentado, actualizado y divulgado a los usuarios que lo requieran.

Observación: Se recomienda formalizar los análisis de gestión de capacidad con el software que el IDPC pueda adquirir para tener mediciones precisos y reales que monitoreen los recursos de capacidad de procesamiento de datos requeridos tales como capacidad de disco, memoria RAM, velocidad de los canales de internet y demás recursos. Se debe hacer un análisis para:

1. Borrado de datos obsoletos (espacio de disco).
2. Desmantelamiento de aplicaciones, sistemas, bases de datos o entornos.
3. Optimizando el tratamiento por lotes y la planificación.
4. Optimizando la lógica de la aplicación o las consultas de base de datos.
5. Denegando o restringiendo el ancho de banda para servicios consumidores de muchos recursos, si estos no son críticos para el negocio (por ejemplo, la transmisión de vídeo).



Cumplimiento Parcial: La evidencia cumple parcialmente porque no hay evidencia de estudios sobre la capacidad de procesamiento de los sistemas con base en la demanda y con proyección basada en requerimientos futuros. Igualmente, en el Informe de 2020 se deja constancia de que no existe "Procedimiento de Gestión de Capacidad".

### **1.1.6. A13-Seguridad de las comunicaciones**

Descripción: A13-5.14-9-Definir los protocolos para desarrollar el comercio electrónico entre los socios comerciales o terceras partes e incluir un acuerdo, que compromete a ambas partes en la negociación de los términos convenidos, incluidos los detalles de las cuestiones de seguridad.

Observación: Se deben definir los procedimientos de comercio electrónico con terceras partes de la información tal como lo exige la norma ISO-27001 numeral 5.14 Políticas y procedimientos de transferencia de información como una OPORTUNIDAD DE MEJORA, pues, aunque actualmente no se tiene actividades de comercio electrónico si es mejor estar preparados para tal efecto en un futuro inmediato. Se debe incluir los siguientes tópicos que apliquen en el IDPC. Los procedimientos y controles que



	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 17 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	



deberían seguirse cuando se usan recursos de comunicación para la transferencia de información deberían considerar los siguientes aspectos:

1. El diseño de procedimientos para proteger la información transferida de interceptación, copia, modificación, errores de enrutamiento y destrucción.
2. Procedimientos para la detección y la protección contra el malware que podría ser transmitido a través del uso de comunicaciones electrónicas.
3. Procedimientos para proteger información electrónica sensible que tiene la forma de adjuntos.
4. Políticas o directrices describiendo el uso aceptable de los recursos de comunicación.
5. Responsabilidades del personal, partes externas y de cualquier otro usuario para no comprometer a la organización, por ejemplo, mediante la difamación, el acoso, la suplantación, el reenvío de mensajes en cadena, las compras no autorizadas, etc.
6. Uso de técnicas criptográficas, por ejemplo, para proteger la confidencialidad, integridad y autenticidad de la información.
7. Directrices para la retención y eliminación de toda la correspondencia comercial, incluidos los mensajes, de acuerdo con la legislación y las reglamentaciones nacionales y locales pertinentes.
8. Controles y las restricciones asociadas con el uso de los recursos de comunicación, por ejemplo, reenvío automático del correo electrónico a las direcciones de correo externas.
9. Asesorar al personal para que tome las precauciones necesarias de no revelar información confidencial.
10. No dejar mensajes que contengan información confidencial en los contestadores automáticos dado que estos podrían ser reproducidos por personas no autorizadas, almacenados en sistemas públicos o almacenados incorrectamente como consecuencia de un error en la marcación de un teléfono.

Cumplimiento Parcial: La evidencia cumple parcialmente porque no existen acuerdos para el intercambio seguro de información del negocio y software entre IDPC y terceras partes.

#### **1.1.7. A14-Adquisición, desarrollo y mantenimiento del sistema**

Descripción: A14-8.25-3-Definición de protocolos o metodologías de desarrollo de software seguro en la organización

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 18 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

Observación: Se debe documentar e implementar la política de desarrollo seguro de acuerdo con el numeral 8.25 Política de desarrollo segura de la norma ISO-27001-V2022

Cumplimiento Parcial: La evidencia cumple parcialmente porque describe muy brevemente, pero no es suficiente, el proceso para el desarrollo o adquisición de software.

Descripción: A14-8.26-5-Deben estar identificados y especificados los requisitos de seguridad de las aplicaciones.

Observación: Se debe complementar los requisitos de seguridad de las aplicaciones tal como le exige el numeral 8.25 de la Norma ISO-27001-V2022 Ciclo de vida de desarrollo seguro

Cumplimiento Parcial: La evidencia cumple parcialmente porque no está descrita en forma detallada ni especificados los requisitos de seguridad de las aplicaciones. Por tanto, se debe incluir en la política en forme breve y concisa los requisitos de seguridad para tener en cuenta en los Aplicativos del IDPC.

Se recomienda detallar más el protocolo o técnicas de desarrollo seguro de software.



Descripción: A14-8.27-8-Están identificados e implementados principios de desarrollo seguros, tales como mínimos permisos, limpiar los códigos en producción, validar todos los datos y accesos, actualizaciones permanentes de seguridad, determinar los puntos débiles, entre otros.

Observación: Se debe complementar los requisitos principios de desarrollo seguros tal como lo exige el numeral 8.27. Arquitectura de sistemas seguros y principios de ingeniería segura de la norma ISO-27001-V2022.

Cumplimiento Parcial: La evidencia cumple parcialmente porque describe muy superficialmente los controles de seguridad de ingeniera segura, tales como borrado seguro, mínimos privilegios de acceso entre otros. Se recomienda brindar una descripción más detallada y profunda.

Descripción: A14-8.32-17-Implementar un procedimiento riguroso para realización de modificaciones en los paquetes de software (los cuales deben estar limitados y solo se deben realizar cuando sea estrictamente necesario)

Observación: Se recomienda complementar POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IDPC con la descripción del procedimiento

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 19 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

riguroso para realización de modificaciones en los paquetes de software, de acuerdo con el numeral 8.32 Procedimientos de control de cambios del sistema.

Cumplimiento Parcial: La evidencia cumple parcialmente porque no está definido claramente cuáles son las modificaciones en los paquetes de software, estrictamente necesarias. Todos los cambios deben ser objeto de un control riguroso.

Descripción: A14-8.33-18-La información para las pruebas debe estar seleccionadas, protegidas y gestionadas adecuadamente.

Observación: Se recomienda complementar POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN IDPC con la definición de la información para las pruebas, para que estén seleccionadas, protegidas y gestionadas adecuadamente, de acuerdo con el numeral 8.33 Protección de los datos de prueba de la norma ISO-27001-V2022.

Cumplimiento Parcial: La evidencia cumple parcialmente porque no se tiene una evidencia de que la información para las pruebas está seleccionadas, protegidas y gestionadas adecuadamente, tal como lo exige el numeral 8.33. Información para las pruebas de la norma ISO-27001. Se hacen pruebas de los cambios, pero no se tiene evidencia de la protección de la información utilizada en las pruebas.



Descripción: A14-8.33-20-Implementación de un procedimiento formal de borrado seguro de los datos de prueba.

Observación: Se recomienda describir en forma más detallada el procedimiento de borrado seguro de acuerdo con el numeral 8.33. Información para las pruebas de la norma ISO-27001

Cumplimiento Parcial: La evidencia cumple parcialmente porque describe muy superficialmente los controles de seguridad de ingeniería segura, tales como borrado seguro, mínimos privilegios de acceso entre otros. Se recomienda brindar una descripción más detallada y profunda.

Descripción: A14-8.33-21-Utilización de información personal o cualquier información sensible para propósitos de testeos, debe estar prohibida.

Observación: Se recomienda describir claramente como se debe hacer la utilización de información personal o cualquier información sensible para propósitos de testeos, de acuerdo con el numeral 8.33. Información para las pruebas de la norma ISO-27001-V2022.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 20 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

Cumplimiento Parcial: La evidencia cumple parcialmente porque no está definida, reglamentada o prohibida la utilización de información personal o cualquier información sensible para propósitos de testeo tal como lo exige el numeral 8.33. Información para las pruebas de la norma ISO-27001.

Descripción: A14-8.33-22-La información involucrada en transacciones en línea debe estar protegida contra transmisiones incompletas, mal ruteo, alteración de mensajería, divulgación no autorizada, duplicación no autorizada o replicación.

Observación: Se recomienda describir en las transacciones en línea como está protegida contra transmisiones incompletas, mal ruteo, alteración de mensajería, divulgación no autorizada, duplicación no autorizada o replicación de la información, para cumplir lo exigido por el numeral 8.33 Protección de los datos de prueba de la Norma ISO-27001-V2022.

Cumplimiento Parcial: La evidencia cumple parcialmente porque describe muy superficialmente los controles de seguridad de ingeniería segura, pero faltan aspectos tales como transmisiones incompletas, mal ruteo, alteración de mensajería, divulgación no autorizada, duplicación no autorizada o replicación. Se recomienda brindar una descripción más detallada y profunda sobre estos temas.

#### **1.1.8. A16-Gestión e incidentes de SI**



Descripción: A16-5.28-12-Las medidas de seguimiento después de un incidente de seguridad de la información que implican una acción legal (ya sea civil o penal) deben ser ejecutadas para cumplir con los requerimientos de ley.

Observación: Se recomienda actualizar el Procedimiento, Atención de requerimientos de recursos tecnológicos, para describir como se debe hacer el seguimiento a los requerimientos en caso de que se presenten procesos legales,

Cumplimiento Parcial: La evidencia cumple parcialmente porque no se tiene evidencia del seguimiento que se hace a los requerimientos con implicaciones legales.

Descripción: A16-5.28-14-Los procedimientos internos desarrollados que se emplean para recolectar y presentar evidencia para propósitos disciplinarios dentro de la organización deben estar claramente definidos

Observación: Se recomienda actualizar el procedimiento, Atención de requerimientos de recursos tecnológicos, para incluir el proceso a seguir en caso de que se presenten procesos disciplinarios, de acuerdo con el numeral 5.28. Recopilación de pruebas de la norma ISO-27011-V2022

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 21 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

Cumplimiento Parcial: La evidencia cumple parcialmente porque no se tiene definido el procedimiento que debe desarrollar cuando se presenten procesos disciplinarios derivados de incidentes de seguridad.

### **1.1.9. A17-Aspectos de la SI en la gestión de la continuidad de la actividad**

Descripción: A17-5.29-2-Como se ha implementado la continuidad de operaciones en IDPC y cuál es el impacto en la seguridad de la información.

Observación: Se debe hacer las pruebas de continuidad de operaciones en IDPC

Cumplimiento Parcial: La evidencia cumple parcialmente porque no se tiene evidencia de que se hayan realizados para para probar el plan de continuidad de operaciones en IDPC y tampoco se tiene cuantificado el impacto en la seguridad de la información.

Descripción: A17-5.29-6-Debe estaré definido quién o quiénes son los responsables de activar el plan de contingencia. Debe estar conformado un comité de crisis.

Observación: Se debe definir el equipo que debe activar el plan de contingencia y documentar toda la información relacionada con números de celular, dirección de correo electrónico y demás información que permita mantener una comunicación constante y efectiva con el equipo, para cumplir el numeral 5.29. SI durante una interrupción de la norma SIO-27001-V2022

Cumplimiento Parcial: La evidencia cumple parcialmente porque no se tiene un organigrama del equipo responsable de activar el plan de contingencia.



### **1.2. Detalle de las No Conformidades**

Durante el desarrollo de la auditoría y al revisar cada una de las 203 evidencias entregadas, se encontraron diez y ocho [18] hallazgos en la ejecución de los controles, por lo cual se recomienda desarrollar las siguientes Planes de Acción para lograr la efectividad de los controles.

A continuación, se hace una presentación de las no-conformidades o hallazgos, partiendo de un nivel global o general y luego se va mostrando con más detalle para que sea más fácil su análisis y corrección. Esto es similar a un esquema de Drill-Down.

Es de anotar, que corrigiendo un tema global se pueden corregir varias no-conformidades, esto es, que de acuerdo con la estructura de la norma ISO-27001-V2022 se aborda el análisis de un control en diferentes dominios de la norma.

Aunque pueden ser demasiados hallazgos o no conformidades, se recomienda mirar a nivel de proceso para que sea más fácil su corrección o ajuste, la norma evalúa algunos

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 22 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

controles en diferentes dominios de esta y da la impresión de redundancia. Los temas globales sobre las cuales se encontraron los hallazgos son los siguientes:

1. Perfiles de acceso para Administradores y usuarios con privilegios [A9-Control de acceso, A12-Seguridad de las operaciones]
2. Pistas de Auditoria [A9- Control de acceso A12-Seguridad de las operaciones]
3. Riesgos en el manejo de activos. [A11-11-Seguridad física y medioambiental]
4. Política Gestión de Cambios [A12-Seguridad de las operaciones, A14-14-Adquisición, desarrollo y mantenimiento del sistema]
5. Intercambio de información [A13-Seguridad de las comunicaciones]
6. Contingencia y procesos de continuidad del negocio [A17-17-Aspectos de la SI en la gestión de la continuidad de la actividad]

Las no conformidades encontradas se resumen y se consolidan en los siguientes dominios de la norma ISO-27001-V2022-

#### **1.2.1. A9-Control de acceso**

Criterio: Numeral: 8.2. Derechos de acceso privilegiados. La asignación y el uso de los derechos de acceso privilegiados deberían ser restringidos y gestionados.



Condición: A9-8.2-17-Los administradores de Sistemas Operativos, Base de Datos, Correo y demás Sistemas de Información, deben tener perfiles específicos.

Causa: No se han definidos los perfiles porque se hace una supervisión manual de acuerdo con las funciones definidas en los documentos de contratación (Estudios previos de contratación). Por otro lado, no se tiene el Personal suficiente y calificado para desarrollar las labores de administradores de Sistemas Operativos, DBA o similares.

Consecuencia: No se puede hacer un monitoreo y seguimiento de las labores de los usuarios privilegiados porque no se tiene un perfil creado y tampoco se guarda un registro en los LOGS de los Sistemas Operativos, Bases de Datos, Aplicativos, lo cual puede generar impactos en la seguridad de la información que comprometan la integridad, disponibilidad y confidencialidad de la información.

Plan de Acción: Se deben crear los perfiles de acceso de los administradores de Sistema Operativo, Base de Datos o Aplicativos, las cuales deben ser monitoreados por La Profesional Especializada de Gestión de Sistemas y Tecnologías de la Información.

Criterio: Numeral 8.5. Autenticación segura. Las tecnologías y los procedimientos de autenticación segura deberían implementarse en función de las restricciones de acceso

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 23 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

a la información y de la política de control de acceso específica del tema, así como registros en los LOGS que se tengan implementados.

**Condición:** A9-8.5-21-Política del proceso de seguimiento de auditoría para las pistas de auditoría (LOGS)

El proceso debe incluir los requisitos de auditoría (cuando corresponda):

1. Requisitos estándar de auditoría / registro
2. Detalles de cualquier pista de auditoría adicional (informes) que solicite el IDPC, incluidos los campos de datos clave que se deben rastrear, el destinatario del informe y si el informe se produce a pedido o automáticamente.
3. Detalles de cualquier registro de auditoría adicional que esté habilitado en el sistema, incluido quién usa los datos y con qué propósito. Nota: Los registros de la actividad de acceso al sistema se utilizan a menudo como una mitigación para la segregación de funciones o problemas de acceso privilegiado
4. Cuánto tiempo se deben conservar los datos de auditoría / registro
5. Cómo se almacenan y protegen los datos de auditoría / registro
6. Detalles de las revisiones / pruebas periódicas que se realizan para garantizar que se cumplen los requisitos.

El proceso también debe incluir detalles de los parámetros del sistema que se activan para permitir el registro / pistas de auditoría.



**Causa:** No se tiene establecida una Política de LOGS (Pistas de Auditoría) para los aplicativos (Sistema Integrado de Información Gerencial Operativo SIIGO, SIIGO NOMINA, SISBIC, Koha, ORFEO, A un Click del Patrimonio) que utiliza el IDPC, porque no se cuenta con el personal suficiente para su implementación, revisión y seguimiento.

**Consecuencia:** No se pueden desarrollar las labores de monitoreo de todas las actividades de los usuarios, incluyendo las acciones de los usuarios con privilegios como los administradores del sistema, los cuales no deberían tener permiso para borrar o desactivar los registros de sus propias actividades.

**Plan de Acción:** Se debe elaborar un Manual de la Política de Pistas de Auditoría. Se recomienda tomar como marco de referencia lo que establece la norma ISO ISO/IEC 27002, numeral 12.4.1 Registro de eventos, la cuales establece los siguientes criterios para que sean registrados en los archivos de los registros de Auditoría, se debe utilizar los que sean relevantes para el IDPC:

1. Identificadores (ID) de usuario.
2. Actividades del sistema.



 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 24 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

3. Fechas, hora y detalles de eventos clave, por ejemplo, conexión (log-on) y desconexión (log-off).
4. Identidad o localización del dispositivo, si es posible e identidad del sistema.
5. Definir las transacciones/procesos críticos que el IDPC considere extremadamente sensibles para poder hacer un registro y seguimiento en los LOGS.
6. Registro de intentos de acceso a los sistemas exitosos y fallidos.
7. Registro de intentos de acceso a los recursos y a los datos exitosos y fallidos.
8. Cambios en la configuración del sistema.
9. Uso de privilegios.
10. Uso de utilidades y aplicaciones del sistema.
11. Tablas/archivos a los que se ha accedido y el tipo de acceso.
12. Direcciones y protocolos de red.
13. Alarmas generadas por el sistema de control de acceso.
14. Activación y desactivación de los sistemas de protección, tales como sistemas de antivirus y de detección de intrusión.
15. Registro de transacciones ejecutadas por usuarios en las aplicaciones.
16. Registro antes y registro después del cambio (cuando sea posible).
17. Cuánto tiempo se deben conservar los datos de auditoría / registro.
18. Cómo se almacenan y protegen los datos de auditoría / registro.
19. Detalles de las revisiones / pruebas periódicas que se realizan para garantizar que se cumplen los requisitos para garantizar la seguridad de la información.



Criterio: Numeral 8.15 Registro de evento. Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

Condición: A9-8.5-23-Llevar un registro adecuado para cada uno de los aplicativos del IDPC en las aplicaciones (LOG).

Causa: No se tiene implementados los LOGS de los aplicativos desarrollos y/o contratados por el IDPC porque no se han estructurado adecuadamente como parte de su desarrollo.

Consecuencia: No se pueden desarrollar las labores de monitoreo de todas las actividades de los usuarios en los aplicativos, sistemas operacionales o Bases de Datos de todos los usuarios del IDPC. Esto incluye las acciones de los usuarios con privilegios como los administradores del sistema, los cuales no deberían tener permiso para borrar o desactivar los registros de sus propias actividades.



	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 25 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

Plan de Acción: Es necesario elaborar un plan de remediación para estructurar, estandarizar e implementar el uso de las PISTAS DE AUDITORIA de acuerdo con los lineamientos definidos en la norma ISO ISO/IEC 27002, numeral 12.4.1 Registro de eventos y tener la información necesaria para hacer la trazabilidad de las actividades de todos los usuarios en las diferentes plataformas del IDPC.

### **1.2.2. A11-Seguridad física y medioambiental**

Criterio: Numeral 7.9 Seguridad de los activos fuera de las instalaciones.\_Los activos fuera de las instalaciones deberían estar protegidos.

Condición: A11-7.9-30-Se deben implementar los mecanismos de control y mitigación de riesgos implementados en relación con equipos utilizados fuera de la organización Los activos fuera de las instalaciones deberían estar protegidos. (encriptación de discos de los portátiles, seguro, guaya, etc.)

Causa: No se ha implementado mecanismos de control lógicos y físicos para proteger la información de los equipos cuando estos están fuera de las instalaciones del IDPC porque se no han presentado casos de eventos que afecten la seguridad de la información.



Consecuencia: En el evento que se presente un robo, pérdida de un equipo, ataque informático que comprometa la seguridad de la información no se tienen definidos ni implementados los protocolos de seguridad que garanticen la protección de la información que afecte la integridad, disponibilidad y confidencialidad de esta.

Plan de Acción: Se debe implementar el proceso de encriptación de los discos duros y adoptar medidas de protección física como guayas, candados, etc.

### **1.2.3. A12-Seguridad de las operaciones**

Criterio: Numeral 8.15. Registros. Deben producirse, almacenarse, protegerse y analizarse los registros que recogen las actividades, las excepciones, los fallas y otros eventos relevantes.

Condición: A12-8.15-7-Los registros de auditoría que guardan la actividad de todos los usuarios, excepciones, eventos de seguridad de información que ocurren, se guardan por un período razonable de tiempo de tal modo que puedan realizarse investigaciones futuras y monitoreo de acceso.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 26 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

**Causa:** Los LOGS existentes para los aplicativos de SISBIC, ORFEO, “A un clic del Patrimonio”, Koha no tienen la información básica necesaria definida en la norma ISO/IEC 27002, numeral 8.15. Registros, la información que muestra no está estructurada, no es fácilmente entendible ni legible, lo cual no les da ninguna utilidad para realizar labores de análisis, investigaciones, monitoreo o trazabilidad.

**Consecuencia:** No tener unas Pistas de Auditoria adecuadas compromete la seguridad de la información porque no se dispone de información para para realizar labores de análisis, investigaciones, monitoreo o trazabilidad, cuando se presente un evento que necesite ser analizado o revisado.

**Plan de Acción:** Es necesario estructurar, estandarizar e implementar el uso de las PISTAS DE AUDITOIRIA de acuerdo con los lineamientos definidos en la norma ISO ISO/IEC 27002, numeral 8.15. Registros y tener la información necesaria para tener la trazabilidad de las actividades de todos los usuarios en las diferentes plataformas del IDPC.



**Criterio:** Numeral 8.15. Registros. Deben producirse, almacenarse, protegerse y analizarse los registros que recogen las actividades, las excepciones, los fallas y otros eventos relevantes.

**Condición:** A12-8.15-8-Se deben tener medidas de protección para los registros de auditoría, Por ejemplo, los registros de auditoria no se pueden borrar, modificar o editar, inactivar.

**Causa:** No se tiene medidas de protección a nivel físico y lógico de los registros de auditoría a nivel del Servidor, Nivel de las tablas, Nivel de los atributos de los de los campos de la tabla donde esta registrados los LOGS. En lo posible se debe llegar a una protección a nivel de campo de información para evitar que se puedan borrar, modificar o editar, inactivar los registros de auditoría.

**Consecuencia:** No tener un adecuado de registro de eventos y operaciones de todos los usuarios pueden llevar afectar la seguridad de la información porque se pueden violar los criterios que garanticen la integridad, disponibilidad y confidencialidad de la información del IDPC.

**Plan de Acción:** Es necesario que las tablas y archivos donde estén guardados los registros de auditoria están protegidas y los registros de cada tabla tenga bloqueado los atributos de borrar, modificar o editar, inactivar los registros de auditoría.

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 27 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

**Criterio:** Numeral 8.15. Registros.\_Deben producirse, almacenarse, protegerse y analizarse los registros que recogen las actividades, las excepciones, los fallas y otros eventos relevantes.

**Condición:** A12-8.15-10. Se deben desarrollar una actividad de monitoreo regularmente de forma periódica.

**Causa:** No se tiene una actividad de revisión periódica de las PISTAS DE AUDITORIA, porque esta función no se tiene asignada a ninguna persona en el IDPC.

**Consecuencia:** No tener un adecuado monitoreo y revisión de eventos y operaciones de todos los usuarios pueden llevar afectar la seguridad de la información porque se pueden violar los criterios que garanticen la integridad, disponibilidad y confidencialidad de la información del IDPC

**Plan de Acción:** Es necesario definir en la Política de Pistas de Auditoria la frecuencia, responsable y acciones que se derivan de la revisión de las pistas de auditoría.

**Criterio:** Numeral 8.15. Registros.\_Deben producirse, almacenarse, protegerse y analizarse los registros que recogen las actividades, las excepciones, los fallas y otros eventos relevantes.



**Condición:** A12-8.15-13-Las actividades de los Administradores y Operadores de sistemas deben ser registradas en los logs.

**Causa:** Las actividades de los administradores, Operadores de Sistemas y usuarios con privilegios no están registradas en los LOGS de Los Sistemas Operativos, Bases de Datos, Aplicativos porque no se han implementado ni los registros de los LOGS de acuerdo con las metodologías o mejores prácticas existentes.

**Consecuencia:** En el evento que se presente una falla, fraude, ataque a los sistemas informáticos del IDPC no se cuenta con los registros de pistas de auditoría que permitan hacer una investigación, análisis o tomar acciones correctivas.

**Plan de Acción:** Se debe ejecutar las siguientes acciones:

1. Crear los perfiles de usuarios administradores, Operadores de Sistemas y usuarios con privilegios.
2. Activar los LOGS, para que toda su actividad en las plataformas informáticas del IDPC queden registradas en los diferentes sistemas operativos, aplicativos, bases de datos con el fin de cumplir lo exigido por el numeral 8.15. Registros de la norma ISO-27001 v2022.

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 28 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

**Criterio:** Numeral 8.31. Separación de los entornos de desarrollo, pruebas y producción. Los entornos de desarrollo, prueba y producción deben estar separados y protegidos. Proteger el entorno de producción y los datos del peligro que suponen las actividades de desarrollo y prueba.

**Condición:** A12-8.31-25-Se deben tener perfiles de acceso mediante reglas supervisadas para cada uno de los ambientes de trabajo definidos.

**Causa:** No se han definido los perfiles de acceso para los ambientes de trabajo de desarrollo y pruebas que los diferencien y garanticen su total independencia y configuración.



**Consecuencia:** Se puede afectar la información de cada uno de los ambientes de trabajo definidos, dado que se puede generar confusión y alterar, dañar la información de cada uno de los ambientes de trabajo creados. Se debe reducir los riesgos de acceso no autorizado o los cambios del sistema en producción. Cuando el personal de desarrollo y de prueba tiene acceso al sistema de producción y a su información, pueden introducir código no autorizado y que no ha sido probado o datos operativos modificados. En algunos sistemas, esta capacidad podría utilizarse para cometer fraude o para introducir un código malicioso o no probado, que puede causar problemas operacionales serios.

**Plan de Acción:** Definir los perfiles de acceso para cada uno de los ambientes de trabajo con el fin de cumplir con los protocolos de seguridad de la información que haya en cada ambiente de trabajo, tal como lo exige el numeral 8.31. Separación de los entornos de desarrollo, pruebas y producción.

**Criterio:** Numeral 8.32. Gestión de cambios.\_Los cambios en las instalaciones de procesamiento de la información y en los sistemas de información deben estar sujetos a procedimientos de gestión del cambio.

**Condición:** A12-8.32-27-La política de Gestión de Cambios debe estar formalmente documentada, actualizada y divulgada a los usuarios que la requieran.

**Causa:** No se ha elaborado una Política de control de cambios porque no se cuenta con los recursos humanos necesarios que permite tener una Segregación de funciones para

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 29 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	



desarrollar el control de cambios de acuerdo con mejores metodologías o prácticas de la industria.

**Consecuencia:** La falta de una Política de Control de cambios puede generar riesgos en la seguridad de las aplicaciones y su funcionalidad porque se pueden afectar funciones y procedimientos vitales para el funcionamiento del IDPC.

Este proceso debería incluir una evaluación del riesgo, el análisis de los impactos de los cambios y la especificación de los controles de seguridad necesarios. Este proceso también debería asegurarse de que los procedimientos de seguridad y de control existentes no se vean comprometidos, que a los programadores de apoyo se les da acceso sólo a aquellas partes del sistema necesarias para su trabajo y que se obtiene el acuerdo formal y la aprobación de cualquier cambio.

**Plan de Acción:** Redactar e implementar formalmente una Política de control de cambios de acuerdo con las guías dadas por la norma ISO-SO/IEC 27002:

1. Diligenciar el formato de solicitud de cambios donde se detalle la identificación y registro de los cambios significativos.
2. Análisis de la evaluación de los impactos potenciales, incluyendo los impactos en la seguridad de la información de dichos cambios.
3. Realizar la planificación, escritura o generación del código de software necesario.
4. Realizar las pruebas por parte del usuario; documentación de las pruebas.
5. Verificar que los requisitos de seguridad de la información se cumplen.
6. Comunicación de los detalles de los cambios a todas las personas correspondientes.
7. Procedimientos de vuelta atrás, incluyendo los procedimientos y responsabilidades para abortar y recuperar los cambios infructuosos y los eventos imprevistos.
8. Procedimiento de aprobación formal de los cambios propuestos por parte del dueño del proceso o del Comité de Cambios.
9. Disposición de un proceso de cambio de emergencia que habilite la implantación rápida y controlada de los cambios necesarios para resolver un incidente.
10. Guardar toda la documentación de los cambios realizados para tener las memorias y constituir una base de datos de conocimiento y lecciones aprendidas.

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 30 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

#### **1.2.4. A13-Seguridad de las comunicaciones**

##### **1.2.5. A14-Adquisición, desarrollo y mantenimiento del sistema**

Criterio: Numeral 8.32. Gestión de cambios.\_Los cambios en las instalaciones de procesamiento de la información y en los sistemas de información deben estar sujetos a procedimientos de gestión del cambio.

Condición: A14-8.32-14-Se debe una política de control de cambios (Esto es para minimizar la posible corrupción de los sistemas de información, especialmente cuando se contrate el desarrollo de software con terceras partes)

Causa: No se tiene redactada ni implementada una Política de Control de Cambios tal como lo exige la norma ISO-27001, numeral 8.32 Procedimientos de control de cambios del sistema

Consecuencia: La falta de una Política de Control de cambios puede generar riesgos en la seguridad de las aplicaciones y su funcionalidad porque se pueden afectar funciones y procedimientos vitales para el funcionamiento del IDPC. Este proceso debería incluir una evaluación del riesgo, el análisis de los impactos de los cambios y la especificación de los controles de seguridad necesarios. Este proceso también debería asegurarse de que los procedimientos de seguridad y de control existentes no se vean comprometidos, que a los programadores de apoyo se les da acceso sólo a aquellas partes del sistema necesarias para su trabajo y que se obtiene el acuerdo formal y la aprobación de cualquier cambio.

Plan de Acción: Se debe redactar la política de Control de Cambios, de acuerdo con lo descrito en el numeral 8.32 Procedimientos de control de cambios del sistema de la norma ISO-27001.



##### **1.2.6. A17-Aspectos de la SI en la gestión de la continuidad de la actividad**

Criterio: Numeral 5.29. Seguridad de la Información durante una interrupción.\_La organización debería planificar cómo mantener la SI en un nivel adecuado durante la interrupción.

Condición: A17-5.29-3- ¿Existe un Plan de Continuidad de Negocio?

Causa: No se tiene un Plan de Continuidad de negocio BCP porque no se cuenta con los recursos técnicos, financieros y humanos para su elaboración, prueba e implementación.

Consecuencia: No tener un BCP puede afectar a continuidad de las actividades y procesos del IDPC. sistemas de gestión de continuidad de negocio de la organización.

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 31 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

Plan de Acción: Se debe elaborar el BCP de acuerdo con las mejores metodologías y guías existentes en la industria para luego hacer pruebas y simulaciones, teniendo en cuenta las limitaciones de recursos financieros, técnicos y humanos.

Criterio: Numeral 5.29. Seguridad de la Información durante una interrupción. La organización debería planificar cómo mantener la SI en un nivel adecuado durante la interrupción.

Condición: A17-5.29-4-Se debe tener evidencia de las pruebas piloto realizadas en caso de caída total del sistema. Evidencia del último simulacro realizado y documentación de las lecciones aprendidas.

Causa: No se tiene evidencias de las pruebas realizadas del DRP.

Consecuencia: No hacer los simulacros de contingencia puede llevar a una parálisis de las actividades del IDPC. Si se realizan simulacros o ensayos, se puede tener información de las fallas y/o de los puntos fuertes para enfrentar una emergencia y también para evaluar la reacción del elemento humano ante una situación inesperada.

Plan de Acción: Se deben realizar las pruebas y simulacros del DRP, generar las memorias para tomar las acciones correctivas a que haya lugar.

Criterio: Numeral 8.14. Redundancia de las instalaciones de tratamiento de información. Las instalaciones de procesamiento de información deberían implementarse con redundancia suficiente para satisfacer los requisitos de disponibilidad.



Condición: A17-8.14-7-Las instalaciones de procesamiento de información deberían tener la redundancia suficiente para asegurar la disponibilidad del servicio.

Causa: No se cuenta con la suficiente capacidad de redundancia para atender una contingencia o emergencia debido a la limitación de recursos financieros, técnicos y humanos.

Consecuencia: Si no se cuenta con un esquema de redundancia adecuado para el IDPC, se puede afectar los procesos críticos del IDPC.

Plan de Acción: Se debe hacer un estudio para determinar cuál es la capacidad de redundancia adecuada para el IDPC, sin incurrir en demasiados costos financieros, técnicos y humanos. Pero si se debe buscar alternativas para garantizar una redundancia acorde con los recursos disponible del IDPC.



	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 32 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

**Criterio:** Numeral 8.14. Redundancia de las instalaciones de tratamiento de información. Las instalaciones de procesamiento de información deberían implementarse con redundancia suficiente para satisfacer los requisitos de disponibilidad.

**Condición:** ~~A17-8.14-8~~-Se debería tener la opción de computación en la nube para disponer de varias versiones en directo de las instalaciones de procesamiento de información, que existen en varias ubicaciones físicas independientes con FAILOVER automático.

**Causa:** No se tiene disponible la opción de computación en la nube como medida de mitigación en caso de una emergencia, debido a la estrechez de los recursos con que dispone el IDPC.

**Consecuencia:** No tener esquemas o sistemas de Redundancia de las instalaciones de tratamiento de información, puede afectar los procesos misionales, críticos del IDPC.

**Plan de Acción:** Analizar los esquemas de computación en la nube para disponer de varias versiones en directo de las instalaciones de procesamiento de información, que existen en varias ubicaciones físicas independientes con FAILOVER r automático. Esta alternativa constituye una herramienta valiosa y útil para mitigar los riesgos en caso de una contingencia grave.

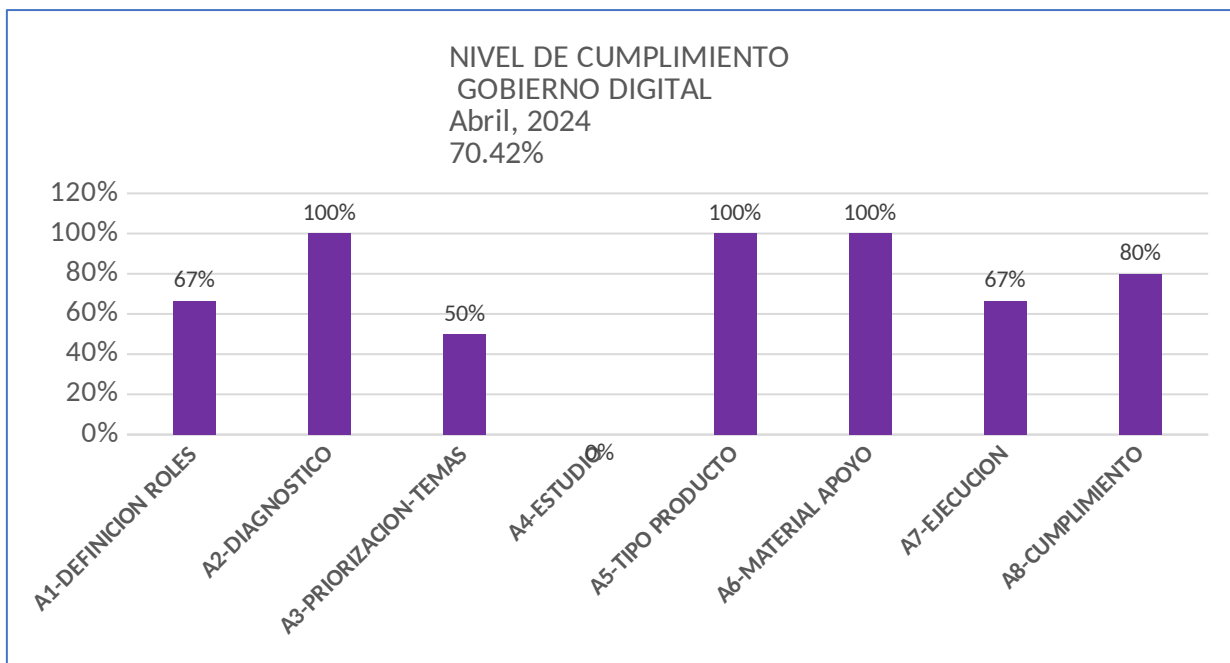
## 2. POLITICA DE GOBIERNO DIGITAL

La Auditoria se hizo bajo el marco de referencia de las normas y directrices que ha dado Ministerio de Tecnologías de la Información y Comunicaciones de Colombia. Se revisaron 40 archivos de evidencias para comprobar que los controles existen y son eficaces. Se hizo una cuantificación de los controles de la siguiente forma:

1. Verificar que el control exista y sea efectivo puntaje 1
2. Si el control no existe el puntaje es 0
3. Si el control existe, pero no es efectivo 0
4. La escala es 1 a 100

De acuerdo con la cuantificación que se hizo, el nivel de cumplimiento es 70.42% cuya grafica se muestra a continuación:






El detalle de las evidencias analizadas, se muestran a continuación:

- 28 evidencias son satisfactorias, es decir los controles están funcionando adecuadamente
- 11 hallazgos, lo cual significa que los controles no existen
- 1 evidencia que **Cumple Parcialmente**, por lo tanto, su evaluación como **Oportunidades de Mejora**. Es decir que el control existe, pero no está funcionando en forma eficaz y por tanto requiere un ajuste o mejora para mitigar el riesgo asociado y lograr el funcionamiento de eficacia que se requiere.

No.	Proceso	FECHA DE ENTREGA 10:AM	Total Evidencias Recibidas	% Analizado	CONTROL EXISTE	CONTROL NO EXISTE	SI EXISTE PERO NO ES EFECTIVO
A1	A1-DEFINICION ROLES	21/mar/2024	3	100%	2	1	0
A2	A2-DIAGNOSTICO	21/mar/2024	2	100%	2	0	0
A3	A3-PRIORIZACION-TEMAS	21/mar/2024	4	100%	2	2	0
A4	A4-ESTUDIO	22/mar/2024	2	100%	0	2	0
A5	A5-TIPO PRODUCTO	22/mar/2024	3	100%	3	0	0
A6	A6-MATERIAL APOYO	22/mar/2024	1	100%	1	0	0
A7	A7-EJECUCION	22/mar/2024	15	100%	10	4	1
A8	A8-CUMPLIMIENTO	04/abr/2024	10	100%	8	2	0
<b>TOTAL</b>			<b>40</b>	<b>100%</b>	<b>28</b>	<b>11</b>	<b>1</b>
					EFECTIVAS	HALLAZGOS	OPORTUNIDAD DE MEJORA

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 34 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

Durante el desarrollo de la auditoría y al revisar cada una de las 40 evidencias entregadas, se encontró el cumplimiento parcial de la ejecución de un control, por lo cual se recomienda desarrollar la siguiente **Oportunidad de Mejora** para lograr la efectividad del control.

## 2.1. Detalle de observación

### 2.1.1. A7-Ejecución

Descripción: A7-14-Están definidas las funciones del área de control interno para el desarrollo de acciones, métodos y procedimientos de control y de gestión del riesgo en la implementación de la política de Gobierno Digital.

Observación: Es necesario definir los roles y responsabilidades del área de Control Interno para el programa de Gobierno Digital.

Cumplimiento Parcial: La evidencia cumple parcialmente porque NO ESTAN definidos los roles y responsabilidades del área de Control Interno para el programa de Gobierno Digital.

## 2.2. Detalle de las No conformidades / incumplimientos



Durante el desarrollo de la auditoría de Gobierno Digital y al revisar cada una de las 40 evidencias entregadas, se encontraron once [11] hallazgos en la ejecución de los controles, por lo cual se recomienda desarrollar las siguientes Planes de Acción para lograr la efectividad de los controles.

A continuación, se hace una presentación de las no-conformidades o hallazgos, partiendo de un nivel global o general y luego se va mostrando con más detalle para que sea más fácil su análisis y corrección. Esto es similar a un esquema de Drill-Down.

Es de anotar, que corrigiendo un tema global se pueden corregir varias no-conformidades, esto es, que de acuerdo con la estructura de la evaluación de la Política de Gobierno Digital dado por el Ministerio de Tecnologías de la Información y Comunicaciones de Colombia, se aborda el análisis de un control en diferentes dominios de la política.

Aunque pueden ser demasiados hallazgos o no conformidades, se recomienda mirar a nivel de proceso para que sea más fácil su corrección o ajuste. Los temas globales sobre las cuales se encontraron los hallazgos son los siguientes:

1. Definición de Roles y funciones.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 35 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

2. Capacitación.
3. Retroalimentación, acompañamiento y asesoría del MinTIC.
4. Análisis de riesgo.
5. Autodiagnóstico y evaluación de la implementación.

Las no conformidades encontradas se resumen y se consolidan en los siguientes temas de la Política de Gobierno Digital.

### 2.2.1. A1-Definición Roles

Criterio: Definición de los roles. Definir roles y compromisos en la entidad: detallar el liderazgo y responsabilidad del CIO en el despliegue de la política e identificar quién será el líder de Gobierno Digital en la entidad.

Condición: A1-2- Quien es el líder del Programa de Gobierno Digital en la entidad.

Causa: No se tiene asignado un Líder de la Política de Gobierno Digital en el IDPC.

Consecuencia: El no tener un Líder del Programa de Gobierno Digital en la entidad, dificulta la implementación del programa de acuerdo con los lineamientos del Ministerio de Tecnologías de la Información y Comunicaciones de Colombia y eso retrasa el cumplimiento de los objetivos del IDPC relacionado con este programa de Gobierno digital.

Plan de Acción: Se debe nombrar el líder del Gobierno Digital en el IDPC.


### 2.2.2. A3-Priorización Temas

Criterio: Priorizar temas: Priorizar las temáticas a desplegar por parte de la entidad, de acuerdo con las necesidades y capacidades, por ejemplo, cantidad de personas en el equipo, recursos presupuestales, asignación de tiempo, etc.

Condición: A3-1- Se deben definir los perfiles de las personas que están asignadas al equipo de Gobierno Digital.

Causa: No hay personal asignado a la implementación del programa de Gobierno Digital.

Consecuencia: El no contar con personal dedicado exclusivamente a la implementación del programa de Gobierno Digital, causa demora en el proceso de cumplimiento y efectividad de esta iniciativa estatal.

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 36 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

Plan de Acción: Se debe conformar el equipo para la implementación de la Política de Gobierno Digital y definir los perfiles de las personas que se asignen a este equipo. Priorizar temas:

Criterio: Priorizar las temáticas a desplegar por parte de la entidad, de acuerdo con las necesidades y capacidades, por ejemplo, cantidad de personas en el equipo, recursos presupuestales, asignación de tiempo, etc.

Condición: A3-4-Es necesario definir las funciones y asignación de tiempo del personal del IDPC para la implementación de la política de Gobierno Digital.

Causa: No hay personal asignado a la implementación del programa de Gobierno Digital.

Consecuencia: El no contar con personal dedicado exclusivamente a la implementación del programa de Gobierno Digital, causa demora en el proceso de cumplimiento y efectividad de esta iniciativa estatal.

Plan de Acción: Se deben definir las funciones y hacer la asignación de tiempo del personal del IDPC que trabaje exclusivamente para la implementación de la política de Gobierno Digital.

### 2.2.3. A4-Estudio



Criterio: Estudio: Identificar los cursos libres y gratuitos que existen sobre la Política de Gobierno Digital, comenzando por el curso de la nueva política y siguiendo con los cursos de los temas identificados en el paso anterior.

Condición: A4-1-Se han tomado los cursos libres y gratuitos que existen sobre la Política de Gobierno Digital.

Causa: No se han tomado los cursos ya que no se cuenta con Líder de Gobierno Digital, ni tampoco hay personal en propiedad asignado para ejecutar la labor de implementación y crecimiento del Programa de Gobierno Digital al interior del IDPC.

Consecuencia: El no tomar los cursos y capacitación para la implementación del programa de Gobierno Digital, puede causar demora en el proceso de implementación y dificultar el cumplimiento de los servicios e iniciativas que benefician a la comunidad al no poder habilitar más procesos virtuales.

Plan de Acción: Se debe programar y recibir toda la capacitación y asesoría que brinde el MinTIC.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 37 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

criterio: Estudio: Identificar los cursos libres y gratuitos que existen sobre la Política de Gobierno Digital, comenzando por el curso de la nueva política y siguiendo con los cursos de los temas identificados en el paso anterior.

Condición: A4-2- Quienes han tomado la capacitación que brinda el MinTIC sobre la Política de Gobierno Digital.

Causa: No se han tomado los cursos ya que no se cuenta con Líder de Gobierno Digital, ni tampoco hay personal en propiedad asignado para ejecutar la labor de implementación y crecimiento del Programa de Gobierno Digital al interior del IDPC.

Consecuencia: El no tomar los cursos y capacitación para la implementación del programa de Gobierno Digital, puede causar demora en el proceso de implementación y dificultar el cumplimiento de los servicios e iniciativas que benefician a la comunidad al no poder habilitar más procesos virtuales.

Plan de Acción: Seleccionar las personas del IDPC que deben tomar la capacitación que brinda el MinTIC sobre la Política de Gobierno Digital para que el proyecto sea exitoso y este en total concordancia con las políticas dictadas por MinTIC relacionadas con esta iniciativa.

#### **2.2.4. A7-Ejecución**



criterio: Ejecutar y desarrollar: Iniciar el desarrollo del producto tipo: después de revisar el material de ayuda de la Caja de Herramientas, la entidad deberá seguir las instrucciones y recomendaciones allí descritas para desarrollar el producto tipo de su interés.

Condición: A7-3- Se ha solicitado una retroalimentación metodológica por parte del equipo técnico de la Dirección de Gobierno Digital del MinTIC.

Causa: No se ha realizado esta solicitud de una retroalimentación metodológica al equipo técnico de la Dirección de Gobierno Digital del MinTIC, dado que no se cuenta con el personal asignado en el IDPC.

Consecuencia: El no contar con la guía, acompañamiento del Dirección de Gobierno Digital del MinTIC puede desviar o retrasar la implementación de los servicios que el IDPC implemente para mejorar los procesos virtuales que benefician al ciudadano.

Plan de Acción: Solicitar una retroalimentación metodológica por parte del equipo técnico del IDPC a la Dirección de Gobierno Digital del MinTIC. Igualmente, solicitar la

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 38 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

asesoría y acompañamientos necesarios para cumplir cabalmente con los objetivos del programa de Gobierno Digital.

Criterio: Ejecutar y desarrollar: Iniciar el desarrollo del producto tipo: después de revisar el material de ayuda de la Caja de Herramientas, la entidad deberá seguir las instrucciones y recomendaciones allí descritas para desarrollar el producto tipo de su interés.

Condición: A7-4-Se tiene un concepto técnico sobre la aplicabilidad de los lineamientos de la Política de Gobierno Digital por parte del MinTIC.

Causa: No se tiene un concepto técnico sobre la aplicabilidad de los lineamientos de la Política de Gobierno Digital por parte del MinTIC, dado que no se ha recibido la retroalimentación y asesoría, dado que no hay Líder de la Política de Gobierno Digital en el IDPC.

Consecuencia: No contar con la asesoría y acompañamiento del personal experto en la implementación del Programa de Gobierno Digital, pone en peligro la implementación correcta de este programa estatal para la optimización de los procesos virtuales que benefician a la ciudadanía.

Plan de Acción: Solicitar un concepto técnico sobre la aplicabilidad de los lineamientos de la Política de Gobierno Digital por parte del MinTIC.


Criterio: Ejecutar y desarrollar: Iniciar el desarrollo del producto tipo: después de revisar el material de ayuda de la Caja de Herramientas, la entidad deberá seguir las instrucciones y recomendaciones allí descritas para desarrollar el producto tipo de su interés.

Condición: A7-6-No Se ha realizado una campaña de conocimiento con el equipo interno.

Causa: No se ha realizado capacitaciones a la entidad sobre el programa de Gobierno Digital dado que no se tiene asignado y nombrado personal en propiedad para trabajar exclusivamente en la implementación de este programa estatal.

Consecuencia: No contar con las capacitaciones y entrenamiento pone en peligro la implementación correcta de este programa estatal para la optimización de los procesos virtuales que benefician a la ciudadanía.

Plan de Acción: Realizar la divulgación y concientización de la Política de Gobierno digital mediante una campaña de conocimiento con el equipo interno, una vez que se

	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 39 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

tenga el equipo encargado de llevar a cabo la implementación de este programa estatal.

Criterio: Ejecutar y desarrollar: Iniciar el desarrollo del producto tipo: después de revisar el material de ayuda de la Caja de Herramientas, la entidad deberá seguir las instrucciones y recomendaciones allí descritas para desarrollar el producto tipo de su interés.

Condición: A7-9-Se ha hecho un análisis de riesgo de la implementación de la política de Gobierno Digital.

Causa: No se ha hecho un análisis de riesgos de implementación de la política de gobierno digital. Una vez se conforme el equipo responsable de implementar la Política de Gobierno Digital, se debe hacer un análisis de riesgos y vulnerabilidades de acuerdo con la metodología interna del IDPC.

Consecuencia: No hacer un análisis de riesgo en la implementación de la política de Gobierno Digital, deja una exposición y un vacío que puede comprometer la seguridad de la información de este proceso.

Plan de Acción: Ejecutar análisis de riesgo de la implementación de la política de Gobierno Digital, de acuerdo con la metodología interna del IDPC.

### **2.2.5. A8-Cumplimiento**

Criterio: Muéstranos tu producto terminado: Remitir el producto tipo desarrollado para recibir una retroalimentación metodológica por parte del equipo técnico de la Dirección de Gobierno Digital.

Condición: A8-5-Se debe revisar el estado de implementación del Marco de Referencia de Arquitectura Empresarial: Se debe hacer el proceso de autodiagnóstico disponible en el sitio web del Modelo Integrado de Planeación y Gestión - MIPG7.

Causa: No se ha aplicado el formato de autodiagnóstico, que es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.

Consecuencia: Si no hace los procesos de evaluación y diagnóstico no es posible saber si el proceso de implementación está en concordancia con los lineamientos dados por MinTIC en relación con el programa de Gobierno Digital.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</p>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 40 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

**Plan de Acción:** Se debe hacer una revisión del estado de implementación del Marco de Referencia de Arquitectura Empresarial. Se debe aplicar el formato de autodiagnóstico disponible en el sitio web del Modelo Integrado de Planeación y Gestión - MIPG7, de acuerdo con las directrices dadas por MinTIC relacionado con la implementación del Programa de Gobierno Digital.

**Criterio:** Muéstranos tu producto terminado: Remitir el producto tipo desarrollado para recibir una retroalimentación metodológica por parte del equipo técnico de la Dirección de Gobierno Digital.

**Condición:** A8-7-Se ha solicitado o recibido acompañamiento desde la Dirección de Gobierno Digital del MinTIC.

**Causa:** No se ha solicitado o recibido acompañamiento desde la Dirección de Gobierno Digital del MinTIC.

**Consecuencia:** El no contar con el acompañamiento, asesoría, capacitación y procesos de acompañamiento que ha definido el MinTIC para el programa de Gobierno Digital, puede demorar y dificultar el logro de los objetivos y resultados de este programa.

**Plan de Acción:** Es necesario solicitar todo el acompañamiento, asesoría, capacitación y procesos de acompañamiento que ha definido el MinTIC para el programa de Gobierno Digital.

## CONCLUSIONES DE AUDITORÍA

De acuerdo con la información detallada que se muestra en este informe, estas son las conclusiones de la auditoría:

1. Los niveles de cumplimiento tanto de seguridad de la información, 79.27%, como de la Política de Gobierno Digital 70.42%, son buenos, pero no son los óptimos esperados, y reflejan el gran esfuerzo de todo el personal de empleados y contratistas en lograr el cumplimiento de los controles relacionados con la Seguridad de la información y el cumplimiento de implementación de la Política de Gobierno Digital.
2. El nivel y rigurosidad de la auditoría del análisis y evaluación que se aplicó en esta auditoría obedece a las mejores prácticas y normas internacionales, por lo cual se entrega un detalle muy completo de los hallazgos y oportunidades de mejora para que se facilite su corrección o aplicación.



	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 41 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

3. La corrección de las no conformidades debe incluir el análisis de la no conformidad, la elaboración y redacción de los manuales o políticas requeridas y finalmente la implementación y ejecución de lo descrito en los documentos que se elaboren.
4. Se pudo evidenciar que los recursos financieros, técnicos y humanos están muy ajustados, pero aun así se están cumpliendo los objetivos de control.
5. Se debe mantener el nivel de compromiso y liderazgo del Área de Gestión de Sistemas y Tecnologías de la Información para que se mejore los niveles de cumplimiento relacionados con la seguridad de la información y el cumplimiento de implementación de la Política de Gobierno Digital.
6. No se detectaron casos o eventos que comprometan la seguridad de la información, pero si es importante efectuar a la mayor brevedad posible los planes de remediación de las no-conformidades detectadas y atender las recomendaciones presentadas como Oportunidades de Mejora.


## RECOMENDACIONES

Las recomendaciones de esta auditoria para mejorar el Sistema de Gestión de Seguridad de la Información SGSI y una exitosa implementación y cumplimiento de la Política de Gobierno Digital son las siguientes:

1. Es importante contar con el apoyo y liderazgo de la Alta Dirección del IDPC para mejorar los niveles de cumplimiento tanto con el Sistema de Gestión de Seguridad de la Información SGSI como la Política de Gobierno Digital.
2. Analizar y mejorar los planes de contingencia y continuidad del negocio de acuerdo con las necesidades y recursos del IDPC.
3. Asignar a la mayor brevedad posible la asignación del personal con la suficiente experiencia y conocimiento en el manejo de la Política de Gobierno Digital.
4. Dado el permanente cambio en las áreas de tecnología de la información, incrementar los procesos de capacitación y actualización para todo el personal del IDPC.
5. Apoyar con la asignación de los recursos financieros, técnicos y humanos para mejorar los niveles de cumplimiento de Sistema de Gestión de Seguridad de la Información SGSI y la Política de Gobierno Digital.

<b>Documento 20241200083623 firmado electrónicamente por:</b>	
<b>ELEANA MARCELA PÁEZ</b>	Asesora de Control Interno Control Interno

 <b>ALCALDÍA MAYOR DE BOGOTÁ D.C.</b> <small>CULTURA, RECREACIÓN Y DEPORTE Instituto Distrital de Patrimonio Cultural</small>	<b>INSTITUTO DISTRITAL DE PATRIMONIO CULTURAL</b>	 Radicado: <b>20241200083623</b> Fecha: 20-05-2024 Pág. 42 de 42
	<b>SEGUIMIENTO Y EVALUACIÓN</b>	
	<b>INFORME DE AUDITORÍA</b>	

<b>URREGO</b>	Fecha firma: 20-05-2024 19:26:42
<b>Proyectó:</b>	JOSÉ GUILLERMO BENAVIDES GONZÁLEZ - Contratista - Control Interno
 8dc118ee54b14da42af9abe7a8811d62294108b91ffd1704403dc98db2ce36a5 Codigo de Verificación CV: 099e1	