	INFORME DE ACTIVIDADES DEL CONTRATISTA Y RECIBO A SATISFACCIÓN DEL SUPERVISOR	Código del Documento	PGAF-06 Versión 9
		Código del Formato	PGAF-06-03 Versión 1.0

1. IDENTIFICACIÓN

CONTRATO/CONVENIO:	DE PRESTACIÓN DE SERVICIOS	**NÚMERO DE CONTRATO**	036-2025	**VIGENCIA**	2025		
OBJETO CONTRACTUAL	Prestar servicios profesionales especializados para apoyar la gestión de la Dirección de Planeación de la Contraloría de Bogotá D.C.			**DEPENDENCIA**	DIRECCION DE PLANEACION		
CONTRATISTA	JOHANN MILLER ARCE RUBIO	**TIPO DE IDENTIFICACIÓN**	CÉDULA DE CIUDADANÍA	**NÚMERO DE IDENTIFICACIÓN**	80.038.894		
CONTRATISTA CESIONARIO	N/A	**TIPO DE IDENTIFICACIÓN**	N/A	**NÚMERO DE IDENTIFICACIÓN**	N/A		

PLAZO DE EJECUCIÓN DEL CONTRATO										
PLAZO INICIAL	**FECHA DE INICIO**			**FECHA INICIO CESIÓN** (SI APLICA)			**FECHA DE TERMINACIÓN INICIAL**			
Cinco (5) meses Dieciséis (16) dias	**DÍA**	**MES**	**AÑO**	**DÍA**	**MES**	**AÑO**	**DÍA**	**MES**	**AÑO**	
	16	ENERO	2025	N/A	N/A	N/A	30	JUNIO	2025	
PLAZO PRORROGADO	**FECHA DE INICIO (PRORRÓGA 1)**			**FECHA DE INICIO (PRORRÓGA 2)**			**FECHA DE INICIO (PRORRÓGA 3)**			
Tres (3) meses	**DÍA**	**MES**	**AÑO**	**DÍA**	**MES**	**AÑO**	**DÍA**	**MES**	**AÑO**	
	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	
PLAZO TOTAL	**FECHA DE INICIO SUSPENSIÓN**			**FECHA DE REINICIO SUSPENSIÓN**			**FECHA DE TERMINACIÓN** (tenga en cuenta prórrogas y suspensiones)			
Cinco (5) meses Dieciséis (16) dias	**DÍA**	**MES**	**AÑO**	**DÍA**	**MES**	**AÑO**	**DÍA**	**MES**	**AÑO**	
	N/A	N/A	N/A	N/A	N/A	N/A	30	JUNIO	2025	

2. DATOS PARA EL PAGO

RÉGIMEN CONTRATISTA Y/O PROVEEDOR	☐ NO RESPONSABLE DE IVA ☐ GRAN CONTRIBUYENTE ☑ RESPONSABLE DE IVA ☐ AUTORRETENEDOR ☑ DECLARANTE DE RENTA ☐ N.A ☐ OTRO				**REQUIERE INGRESO A ALMACÉN**	N/A	

	REGISTRO PRESUPUESTAL	**REGISTRO PRESUPUESTAL ADICIÓN 1**	**REGISTRO PRESUPUESTAL ADICIÓN 2**	**REGISTRO PRESUPUESTAL ADICIÓN 3**
NÚMERO REGISTRO PRESUPUESTAL	35	N/A	N/A	N/A
DESCRIPCIÓN DEL RUBRO (CONCEPTO DEL GASTO PARA CONTRATOS DE PROYECTOS DE INVERSIÓN)	O21202020080383990 - Otros servicios profesionales, técnicos y empresariales n.c.p.	N/A	N/A	N/A

VALOR DEL CONTRATO	**CONTRATO**	**ADICIÓN 1 (Si la hubiere)**	**ADICIÓN 2 (Si la hubiere)**	**ADICIÓN 3 (Si la hubiere)**	**VALOR TOTAL DEL CONTRATO**
	$ 38.733.333	N/A	N/A	N/A	**$ 38.733.333**

TIPO DE PAGO	PAGO PARCIAL	**NÚMERO DE PAGO**	2	**TIPO DE PERSONA**	NATURAL	**TIPO DOCUMENTO**	FACTURA	**NÚMERO**	JM24
VALOR MENSUAL A PAGAR (PERSONAS NATURALES)	**$ 7.000.000**	**VALOR SIN IVA**	$ 5.882.353	**IVA**	$ 1.117.647	**VALOR A PAGAR (PERSONAS JURÍDICAS)**	N/A	**VALOR DIARIO**	**$ 233.333**
DATOS PARA CONSIGNACIÓN	**TPO DE CUENTA**	CORRIENTE	**NÚMERO DE CUENTA**	288070964	**BANCO**	BANCO DE OCCIDENTE			

PERIODO Y VALOR DEL PAGO	**DEL**			**AL**			**VALOR**	
	DÍA	**MES**	**AÑO**	**DÍA**	**MES**	**AÑO**	**DÍAS A COBRAR**	30
	1	FEBRERO	2025	28	FEBRERO	2025	**$ 7.000.000**	

VALOR EJECUTADO DEL CONTRATO	**$ 3.500.000**	**TERMINACIÓN ANTICIPADA O REQUIERE LIQUIDACIÓN (SI APLICA)**	**DÍA**	**MES**	**AÑO**	**SALDO A FAVOR DEL CONTRATISTA**	**N/A**
SALDO DEL CONTRATO	**$ 28.233.333**		N/A	N/A	N/A	**SALDO A LIBERAR A FAVOR DE LA ENTIDAD**	**N/A**

* EN CASO DE REQUERIR MÁS FILAS PARA RUBROS PRESUPUESTALES Y SU VALOR, AL IGUAL QUE DISTRIBUCIÓN POR CONCEPTO DE GASTO SE PUEDE AÑADIR TANTAS COMO SE NECESITE
** EN CASO DE REQUERIR MAS COLUMNAS PARA LA SECCIÓN DE ADICIONES, SE PUEDEN AÑADIR TANTAS COMO SE NECESITEN ; DIVIDENDO LA COLUMNA "ADICIÓN" LAS VECES QUE SEAN NECESARIAS

3. DETALLE DE PAGO SEGURIDAD SOCIAL Y OTROS PARA DISMINUCIÓN DE BASE GRAVABLE (APLICA SOLO PARA PERSONAS NATURALES).

No. PLANILLA	**FECHA DE PAGO PLANILLA**	**PERÍODO COTIZADO**	**PENSIÓN**		**SALUD**		**ARL**	
			ENTIDAD	**VALOR**	**ENTIDAD**	**VALOR**	**ENTIDAD**	**VALOR**
84261580	19/02/2025	FEBRERO	Skandia Pensiones Obligatorias	1.071.000	Salud Total EPS	787.500	POSITIVA	32.900
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

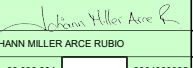
4. TODAS LAS OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA Y ACTIVIDADES REALIZADAS (Ver NOTA Uno).

OBLIGACIONES	**ACTIVIDADES**	**UBICACIÓN DE LAS EVIDENCIAS**
1. Apoyar la ejecución de las actividades derivadas de la estrategia de analítica de datos institucional liderada por la Subdirección de Análisis, Estadísticas e Indicadores.	Se está apoyando de forma continua el proyecto de Alertas Tempranas (definición de alcance técnico y la línea base para la ejecución), Se está trabajando en conjunto con el equipo de tecnología y comunicaciones para realizar el desarrollo de la interfaz con la integración y desarrollo realizada en Power Bi.	https://contraloriadebogotadc-my.sharepoint.com/:f:/g/personal/planeacion_contraloriabogota_gov_co/EvtO4MmQvq5HmrFJEG0jhuABs75aYQqhKHAu26bB3kY6tw?e=jZTaTQ
2. Apoyar los procesos de mejora, actualización y divulgación de los tableros de control desarrollados por la Subdirección de Análisis, Estadísticas e Indicadores.	Se realizó mejoras y actualizaciones al dashboard de mallas de contratación para los seguimientos pertinentes y uso en auditorias.	https://contraloriadebogotadc-my.sharepoint.com/:f:/g/personal/planeacion_contraloriabogota_gov_co/Er0j1gC2q7xAuBu7BXbf2jYByR9Opyg395tgd9zvnGJwFg?e=XnQRQZ
3. Participar activamente en las reuniones, mesas de trabajo, talleres o cualquier otro escenario que se requiera, según las orientaciones del supervisor del contrato.	Se participó en las sesiones convocadas por el equipo de trabajo.	https://contraloriadebogotadc-my.sharepoint.com/:f:/g/personal/planeacion_contraloriabogota_gov_co/Er_fhGaac5EsRLcWSo-kbMBGNHU_xUZ6z48cK4ezoZhWA?e=uvSW66
4. Asistir a los espacios que convoque la Entidad con el fin de orientar las acciones relacionadas con los procesos administrativos, logísticos y de gestión de información de la Contraloría de Bogotá.	Se realizo actualizaciones sobre el documento de Gobierno de Datos.	https://contraloriadebogotadc-my.sharepoint.com/:f:/g/personal/planeacion_contraloriabogota_gov_co/EvuYYeTikwFNvzKsMt5-XKgBgI7yK1IkVLAKATEqXMBvg?e=MtDQkZ

* EN CASO DE REQUERIR MÁS FILAS PARA LAS OBLIGACIONES Y LAS ACTIVIDADES SE PUEDE AÑADIR TANTAS COMO SE NECESITE O ELIMINAR LAS QUE NO SEAN NECESARIAS

Certifico que el contratista en mención, se encuentra al día en los pagos de Aportes al Sistema de Seguridad Social y/o Parafiscales, y que realice la verificación y consistencia de la información de cada uno de los documentos soportes para adelantar el respectivo pago del contrato/convenio y que los mismos se generaron por el cumplimiento del contratista/asociado a entera satisfacción en el período de ejecución certificado y de conformidad con lo establecido en el objeto y obligaciones contractuales y demás normas aplicables.

Expedido en Bogotá D.C , el **lunes, 3 de marzo de 2025**

CONTRATISTA Y/O PROVEEDEOR				**SUPERVISOR Y/O INTERVENTOR DE CONTRATO**				**APOYO A LA SUPERVISIÓN DE CONTRATO (en caso de aplicar)**			
FIRMA				**FIRMA**				**FIRMA**	**N/A**		
NOMBRE	JOHANN MILLER ARCE RUBIO			**NOMBRE**	ANA MARIA OCHOA VILLEGAS			**NOMBRE**			
No. IDENTIFICACIÓN	80.038.894	**TELF O CEL**	3004009005	**No. IDENTIFICACIÓN**	1.013.579.678		3007618180	**No. IDENTIFICACIÓN**			
CORREO	jmarce@contraloriabogota.gov.co			**CARGO**	SUBDIRECTORA TÉCNICA	**DEPENDENCIA**	SUBDIRECCION DE ANALISIS, ESTADISTICAS E INDICADORES	**CARGO**			

Outlook

RE: Seguimiento Integración de servicios | Políticas Contraloría de Bogotá Proyecto Alertas Tempranas

Desde JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>
Fecha Lun 24/02/2025 15:34
Para Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>
CC Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <MBarrientos@martinexsa.com>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>

Buenas Tardes:

Apreciado Ing. Johann Miller gracias por la información, el equipo valido pero informa que aún no se pueden crear los recursos, les agradezco el apoyo y gestión.

Atte.

José Alfonso García T
Program Manager
Proyecto Contraloría Alertas Tempranas
e-mail jose.garciat.telefonica@fractaliasystems.es
Cel: 3164729458

De: Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>
Enviado: lunes, 24 de febrero de 2025 13:18
Para: JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; JUAN CARLOS HERRERA CEBALLOS <j.herrera@telefonica.com>; mbarrientos@martinexsa.com <MBarrientos@martinexsa.com>
Cc: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>
Asunto: RV: Seguimiento Integración de servicios | Políticas Contraloría de Bogotá Proyecto Alertas Tempranas

Buenas tardes ing José Alfonso

las políticas fueron aplicadas de acuerdo a la cadena de correos,por favor validar

Quedo atento a los comentarios.

Cordialmente,

Ing. Johann Miller Arce Rubio
SUBDIRECCION DE ANALISIS, ESTADISTICAS E INDICADORES

De: Roberto Trillos <roberto.trillos@bmind.com>
Enviado: lunes, 24 de febrero de 2025 13:10
Para: Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Alvaro Fernando Vallejo Moran <avallejo@contraloriabogota.gov.co>
Cc: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Luz Sarmiento <luz.sarmiento@bmind.com>
Asunto: RE: Seguimiento Integración de servicios | Políticas Contraloría de Bogotá Proyecto Alertas Tempranas

Buenas tardes

Por favor validar, que la mayoría de los servicios y permisos no son correctos en la sintaxis.

Estoy buscando las listas de referencias para aplicar los permisos y compartir con ustedes las mismas.

Atentamente,

Roberto Trillos

Consultor Principal

roberto.trillos@bmind.com

+57 301 1268357

De: Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>
Enviado: jueves, 20 de febrero de 2025 16:14

Para: Alvaro Fernando Vallejo Moran <avallejo@contraloriabogota.gov.co>; Roberto Trillos <roberto.trillos@bmind.com>; Julián Díaz <julian.diaz@bmind.com>
Cc: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>
Asunto: RV: Seguimiento Integración de servicios | Políticas Contraloría de Bogotá Proyecto Alertas Tempranas

Buenas tardes ing Roberto

Solicitamos tu apoyo para que ayudarnos con la validación y configuración de las políticas de acceso para el proyecto de Alertas Tempranas.

Políticas de acceso según el diagrama de arquitectura.

```
########################################
# Archivo de Políticas IAM - Arquitectura Sistema de Alertas Tempranas v2
# Reemplazar pre_altemp con el nombre de tu compartimento
########################################

########################################
# 1. Políticas para OCI Data Science
########################################
# Permite a OCI Data Science gestionar funciones en OCI Functions
allow service oracle.datascience to manage functions-family in compartment pre_altemp

# Permite a OCI Data Science gestionar Object Storage (acceso a archivos CSV, Excel, etc.)
allow service oracle.datascience to manage object-family in compartment pre_altemp

# Permite a OCI Data Science consumir eventos de OCI Events
allow service oracle.datascience to use events-family in compartment pre_altemp

# Permite a OCI Data Science gestionar Autonomous Data Warehouse, si es parte de la integración
allow service oracle.datascience to manage autonomousdwh-family in compartment pre_altemp

########################################
# 2. Políticas para OCI Data Integrator
########################################
# Permite a OCI Data Integrator gestionar Object Storage (para extracción y carga de datos desde fuentes como SharePoint, CSV, Excel)
allow service oracle.dataintegrator to manage object-family in compartment pre_altemp
```

```
# Permite a OCI Data Integrator gestionar OCI Events para publicar o reaccionar a eventos de integración
allow service oracle.dataintegrator to manage events-family in compartment pre_altemp

# Permite a OCI Data Integrator gestionar notificaciones si emite alertas en el proceso de integración
allow service oracle.dataintegrator to manage notifications-family in compartment pre_altemp

########################################
# 3. Políticas para OCI Data Flow
########################################
# Permite a OCI Data Flow gestionar funciones en OCI Functions (para ejecutar procesos o transformar datos)
allow service oracle.dataflows to manage functions-family in compartment pre_altemp

# Permite a OCI Data Flow gestionar Object Storage (para lectura y escritura de datos intermedios)
allow service oracle.dataflows to manage object-family in compartment pre_altemp

# Permite a OCI Data Flow consumir eventos de OCI Events
allow service oracle.dataflows to use events-family in compartment pre_altemp

########################################
# 4. Políticas para Oracle Autonomous Data Warehouse (DWH)
########################################
# Permite integrar el Autonomous DWH en la arquitectura de explotación de datos.
allow service oracle.autonomousdwh to manage dwh-family in compartment pre_altemp

# Permite que el Autonomous DWH consuma eventos de OCI Events (si requiere reaccionar a disparadores)
allow service oracle.autonomousdwh to use events-family in compartment pre_altemp

########################################
# 5. Políticas para OCI Functions
########################################
# Permite a OCI Functions gestionar notificaciones (Notifications Service) para emitir alertas y mensajes
allow service oracle.functions to manage notifications-family in compartment pre_altemp

# Permite a OCI Functions gestionar Email Delivery para enviar correos electrónicos
allow service oracle.functions to manage emaildelivery-family in compartment pre_altemp

# Permite a OCI Functions gestionar eventos en OCI Events (para emitir o reaccionar ante eventos en la arquitectura)
```

allow service oracle.functions to manage events-family in compartment pre_altemp

##
6. Políticas Generales para Consumir OCI Events
##
Estas políticas complementan el acceso a eventos para otros servicios que deban suscribirse o reaccionar a ellos.
allow service oracle.datascience to use events-family in compartment pre_altemp
allow service oracle.dataflows to use events-family in compartment pre_altemp
allow service oracle.autonomousdwh to use events-family in compartment pre_altemp
allow service oracle.dataintegrator to use events-family in compartment pre_altemp

Quedo atento a los comentarios.

Cordialmente,

Ing. Johann Miller Arce Rubio
SUBDIRECCION DE ANALISIS, ESTADISTICAS E INDICADORES

De: JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>
Enviado: miércoles, 19 de febrero de 2025 19:27
Para: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>
Cc: Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; DARIO EDILBRANDO ORTIZ ARAQUE <dario.ortiz@telefonica.com>; MARTHA LILIANA AMORTEGUI SAAVEDRA <martha.amortegui@telefonica.com>; Julio Cordero <JCordero@martinexsa.com>; Jorge Miguel Bohl Jop <jmbohl@martinexsa.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Mario Francisco Barrientos Alejos <MBarrientos@martinexsa.com>
Asunto: Seguimiento Integración de servicios | Políticas Contraloría de Bogotá Proyecto Alertas Tempranas

Buenas Tardes:

Apreciada Vanessa agradezco su apoyo y gestión para resolver las siguientes inquietudes que tiene el equipo referente a la implementación de las siguientes políticas para finalizar la integración de los diferentes servicios, esto lo deben gestionar con Oracle:

Políticas de acceso según el diagrama de arquitectura.

##
Archivo de Políticas IAM - Arquitectura Sistema de Alertas Tempranas v2
Reemplazar pre_altemp con el nombre de tu compartimento

```
########################################

########################################
# 1. Políticas para OCI Data Science
########################################
# Permite a OCI Data Science gestionar funciones en OCI Functions
allow service oracle.datascience to manage functions-family in compartment pre_altemp

# Permite a OCI Data Science gestionar Object Storage (acceso a archivos CSV, Excel, etc.)
allow service oracle.datascience to manage object-family in compartment pre_altemp

# Permite a OCI Data Science consumir eventos de OCI Events
allow service oracle.datascience to use events-family in compartment pre_altemp

# Permite a OCI Data Science gestionar Autonomous Data Warehouse, si es parte de la integración
allow service oracle.datascience to manage autonomousdwh-family in compartment pre_altemp

########################################
# 2. Políticas para OCI Data Integrator
########################################
# Permite a OCI Data Integrator gestionar Object Storage (para extracción y carga de datos desde fuentes como SharePoint, CSV, Excel)
allow service oracle.dataintegrator to manage object-family in compartment pre_altemp

# Permite a OCI Data Integrator gestionar OCI Events para publicar o reaccionar a eventos de integración
allow service oracle.dataintegrator to manage events-family in compartment pre_altemp

# Permite a OCI Data Integrator gestionar notificaciones si emite alertas en el proceso de integración
allow service oracle.dataintegrator to manage notifications-family in compartment pre_altemp

########################################
# 3. Políticas para OCI Data Flow
########################################
# Permite a OCI Data Flow gestionar funciones en OCI Functions (para ejecutar procesos o transformar datos)
allow service oracle.dataflows to manage functions-family in compartment pre_altemp

# Permite a OCI Data Flow gestionar Object Storage (para lectura y escritura de datos intermedios)
allow service oracle.dataflows to manage object-family in compartment pre_altemp
```

Permite a OCI Data Flow consumir eventos de OCI Events
allow service oracle.dataflows to use events-family in compartment pre_altemp

##
4. Políticas para Oracle Autonomous Data Warehouse (DWH)
##
Permite integrar el Autonomous DWH en la arquitectura de explotación de datos.
allow service oracle.autonomousdwh to manage dwh-family in compartment pre_altemp

Permite que el Autonomous DWH consuma eventos de OCI Events (si requiere reaccionar a disparadores)
allow service oracle.autonomousdwh to use events-family in compartment pre_altemp

##
5. Políticas para OCI Functions
##
Permite a OCI Functions gestionar notificaciones (Notifications Service) para emitir alertas y mensajes
allow service oracle.functions to manage notifications-family in compartment pre_altemp

Permite a OCI Functions gestionar Email Delivery para enviar correos electrónicos
allow service oracle.functions to manage emaildelivery-family in compartment pre_altemp

Permite a OCI Functions gestionar eventos en OCI Events (para emitir o reaccionar ante eventos en la arquitectura)
allow service oracle.functions to manage events-family in compartment pre_altemp

##
6. Políticas Generales para Consumir OCI Events
##
Estas políticas complementan el acceso a eventos para otros servicios que deban suscribirse o reaccionar a ellos.
allow service oracle.datascience to use events-family in compartment pre_altemp
allow service oracle.dataflows to use events-family in compartment pre_altemp
allow service oracle.autonomousdwh to use events-family in compartment pre_altemp
allow service oracle.dataintegrator to use events-family in compartment pre_altemp

Agradezco confirmar cuando se encuentren implementadas.

Atte.

José Alfonso García T
Program Manager
Proyecto Contraloria Alertas Tempranas
e-mail jose.garciat.telefonica@fractaliasystems.es
Cel: 3164729458

De: JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>
Enviado: lunes, 10 de febrero de 2025 12:09
Para: vanarango@contraloriabogota.gov.co <vanarango@contraloriabogota.gov.co>
Cc: Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; DARIO EDILBRANDO ORTIZ ARAQUE <dario.ortiz@telefonica.com>; MARTHA LILIANA AMORTEGUI SAAVEDRA <martha.amortegui@telefonica.com>; Julio Cordero <JCordero@martinexsa.com>; Jorge Miguel Bohl Jop <jmbohl@martinexsa.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Mario Francisco Barrientos Alejos <MBarrientos@martinexsa.com>
Asunto: RE: Seguimiento Solicitud VPN Site to Site Proyecto Contraloría de Bogotá Proyecto Alertas Tempranas

Buenos Días:

Apreciada Vanessa Luego de confirmada el día **viernes 7 de febrero** la creación correcta de la VPN Site-to-Site, los siguientes pasos son:

- Para poder iniciar con la ingesta, necesitamos que Contraloria complete el formulario de ingestas que ya habíamos compartido (adjunto)
- En paralelo, independiente al formulario, para poder hacer ingestas necesitamos que nos den algunos permisos ajustando algunas políticas a nivel del servicio de OCI Data Integration. A continuación el detalle del error y lo que necesitamos del lado del Contraloria/Oracle.:

Validando las flujos de integración se requieren crear las siguientes políticas para que el WORKSPACE de ODI pueda visualizar todos los componentes del COMPARTMENT, se solicita a Contraloria configurar las políticas (IAM) y privilegios necesarios en nuestra cuenta de **Oracle Cloud Infrastructure (OCI)** para que el grupo **`odi_dev_prealtemp (crear este grupo y agregar al usuario)`** y el servicio de **Data Integration** (DIS Workspace) puedan operar correctamente en el *compartment* **`pre_altemp`**.
Nota: crear el grupo odi_dev_prealtemp para que sea a través de ese grupo que se tengan los privilegios solicitados.
A continuación, detallo las políticas que se requiere implementar:

1. **En el root compartment (Tenancy)**
   allow group odi_dev_prealtemp to inspect compartments in tenancy

- Permite al grupo `odi_dev_prealtemp` visualizar (inspect) los compartments dentro de la tenancy.
- **En el compartment `pre_altemp`**
  - **Servicio Data Integration**:
    allow service `dataintegration` to use virtual-network-family in compartment pre_altemp

- **Permisos para usuarios no administradores**:
  - `allow group odi_dev_prealtemp to manage dis-workspaces in compartment pre_altemp`
  - `allow group odi_dev_prealtemp to manage dis-work-requests in compartment pre_altemp`
  - `allow group odi_dev_prealtemp to use virtual-network-family in compartment pre_altemp`
  - `allow group odi_dev_prealtemp to manage tag-namespaces in compartment pre_altemp`
  - `allow group odi_dev_prealtemp to inspect instance-family in compartment pre_altemp`

- **Para usar Object Storage**:
  - `allow group odi_dev_prealtemp to use object-family in compartment pre_altemp`
  - `allow any-user to use buckets in compartment pre_altemp`
  - `where ALL {request.principal.type='disworkspace', request.principal.id='ocid1.disworkspace.oc1.sa-bogota-1.anrgcljr2ow634ya6kk5k2ovc5btfzcxu7s2eapfyoa4sjp7ae23lxgj55nq'}`
  - `allow any-user to manage objects in compartment pre_altemp`
  - `where ALL {request.principal.type='disworkspace', request.principal.id='ocid1.disworkspace.oc1.sa-bogota-1.anrgcljr2ow634ya6kk5k2ovc5btfzcxu7s2eapfyoa4sjp7ae23lxgj55nq'}`

- **Para usar Autonomous Database (ADW/ATP) como destino**:
  - `allow any-user {PAR_MANAGE} in compartment pre_altemp`
  - `where ALL {request.principal.type='disworkspace', request.principal.id='ocid1.disworkspace.oc1.sa-bogota-1.anrgcljr2ow634ya6kk5k2ovc5btfzcxu7s2eapfyoa4sjp7ae23lxgj55nq'}`

Motivo de la solicitud

- El grupo `odi_dev_prealtemp` requiere crear y administrar Workspaces de Data Integration y sus *work requests* en el compartimento `pre_altemp`.
- El servicio de Data Integration (DIS Workspace) necesita acceso a redes (VCN, subnets), Object Storage (para leer y/o escribir objetos) y la posibilidad de generar *Pre-Authenticated Requests (PAR)* que permite cargar datos a Autonomous Database y Object Storage.

Agradecemos su apoyo y gestión para que apliquen dichas políticas a la brevedad. Si requieren más información o tienen alguna duda adicional, no duden en hacérnoslo saber.

Atte.

José Alfonso García T
Program Manager
Proyecto Contraloria Alertas Tempranas
e-mail jose.garciat.telefonica@fractaliasystems.es
Cel: 3164729458

De: JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>
Enviado: martes, 21 de enero de 2025 08:24

Para: vanarango@contraloriabogota.gov.co <vanarango@contraloriabogota.gov.co>
Cc: Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; DARIO EDILBRANDO ORTIZ ARAQUE <dario.ortiz@telefonica.com>; MARTHA LILIANA AMORTEGUI SAAVEDRA <martha.amortegui@telefonica.com>; Julio Cordero <JCordero@martinexsa.com>; Jorge Miguel Bohl Jop <jmbohl@martinexsa.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Mario Francisco Barrientos Alejos <MBarrientos@martinexsa.com>
Asunto: RE: Seguimiento Solicitud VPN Site to Site Proyecto Contraloría de Bogotá Proyecto Alertas Tempranas

Buenos Días:

Apreciada Vanessa comparto información relevante y quedo atento a los comentarios.

Se realizaron las siguientes actividades:

- Creación de la Autonomous Database DWH en el compartment pre_altemp con el nombre: PREALTEMP
- Creación del Object Storage en el compartment pre_altemp con el nombre: bucket-files-prealtemp

Se notifica que el usuario en OCI proporcionado no tiene todos los privilegios solicitados.

Unauthorized access
To create a workspace, you must have some required policies. If you don't have permission to create these policies, your tenancy administrator should create them for you.

Por lo que es importante que nos den los privilegios previamente solicitados. Comparto los pasos para resolver el error:

Pasos para Resolver el Error

1. Validar que el usuario provisto esté en un grupo

- Validar que tu usuario esté asignado a un grupo en OCI. Puedes verificar esto en:
  - Consola de OCI > **Identity & Security** > **Users** > Selecciona tu usuario > **Groups**.

2. Políticas necesarias para Data Integration

Para crear un workspace en OCI Data Integration, el grupo al que pertenece el usuario necesita las siguientes políticas:
Allow group <GROUP_NAME> to manage integration-instance-family in compartment <COMPARTMENT_NAME>
Allow group <GROUP_NAME> to manage data-integration-family in compartment <COMPARTMENT_NAME>

Detalles de las políticas:

- **integration-instance-family**: Permite administrar los recursos relacionados con el servicio de integración, como los workspaces.
- **data-integration-family**: Permite gestionar los recursos dentro del servicio de integración de datos.

3. Solicitar al Administrador del Tenancy

Si no tienes permisos para crear o modificar políticas, debes contactar al **Administrador del Tenancy** (usualmente el rol Administrators en OCI) y pedir que creen estas políticas por ti.

Ejemplo de Configuración de Políticas

Se tiene un grupo que se llama DataIntegrationUsers y el compartimento donde quieres crear el workspace es pre_altemp. El administrador debe agregar las siguientes políticas:
Allow group DataIntegrationUsers to manage integration-instance-family in compartment MyCompartment
Allow group DataIntegrationUsers to manage data-integration-family in compartment pre_altemp
Con esto podríamos continuar con la creación del Oracle Data Integration.

Atte.

José Alfonso García T
Program Manager
Proyecto Redsumma Contraloria de Bogota Alertas Tempranas
e-mail jose.garciat.telefonica@fractaliasystems.es
Cel: 3164729458

De: JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>
Enviado: jueves, 16 de enero de 2025 09:45
Para: vanarango@contraloriabogota.gov.co <vanarango@contraloriabogota.gov.co>
Cc: Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; DARIO EDILBRANDO ORTIZ ARAQUE <dario.ortiz@telefonica.com>; MARTHA LILIANA AMORTEGUI SAAVEDRA <martha.amortegui@telefonica.com>; Julio Cordero <JCordero@martinexsa.com>; Jorge Miguel Bohl Jop <jmbohl@martinexsa.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Mario Francisco Barrientos Alejos <MBarrientos@martinexsa.com>
Asunto: Seguimiento Solicitud VPN Site to Site Proyecto Contraloría de Bogotá Proyecto Alertas Tempranas

Buenos Días:

Apreciada Vanessa agradezco el apoyo y gestión para la creación de la **VPN Site to Site** la cual fue informada en el comité del pasado martes **14 de enero de 2025**, adjunto la información y quedo atento al avance.

Lo anterior a fin de dar continuidad a la fase de despliegue.

Adjunto una plantilla en Excel la cual contiene los parámetros requeridos del lado del equipo de redes, esto con el objetivo de poder configurar la conectividad con la red de OCI. La plantilla está construida de la siguiente forma:

- Categoría: Se describe la parte específica de la configuración que requiere información.
- Parámetro: Se define el elemento específico que necesitas del administrador.
- Descripción: Se explica por qué se requiere el parámetro o qué representa.
- Ejemplo: Se proporciona un valor de referencia para que el administrador sepa qué tipo de datos debe suministrar.

La pestaña a llenar por parte del equipo de redes es: ***Registro-NetInfo***

Tareas realizadas.

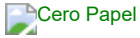
1. Creación de la VCN: vcn_pre_altemp con el IPv4 CIDR Block: **10.0.0.0/16** **(Compartir con el equipo de redes) dentro del Compartment: pre_altemp**
2. Creación de las subredes:
    1. net-pub-pre con el IPv4 CIDR Block: 10.0.1.0/24
    2. net-priv-pre con el IPv4 CIDR Block: 10.0.2.0/24

Nota: Una vez obtenida la información de la plantilla de excel se procederá a realizar la configuración de la VPN Site to Site bajo este modelo:

Los demás servicios se desplegarán posterior a tener la configuración de la VPN site to site para el tema de la conectividad con la base de datos de SQL Server y así evitar el consumo de créditos previo a esta configuración.

Atte.

José Alfonso García T
Program Manager
Proyecto Redsumma Contraloría de Bogotá Alertas Tempranas
e-mail jose.garciat.telefonica@fractaliasystems.es
Cel: 3164729458



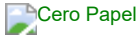
AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..



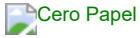
AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en

consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Outlook

Re: Seguimiento Solicitud VPN Site to Site Proyecto Contraloría de Bogotá Proyecto Alertas Tempranas

Desde Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>
Fecha Mar 18/02/2025 20:49
Para JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>
CC Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; DARIO EDILBRANDO ORTIZ ARAQUE <dario.ortiz@telefonica.com>; MARTHA LILIANA AMORTEGUI SAAVEDRA <martha.amortegui@telefonica.com>; Julio Cordero <JCordero@martinexsa.com>; Jorge Miguel Bohl Jop <jmbohl@martinexsa.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Mario Francisco Barrientos Alejos <MBarrientos@martinexsa.com>

3 archivos adjuntos (745 KB)

2. CBO - Inventario Ingesta Incremental 11022025 (CONTRABOG).xlsx; 3. Informacion Tablas SAEI_CONTRATACION.xlsx; 1. script_Base de datos Contraloria.sql;

Buenas noches

Remito plantilla "CBO - Inventario Ingesta Incremental" actualizada con las tablas que se debe ingestar.

También remito

1. Excel con las tablas, su estructura y una muestra de los datos.
2. archivo sql con el schema completo de SQL SERVER donde están las tablas y sus estructuras a nivel de detalle.

Quedo atento a los comentarios.

Cordialmente,

Ing. Johann Miller Arce Rubio
SUBDIRECCION DE ANALISIS, ESTADISTICAS E INDICADORES

De: JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>
Enviado: martes, 11 de febrero de 2025 14:02
Para: Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>

Cc: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; DARIO EDILBRANDO ORTIZ ARAQUE <dario.ortiz@telefonica.com>; MARTHA LILIANA AMORTEGUI SAAVEDRA <martha.amortegui@telefonica.com>; Julio Cordero <JCordero@martinexsa.com>; Jorge Miguel Bohl Jop <jmbohl@martinexsa.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Mario Francisco Barrientos Alejos <MBarrientos@martinexsa.com>
Asunto: RE: Seguimiento Solicitud VPN Site to Site Proyecto Contraloría de Bogotá Proyecto Alertas Tempranas

Buenas Tardes:

Apreciado Ing. Johann Miller gracias por la información, ya solicite al equipo la revisión y validación.

Atte.

José Alfonso García T
Program Manager
Proyecto Contraloría Alertas Tempranas
e-mail jose.garciat.telefonica@fractaliasystems.es
Cel: 3164729458

De: Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>
Enviado: martes, 11 de febrero de 2025 13:57
Para: JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>; Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>
Cc: Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; DARIO EDILBRANDO ORTIZ ARAQUE <dario.ortiz@telefonica.com>; MARTHA LILIANA AMORTEGUI SAAVEDRA <martha.amortegui@telefonica.com>; Julio Cordero <JCordero@martinexsa.com>; Jorge Miguel Bohl Jop <jmbohl@martinexsa.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Mario Francisco Barrientos Alejos <MBarrientos@martinexsa.com>
Asunto: Re: Seguimiento Solicitud VPN Site to Site Proyecto Contraloría de Bogotá Proyecto Alertas Tempranas

Buenas tardes

Se crea el grupo y las políticas solicitadas.

Por favor validar.

Quedo atento a los comentarios.

Cordialmente,

Ing. Johann Miller Arce Rubio

SUBDIRECCION DE ANALISIS, ESTADISTICAS E INDICADORES

De: JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>
Enviado: lunes, 10 de febrero de 2025 12:09
Para: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>
Cc: Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; DARIO EDILBRANDO ORTIZ ARAQUE <dario.ortiz@telefonica.com>; MARTHA LILIANA AMORTEGUI SAAVEDRA <martha.amortegui@telefonica.com>; Julio Cordero <JCordero@martinexsa.com>; Jorge Miguel Bohl Jop <jmbohl@martinexsa.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Mario Francisco Barrientos Alejos <MBarrientos@martinexsa.com>
Asunto: RE: Seguimiento Solicitud VPN Site to Site Proyecto Contraloría de Bogotá Proyecto Alertas Tempranas

Buenos Días:

Apreciada Vanessa Luego de confirmada el día **viernes 7 de febrero** la creación correcta de la VPN Site-to-Site, los siguientes pasos son:

- Para poder iniciar con la ingesta, necesitamos que Contraloria complete el formulario de ingestas que ya habíamos compartido (adjunto)
- En paralelo, independiente al formulario, para poder hacer ingestas necesitamos que nos den algunos permisos ajustando algunas políticas a nivel del servicio de OCI Data Integration. A continuación el detalle del error y lo que necesitamos del lado del Contraloria/Oracle.:

Validando las flujos de integración se requieren crear las siguientes políticas para que el WORKSPACE de ODI pueda visualizar todos los componentes del COMPARTMENT, se solicita a Contraloria configurar las políticas (IAM) y privilegios necesarios en nuestra cuenta de **Oracle Cloud Infrastructure (OCI)** para que el grupo **`odi_dev_prealtemp (crear este grupo y agregar al usuario)`** y el servicio de **Data Integration** (DIS Workspace) puedan operar correctamente en el *compartment* **`pre_altemp`**.
Nota: crear el grupo odi_dev_prealtemp para que sea a través de ese grupo que se tengan los privilegios solicitados.
A continuación, detallo las políticas que se requiere implementar:

1. **En el root compartment (Tenancy)**
   allow group odi_dev_prealtemp to inspect compartments in tenancy

- Permite al grupo `odi_dev_prealtemp` visualizar (inspect) los compartments dentro de la tenancy.
- **En el compartment `pre_altemp`**

  - **Servicio Data Integration**:
    allow service `dataintegration` to use virtual-network-family in compartment pre_altemp

  - **Permisos para usuarios no administradores**:
    - `allow group odi_dev_prealtemp to manage dis-workspaces in compartment pre_altemp`
    - `allow group odi_dev_prealtemp to manage dis-work-requests in compartment pre_altemp`
    - `allow group odi_dev_prealtemp to use virtual-network-family in compartment pre_altemp`
    - `allow group odi_dev_prealtemp to manage tag-namespaces in compartment pre_altemp`
    - `allow group odi_dev_prealtemp to inspect instance-family in compartment pre_altemp`

- **Para usar Object Storage**:
  - `allow group odi_dev_prealtemp to use object-family in compartment pre_altemp`
  - `allow any-user to use buckets in compartment pre_altemp`
  - `where ALL {request.principal.type='disworkspace', request.principal.id='ocid1.disworkspace.oc1.sa-bogota-1.anrgcljr2ow634ya6kk5k2ovc5btfzcxu7s2eapfyoa4sjp7ae23lxgj55nq'}`
  - `allow any-user to manage objects in compartment pre_altemp`
  - `where ALL {request.principal.type='disworkspace', request.principal.id='ocid1.disworkspace.oc1.sa-bogota-1.anrgcljr2ow634ya6kk5k2ovc5btfzcxu7s2eapfyoa4sjp7ae23lxgj55nq'}`

- **Para usar Autonomous Database (ADW/ATP) como destino**:
  - `allow any-user {PAR_MANAGE} in compartment pre_altemp`
  - `where ALL {request.principal.type='disworkspace', request.principal.id='ocid1.disworkspace.oc1.sa-bogota-1.anrgcljr2ow634ya6kk5k2ovc5btfzcxu7s2eapfyoa4sjp7ae23lxgj55nq'}`

Motivo de la solicitud

- El grupo `odi_dev_prealtemp` requiere crear y administrar Workspaces de Data Integration y sus *work requests* en el compartimento `pre_altemp`.
- El servicio de Data Integration (DIS Workspace) necesita acceso a redes (VCN, subnets), Object Storage (para leer y/o escribir objetos) y la posibilidad de generar *Pre-Authenticated Requests (PAR)* que permite cargar datos a Autonomous Database y Object Storage.

Agradecemos su apoyo y gestión para que apliquen dichas políticas a la brevedad. Si requieren más información o tienen alguna duda adicional, no duden en hacérnoslo saber.

Atte.

José Alfonso García T
Program Manager
Proyecto Contraloria Alertas Tempranas
e-mail jose.garciat.telefonica@fractaliasystems.es
Cel: 3164729458

De: JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>
Enviado: martes, 21 de enero de 2025 08:24
Para: vanarango@contraloriabogota.gov.co <vanarango@contraloriabogota.gov.co>
Cc: Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; DARIO EDILBRANDO ORTIZ ARAQUE <dario.ortiz@telefonica.com>; MARTHA LILIANA AMORTEGUI SAAVEDRA <martha.amortegui@telefonica.com>; Julio Cordero <JCordero@martinexsa.com>; Jorge Miguel Bohl Jop <jmbohl@martinexsa.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Mario Francisco Barrientos Alejos <MBarrientos@martinexsa.com>
Asunto: RE: Seguimiento Solicitud VPN Site to Site Proyecto Contraloría de Bogotá Proyecto Alertas Tempranas

Buenos Días:

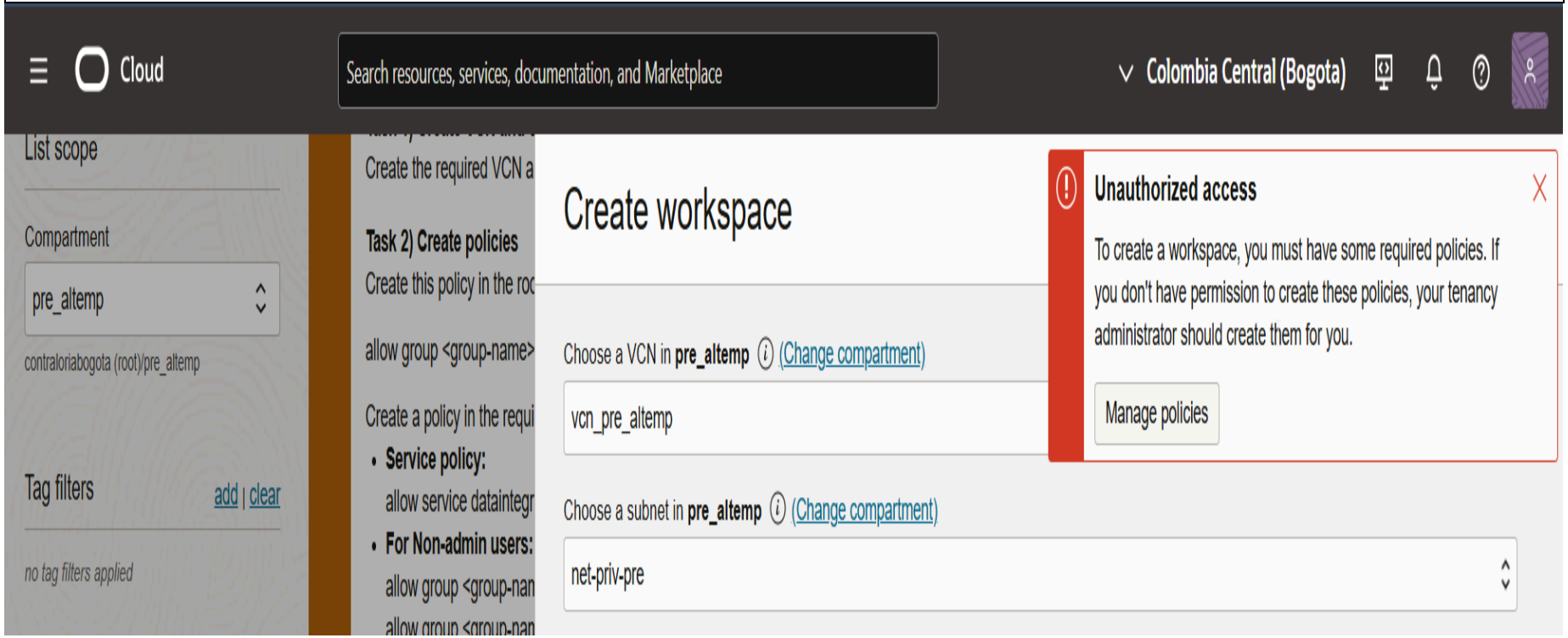
Apreciada Vanessa comparto información relevante y quedo atento a los comentarios.

Se realizaron las siguientes actividades:

- Creación de la Autonomous Database DWH en el compartment pre_altemp con el nombre: PREALTEMP
- Creación del Object Storage en el compartment pre_altemp con el nombre: bucket-files-prealtemp

Se notifica que el usuario en OCI proporcionado no tiene todos los privilegios solicitados.

Unauthorized access
To create a workspace, you must have some required policies. If you don't have permission to create these policies, your tenancy administrator should create them for you.



Por lo que es importante que nos den los privilegios previamente solicitados. Comparto los pasos para resolver el error:

Pasos para Resolver el Error

1. Validar que el usuario provisto esté en un grupo

- Validar que tu usuario esté asignado a un grupo en OCI. Puedes verificar esto en:
  - Consola de OCI > **Identity & Security** > **Users** > Selecciona tu usuario > **Groups**.

2. Políticas necesarias para Data Integration

Para crear un workspace en OCI Data Integration, el grupo al que pertenece el usuario necesita las siguientes políticas:
Allow group <GROUP_NAME> to manage integration-instance-family in compartment <COMPARTMENT_NAME>
Allow group <GROUP_NAME> to manage data-integration-family in compartment <COMPARTMENT_NAME>

Detalles de las políticas:

- **integration-instance-family**: Permite administrar los recursos relacionados con el servicio de integración, como los workspaces.
- **data-integration-family**: Permite gestionar los recursos dentro del servicio de integración de datos.

3. Solicitar al Administrador del Tenancy

Si no tienes permisos para crear o modificar políticas, debes contactar al **Administrador del Tenancy** (usualmente el rol Administrators en OCI) y pedir que creen estas políticas por ti.

Ejemplo de Configuración de Políticas

Se tiene un grupo que se llama DataIntegrationUsers y el compartimento donde quieres crear el workspace es pre_altemp. El administrador debe agregar las siguientes políticas:
Allow group DataIntegrationUsers to manage integration-instance-family in compartment MyCompartment
Allow group DataIntegrationUsers to manage data-integration-family in compartment pre_altemp
Con esto podríamos continuar con la creación del Oracle Data Integration.

Atte.

José Alfonso García T
Program Manager

Proyecto Redsumma Contraloria de Bogota Alertas Tempranas
e-mail jose.garciat.telefonica@fractaliasystems.es
Cel: 3164729458

De: JOSE ALFONSO GARCIA TIBADUIZA <jose.garciat.telefonica@fractaliasystems.es>
Enviado: jueves, 16 de enero de 2025 09:45
Para: vanarango@contraloriabogota.gov.co <vanarango@contraloriabogota.gov.co>
Cc: Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; DARIO EDILBRANDO ORTIZ ARAQUE <dario.ortiz@telefonica.com>; MARTHA LILIANA AMORTEGUI SAAVEDRA <martha.amortegui@telefonica.com>; Julio Cordero <JCordero@martinexsa.com>; Jorge Miguel Bohl Jop <jmbohl@martinexsa.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Mario Francisco Barrientos Alejos <MBarrientos@martinexsa.com>
Asunto: Seguimiento Solicitud VPN Site to Site Proyecto Contraloría de Bogotá Proyecto Alertas Tempranas

Buenos Días:

Apreciada Vanessa agradezco el apoyo y gestión para la creación de la **VPN Site to Site** la cual fue informada en el comité del pasado martes **14 de enero de 2025**, adjunto la información y quedo atento al avance.

Lo anterior a fin de dar continuidad a la fase de despliegue.

Adjunto una plantilla en Excel la cual contiene los parámetros requeridos del lado del equipo de redes, esto con el objetivo de poder configurar la conectividad con la red de OCI. La plantilla está construida de la siguiente forma:

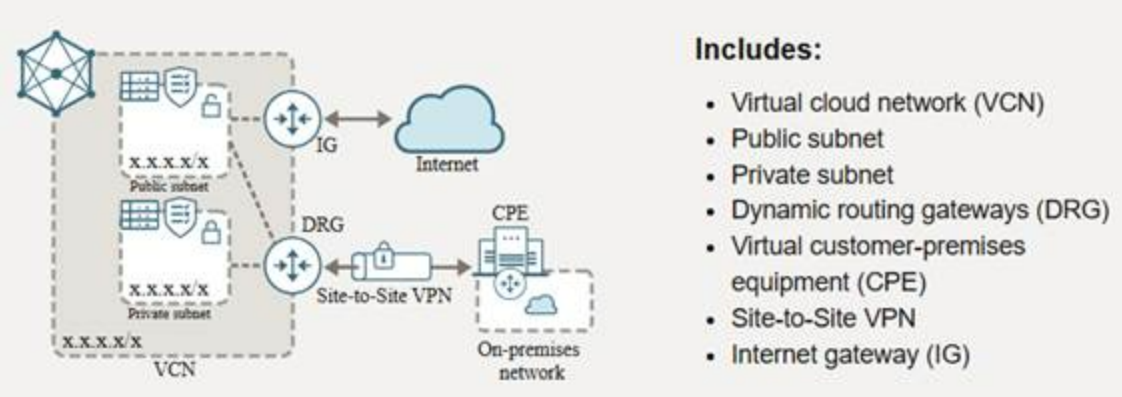
- Categoría: Se describe la parte específica de la configuración que requiere información.
- Parámetro: Se define el elemento específico que necesitas del administrador.
- Descripción: Se explica por qué se requiere el parámetro o qué representa.
- Ejemplo: Se proporciona un valor de referencia para que el administrador sepa qué tipo de datos debe suministrar.

La pestaña a llenar por parte del equipo de redes es: ***Registro-NetInfo***

Tareas realizadas.

1. Creación de la VCN: vcn_pre_altemp con el IPv4 CIDR Block: **10.0.0.0/16** **(Compartir con el equipo de redes) dentro del Compartment: pre_altemp**
2. Creación de las subredes:
    1. net-pub-pre con el IPv4 CIDR Block: 10.0.1.0/24
    2. net-priv-pre con el IPv4 CIDR Block: 10.0.2.0/24

Nota: Una vez obtenida la información de la plantilla de excel se procederá a realizar la configuración de la VPN Site to Site bajo este modelo:



Los demás servicios se desplegarán posterior a tener la configuración de la VPN site to site para el tema de la conectividad con la base de datos de SQL Server y así evitar el consumo de créditos previo a esta configuración.

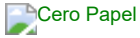
Atte.

José Alfonso García T
Program Manager
Proyecto Redsumma Contraloría de Bogotá Alertas Tempranas
e-mail jose.garciat.telefonica@fractaliasystems.es
Cel: 3164729458

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Outlook

Re: Validación técnica Sistema de Alertas

Organizer	Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>
Hora de la reunión	Este evento ocurrió hace 1 semana (Mar 18/02/2025, 'de' 17:00 a 18:00)
Ubicación	Reunión de Microsoft Teams
Mi respuesta	Aún no respondido
Asistentes requeridos	Vanessa Arango Cano, jcordero@martinexsa.com, Johann Miller Arce Rubiano, jmbohl@martinexsa.com, jose.garciat.telefonica@fractaliasystems.es, Javier Tafur Díaz, mbarrientos@martinexsa.com
Asistentes opcionales	Johann Miller Arce Rubio
Mensaje enviado	Mar 18/02/2025 18:52

2 archivos adjuntos (73 KB)

Querys.txt; datos diferentes en ingesta.xlsx;

Buenas noches,

Realizamos validación de la ingesta encontrados dos temas principales.
1. falta actualizar el inventario de tablas a ingestar con base a que yo envié menos de las que habíamos presupuestado inicialmente
2. hay diferencia en datos ingestados, con relevancia en la tabla de contratos en las columnas VALOR_SAEI y ID_CONTRATISTA_SAEI
(Adjuntamos archivos del ejercicio de verificación)

Quedo atento a los comentarios.

Cordialmente,

Ing. Johann Miller Arce Rubio
SUBDIRECCION DE ANALISIS, ESTADISTICAS E INDICADORES

De: Vanessa Arango Cano
Enviado: martes, 18 de febrero de 2025 9:21
Para: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jcordero@martinexsa.com <jcordero@martinexsa.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es

<jose.garciat.telefonica@fractaliasystems.es>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>
Cc: Johann Miller Arce Rubio <johannmillerarce@gmail.com>
Asunto: Validación técnica Sistema de Alertas
Cuándo: martes, 18 de febrero de 2025 05:00 p. m.-06:00 p. m..
Dónde: Reunión de Microsoft Teams

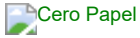
Microsoft Teams Need help?

Join the meeting now

Meeting ID: 234 987 966 375

Passcode: Qi9aM97x

For organizers: Meeting options



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of

CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Outlook

RE: Reporte de extemporáneos e inconsistencias

Desde Julian David Moya Benavides <jmoya@ContraloriadeBogotaDC.onmicrosoft.com>
Fecha Vie 21/02/2025 10:03
Para Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>

2 archivos adjuntos (72 KB)
EXTEMPORÁNEOS DIRECCIÓN DE PARTICIPACIÓN CIUDADANA Y DESARROLLO LOCAL.xlsx; INCONSISTENCIAS DIRECCIÓN DE PARTICIPACIÓN CIUDADANA Y DESARROLLO LOCAL.xlsx;

Buen día Johan,

La tabla que se utiliza exactamente, desde acá no tengo acceso, pero es la misma que se utiliza para actualizar el tablero de contratación; y adjunto encuentras los archivos solicitados.

Cordialmente,
Julian Moya.

De: Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>
Enviado: viernes, 21 de febrero de 2025 6:13
Para: Julian David Moya Benavides <jmoya@ContraloriadeBogotaDC.onmicrosoft.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>
Asunto: Re: Reporte de extemporáneos e inconsistencias

Hola Juli,

muchas gracias por la información, unos datos adicionales

1. sobre que tablas haces la consulta?
2. nos puedes compartir un archivo de extemporaneos
3. nos puedes compartir un archivo de inconsistencias

Quedo atento a los comentarios.

Cordialmente,

Ing. Johann Miller Arce Rubio
SUBDIRECCION DE ANALISIS, ESTADISTICAS E INDICADORES

De: Julian David Moya Benavides <jmoya@ContraloriadeBogotaDC.onmicrosoft.com>
Enviado: jueves, 20 de febrero de 2025 16:06
Para: Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>
Asunto: Reporte de extemporáneos e inconsistencias

Cordial saludo para tod@s,

Adjunto envío el archivo relacionado en el asunto.

Cordialmente,
Julian Moya.


Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..


Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Febrero 2025

Calendario

Martes, 04 de Febrero de 2025

Seguimiento Sistema de Alertas Tempranas-Contraloría de Bogotá

Mar 04/02/2025, 'de' 9:00 a 10:00

Ubicación: Microsoft Teams Meeting
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; j.herrera@telefonica.com <j.herrera@telefonica.com>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>; jcordero@martinexsa.com <jcordero@martinexsa.com>; martha.amortegui@telefonica.com <martha.amortegui@telefonica.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; Luis Armando Sánchez Oliveros <lsanchez@contraloriabogota.gov.co>; Alvaro Fernando Vallejo Moran <avallejo@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 262 575 300 925

Passcode: uX3fS9tW

For organizers: Meeting options

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Viernes, 07 de Febrero de 2025

Bases De Datos Sistema De Alertas

Vie 07/02/2025, 'de' 8:00 a 8:30

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams ¿Necesita ayuda?

Unirse a la reunión ahora

Id. de reunión: 227 723 698 073

Código de acceso: iM7UX72d

Para organizadores: Opciones de la reunión

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Configuración VPN-Sistema De Alertas

Vie 07/02/2025, 'de' 9:00 a 10:00

Ubicación: Reunión de Microsoft Teams

Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; julian.diaz@bmind.com <julian.diaz@bmind.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Alvaro Fernando Vallejo Moran <avallejo@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jcordero@martinexsa.com <jcordero@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; Luis Armando Sánchez Oliveros <lsanchez@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams ¿Necesita ayuda?

Unirse a la reunión ahora

Id. de reunión: 238 581 691 95

Código de acceso: Pu7CF3g8

Para organizadores: Opciones de la reunión

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this

message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Lunes, 10 de Febrero de 2025

Reunión virtual pasos a seguir observatorio

Lun 10/02/2025, 'de' 10:00 a 10:30

Ubicación: Reunión de Microsoft Teams
Organizador: Ana María Ochoa Villegas
Asistentes obligatorios: Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Laura Catalina Barrera Rocha <lbarrera@contraloriabogota.gov.co>; Juliana Revollo Balseiro <jrevollo@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams ¿Necesita ayuda?

Unirse a la reunión ahora

Id. de reunión: 238 533 864 225

Código de acceso: Jh6RR6iq

Para organizadores: Opciones de la reunión

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Virtual - Priorización temas observatorio

Lun 10/02/2025, 'de' 10:30 a 11:30

Ubicación: Reunión de Microsoft Teams
Organizador: Ana María Ochoa Villegas
Asistentes obligatorios: Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>; Juliana Revollo Balseiro <jrevollo@contraloriabogota.gov.co>;

Matriz de inventarios
Priorización temas para desarrollo de tablero
Pasos a seguir para estructura observatorio

Microsoft Teams ¿Necesita ayuda?

Unirse a la reunión ahora

Id. de reunión: 254 579 155 712

Código de acceso: Pv9Q9ms7

Para organizadores: Opciones de la reunión

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Revisión modulo Power BI funcional

Lun 10/02/2025, 'de' 14:30 a 15:00

Ubicación: Reunión de Microsoft Teams
Organizador: Kevin Alejandro Garzón Corredor
Asistentes obligatorios: Kevin Alejandro Garzón Corredor <kgarzon@contraloriabogota.gov.co>; Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams ¿Necesitas ayuda?

Unirse a la reunión ahora

Id. de reunión: 241 980 569 187

Código de acceso: 3Z9GF3QH

Para organizadores: Opciones de la reunión



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Martes, 11 de Febrero de 2025

Seguimiento Sistema de Alertas Tempranas-Contraloría de Bogotá

Mar 11/02/2025, 'de' 9:00 a 10:00

Ubicación: Microsoft Teams Meeting
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; j.herrera@telefonica.com <j.herrera@telefonica.com>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>; jcordero@martinexsa.com <jcordero@martinexsa.com>; martha.amortegui@telefonica.com <martha.amortegui@telefonica.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 262 575 300 925

Passcode: uX3fS9tW

For organizers: Meeting options

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this

message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Miércoles, 12 de Febrero de 2025

Observatorio-desarrollo página web

Mié 12/02/2025, 'de' 10:00 a 11:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Kevin Alejandro Garzón Corredor <kgarzon@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 264 255 056 832

Passcode: QC2M5Ny3

For organizers: Meeting options

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Martes, 18 de Febrero de 2025

Seguimiento Sistema de Alertas Tempranas-Contraloría de Bogotá

Mar 18/02/2025, 'de' 9:00 a 10:00

Ubicación: Microsoft Teams Meeting
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; j.herrera@telefonica.com <j.herrera@telefonica.com>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>; jcordero@martinexsa.com <jcordero@martinexsa.com>; martha.amortegui@telefonica.com <martha.amortegui@telefonica.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

[Join the meeting now]

Meeting ID: 262 575 300 925

Passcode: uX3fS9tW

For organizers: Meeting options



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Revisión documento final Manual de Gobierno de Datos

Mar 18/02/2025, 'de' 10:00 a 11:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; Carlos Andres Prada Duran <cprada@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Jorge Orlando Murcia Sequeda <jmurcia@contraloriabogota.gov.co>;

Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>; Ana Milena Contreras Cifuentes <acontreras@contraloriabogota.gov.co>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 231 006 214 009

Passcode: SE75De3Z

For organizers: Meeting options



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Validación técnica Sistema de Alertas

Mar 18/02/2025, 'de' 17:00 a 18:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jcordero@martinexsa.com <jcordero@martinexsa.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 234 987 966 375

Passcode: Qi9aM97x

For organizers: Meeting options



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Miércoles, 19 de Febrero de 2025

Validación técnica Sistema de Alertas

Mié 19/02/2025, 'de' 16:00 a 18:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jcordero@martinexsa.com <jcordero@martinexsa.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 297 654 877 371

Passcode: av3oK3kP

For organizers: Meeting options



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Jueves, 20 de Febrero de 2025

Mesa de trabajo para configuración Micrositio Observatorio

Jue 20/02/2025, 'de' 10:00 a 12:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Kevin Alejandro Garzón Corredor <kgarzon@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams [Need help?]

Join the meeting now

Meeting ID: 254 813 870 858

Passcode: 3T2oi3WW

For organizers: Meeting options

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Validación técnica Sistema de Alertas

Jue 20/02/2025, 'de' 16:00 a 18:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano

Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jcordero@martinexsa.com <jcordero@martinexsa.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams [Need help?]

Join the meeting now

Meeting ID: 297 654 877 371

Passcode: av3oK3kP

For organizers: Meeting options

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information

contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Viernes, 21 de Febrero de 2025

Explicación archivos extemporáneos e inconsistencias

Vie 21/02/2025, 'de' 11:30 a 12:30

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Julian David Moya Benavides <jmoya@ContraloriadeBogotaDC.onmicrosoft.com>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 215 899 815 375

Passcode: DP7U3cY3

For organizers: Meeting options

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Validación técnica Sistema de Alertas

Vie 21/02/2025, 'de' 12:00 a 13:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jcordero@martinexsa.com <jcordero@martinexsa.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 297 654 877 371

Passcode: av3oK3kP

For organizers: Meeting options



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Lunes, 24 de Febrero de 2025

Revisar Planner y Agenda estratégica- Contraloria Sesion fin de mes

Lun 24/02/2025, 'de' 14:00 a 15:00

Ubicación: Microsoft Teams Meeting
Organizador: Johann Miller Arce Rubio
Asistentes obligatorios: Johann Miller Arce Rubio <j.arcer@uniandes.edu.co>; johannmillerarce@gmail.com <johannmillerarce@gmail.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>;

Microsoft Teams ¿Necesitas ayuda?

Unirse a la reunión ahora

Id. de reunión: 263 080 287 477

Código de acceso: Y7zUAu

Unirse en un dispositivo de videoconferencia

Clave de inquilino: uniandes@m.webex.com

Id. de video: 114 900 804 4

Más información

Para organizadores: Opciones de la reunión

Ayuda de la organización | Privacidad y seguridad

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Martes, 25 de Febrero de 2025

Seguimiento Sistema de Alertas Tempranas-Contraloría de Bogotá

Mar 25/02/2025, 'de' 9:00 a 10:00

Ubicación: Microsoft Teams Meeting
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; j.herrera@telefonica.com <j.herrera@telefonica.com>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>; jcordero@martinexsa.com <jcordero@martinexsa.com>; martha.amortegui@telefonica.com <martha.amortegui@telefonica.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 262 575 300 925

Passcode: uX3fS9tW

For organizers: Meeting options

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Sistema de Alertas-sesión técnica

Mar 25/02/2025, 'de' 10:00 a 11:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jcordero@martinexsa.com <jcordero@martinexsa.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>; **Asistentes opcionales:** Johann Miller Arce Rubio <johannmillerarce@gmail.com>; Allan Josue Dueñas <allan.duenas@gmail.com>;

Microsoft Teams [Need help?]

Join the meeting now

Meeting ID: 252 029 447 194

Passcode: 47WT3AP9

For organizers: Meeting options

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Mar 25/02/2025, 'de' 17:00 a 18:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano

Sistema de alertas- verificación ingesta de tablas

Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jcordero@martinexsa.com <jcordero@martinexsa.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 273 655 563 639

Passcode: u6De3Yy9

For organizers: Meeting options



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information

contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Miércoles, 26 de Febrero de 2025

REUNION CONTRATISTAS - PROCEDIMIENTO PARA LA PRESENTACIÓN DE INFORMES Y

RADICACIÓN DE CUENTAS

Mié 26/02/2025, 'de' 8:00 a 8:30

Ubicación: Reunión de Microsoft Teams
Organizador: Sonia Margarita Ontiveros Gil
Asistentes obligatorios: Sonia Margarita Ontiveros Gil <sontiveros@contraloriabogota.gov.co>; anitagiraldo24@gmail.com <anitagiraldo24@gmail.com>; Blanca Deicy Pineda <bdpineda@contraloriabogota.gov.co>; Carlos Javier Rodríguez Ordoñez <crodriguezo@contraloriabogota.gov.co>; diego.apr@hotmail.com <diego.apr@hotmail.com>; Juan Diego Chiquiza Nivia <jchiquiza@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Julian David Moya Benavides <jmoya@ContraloriadeBogotaDC.onmicrosoft.com>; Juliana Revollo Balseiro <jrevollo@contraloriabogota.gov.co>; Laura Catalina Barrera Rocha <lbarrera@contraloriabogota.gov.co>; Luisa Fernanda Castro Torres <lfcastro@contraloriabogota.gov.co>; Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>;

_____

Microsoft Teams ¿Necesitas ayuda?

Unirse a la reunión ahora

Id. de reunión: 283 354 460 543

Código de acceso: up3Ay2aT

Para organizadores: Opciones de la reunión



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Diseño gráfico Observatorio de Vigilancia y Control

Mié 26/02/2025, 'de' 9:00 a 10:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Andres Mauricio Valencia Ramirez <amvalencia@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Kevin Alejandro Garzón Corredor <kgarzon@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams [Need help?]

Join the meeting now

Meeting ID: 275 808 957 316

Passcode: sT7MG2Bo

For organizers: Meeting options



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Jueves, 27 de Febrero de 2025

Sistema de Alertas-sesión técnica

Jue 27/02/2025, 'de' 16:00 a 17:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jcordero@martinexsa.com <jcordero@martinexsa.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 271 589 642 549

Passcode: rh2i3w7r

For organizers: Meeting options



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Viernes, 28 de Febrero de 2025

Preparación plan de trabajo tableros priorizados Power BI Observatorio

Vie 28/02/2025, 'de' 10:00 a 10:30

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Ana María Ochoa Villegas <aochoa@contraloriabogota.gov.co>; José Tobías Infante Morales <jinfantem@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 217 572 212 961

Passcode: Kj6YY2tv

For organizers: Meeting options

Cero Papel

AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Preparación repositorio sistema de alertas

Vie 28/02/2025, 'de' 11:00 a 12:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>;

Microsoft Teams Need help?

Join the meeting now

Meeting ID: 271 296 288 493

Passcode: s9CK2QR3

For organizers: Meeting options

Cero Papel
AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

Sistema de Alertas- Producto mínimo viable

Vie 28/02/2025, 'de' 14:00 a 16:00

Ubicación: Reunión de Microsoft Teams
Organizador: Vanessa Arango Cano
Asistentes obligatorios: Vanessa Arango Cano <vanarango@contraloriabogota.gov.co>; jcordero@martinexsa.com <jcordero@martinexsa.com>; Johann Miller Arce Rubiano <jmarce@contraloriabogota.gov.co>; jmbohl@martinexsa.com <jmbohl@martinexsa.com>; jose.garciat.telefonica@fractaliasystems.es <jose.garciat.telefonica@fractaliasystems.es>; Javier Tafur Díaz <jtafur@contraloriabogota.gov.co>; mbarrientos@martinexsa.com <mbarrientos@martinexsa.com>;
Asistentes opcionales: Johann Miller Arce Rubio <johannmillerarce@gmail.com>; Allan Josue Dueñas <allan.duenas@gmail.com>;

Microsoft Teams [Need help?]

Join the meeting now

Meeting ID: 258 694 049 423

Passcode: tN9tK3wv

For organizers: Meeting options



AVISO LEGAL: Este mensaje y cualquier archivo adjunto son confidenciales, no pueden ser utilizados ni divulgados por personas diferentes a su destinatario. Si usted no es la persona a la cual está dirigido, por favor avise a su remitente y destruya todas las copias del mismo y de los archivos adjuntos. Cualquier uso, divulgación, copia, distribución, impresión o acto derivado del conocimiento total o parcial de este mensaje sin autorización de la CONTRALORÍA DE BOGOTÁ, D.C. será sancionado de acuerdo con las normas legales vigentes. Este mensaje ha sido verificado con software antivirus, en consecuencia la CONTRALORÍA DE BOGOTÁ, D.C. no asume ninguna responsabilidad por daños causados en el recibo y uso del presente. De otra parte, al destinatario se le considera custodio de la información contenida y debe velar por su confidencialidad, integridad y privacidad. El presente correo electrónico solo refleja la opinión de su Remitente y no representa necesariamente la opinión de la CONTRALORÍA DE BOGOTÁ, D.C.

DISCLAIMER: This message and any attachment are confidential, may not be used or reported by persons other than the addressee. If you are not the person to which it is addressed, please advice the sender and destroy all copies thereof and file attachments. Any use, disclosure, copying, distribution, printing or act resulting from the total or partial knowledge of this message without permission of CONTRALORÍA DE BOGOTÁ, D.C. will be punished in accordance with current legal standards. This message has been checked with anti-virus software, therefore CONTRALORÍA DE BOGOTÁ, D.C. assumes no responsibility for damage caused in the receipt and use of the present. On the other hand, custodian of the information contained is considered the recipient and should ensure its confidentiality, integrity, and privacy. The present email only reflects the opinion of the sender and do not necessarily represent the opinion of CONTRALORÍA DE BOGOTÁ, D.C..

GOBIERNO DE DATOS INSTITUCIONAL

Manual de lineamientos técnicos y metodológicos



CONTRALORÍA

DE BOGOTÁ, D.C.

Contenido

Introducción 4
Objetivo general....6
Objetivos específicos....6
Glosario 6
1. Principios del Gobierno de Datos 9
2. Marco legal 10
3. Marco de referencia....12
3.1 Áreas de conocimiento clave 13
4. Roles y responsabilidades del Gobierno de Datos....13
4.1 Autoridad y responsabilidad 14
4.1.1 Nivel Estratégico 14
4.1.2 Nivel Táctico.... 16
4.1.3 Nivel Operativo.... 17
4.2 Matriz RACI 18
4.3 Roles de acceso a los datos 18
5. Lineamientos y políticas del gobierno de datos....20
5.1 Política de Seguridad de la Información.... 20
5.1.1 Principios y controles de seguridad para el tratamiento de datos personales 20
5.1.2 Principios de seguridad para el tratamiento de información pública.... 25
5.1.3 Principios de seguridad para la interoperabilidad 26
5.2 Política de gestión de continuidad para el Gobierno de Datos 28
5.3 Arquitectura TIC 29
5.3.1 Arquitectura de Datos Maestros.... 29
5.3.2 Línea base tecnológica recomendada para analítica de datos.... 30
5.3.2 Integración e interoperabilidad.... 35
5.4 Política de calidad de los datos.... 36
5.4.1 Actividades preventivas y correctivas 37
5.4.2 Indicadores de calidad 38
5.5 Política de gestión del cambio.... 38
6. Metodología para proyectos de datos 39

Paso 1: Diagnóstico y planeación 40
Paso 2: Implementación y monitoreo 41
Paso 3: Evaluación y mejora continua 42
6.1 Consideraciones transversales a los 3 pasos. 42
6.2 Técnicas para proyectos de analítica de datos. 43
7. Herramientas recomendadas para el Gobierno de Datos 45
8. Procedimiento de uso de datos 46
8.1 Datos maestros y datos críticos 46
8.1.1 Datos maestros 46
8.1.2 Datos críticos 47
8.2 Ciclo de vida de los datos 47
8.3 Catálogo de datos 50
8.4 Datos abiertos 51
9. Consideraciones finales 54
Bibliografía 55
Anexos 57
Anexo 1. Matriz RACI 57

Tablas

Tabla 1 Nivel estratégico del Gobierno de Datos de la Contraloría de Bogotá 15
Tabla 2 Nivel táctico del Gobierno de Datos de la Contraloría de Bogotá 16
Tabla 3 Nivel operativo del Gobierno de Datos de la Contraloría de Bogotá 17
Tabla 5 Descripción de la línea base tecnológica para analítica de datos de la Contraloría de Bogotá 31
Tabla 6 Indicadores del Gobierno de Datos 38
Tabla 7 Descripción del ciclo de vida de los datos 48
Tabla 8 Ejes ciclo de vida del dato 50

Ilustraciones

Ilustración 1 Niveles de responsabilidad 14
Ilustración 2 Arquitectura de Datos Maestros de la Contraloría de Bogotá 30
Ilustración 3 Línea base tecnológica recomendada para analítica de datos de la Contraloría de Bogotá 31
Ilustración 4 Arquitectura de referencia de información por capas 33
Ilustración 5 Arquitectura de analítica de datos 34
Ilustración 6 Criterios de calidad 36
Ilustración 7 Metodología para proyectos de datos 40
Ilustración 8 Ciclo de vida del dato 48
Ilustración 9 Ciclo de vida de los datos abiertos 53

Introducción

El Gobierno de Datos permite establecer la información como un activo y tratarla como tal, asegurando la integridad de todo el ciclo de vida del dato. Mantener la información disponible y de calidad son condiciones esenciales para la toma de decisiones y para respaldar las funciones de la Contraloría de Bogotá.

La Contraloría de Bogotá es un organismo técnico, con autonomía administrativa y presupuestal, encargado de vigilar la gestión fiscal del Distrito Capital y de los particulares que manejen fondos o bienes de este, según lo estipulado en la Constitución Política, las leyes y los acuerdos, según establece el artículo No. 1 del Acuerdo 658 de 2016.

Uno de sus principales objetivos es ejercer, en representación de la comunidad, la vigilancia de la gestión fiscal de la administración del Distrito Capital y de los particulares que manejen bienes o fondos de este. Esto implica evaluar los resultados obtenidos por las diferentes organizaciones y entidades del Sector Público Distrital, asegurando una administración correcta, eficiente, económica, eficaz y equitativa del patrimonio público, de los recursos naturales y del medio ambiente. Estas funciones están detalladas en el artículo 2 del Acuerdo 664 de 2017, el cual destaca en su numeral 4 la promoción de la participación ciudadana y el control social en los procesos de control y vigilancia fiscal.

Para cumplir con nuestra misión, las condiciones de calidad y confiabilidad de la información son fundamentales para la vigilancia de la gestión fiscal del Distrito Capital y de los particulares que manejen fondos o bienes del mismo.

Nuestra entidad depende de la fiabilidad, precisión y calidad de los datos que requiere para cumplir con su misión. Esto demanda la definición de lineamientos y principios del Gobierno de Datos institucional, una estructura que las implemente y un conjunto de indicadores que permitan verificar la condición de los datos, asegurando así el buen desempeño de la entidad.

El presente Manual pretende ser una guía estructurada que reúne de forma clara y sistemática las instrucciones, directrices y procedimientos necesarios para cumplir con las obligaciones normativas relacionadas con la Gestión de Datos. Es una herramienta clave para garantizar la correcta implementación de las políticas relacionadas, promover la estandarización de procesos y facilitar el cumplimiento normativo

¿Por qué leer este documento?

Este documento presenta los principios, lineamientos, metodologías y recomendaciones para facilitar el cumplimiento normativo durante todo el Ciclo de Vida del como un marco clave para gestionar los datos desde su creación hasta su eliminación, garantizando su calidad, seguridad y valor estratégico.

¿A quién va dirigido este documento?

Este documento está dirigido a los servidores públicos, contratistas y proveedores de la Contraloría de Bogotá que deben diseñar, desarrollar y gestionar proyectos en torno a los datos que administra y gestiona la entidad. El cumplimiento del Gobierno de Datos es responsabilidad de los servidores públicos y contratistas de la Entidad que tienen a su cargo el diseño, desarrollo y gestión de proyectos relacionados con los datos. El desarrollo y asesoría técnica de la política de datos e información están a cargo de la Subdirección de Análisis, Estadística e Indicadores.

¿Cuáles son los beneficios de tener un Gobierno de Datos?

- **Calidad de los datos:** Gestionar integralmente los datos de la entidad, garantizando su **disponibilidad, integridad y seguridad** para incrementar el valor de los datos y activos de información a lo largo de su ciclo de vida. Así mismo, garantizar que los datos sean precisos, actualizados, consistentes en toda la organización y minimiza problemas como duplicación, datos obsoletos o incompletos.
- **Seguridad y Cumplimiento:** Asegura que los datos confidenciales se manejen adecuadamente, reduciendo riesgos de fugas de información, brindando una adecuada Protección de Datos Sensibles. De este modo se da cumplimiento a las normativas evitando multas y sanciones.
- **Toma de decisiones basadas en datos:** Los datos tienen características confiables, precisos, completos, consistentes y de alta calidad en las organizaciones, facilita el desarrollo de análisis más complejos, con lo cual se podrán identificar nuevas oportunidades con el aprovechamiento de los patrones y tendencias descubiertos para crear nuevas estrategias. Proporciona a los responsables acceso a información de calidad para análisis y estrategias basadas en evidencia, con lo cual los equipos tienen mayor seguridad en el uso de datos confiables.
- **Mayor Eficiencia Operativa:** El Gobierno de Datos es un factor clave para la eficiencia organizacional, su implementación optimizará los procesos al identificar puntos de mejora en la ruta del dato, lo que permite automatizar tareas repetitivas y liberar tiempo para actividades estratégicas, adicionalmente garantiza el cumplimiento normativo, fortalece la confianza y promueve la eficiencia. Promueve la integración y el intercambio de datos entre departamentos, eliminando redundancias. Finalmente, facilita la implementación de procesos automatizados para gestionar y analizar datos.
- **Optimización de Recursos:** Evita gastos innecesarios en la gestión de datos duplicados o mal estructurados.
- **Uso Estratégico de Datos**: Maximiza el valor de los datos al alinearlos con los objetivos de la organización.
- **Transparencia y Trazabilidad:** Permite rastrear el origen, la modificación y el uso de los datos en tiempo real y facilita procesos de auditoría internos y externos gracias a una gobernanza estructurada.

- **Innovación:** Con datos bien gobernados, se pueden identificar nuevas oportunidades para mejorar los trámites y servicios que ofrece la Entidad.
- **Apoyo a la Transformación Digital:** Un gobierno de datos robusto es esencial para aprovechar tecnologías como inteligencia artificial, Big Data y aprendizaje automático.
- **Mitigación de Riesgos:** Ayuda a prever y mitigar riesgos relacionados con la gestión de datos, como ciberataques o mal uso, además facilita respuestas rápidas a incidentes gracias a una estructura clara.

Objetivo general

Establecer e implementar los lineamientos institucionales para la administración y gestión de los datos bajo la arquitectura empresarial y el ciclo de planeación, ejecución, seguimiento y evaluación, incluyendo roles, responsabilidades y estrategias críticas para la mejora continua de los procesos y la toma de decisiones informadas.

Objetivos específicos

- Definir la estructura de roles y responsables que permitan establecer una cultura institucional para la gestión y calidad de los datos.
- Contar con un marco de políticas, lineamientos metodológicos y procedimientos para la gestión de los datos institucionales.
- Gestionar los datos a partir de estándares de calidad que faciliten su análisis y tratamiento
- Facilitar la identificación de los componentes de información de la Entidad y los datos que los componen, así como sus diferentes flujos o rutas críticas.
- Brindar lineamientos para asegurar la disponibilidad, seguridad y privacidad de los datos de acuerdo con la normatividad vigente.

Glosario

- **¿Qué es el Gobierno de Datos?**

El Gobierno de Datos es el conjunto de procesos, principios, normas y métricas que aseguran la efectiva y eficiente gestión de la información en una organización, permitiendo cumplir con las regulaciones, políticas internas y externas, y facilitando la toma de decisiones basada en datos de calidad. (IBM, 2024).

- **¿Qué son datos abiertos?**

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las

entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712/2014)

Están disponibles bajo términos que permiten su uso libre, incluyendo la mezcla con otros conjuntos de datos o su transformación en nuevos productos y servicios. La condición esencial de los datos abiertos es que deben ser accesibles en formatos estandarizados y de fácil uso, lo que facilita su procesamiento y análisis por máquinas, y deben estar bajo licencias que no restrinjan su uso, reutilización ni exposición. El objetivo de los datos abiertos es promover la innovación, mejorar la eficiencia de los servicios públicos, aumentar la transparencia del gobierno y fomentar el desarrollo económico y social.

- **¿Qué es el DMBok?**

DMBOK (Data Management Body of Knowledge) es un marco de referencia comprensivo desarrollado por DAMA International que describe las prácticas y principios fundamentales de la gestión de datos. Proporciona un esquema detallado de las áreas de conocimiento que deben ser consideradas para la gestión de datos eficaz. (DAMA, s.f.)

- **¿Qué es el DAMA?**

DAMA (Data Management Association) es una asociación global de profesionales de la gestión de datos que promueve las mejores prácticas y establece estándares para la calidad en las áreas de gestión de datos, como el desarrollo de DMBOK. (Puig & Mañes, 2021)

- **¿Qué es Arquitectura de Datos?**

La Arquitectura de Datos se refiere al modelo o diseño que describe cómo se recopilan, almacenan, transforman, distribuyen y consumen los datos dentro de una organización. Define las reglas y políticas que gobiernan la gestión de datos a lo largo de todo su ciclo de vida. (IBM, 2024)

- **¿Qué es Almacenamiento de Datos?**

El Almacenamiento de Datos es la recopilación y retención de información en medios electrónicos. Incluye soluciones tanto físicas (como discos duros) como virtuales (como la nube), diseñadas para mantener seguros y accesibles los datos. (IBM, 2023)

- **¿Qué es Analítica Prescriptiva?**

La Analítica Prescriptiva utiliza técnicas de análisis de datos, modelado predictivo y reglas de decisión para recomendar acciones para manejar situaciones futuras. (Sicex, 2022)

- **¿Qué es Analítica Diagnóstica?**

La Analítica Diagnóstica se centra en el análisis de datos para determinar las causas de los eventos pasados. Su objetivo es entender por qué ocurrió un evento, analizando los datos históricos para identificar patrones y causas. (Sicex, 2022)

- **¿Qué es Analítica Descriptiva?**

La Analítica Descriptiva se enfoca en analizar datos pasados para entender lo que ha ocurrido en un período determinado. Utiliza datos históricos para identificar tendencias, patrones y comportamientos. (Sicex, 2022)

- **¿Qué es Calidad de Datos?**

La Calidad de Datos se refiere a la condición de un conjunto de valores de datos respecto a su completitud, validez, consistencia, integridad y precisión. Una alta calidad de datos permite a las organizaciones tomar decisiones basadas en información fiable y precisa. (Haider, 2024)

- **¿Qué es la Analítica Predictiva?**

La Analítica Predictiva utiliza técnicas estadísticas y de modelado para analizar datos históricos y actuales con el fin de hacer predicciones sobre eventos futuros o desconocidos. (Sicex, 2022)

- **¿Qué son Datos Maestros y de Referencia?**

Los Datos Maestros son un conjunto de datos que son críticos para las operaciones de una empresa, proporcionando un punto de referencia común para diferentes sistemas y departamentos. Los Datos de Referencia son subconjuntos de datos maestros utilizados para clasificar o categorizar otros datos. (SDNA Digital)

- **¿Qué es Fuente de Confianza?**

Una Fuente de Confianza es un origen de datos considerado autoritativo y fiable para la toma de decisiones. Estos datos han sido validados y son mantenidos de manera que aseguran su precisión y actualidad. (Universitat de Valencia, s.f.)

- **¿Qué es Fuente de Información?**

Una fuente de Información es cualquier origen de datos que puede ser utilizado para recopilar información. Puede ser primaria o secundaria y varía desde documentos y encuestas hasta bases de datos y registros en línea. (Universitat de Valencia, s.f.)

- **¿Qué es Integración de Datos?**

La Integración de Datos es el proceso de combinar datos de diferentes fuentes para proporcionar una vista unificada. Facilita el análisis y el acceso a los datos de manera coherente a través de las distintas áreas de una organización. (Microsoft, s.f.)

- **¿Qué son Metadatos?**

Los Metadatos son datos que describen otros datos. Proporcionan información sobre el contenido, calidad, condición, y otros aspectos de los datos, facilitando su gestión, uso y comprensión. (PowerData, 2016)

1. Principios del Gobierno de Datos

Además de los principios previstos en los artículos 209 de la Constitución Política, 4° de la Ley 1266 de 2008, 2° de la Ley 1341 de 2009, 3° de la Ley 1437 de 2011, 4° de la Ley 1581 de 2012, 3 de la Ley 1712 de 2014, los atinentes a la Política de Gobierno Digital contenidos en el artículo 2.2.9.1.1.3 del Decreto 1078 de 2015, los principios de gestión documental contenidos en el artículo 2.8.2.8.5.5 del Decreto 1080 de 2015, para los efectos del presente título se aplicarán los siguientes:

Adaptabilidad: El diseño e implementación de políticas y estrategias son escalables, dinámicos y flexibles, y podrán adaptarse a las necesidades y oportunidades del contexto nacional e internacional conforme a las condiciones que lo requieran.

Coordinación: En el diseño e implementación de las políticas, estrategias y acciones relacionadas con la Gobernanza de la Infraestructura de Datos se fomentará la participación y articulación entre los actores.

Eficiencia: Los sujetos obligados buscarán que los procedimientos y actividades logren su finalidad y, para el efecto, dispondrán de personas, procesos y tecnología que apoyen la estrategia de gobernanza de la infraestructura de datos, con el fin de disminuir costos operativos y controlar riesgos en torno a la calidad de los datos.

Enfoque al usuario: Las políticas y procesos de la Gobernanza de la Infraestructura de Datos deberán responder a las necesidades de los usuarios en materia de datos, por lo cual el modelo buscará implementar mecanismos de participación e inclusión de distintos actores**.**

Gestión de datos como activo estratégico: Los datos se consideran activos valiosos, cuya gestión eficiente es vital para el éxito y el cumplimiento de los objetivos de la entidad.

Cumplimiento y Responsabilidad: Se garantiza que todos los niveles de la organización, desde la alta dirección hasta los operativos, cumplan con las políticas y estándares de gestión de datos establecidos.

Calidad de los datos: Se refiere a la medida en que los datos son precisos, completos, oportunos, consistentes y confiables para su uso previsto. La calidad de los datos es esencial para garantizar la eficacia y la precisión de cualquier análisis o proceso que dependa de ellos.

Cumplimiento normativo: Hace referencia al conjunto de leyes, regulaciones y estándares que una organización debe cumplir en relación con el manejo, almacenamiento y procesamiento de datos. Esto incluye normativas de privacidad de datos, protección de información personal, seguridad de datos y otras regulaciones específicas de la industria.

Toma de decisiones informadas: Significa utilizar datos confiables y relevantes para respaldar la toma de decisiones en una organización. Esto implica recopilar, analizar y comprender los datos de manera efectiva para obtener información útil que guíe las decisiones estratégicas y operativas.

Confianza y transparencia: La confianza en los datos se refiere a la creencia de que los datos son precisos, confiables y están libres de sesgos o manipulaciones indebidas. La transparencia implica que las organizaciones sean abiertas y honestas sobre cómo recopilan, procesan y utilizan los datos, así como sobre los algoritmos y modelos utilizados en sus procesos de toma de decisiones.

Accesibilidad y usabilidad: Los datos deben ser accesibles y fáciles de usar para los usuarios autorizados, de manera oportuna y a través de canales adecuados, con el fin de aprovechar al máximo su valor.

2. Marco legal

Ley 1581 de 2012- Ley de protección de datos personales: Tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Ley 1712 de 2014- Ley de Transparencia y Acceso a Información Pública: Tiene por objeto regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información y cuyo principio dictamina que toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal, de conformidad con ley expuesta

La Ley 1712 de 2014 es una herramienta fundamental para el Gobierno de Datos, ya que permite fortalecer la transparencia, la rendición de cuentas, la participación ciudadana, la innovación y la lucha contra la corrupción.

Fortalecer la confianza en las instituciones públicas, la transparencia y el acceso a la información pública pueden contribuir a fortalecer la confianza de la ciudadanía en las instituciones públicas.

Literal K, artículo 11, Ley 1712 de 2014- Datos abiertos: La Ley define los datos abiertos como información pública que se encuentra en formatos estándar e interoperables, lo que facilita su reutilización por parte de la ciudadanía para generar nuevos productos y servicios. Las entidades públicas deben publicar sus datos abiertos en el portal datos.gov.co.

La publicación de datos abiertos permite a los ciudadanos tener acceso a información sobre la gestión pública, la toma de decisiones y el uso de los recursos públicos. Esto fortalece la transparencia y el control social sobre las entidades públicas.

Decreto 1389 de 2022- Decreto reglamentario sector TIC: Por el cual se adiciona el Título 24 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para la gobernanza en la infraestructura de datos y se crea el Modelo de gobernanza de la infraestructura de datos".

Decreto Distrital 575 de 2023: Por medio del cual se definen los componentes de la Infraestructura de Datos y establece el modelo de gobernanza correspondiente en el Distrito Capital.

CONPES 3920-Política Nacional de Explotación de Datos (Big Data): Tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales. (DNP, 2018)

G.INF.06 Guía Técnica de Información - Gobierno del dato guía técnica del Gobierno del Dato: En ella se soportan los componentes necesarios para la implementación de los lineamientos asociados a: registro y mantenimiento de información, establecimiento de los mecanismos de actualización de los componentes informacionales, la creación y mantenimiento del repositorio unificado de datos con el fin de realizar adecuado gobierno del dato en las organizaciones (MinTIC, 2014)

G.INF.02 Guía técnica de Información- Administración del dato maestro: Donde se enmarcan un conjunto de pasos y actividades para una adecuada administración de datos maestros, y se aporta en la definición de procesos que permitan apoyar la mejora de la calidad de los datos, a partir del gobierno de datos. (MinTIC, 2014)

Política de Gobierno Digital: Define los lineamientos, estándares y proyectos estratégicos, que permiten llevar a cabo la transformación digital del Estado, a fin de lograr una mejor interacción con ciudadanos, usuarios y grupos de interés; permitiendo resolver necesidades satisfactoriamente, resolver problemáticas públicas, posibilitar el desarrollo sostenible y en general, crear valor público. (MinTIC, 2022)

Política de Gestión de la Información Estadística: Busca que las entidades generen y dispongan la información estadística, así como la de sus registros administrativos, de acuerdo con los lineamientos establecidos por el líder de Política, para mejorar la efectividad de su gestión y planeación basada en evidencias; garantizando una continua disponibilidad de información de calidad a lo largo del ciclo de la política pública; fomentando el diálogo social con la ciudadanía y los grupos de interés, en el marco de la construcción participativa de las soluciones sociales, y generando una herramienta de control político y social que permita la transparencia de las actuaciones del Estado. (Función Pública, 2023)

Política de Seguridad de la información: Busca que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información de las entidades del Estado, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos. Este habilitador se desarrolla a través del Modelo de Seguridad y Privacidad de la Información, que orienta la gestión e implementación de la seguridad de la información en el Estado. (Función Pública, 2023).

3. Marco de referencia

Se adopta el marco Data Management Body of Knowledge- DMBok (por sus siglas en inglés), para la gestión de datos, complementado por las prácticas y metodologías señaladas en el modelo de gobernanza de datos de la entidad, garantizando así una estrategia integral que abarca:

1. **Entendimiento de necesidades:** Alineación con las demandas de información de todas las partes interesadas.
2. **Seguridad, Integridad y Privacidad de los datos:** Implementación de medidas de protección, garantía de la fiabilidad de los datos y salvaguarda de la privacidad de la información.
3. **Mejora Continua:** Fomento de la exactitud, claridad y aceptación común de los datos mediante procesos iterativos de calidad.

Se puede aplicar en cualquier etapa de un proyecto de la entidad que involucre la gestión de datos. Sin embargo, es especialmente útil al comienzo de un proyecto para establecer una base sólida de gestión de datos desde el principio. También puede ser útil en etapas posteriores del proyecto para abordar problemas específicos de calidad de datos, gobernanza de datos u otros desafíos relacionados con los datos. Además, es recomendable aplicar el marco DAMA durante la revisión o actualización de procesos y sistemas existentes relacionados con la gestión de datos.

3.1 Áreas de conocimiento clave

Incorpora las áreas de conocimiento de DAMA, ajustadas y expandidas para satisfacer las especificidades de la Contraloría de Bogotá:

- **Gobierno de datos:** Establecimiento de políticas, estándares y monitoreo del cumplimiento para la gestión efectiva de datos.
- **Arquitectura de datos:** Diseño de estructuras de datos que faciliten la evolución tecnológica y satisfagan las necesidades organizacionales actuales y futuras, tomando como base una arquitectura de referencia por capas.
- **Operaciones y gestión del ciclo de vida de los datos:** Aseguramiento de la disponibilidad, integridad y administración eficiente de los datos a lo largo de su ciclo de vida.
- **Seguridad de datos e información:** Control de acceso, cumplimiento de regulaciones, protección de la privacidad y gestión de riesgos de datos.
- **Interoperabilidad e integración de datos:** Facilitación del intercambio seguro, eficiente y consistente de datos entre sistemas y organizaciones.
- **Gestión documental y de contenidos:** Administración eficaz de documentos, registros y otros tipos de contenido no estructurado.
- **Datos maestros y de referencia:** Garantía de calidad, consistencia y gobierno de las fuentes autorizadas de información crítica.
- **Inteligencia de negocios y analítica de datos:** Soporte a la toma de decisiones mediante análisis de datos integrados y generación de insights.
- **Gestión de metadatos:** Gestión, comprensión y aprovechamiento de metadatos y términos de negocio.
- **Gestión de la calidad de datos:** Establecimiento de procesos, métricas y controles para el mantenimiento y mejora continua de la calidad de los datos.

4. Roles y responsabilidades del Gobierno de Datos

Los roles de gobierno de datos son las diferentes funciones que se asignan a los servidores públicos o a los procesos dentro de la Contraloría de Bogotá, para garantizar que los datos se administren y utilicen de manera efectiva. Esta estructura organizacional es vital para la adecuada administración del gobierno de datos institucional, garantizando la toma de decisiones y la operatividad.

Estos roles se pueden dividir en tres categorías amplias: nivel estratégico, nivel táctico y nivel operativo. Se incluye un nivel transversal liderado por la Dirección de Tecnologías de la Información y las Comunicaciones, la cual debe participar activamente en la gestión de la

infraestructura de hardware, software, seguridad de la información y los proyectos que requieran la implementación de tecnologías emergentes.

Ilustración 1 Niveles de responsabilidad



Fuente: Elaboración propia

4.1 Autoridad y responsabilidad

Los criterios de autoridad y responsabilidad se determinan para los tres niveles indicados (estratégico, táctico y operativo). Se debe entender el criterio de **Autoridad** como aquel que cuenta con las competencias funcionales para tomar decisiones sobre cómo se administran y utilizan los datos. A su vez, el criterio de **Responsabilidad** se refiere a la obligación de rendir cuentas por el uso de los datos.

4.1.1 Nivel Estratégico

El nivel estratégico del Gobierno de Datos se conforma por tres roles: Comité de Gobierno de Datos, Director de Datos y Equipo de Datos.

El Comité de Gobierno de Datos se desempeña bajo los criterios de autoridad, con lo cual proporciona supervisión de alto nivel a las políticas, planes y proyectos del Gobierno de Datos, tomando decisiones estratégicas. De esta manera, su responsabilidad se enmarca en la aprobación de políticas y de asignación de los recursos necesarios para su cumplimiento.

El Director de Datos y el Equipo de Datos tiene la visión global, por lo tanto, la responsabilidad se enmarca en la coordinación y ejecución del Gobierno de Datos, adicionalmente deben

propender por una gestión adecuada de la información y es el articulador entre el Comité del Gobierno de Datos y el nivel operativo.

A continuación, se presenta la estructura definida en la Contraloría de Bogotá:

Tabla 1 Nivel estratégico del Gobierno de Datos de la Contraloría de Bogotá

Rol	Comité de Gobierno de Datos	Director de datos	Equipo de datos
Cargo	• Contralor Auxiliar • Director de Planeación • Director de Tecnologías de la Información y las Comunicaciones • Director de Estudios de Economía y Política Pública • Subdirector de Análisis, Estadísticas e Indicadores	• Director de Planeación a través del subdirector de Análisis, Estadísticas e Indicadores. (Desde la perspectiva de centralidad de la información institucional). • Director de Tecnologías de la Información y las Comunicaciones (Desde la perspectiva de la política de Gobierno Digital)	• Dirección de Planeación a través de la Subdirección de Análisis Estadísticas e Indicadores • Director de Estudios de Economía y Política Pública a través de las Subdirecciones. • Director de Tecnologías de la Información y las Comunicaciones
Responsabilidad	1. Definir políticas o lineamientos estratégicos relacionados con el gobierno de datos. 2. Gestionar los recursos necesarios para el cumplimiento de las estrategias que se planteen. 3. Revisar y aprobar los planes y proyectos relacionados con el gobierno de datos. 4. Establecer, en caso de requerirse, el nivel de participación de las dependencias involucradas en la atención de la necesidad del usuario. 5. Definir, en caso de requerirse, la dependencia responsable (única) para cada fuente de información 6. Designación de roles y responsabilidades que se requieran para el desarrollo de actividades del gobierno de datos institucional. 7. Coordinarse con los demás Comités para tomar decisiones que afecten el gobierno de datos institucional. 8. Asegurar la implementación y desarrollo del Observatorio de Vigilancia y Control Fiscal.	1. Convocar y liderar las sesiones de comité de gobierno de datos. 2. Liderar el seguimiento de los compromisos del gobierno de datos y de los generados en el comité. 3. Coordinar los planes, proyectos y actividades del gobierno de datos. 4. Liderar las evaluaciones periódicas al gobierno de datos en materia de políticas, calidad de datos, riesgos de privacidad, entre otros 5. Gestionar las relaciones como usuario autorizado en procesos de intercambio de datos con fuentes externas. 6. Determinar las estrategias más adecuadas de divulgación o socialización de las decisiones tomadas en todo lo relacionado a gobierno de datos.	1. Desarrollar los compromisos del gobierno de datos y de los generados en el comité. 2. Formular o apoyar la formulación de los planes, proyectos y actividades del gobierno de datos. 3. Realizar evaluaciones periódicas al gobierno de datos en materia de políticas, calidad de datos, riesgos de privacidad, entre otros 4. Elaborar los documentos requeridos para procesos de intercambio de datos con fuentes externas.

Fuente: Elaboración propia

4.1.2 Nivel Táctico

El nivel táctico del Gobierno de Datos se conforma por tres roles: Administrador de datos, Administrador de seguridad y privacidad de los datos, y Líder de datos.

Las características de estos roles se relacionan con el conocimiento del negocio, las capacidades técnicas y habilidades analíticas e informáticas.

El nivel táctico se desempeña como un articulador entre el nivel estratégico y el nivel operativo, por lo cual debe tener una constante comunicación entre los dos para la toma de decisiones tácticas que permitan una gestión adecuada de la información en el ciclo de vida del dato.

A continuación, se presenta la estructura definida en la Contraloría de Bogotá:

Tabla 2 Nivel táctico del Gobierno de Datos de la Contraloría de Bogotá

Rol	Administrador de datos	Administrador de seguridad y privacidad de los datos	Líder de datos
Cargo	• Director de Tecnologías de la Información y las Comunicaciones • Profesional asignado como administrador de las bases de datos.	• Oficial de seguridad de la Información	• Directores • Subdirectores • Gerentes • Jefes de oficina
Responsabilidad	1. Arquitectura de datos y la integración de los mismos. 2. Desarrollo, mantenimiento y aprovechamiento del modelo de datos empresarial. 3. Administrar las bases de datos, controlando y gestionando las capacidades relacionadas con la infraestructura de almacenamiento de datos.	1. Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información. 2. Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. 3. Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora 4. Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. 5. Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información. 6. Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información	1. Designar los responsables temáticos de cada área para la implementación y seguimiento a los planes, proyectos y actividades del gobierno de datos. 2. Preparar y presentar al nivel estratégico los planes, proyectos y actividades del gobierno de datos y los respectivos reportes de monitoreo. 3. Asegurar el cumplimiento de los criterios de confidencialidad, integridad y disponibilidad de la información en los planes, proyectos y actividades del gobierno de datos. 4. Articular los procesos y procedimientos en los que participa con la gestión de información y el gobierno de datos.

Rol	Administrador de datos	Administrador de seguridad y privacidad de los datos	Líder de datos
		en la implementación de los proyectos de TI y datos.	

Fuente: Elaboración propia

4.1.3 Nivel Operativo

El nivel operativo del Gobierno de Datos se conforma por tres roles: Gestor tecnológico de datos, Analista de datos y Gestor técnico de datos.

El desempeño óptimo del nivel operativo es fundamental para la sostenibilidad del Gobierno de Datos, debido a que en este nivel se producen, captan, procesan y/o analizan los datos que se generan a partir de las actividades misionales y de la gestión en los diferentes sistemas de información de la entidad.

Los roles que participan en este nivel son responsables de la calidad de los datos, por lo tanto, deben tener conocimiento en los procesos y metodologías que intervienen con el dato a gobernar, está conformado por los profesionales de las dependencias que producen información, realizan ejercicios de analítica de datos o capturan datos a través de los sistemas de información.

La Dirección de Tecnologías de la Información y las Comunicaciones, será la encargada de la administración del componente tecnológico de los sistemas de información que centralizan los datos a gobernar, además de brindar apoyo en materia TIC a la dependencia técnica.

Tabla 3 Nivel operativo del Gobierno de Datos de la Contraloría de Bogotá

Rol	Gestor tecnológico de datos	Analista de datos	Gestor técnico de datos
Cargo	• Director de Tecnologías de la Información y las Comunicaciones • Profesional asignado como administrador de los sistemas de información.	• Profesionales especializados en analítica de datos asignados en las áreas funcionales	• Profesionales asignados en las áreas funcionales.
Responsabilidad	1. Aplicar las políticas y lineamientos de gobierno de datos a los sistemas de información. 2. Apoyar en la definición y ajuste de problemas de datos y alternativas de solución. 3. Apoyar en la definición de políticas y estándares de gestión de datos. 4. Apoyar a comprender las necesidades de información. 5. Participar en el modelado y la arquitectura de datos. 6. Apoyar en las definiciones y requisitos de calidad de los datos	1. Producir información estadística de calidad para satisfacer las necesidades del usuario. 2. Liderar la formulación de los proyectos de analítica de datos. 3. Gestionar los ejercicios de analítica de datos que requieran la solicitud o consulta de datos de fuentes externas en coordinación con los usuarios autorizados del gobierno de datos para tal fin. 4. Realizar el cruce de bases de datos internas y externas requeridas para los ejercicios de analítica enmarcadas en las funciones misionales.	1. Definir el flujo de datos en los procesos y los sistemas de información 2. Producir informes, reportes y documentos que generen datos estadísticos e indicadores. 3. Registrar información de las actividades misionales en los sistemas de información. 4. Formular proyectos de analítica de datos.

Rol	Gestor tecnológico de datos	Analista de datos	Gestor técnico de datos
		5. Propender por el mejoramiento continuo de la información estadística que produce. 6. Reportar hallazgos al administrador de datos 7. Comunicar y promover el valor de la información. 8. Monitorear y hacer cumplir las políticas y prácticas de datos en su dependencia.	

Fuente: Elaboración propia

4.2 Matriz RACI

La Matriz RACI[1] complementa la definición de roles descrita en los niveles estratégico, táctico y operativo del Gobierno de Datos, proporcionando una guía detallada para la asignación de responsabilidades en actividades críticas como la implementación de políticas, el aseguramiento de la calidad de los datos y el cumplimiento normativo. El detalle de la matriz se puede consultar en el Anexo 1. Matriz RACI.

4.3 Roles de acceso a los datos

Cada uno de los sistemas de información de la Entidad tienen identificados roles y permisos de acceso, de acuerdo con lo definido por el administrador funcional y técnico, así como en los respectivos manuales y la documentación del sistema de calidad que se relacione.

De acuerdo con esto, en lo que se refiere a los sistemas de información, los roles serán los mismos que ya se encuentran establecidos. De otra parte, para la consulta y acceso de los datos maestros identificados, los datos que se producen o gestionan internamente a través de ejercicios de analítica y los datos que provienen de fuentes externas a la entidad, se tendrán en cuenta los siguientes roles:

Propietarios de datos: Los propietarios de datos son responsables de la calidad, la integridad y la seguridad de sus datos. También son responsables de garantizar que sus datos se utilicen de manera compatible con las políticas y procedimientos de Gobierno de Datos.

Los propietarios de los datos estarán a cargo del usuario funcional o responsable del dato a gobernar y cuentan con acceso a los datos sin restricciones.

[1] Acrónimo en inglés: Responsible, Accountable, Consulted, Informed.

Custodios de datos: Los custodios de datos son responsables de administrar y proteger los datos. También son responsables de garantizar que los datos sean accesibles para aquellos que los necesitan.

Los custodios hacen parte del Equipo de Datos y tendrá acceso a consultas y modificaciones.

Usuarios de datos: Los usuarios de datos son responsables de utilizar los datos de manera responsable y ética. También son responsables de garantizar que los datos no se utilicen para fines ilegales o discriminatorios.

Tendrán acceso todos los usuarios de la información de la entidad, los cuales se podrán configurar de acuerdo con la necesidad especifica de cada uno y las autorizaciones correspondientes.

Cuando un tercero o ente externo solicite tener acceso a algún recurso o servicio de la Entidad, se deberá realizar el correspondiente análisis de riesgo con la participación del propietario de la información y de los activos asociados, con el fin de determinar los privilegios a otorgar y definir los mecanismos necesarios para su protección, el cual se documentará en el acta de inicio del contrato o dentro de la documentación de seguimiento de las labores realizadas. Para ello deberá firmar el acuerdo de confidencialidad que se tiene definido para estos casos.

En ningún caso se otorgará a terceros accesos a la información, a las instalaciones, o a centros de procesamiento de información crítica, si previamente no se han cumplido los controles de seguridad establecidos en el procedimiento de seguridad física y del entorno y/o conexión a terceros.

Las asignaciones de privilegios en las aplicaciones para los diferentes usuarios estarán determinadas por el procedimiento de control de acceso a usuarios, estos privilegios deben revisarse a intervalos regulares y ser modificados o reasignados cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.

Se debe usar una identificación de usuario para permitir que los funcionarios queden vinculados y sean responsables de sus acciones.

Se debe retirar o bloquear a la mayor brevedad los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado de ser parte de la Entidad. Para esto la Dirección de Talento Humano deberá periódicamente remitir las novedades de personal para mantener actualizado los derechos de usuario; en el mismo sentido la Dirección Administrativa y Financiera deberá remitir el listado de los contratistas activos en la entidad. Las novedades de personal deben ser remitidas al proceso que administra el sistema de información correspondiente de manera inmediata al presentarse la novedad.

5. Lineamientos y políticas del gobierno de datos

5.1 Política de Seguridad de la Información

Con base en los principios legales del tratamiento de datos personales y la política de gobierno digital, se ha identificado la necesidad de consolidar los principios que rigen la arquitectura de seguridad digital institucional, con especial énfasis en la privacidad de los datos personales. Siguiendo las directrices de la política de seguridad y privacidad de la información y la política de datos personales, a continuación, se presenta una síntesis de los principios clave para la arquitectura de seguridad digital en el gobierno de datos.

5.1.1 Principios y controles de seguridad para el tratamiento de datos personales

5.1.1.1 Principio de seguridad: La información sujeta a Tratamiento por el responsable del tratamiento o encargado del tratamiento, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Control - Política de Seguridad de la Información y Seguridad Digital: Mediante Resolución 012 del 2021, se formalizó la política, aplicable a toda la entidad, sus funcionarios, contratistas, sujetos de control fiscal, usuarios internos y externos que acceden o hacen uso de cualquier activo de información, así como exfuncionarios y excontratistas que haya tenido acceso a cualquier activo de información, independientemente de su ubicación, medio o formato de la Contraloría de Bogotá, así como la ciudadanía en general que se relacione con el ente de control. De igual manera, aplica a toda la información creada, procesada o utilizada por este Órgano de Control Fiscal, sin importar el medio, formato, presentación, o lugar en el que se encuentre.

La Contraloría de Bogotá, D.C. manifiesta su compromiso con el fortalecimiento de capacidades para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en los que puedan verse comprometidos los activos de Información que soportan los procesos de la entidad, mediante la implementación de medidas para asegurar su confidencialidad, integridad, disponibilidad y privacidad, en el marco de confianza en el ejercicio de sus deberes con el Distrito y los Ciudadanos. bookmark://politica_de_seguridad/

5.1.1.2 Principio de veracidad o calidad: la información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Control - Política de Tratamiento de Datos Personales: Formalizada mediante Resolución 012 de 2019, indica que la Contraloría de Bogotá D.C. manifiesta su compromiso con el tratamiento de los datos personales, garantizando los derechos de la privacidad, la intimidad, el buen nombre y la autonomía, donde todas sus actuaciones se regirán por los principios de legalidad, finalidad,

libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad.

Lineamientos principales: De acuerdo con lo anterior, esta política determina los lineamientos de tratamiento y protección sobre los datos personales, la información considerada como sensible y los controles que se deberán implementar de acuerdo con el nivel de clasificación de dicha información. En lo relacionado con el Gobierno de Datos, se destacan los siguientes lineamientos:

- El ciudadano y/o funcionario reconoce que el ingreso de información personal por cualquiera de los mecanismos establecidos por la entidad, lo realiza de manera voluntaria y lo hará ante la solicitud de requisitos específicos por la Contraloría de Bogotá D.C. para llevar a cabo un trámite, una queja o reclamo o una solicitud o para acceder a los mecanismos interactivos que se le ofrecen.
- Para la recolección y tratamiento automatizado de los datos personales, como consecuencia de la navegación y/o registro por el sitio web, se deberá informar al titular de los datos la finalidad de estos.
- El tratamiento de datos personales debe estar sujeto a lo establecido en la normatividad vigente.
- La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad, evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Al presentar la queja ante la entidad frente al manejo de la privacidad y/o confidencialidad de los datos personales, esta se dirigirá al área o funcionario encargado o designado para responder los temas relacionados con la protección de los datos personales a los que refiera la queja conforme a la normatividad vigente.

Control – Uso de los activos de información: La Contraloría de Bogotá D.C., identifica todos los activos de información, y mantiene un inventario actualizado, exacto, consistente y documentado con todos los aspectos relevantes de cada uno, clasificándolos de acuerdo con la confidencialidad, integridad y disponibilidad de la información, para identificar su valor y criticidad, además, cada activo debe tener un propietario que garantice los niveles de seguridad que correspondan según sea el caso. La actualización de los activos de información es responsabilidad de cada proceso con la respectiva coordinación de equipo de Gestión Documental.

Lineamientos principales:

- La Contraloría de Bogotá D.C. es la dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios y los contratistas,

derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

- Todos los activos de información tienen asignado un custodio que tiene la responsabilidad de mantener los controles adecuados para su protección.
- Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información, de acuerdo con lo establecido en el procedimiento para la gestión de activos.
- El acceso a carpetas compartidas debe delimitarse a los funcionarios que las necesitan y deben ser protegidas con contraseñas y/o acceso por roles y responsabilidades.
- Los funcionarios y contratistas deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por la Contraloría de Bogotá D.C. en el proceso de desvinculación o finalización de la relación laboral o contractual, de igual manera deberán documentar los conocimientos importantes relacionados con la labor ejecutada.
- La Contraloría de Bogotá D.C., de acuerdo con la normatividad y procedimientos vigentes ejecutará las actividades necesarias para garantizar la eliminación, retiro, traslado o reúso de los activos, de forma segura y correcta.

5.1.1.3 Principio de acceso y circulación restringida: El Tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones legales y la Constitución. En este sentido, el Tratamiento sólo podrá hacerse por personas autorizadas por el Titular y/o por las personas previstas por la ley.

Control - Restricciones de acceso a la información: En la Contraloría de Bogotá D.C., se establecen medidas de control de acceso a la información y demás servicios de TI, estos controles limitan el acceso a la información de acuerdo con la clasificación de la información, las funciones y cargos que desempeñen los funcionarios, contratistas y terceros. Siempre se brindarán accesos de acuerdo con el principio de privilegio más bajo, con los cuales todos los funcionarios, contratistas y terceros puedan desempeñar correctamente sus funciones sin brindar accesos de mayor alcance a los que se requiere, de acuerdo con el procedimiento vigente para el control de acceso.

Lineamientos principales:

- La Contraloría de Bogotá D.C, aplica un procedimiento mediante el cual se brindan las pautas para una correcta gestión del control de acceso a usuarios en todos sus niveles; en este procedimiento se contempla la restricción y control de los accesos privilegiados

a la información y los sistemas de información, así como establecer las definiciones para el monitoreo periódico de las acciones y los cambios a las cuentas privilegiadas.

- En ningún caso se otorga a terceros accesos a la información, a las instalaciones, o a centros de procesamiento de información crítica, si previamente no se han cumplido los controles de seguridad establecidos en el procedimiento de control de acceso mediante el cual se garantiza la seguridad física y del entorno y/o conexión a terceros.
- Las asignaciones de privilegios en las aplicaciones para los diferentes usuarios están determinadas por el procedimiento de control de acceso a usuarios, estos privilegios se revisan a intervalos regulares y son modificados o reasignados cuando se presenten cambios en el perfil del usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.
- Se usa una identificación de usuario (ID) para permitir que los funcionarios queden vinculados y sean responsables de sus acciones.
- Se retiran o bloquean a la mayor brevedad los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado de ser parte de la Entidad. En el mismo sentido la Dirección Administrativa y Financiera remite periódicamente el listado de los contratistas activos en la entidad.
- Los privilegios de administración de cualquier equipo de cómputo (servidor, estación de trabajo, desktop, portátil, o equipo activo de red), son asignados exclusivamente a los administradores del sistema designados en la Dirección de Tecnologías de la Información y las Comunicaciones de la Entidad, en ningún caso se debe autorizar estos privilegios de acceso al usuario del equipo.
- Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debe suministrar de manera segura una contraseña temporal, la cual se debe forzar a cambiar inmediatamente realice el siguiente ingreso al sistema.
- Las contraseñas nunca se deben almacenar en sistemas, medios o formatos no protegidos.
- Las contraseñas predeterminadas por el fabricante se deben cambiar inmediatamente después de la instalación de los sistemas o del software.
- Toda contraseña es personal e intransferible, y cada usuario es responsable de las acciones que se ejecuten con el usuario que se le ha asignado.

5.1.1.4 Principio de Confidencialidad: El principio de confidencialidad, establece la obligación de todas las personas que manejan información privada de garantizar la reserva de esa información. Es decir, esta información no debe ser revelada a terceros sin el consentimiento expreso del titular de los datos, a menos que exista una autorización legal para hacerlo.

En este sentido, todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información,

inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley y en los términos de la misma.

Las categorías de estos datos y el alcance de su protección corresponden a los responsables de los datos, quienes deberán adoptar medidas de privacidad y de seguridad que sean acordes con la sensibilidad de los datos y su capacidad de afectar a los titulares. En ese sentido la entidad aplica la normatividad vigente en Colombia sobre la protección de datos personales.

Control – Clasificación de la Información: La clasificación de la información pública es un proceso fundamental para garantizar el acceso a la información, proteger la privacidad de las personas y asegurar la transparencia en la gestión pública. Al categorizar la información según su nivel de sensibilidad y restricciones de acceso, se establece un orden que facilita su gestión, búsqueda y divulgación. Al establecer criterios claros sobre qué información es pública y cómo acceder a ella, se cumple con el derecho fundamental de los ciudadanos a conocer la gestión pública.

Lineamientos principales:

- Los funcionarios de la entidad se deben comprometer a identificar, clasificar, etiquetar, disponer, devolver, y gestionar los activos de información establecidos como tal, de acuerdo con la presente política y el procedimiento establecido para la gestión de activos.
- La identificación, clasificación y valoración de los activos de información se debe realizar de acuerdo con el procedimiento vigente establecido para la caracterización de activos de información.
- Toda la información producida, tratada, procesada, almacenada o transmitida en la Contraloría de Bogotá D.C., debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad según metodología y/o proceso debe mantener un registro actualizado y exacto de todos los activos de información necesarios para la prestación de servicios, de acuerdo con lo establecido en el procedimiento para la gestión de activos.
- Los documentos de la Contraloría de Bogotá D.C., que contengan información relacionada con diferentes niveles de clasificación de seguridad, asumirán la del nivel más alto que tenga la información contenida en ellos.
- La identificación de riesgos de seguridad digital contempla la identificación de los activos de información calificados como reservados o clasificados.
- La información calificada como datos abiertos es evaluada por el proceso de gestión documental para autorizar su publicación en el portal datos.gov.co.
- La calificación de la información se debe tener en cuenta al momento de autorizar el acceso a los diferentes activos de información institucionales.
- El índice de información clasificada y reservada debe ser verificado al momento de autorizar acceso o transferencia de información con todas las partes interesadas y grupos de valor.

Control – Acuerdos de Confidencialidad: Los acuerdos de confidencialidad son herramientas esenciales para regular el acceso y uso de la información, garantizando así la protección de datos personales, la transparencia y la buena gobernanza. Permiten definir claramente qué tipo de información está sujeta al acuerdo, con lo cual se evita la divulgación de información que pueda perjudicar la privacidad de las personas o los intereses institucionales, entre otros aspectos.

Lineamientos principales:

- La Contraloría de Bogotá D.C. establece acuerdos de confidencialidad para todos los funcionarios, contratistas y/o terceros vinculados a la entidad que manipulen, requieran o provean información física y/o digital, clasificada, reservada o confidencial.
- Todo funcionario, contratista o tercero debe firmar un acuerdo de confidencialidad, el cual debe contener el compromiso de no divulgación de la información interna y externa que conozca como parte del desarrollo de las funciones que desempeña o de su vinculación con la entidad.
- Este acuerdo de confidencialidad deberá indicar la vigencia, la cual debe mantenerse por un tiempo adicional que considere la Contraloría de Bogotá D.C., luego de terminada la vinculación con la misma.

5.1.2 Principios de seguridad para el tratamiento de información pública

La Contraloría de Bogotá garantiza el cumplimiento de la normatividad relacionada con el acceso a la información, principalmente lo definido por la Ley de Transparencia y Acceso a la Información Pública 1712 de 2014, reconociendo el derecho de todos los ciudadanos y grupos de valor a conocer la información que reposa en las instituciones públicas con las limitaciones que la constitución o la ley impongan.

5.1.2.1 Principio de máxima publicidad para el titular universal: Este principio establece que toda la información que se encuentra en poder de una entidad pública se presume pública y, por tanto, debe ser accesible a cualquier ciudadano que la solicite, a menos que exista una razón legal para reservarla.

Principio de transparencia: Principio conforme al cual toda la información en poder de los sujetos obligados definidos en la ley 1712 de 2014 se presume pública, en consecuencia, de lo cual dichos sujetos están en el deber de proporcionar y facilitar el acceso a la misma en los términos más amplios posibles y a través de los medios y procedimientos que al efecto establezca la ley, excluyendo solo aquello que esté sujeto a las excepciones constitucionales y legales y bajo el cumplimiento de los requisitos establecidos en la ley.

En el tratamiento de datos personales debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Principio de buena fe: En virtud del cual todo sujeto obligado, al cumplir con las obligaciones derivadas del derecho de acceso a la información pública, lo hará con motivación honesta, leal y desprovista de cualquier intención dolosa o culposa.

Control – Clasificación de la información.

Lineamientos principales: La información calificada como datos abiertos es evaluada por el proceso de gestión documental para autorizar su publicación en el portal datos.gov.co.

5.1.3 Principios de seguridad para la interoperabilidad

Corresponde a los principios y lineamientos de seguridad que deben seguirse al intercambiar información entre sistemas y organizaciones. Incluye medidas para garantizar la autenticidad, integridad y confidencialidad de los datos durante su transmisión y recepción, así como protocolos de comunicación segura y mecanismos de autenticación y autorización para asegurar la confianza y la interoperabilidad entre los sistemas.

A su vez, el objetivo de la interoperabilidad es mejorar la experiencia del ciudadano al facilitar el acceso a los servicios estatales de manera integral y segura. Al evitar que los ciudadanos deban acudir a múltiples entidades, se agilizan los procesos y se optimiza el tiempo. Además, se garantiza que la información personal sea manejada con la mayor confidencialidad y que los derechos fundamentales estén protegidos.

En este sentido, se requiere la implementación de sistemas y controles de seguridad avanzados para proteger la información de los ciudadanos y garantizar la confiabilidad de los servicios digitales.

5.1.3.1 Principios de seguridad, protección y preservación de la Información: Deberán aplicarse medidas y controle que aseguren, protejan, preserven y mantengan la privacidad de la información susceptible de interoperar generando un entorno seguro y de confianza que permita transmitir a los ciudadanos una sensación de seguridad, donde se vela por sus intereses y se cuida la privacidad de la información y se respeta plenamente la normativa aplicable cada vez que interactúan con el Estado. Aquellos datos que pertenezcan a ciudadanos y cuya pérdida y/o alteración pueda significar algún tipo de inconveniente para ellos con el Estado, deberán ser especialmente protegidos evitando el uso no autorizado y garantizando su integridad, disponibilidad y resguardo. Los ciudadanos y empresas tendrán el derecho a conocer, actualizar y rectificar la información que se haya recogido las entidades, así como demás derechos, libertades o garantías relacionadas con la recolección, tratamiento y circulación de datos personales. En términos de preservación de la información para las consultas históricas de los

servicios de intercambio de información, las entidades deberán considerar el almacenamiento de históricos de los datos y ofrecer servicios interoperables para que se pueda acceder a la información compartida o intercambiada durante un período de tiempo determinado.

Control – Política de Seguridad de la Información

Lineamientos principales: La Contraloría de Bogotá como órgano de control fiscal del Distrito, está comprometida con preservar la confidencialidad, Integridad, disponibilidad y veracidad de sus activos de información, reduciendo los riesgos de seguridad digital a través del mejoramiento continuo de los controles en sus procesos, planes y proyectos, el cumplimiento de la normatividad vigente, la aplicación de lineamientos de la Política de Gobierno Digital y la adopción de buenas prácticas de seguridad de la información que contribuyan al logro de los objetivos institucionales y faciliten el aprovechamiento de las tecnologías de la información y las comunicaciones para que la entidad constantemente sea más proactiva e innovadora.

5.1.3.2 Principios de Neutralidad tecnológica y adaptabilidad: El desarrollo de servicios de intercambio de información se deberá orientar en la atención de las necesidades manifiestas de los ciudadanos y empresas; por lo tanto, la construcción de estos servicios deberá orientarse por la funcionalidad y no por la tecnología que ofrezca una herramienta o proveedor en particular. Las decisiones de tecnología, durante el desarrollo de un servicio de intercambio de información, deberán guiarse por el uso de especificaciones que faciliten su interconexión con el mayor número de sistemas que conforman el ecosistema de soluciones con el que interopera. Los servicios de intercambio de información no deberán exigir, por parte de las entidades, ninguna tecnología exclusiva o limitada al ámbito de un proveedor o plataforma, así mismo, las entidades públicas deben dar acceso a sus servicios de intercambio de información con independencia de cualquier tecnología o producto concreto y permitir su reutilización.

Control – Seguridad para intercambio de información

Lineamientos principales: Con el fin de adoptar lineamientos que se deben aplicar al momento de realizar intercambios de información con otras entidades con el fin de habilitar el cumplimiento de obligaciones misionales y, facilitar la prestación de servicios o mejorar la entrega de valor, la entidad adopta el documento de “Lineamientos de seguridad para el intercambio, transferencia o transmisión de datos personales”. Disponible en el sistema integrado de planeación y gestión de la entidad.

5.2 Política de gestión de continuidad para el Gobierno de Datos

La gestión de continuidad del Gobierno de Datos de la Contraloría de Bogotá se desarrollará en concordancia con lo definido en el documento técnico de Gestión de Continuidad del negocio[2], con el fin de garantizar la disponibilidad y continuidad de las actividades del Gobierno de Datos.

En este sentido, se acoge el lineamiento mediante el cual se recomienda que, en cada vigencia, se lleven a cabo actividades correspondientes al ciclo PHVA, planificando las actividades para el periodo vigente, seguido de la recopilación de resultados de pruebas centradas en los aplicativos, portales, sistemas de información, procesos, servicios y actividades críticas. Este enfoque permite analizar los riesgos asociados a la continuidad, realizar actividades de continuidad, pruebas y sensibilización, mantener el plan de continuidad del negocio y finalizar con la implementación de los planes de acción generados.

De acuerdo con lo anterior, se deben aplicar los siguientes lineamientos para la continuidad del Gobierno de Datos:

1. **Gestión del riesgo y análisis de impacto al negocio:** Los riesgos asociados a la pérdida de continuidad de los servicios de gobierno de datos se gestionan mediante la metodología de gestión de riesgos institucional. Los riesgos de continuidad de negocio se clasifican como riesgos de seguridad digital y para los riesgos identificados se identifican planes de tratamiento. Cada proceso es el responsable de identificar y definir las actividades de mitigación de sus riesgos.
2. **Gestión frente a fallas del Data Center principal:** En caso de pérdida de continuidad de servicios, la entidad cuenta con copias de respaldo de los sistemas de información cuya administración técnica se encuentran a cargo de la Dirección de TIC. En caso de presentarse activación del plan de continuidad, la entidad debe recurrir a las copias de respaldo más reciente y disponibles, la cuales serán restauradas de acuerdo con los requerimientos de cada sistema según sea el caso**.**
3. **Recuperación de desastres:** Los sistemas de información responsables de las actividades de Gobierno de Datos, se deben incluir en la estrategia de recuperación antes desastres tecnológicos institucional. En este sentido, se busca restablecer con la mayor brevedad posible el funcionamiento de la infraestructura tecnológica por ocurrencia de un evento, en aras de minimizar el impacto y garantizar la correcta recuperación de la información o datos de la entidad que involucren la infraestructura de TI, así como definir el conjunto de actividades, roles y responsabilidades que permitan el restablecimiento de la operación normal de la plataforma tecnológica de la entidad.
4. **Ataques Cibernéticos:** La Contraloría de Bogotá, D.C., siguiendo los lineamientos del Sistema de Gestión de Seguridad de la Información - SGSI, valida el cumplimiento de los

[2] https://contraloriadebogotadc.sharepoint.com/sites/Intranetnew/SitePages/Plan-de-Continuidad-del-Negocio.aspx

controles asociados a la infraestructura tecnológica, principalmente en lo relacionado al Gobierno de Datos.

5. **Proveedores críticos:** De acuerdo con el plan de continuidad de negocio, los proveedores críticos garantizan y/o certifican, que cuentan con un plan de continuidad del Negocio documentado, aprobado y probado anualmente, con el fin de asegurar su efectividad y garantizar la prestación del servicio contratado por la Contraloría de Bogotá, D.C. Para los proveedores que llegaren a ser contratados que cuentan con la infraestructura tecnológica en la nube, y/o soporten los servicios con aplicaciones en la nube se recomienda incluir dentro del plan de continuidad la disponibilidad de los servicios, estrategia de recuperación utilizada y copia de respaldo de la información de la entidad para así garantizar la continuidad y disponibilidad del servicio contratado.
6. **Verificación, revisión y evaluación de la continuidad:** Se deben realizar verificaciones de los procedimientos de operación alterna, evaluación del estado de riesgos de continuidad y pruebas de la estrategia de continuidad de las actividades de Gobierno de Datos, en el marco de la evaluación del plan de continuidad institucional.
7. **Capacitación en procedimientos de operación alterna:** Se deben realizar actividades de socialización de la estrategia de continuidad de negocio y procedimientos alternos de operación que incluyan actividades del Gobierno de Datos.
8. **Redundancias:** La infraestructura de procesamiento de datos requerida para las operaciones de gobierno de datos se soporta en equipos con redundancias a nivel de potencia eléctrica, equipos de procesamiento de datos y almacenamiento en nube.

5.3 Arquitectura TIC

La arquitectura TIC proporciona la base de la infraestructura tecnológica que soporta la gestión de los datos, las herramientas de gestión de datos y las aplicaciones que interactúan con los datos. De igual manera, ayuda a garantizar la calidad de los datos a través de mecanismos como la validación de datos, la transformación de datos y la integración de datos.

Teniendo en cuenta el marco de referencia del Gobierno de Datos (DMBOK-Data Management Body of Knowledge), se define un modelo de arquitectura de datos que proporciona una vista holística de los datos de la entidad, incluyendo su estructura, relaciones y uso.

Bajo esta perspectiva, a continuación, se presentan los lineamientos que soportan la Arquitectura de TI para el Gobierno de Datos.

5.3.1 Arquitectura de Datos Maestros

La arquitectura de los Datos Maestros de la Contraloría de Bogotá, inicia desde la definición del procedimiento para la gestión de los datos, los sistemas de información involucrados, el administrador de datos, el líder de datos y los gestores de los datos.

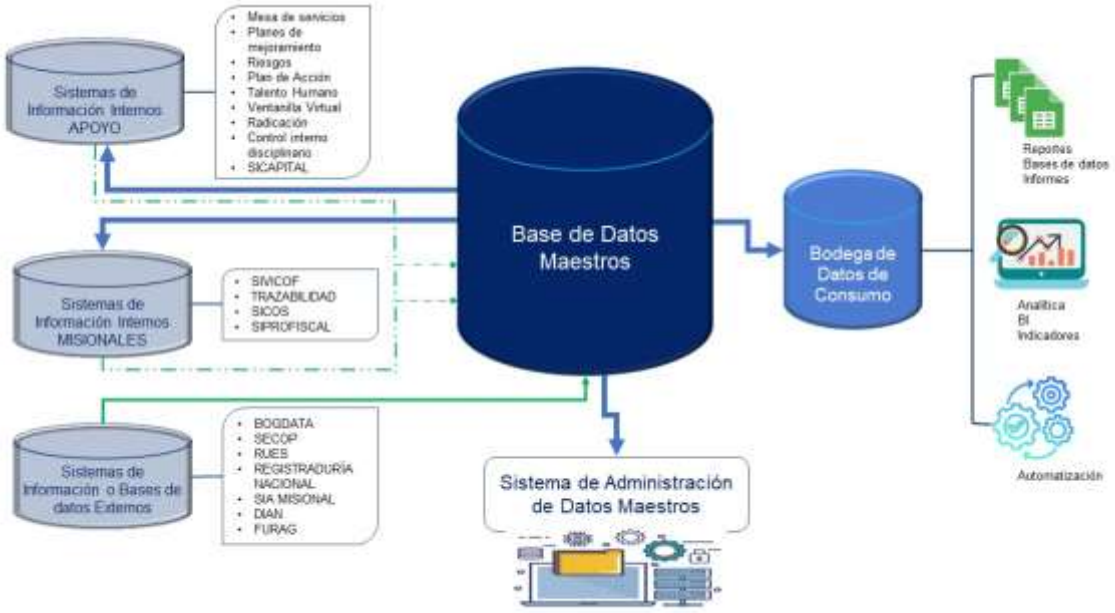
En este sentido, se definen las fuentes de información interna o externas, sobre las cuales se deben desarrollar mecanismos de extracción para cargar la información de Datos Maestros.

El repositorio de datos maestros, contiene los procesos de información que se encargaran de ejecutar las políticas de calidad, almacenamiento de los datos, gestión de usuarios del sistema de gestión de Datos Maestros y políticas de perfilamiento.

El sistema de gestión de datos maestros permite al administrador de datos gestionar las políticas definidas y aprobadas en el Comité de Gobierno de Datos, y contar con una interfaz gráfica donde se podrán administrar las políticas de los datos maestros, definir modelos de datos, crear reglas para actualizar los mismos y controlar quién actualiza los datos.

En cuanto a la trasmisión de datos de los sistemas de información internos y la base de datos maestros se realizará de acuerdo con los lineamientos aplicables de cada sistema de información y los protocolos para el intercambio de datos aprobado por la entidad.

Ilustración 2 Arquitectura de Datos Maestros de la Contraloría de Bogotá



Fuente: Elaboración propia

5.3.2 Línea base tecnológica recomendada para analítica de datos

La siguiente imagen muestra el mapa de habilitadores tecnológicos de referencia para la construcción de sistemas, software u otros habilitadores tecnológicos que pueden ser útiles para la analítica de datos:

Ilustración 3 Línea base tecnológica recomendada para analítica de datos de la Contraloría de Bogotá



Fuente: Elaboración propia

Tabla 4 Descripción de la línea base tecnológica para analítica de datos de la Contraloría de Bogotá

Software	Descripción	Open-premise /Licencia
Python	Es un lenguaje de programación interpretado, de alto nivel y multiplataforma. Es ampliamente utilizado en el análisis de datos, inteligencia artificial, desarrollo web y automatización de tareas.	On-premise/ License (PSF)
Visual Studio Code	Es un editor de código fuente multiplataforma desarrollado por Microsoft. Es altamente personalizable y compatible con una amplia gama de lenguajes de programación, incluido Python, R y SQL.	On-premise/ Licencia MIT Gratuita

Software	Descripción	Open-premise /Licencia
Python Package Index (PyPI)	Es un repositorio de software donde los programadores de Python pueden publicar y descargar paquetes de código reutilizable. Facilita la instalación y gestión de librerías y frameworks para Python.	On-premise/licencia Apache 2.0
R	Es un lenguaje de programación y un entorno de software libre para análisis estadístico y gráficos. Es ampliamente utilizado en investigación, finanzas y ciencia de datos.	On-premise/ License (GPL-2/GPL-3)
Power BI	Es un conjunto de herramientas de análisis de negocios de Microsoft que permite visualizar datos y compartir información a través de paneles e informes interactivos.	SaaS/ Gratuito para uso personal, Licencia por suscripción mensual para power bi pro
SQL Server	Es un sistema de gestión de bases de datos relacional (RDBMS) desarrollado por Microsoft. Se utiliza para almacenar, gestionar y analizar datos estructurados.	Onpremise o Cloud/ Standard y Enterprise (pago por licencia)
Power Platform	Es un conjunto de herramientas de Microsoft que permite a los desarrolladores y analistas de negocios crear aplicaciones, automatizar procesos y analizar datos sin necesidad de codificación tradicional.	SaaS/ Modelo de suscripción basado en usuarios y capacidades
Git	Es un sistema de control de versiones distribuido, utilizado para realizar un seguimiento de cambios en archivos y coordinar el trabajo en proyectos de desarrollo de software.	Onpremise, SaaS/ License version 2.0 (GPL-2.0)
Jenkins	Es una herramienta de integración continua open source que permite automatizar tareas como la compilación, pruebas y despliegue de aplicaciones.	SaaS/ Software libre y de código abierto
Power BI Services	Es un servicio en la nube de Microsoft que permite publicar y compartir informes y paneles de Power BI con otros usuarios.	SaaS/ Modelo de suscripción mensual por usuario
Jupyter	Es una aplicación web de código abierto que permite crear y compartir documentos que contienen código ejecutable, visualizaciones, texto explicativo y ecuaciones matemáticas.	On-premise, SaaS/ Software libre y de código abierto
KNIME	Es una plataforma de análisis de datos open source que permite crear flujos de trabajo de minería de datos, aprendizaje automático y procesamiento de datos.	OnPremise/ GNU General Public License (GPL-3.0)
Hadoop	Es un marco de trabajo de código abierto para el procesamiento distribuido de grandes conjuntos de datos a través de clústeres de computadoras.	On-premise/ Apache License 2.0
Spark	Es un motor de análisis de código abierto que permite el procesamiento de datos a gran escala y el aprendizaje automático en clústeres de computadoras.	On-premise/ Software libre y de código abierto
ETL (Extract, Transform, Load)	Es un proceso que involucra la extracción de datos de diversas fuentes, la transformación de los datos según reglas específicas y la carga de los datos transformados en un almacén de datos o sistema de análisis.	Software libre y de código abierto.

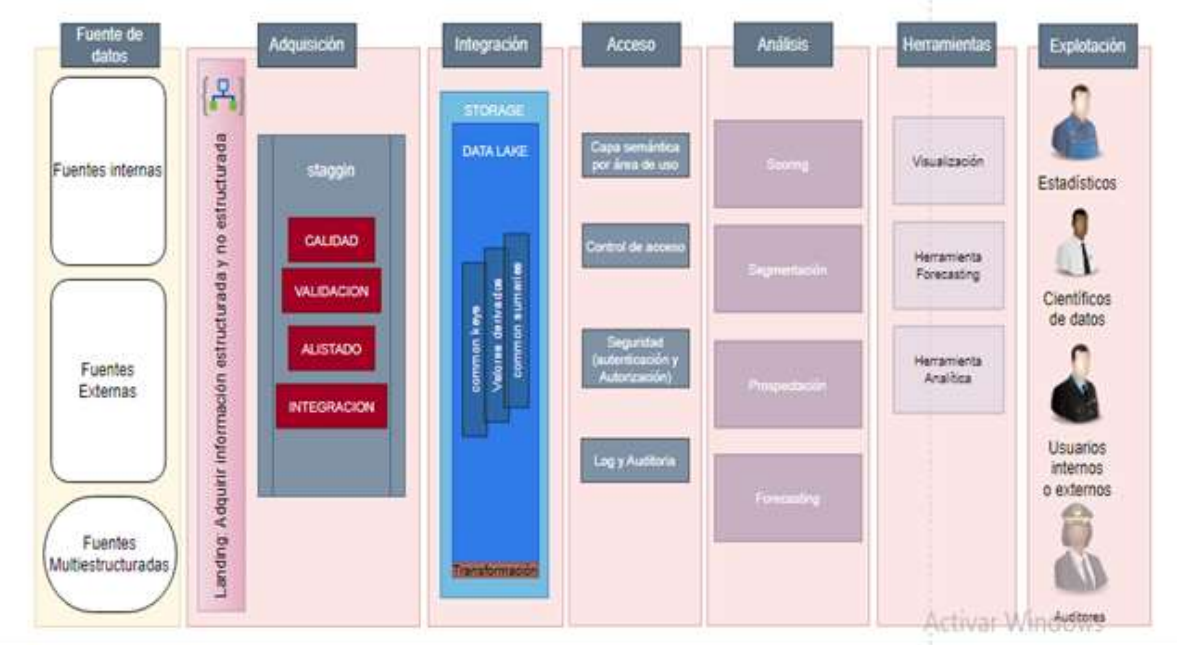
Software	Descripción	Open-premise /Licencia
ELT (Extract, Load, Transform)	Es un enfoque alternativo al ETL donde los datos se extraen y cargan primero en un área de preparación, y luego se transforman allí antes de cargarlos en su destino final.	Software libre y de código abierto.
Power BI Gateway	Es un componente de Power BI que permite conectarse de forma segura a fuentes de datos locales o en la nube desde informes y paneles de Power BI.	SaaS/ Licencia por suscripción

Fuente: Elaboración propia

5.3.2.1 Arquitectura para analítica de datos institucional

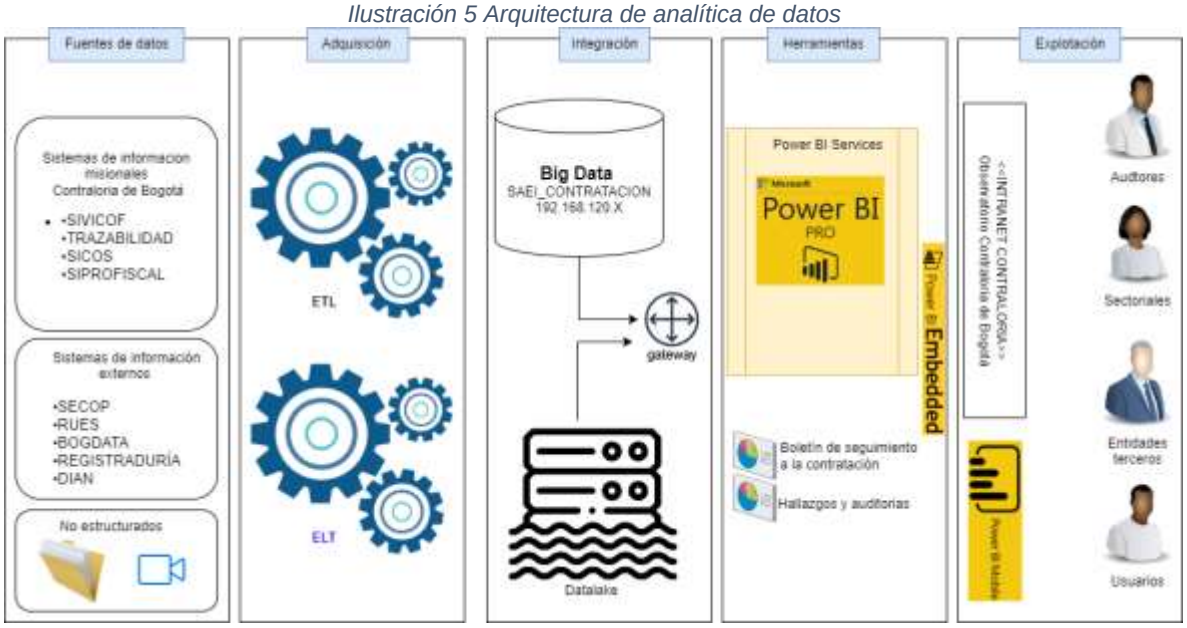
Arquitectura de referencia que tomará la entidad:

Ilustración 4 Arquitectura de referencia de información por capas



Fuente: Elaboración propia

Ilustración 5 Arquitectura de analítica de datos



Fuente: Elaboración propia

Fuentes de datos: Se recomienda dejar la opción para el manejo documentos estructurados y no estructurados.

Adquisición: Se recomienda manejar ETL y ELT para la transferencia de información al repositorio formal

Integración: Se recomienda mejorar las características del Big Data y dejarla en la Nube contratada por la entidad, adicional abastecer un Datalake.

Herramientas: De forma complementaria a las herramientas de Power Bi pro actuales se recomienda manejar Power BI Embedded para mejorar las capacidades de reporterías en los portales.

1. Se extrae información de las fuentes de datos internas mediante consultas a los sistemas de información de la Contraloría de Bogotá, y esta información se transfiere al entorno de Big Data a través de vistas.
2. Las fuentes de datos de SECOP y RUES se integran en el entorno de Big Data mediante la importación directa de datos.
3. El entorno de Big Data está alojado en la plataforma de la Contraloría de Bogotá y se accede a través del ambiente entregado por el Dirección de Tecnologías de la Información y las Comunicaciones en el marco de la política de Seguridad de la Información.
4. Actualmente, los informes se generan y visualizan en Power BI Services, se recomienda contar con un Gateway para facilitar la conexión.
5. Se recomienda que los informes estén disponibles para su consulta en la intranet y página web en la sección que se determine de acuerdo con la naturaleza de dichos informes.

5.3.2 Integración e interoperabilidad

En el marco del Gobierno de Datos, la integración e interoperabilidad desempeñan un papel fundamental para garantizar el intercambio eficiente y transparente de información entre la Entidad y los diferentes actores internos y externos. Esta sección aborda los siguientes aspectos:

Información que se expone desde o hacia la Contraloría:

- Definir claramente los conjuntos de datos, informes y documentos que deben ser compartidos con entidades externas, garantizando el cumplimiento de las regulaciones y normativas aplicables. Cada área o proceso, podrá realizar la identificación del conjunto de datos a intercambiar o interoperar, bajo los lineamientos del presente manual.
- Establecer protocolos y mecanismos seguros para el intercambio de información sensible o confidencial.

Transferencia de Archivos:

- Implementar canales y protocolos estandarizados para la transferencia de archivos, ya sean estructurados o no estructurados, asegurando la integridad, confidencialidad y trazabilidad de los datos.
- Definir formatos de archivo compatibles y promover el uso de estándares abiertos para facilitar la interoperabilidad.

Integración en Línea:

- Habilitar la integración en tiempo real de sistemas y aplicaciones mediante el uso de servicios web, mensajería y protocolos de comunicación seguros.
- Implementar mecanismos de autenticación y autorización robustos para garantizar el acceso controlado a los datos.

APIs (Interfaces de Programación de Aplicaciones):

- Desarrollar y mantener APIs bien documentadas y estandarizadas para facilitar el acceso y la integración de los sistemas y aplicaciones de la Entidad con sistemas externos.
- Establecer políticas y procedimientos para la gestión del ciclo de vida de las APIs, incluyendo el control de versiones, la monitorización y la seguridad.

Información Estructurada y No Estructurada:

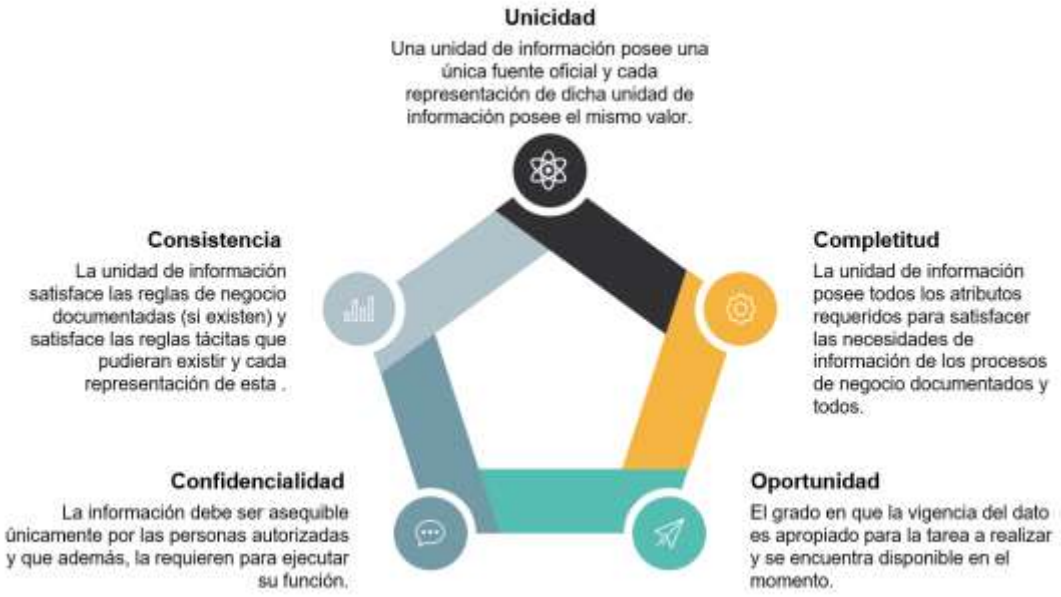
- Implementar estrategias para la gestión y procesamiento de información estructurada (bases de datos, hojas de cálculo, etc.) y no estructurada (documentos, correos electrónicos, redes sociales, etc.).

- Utilizar técnicas de minería de texto, procesamiento de lenguaje natural y otras tecnologías avanzadas para extraer conocimiento valioso de la información no estructurada.

5.4 Política de calidad de los datos

Para el Gobierno de Datos de la Contraloría de Bogotá, la política de calidad se enmarca bajo los lineamientos del modelo de Calidad de Producto de Datos definido por el estándar ISO/IEC 25012[3], tomando como referencia las siguientes características:

Ilustración 6 Criterios de calidad



Fuente: Elaboración propia

Estas características de Calidad de Datos se deben tener en cuenta a la hora de evaluar las propiedades de un producto de datos determinado. En este sentido, la Calidad del Producto de Datos se puede entender como el grado en que los datos satisfacen los requisitos definidos por la organización a la que pertenece el producto.

Por otra parte, la política de Calidad de Datos de la Contraloría de Bogotá, D.C., debe guardar coordinación coherencia con la política de calidad institucional, mediante la cual la entidad asume el compromiso de implementar, mantener y mejorar el Sistema Integrado de Gestión - SIG, bajo los estándares internacionales y nacionales de las normas ISO 27001, ISO 9001, ISO 14001, ISO 45001, Decreto 1072 de 2015 - Resolución 0312 de 2019 y Decreto 1008 de 2018, la Gestión Integral de Riesgos, los Sistemas de Gestión Documental y Archivo – SIGA y la

[3] Tomado de: https://iso25000.com/index.php/normas-iso-25000/iso-25012

Dimensión 7 (Modelo Estándar de Control Interno – MECI) del MIPG, cumpliendo con la legislación vigente y otras responsabilidades aplicables a su naturaleza jurídica.

5.4.1 Actividades preventivas y correctivas

Se deben implementar metodologías para el análisis identificación y mitigación de no conformidades que afecten el buen desempeño del Gobierno de Datos, por lo tanto, se sugieren las siguientes actividades preventivas:

a) Definir procesos y controles para garantizar la calidad, integridad, confidencialidad y disponibilidad de los datos durante todo su ciclo de vida.
b) Establecer mecanismos de monitoreo continuo de la calidad de los datos, incluyendo métricas e indicadores clave de rendimiento (KPIs) alineados con los estándares internacionales y las mejores prácticas.
c) Implementar programas de capacitación y sensibilización para el personal involucrado en la gestión de datos, con el fin de fortalecer sus competencias y promover una cultura orientada a la calidad de los datos.
d) Desarrollar planes de respaldo y recuperación de datos, así como estrategias de preservación y protección de la información institucional, alineados con los sistemas de gestión de riesgos y seguridad de la información.
e) Establecer procesos de revisión periódica y auditoría interna para identificar posibles riesgos, vulnerabilidades o desviaciones en la calidad de los datos y su gestión.

Así mismo como acciones correctivas se aplica:

a) Definir procedimientos y planes de acción para abordar de manera oportuna las no conformidades o incidentes relacionados con la calidad de los datos que sean detectados.
b) Implementar mecanismos de retroalimentación y mejora continua, utilizando los hallazgos y lecciones aprendidas de las actividades de monitoreo, auditoría y revisión.
c) Realizar ajustes y actualizaciones en los procesos, políticas, estándares y herramientas de gestión de datos, según sea necesario, para abordar las áreas de mejora identificadas.
d) Establecer canales de comunicación efectivos con los clientes y partes interesadas, para recibir y atender de manera oportuna las consultas, peticiones o reclamos relacionados con la calidad de los datos.
e) Promover la participación activa de los diferentes actores involucrados en el modelo de gobierno de datos (áreas de negocio, TI, seguridad, etc.) en la identificación, análisis y resolución de problemas o desafíos relacionados con la calidad de los datos.
f) Asignar recursos suficientes (humanos, tecnológicos, financieros) para implementar de manera efectiva las acciones correctivas y preventivas necesarias para mantener y mejorar continuamente la calidad de los datos y su gestión en la organización.

5.4.2 Indicadores de calidad

El seguimiento y medición de los procesos se realiza a través de los indicadores de gestión incorporados en los planes, programas y proyectos, lo cuales permiten una visión clara e integral de su comportamiento, el seguimiento al cumplimiento de metas y de los resultados previstos permite identificar desviaciones sobre las cuales se deben tomar los correctivos que garanticen mantener la orientación de la Entidad hacia el cumplimiento de sus objetivos institucionales.

Con el fin de realizar monitoreo y seguimiento a la implementación del modelo de gobierno de datos en la entidad se establecen los siguientes indicadores con los cuales se medirá la calidad de los datos a gobernar.

Tabla 5 Indicadores del Gobierno de Datos

Tipo de indicador	Característica a medir	Propósito	Formula	Periodicidad de medición	Nivel de referencia	Meta
Operativo	**Completitud de la información**	Medir el grado en que las bases de datos reflejan la totalidad de información requerida por el negocio	Total de datos nulos o campos vacíos/Total de datos sistema de información *100	Trimestral	Aceptable: 60%	Anual
Operativo	**Conformidad de la información**	Medir el grado en que la información es aceptada por el negocio	Total de datos que no cumplen con el dominio o formato definido/Total de datos sistema de información *100	Semestral	Aceptable: 60%	Anual
Operativo	**Consistencia de la información**	Medir que la información sea la misma en todas las áreas o sistemas	Total, de fuentes o atributos diferentes en todos los sistemas de información/Total fuentes y atributos de todos los sistemas de información *100	Trimestral	Aceptable: 70%	Anual
Operativo	**Duplicidad de la información**	Medir e identificar múltiples instancias que son innecesarias frente al mismo objeto	Total de registros duplicados/Total de registros del sistema de información*100	Semestral	Aceptable: Hasta 5%	Anual
Operativo	**Exactitud de la información**	Medir el grado en que la información refleja lo que está pasando en el negocio	Total de registros inexactos o inconsistentes/Total de registros del sistema de información*100	Semestral	Aceptable: 70%	Anual

Fuente: Elaboración propia

5.5 Política de gestión del cambio

Esta política se enfoca en el desarrollo de una cultura organizacional basada en el uso y aprovechamiento de los datos como herramienta fundamental de la gestión institucional.

Bajo este enfoque, la gestión del cambio del Gobierno de Datos, se centrará en la comunicación y colaboración efectiva para involucrar a los servidores, contratistas, proveedores y demás actores que deben participar activamente en el proceso de cambio, asegurando que todos los aspectos estén alineados con los objetivos estratégicos institucionales.

Una cultura institucional fuerte y la gestión eficaz del cambio son fundamentales para que la Contraloría de Bogotá se adapte a las condiciones y avances actuales de la tecnología en lo relacionado con la gestión y uso de los datos, mejorando significativamente los resultados en el corto, mediano y largo plazo.

Para asegurar la aplicación permanente de la política de gestión del cambio del Gobierno de Datos, el Comité del Gobierno de Datos deberá garantizar el desarrollo de las siguientes estrategias:

1. Incluir en la estrategia anual de formación y capacitación temáticas relacionadas con gobierno de datos y datos maestros.
2. Las dependencias técnicas que tengan a cargo sistemas de información deben incluir programas de sensibilización con usuarios con el fin de mejorar la calidad de los datos desde la captura.
3. Elaborar estrategias de difusión de las políticas y estándares definidas o actualizadas en el marco del programa de gobierno de datos.
4. Evaluar la adopción y apropiación de conceptos y lineamientos para el uso adecuado de la información producida y administrada por la Entidad.

6. Metodología para proyectos de datos

La metodología de referencia para el desarrollo de proyectos de datos, en el marco del Gobierno de Datos de la entidad, se concibe como un ciclo continuo de mejora que busca optimizar la toma de decisiones a través de un análisis preciso del comportamiento de los sistemas y el impacto de las acciones ejecutadas. Este proceso se sustenta en un ambiente colaborativo de trabajo, fomentando la interacción entre generadores de información, expertos y usuarios finales.

La efectividad de esta metodología depende de la capacidad del líder del proyecto o líder del habilitador tecnológico para promover un entorno colaborativo donde exista un intercambio constante y constructivo de conocimientos y experiencias entre los diversos actores (generadores de información, expertos y usuarios). Esto permite una evolución continua del Gobierno de Datos que se adapta dinámicamente a las necesidades cambiantes de la entidad.

Los pasos definidos para este ciclo son:

Ilustración 7 Metodología para proyectos de datos



Fuente: Elaboración propia

Paso 1: Diagnóstico y planeación

Este primer paso se enfoca en comprender la necesidad que resolverá el proyecto, los objetivos a conseguir, los elementos clave y las interacciones entre los diferentes actores, así como la planificación de posibles riesgos. La definición y planeación del proyecto se debe realizar con un enfoque de analítica de datos apalancado en tecnologías emergentes como la Inteligencia Artificial y el Block Chain, entre otras que surjan y faciliten el procesamiento de información, identificación de patrones de comportamiento, relaciones de causa-efecto, entre otros ejercicios de inteligencia de negocios, que puedan ser aprovechables para la función de vigilancia y control fiscal.

El proceso de definición deberá contemplar acciones claves como:

- **Definición del problema o necesidad:** En el proceso de identificación del problema o necesidad usualmente se pueden reconocer muchas situaciones negativas que afectan a las personas, recursos o procesos de la entidad, así como a la ciudadanía y grupos de valor. Por lo tanto, se hace necesario disminuir la complejidad mediante la delimitación del ámbito de análisis, estableciendo con la mayor precisión posible el tema propuesto.

  Para mitigar la generalidad en las ideas, se recomienda realizar el listado de aquellas que sean más importantes según la opinión de los miembros que participan en la formulación del proyecto. De llegar a existir algún grado de asociación entre estas situaciones, se deben seleccionar las ideas que tengan relación con la problemática de mayor prioridad de atención.

- **Definición del alcance:** Establecer claramente los objetivos, entregables y alcance del proyecto. De igual manera, se deben proponer los resultados esperados, relacionados con los cambios en las condiciones actuales enmarcadas en el objetivo general del proyecto, por efecto del desarrollo e implementación del proyecto, así como del cumplimiento de los supuestos considerados en el mismo.

- **Modelado:** Corresponde a la descripción detallada de los elementos que componen el sistema, modelo, herramienta o aplicativo de datos, sus interrelaciones, los requerimientos para asegurar la calidad de los datos, y cómo estos influyen en los comportamientos observados o requeridos dentro de la entidad. Se recomienda aplicar técnicas de análisis de datos (estadística, machine learning) para obtener insights relevantes.

- **Identificación y medición de variables:** Seleccionar las variables críticas que afectan el desempeño del sistema y desarrollar mecanismos para su medición y seguimiento, estableciendo indicadores clave de rendimiento (KPIs) que permitan evaluar la efectividad de las estrategias de datos.

Paso 2: Implementación y monitoreo

Durante esta fase, se ejecutan los planes, sistemas o modelos desarrollados en la etapa de planeación, monitorizando continuamente su desempeño a través de las siguientes actividades claves:

- **Implementación:** Integrar los resultados en los procesos de negocio y tomar decisiones basadas en los datos. Se recomienda utilizar servicios de información, reportes y

dashboards para recopilar y analizar datos en tiempo real, asistiendo así la toma de decisiones estratégicas.

- **Monitoreo Continuo:** Evaluación permanente mediante las variables e indicadores definidos, permitiendo ajustes proactivos para mantener o mejorar los niveles de rendimiento.

  Identifique desviaciones y realice ajustes proactivos en los procesos, políticas o recursos asignados para mantener o mejorar los niveles de rendimiento deseados.
- **Gestión del conocimiento:** Capacite a los usuarios clave en el uso efectivo de estas herramientas para facilitar la toma de decisiones basada en datos.

Paso 3: Evaluación y mejora continua

Este paso cierra el ciclo, pero al mismo tiempo abre un nuevo ciclo de mejora, basado en las siguientes actividades claves:

- **Medición del Impacto**: Analizar los resultados obtenidos frente a los objetivos esperados, identificando desviaciones, áreas de oportunidad, desafíos persistentes y lecciones aprendidas durante el ciclo anterior.

- **Retroalimentación y ajustes**: Los hallazgos de la evaluación sirven como base para el ajuste de modelos, estrategias y procesos, con lo cual se inicia un nuevo ciclo de diagnóstico y planeación para refinar continuamente el proyecto de datos en respuesta a los cambios internos y externos, garantizando su alineación con los objetivos estratégicos de la Entidad.

6.1 Consideraciones transversales a los 3 pasos.

Tecnológicas:

- **Infraestructura de datos:** Se deben establecer los requerimientos del proyecto con respecto a la infraestructura para almacenar, procesar y analizar grandes volúmenes de datos.
- **Herramientas de análisis:** Se debe seleccionar herramientas adecuadas para el tipo de análisis a desarrollar con el proyecto (e.g., SQL, Python, R, herramientas de visualización como Tableau, Power BI), verificando la viabilidad técnica y financiera de su adquisición o uso.
- **Ciberseguridad:** Garantizar la seguridad de los datos y el cumplimiento de las regulaciones de privacidad.

- **Integración de sistemas:** Conectar las diferentes fuentes de datos y sistemas de la organización.
- **Procedimientos o lineamientos:** La formulación de los proyectos de datos que impliquen la implementación de una nueva tecnología para la entidad, deberá estructurarse en coherencia a los procedimientos de formulación de proyectos definidos por la Dirección de Tecnologías de la Información y las Comunicaciones o los definidos por la Dirección de Planeación, según aplique en cada caso.

Cultura de datos:

- **Capacitación:** Cada proyecto deberá contemplar un componente de formación dirigido a los usuarios o beneficiarios que puedan utilizar los datos de manera efectiva.
- **Innovación y experimentación:** Crear un ambiente donde se incentive la exploración de nuevos datos y herramientas.
- **Comunicación:** Difundir los resultados de los proyectos y su impacto en la entidad.

6.2 Técnicas para proyectos de analítica de datos.

Los proyectos de analítica de datos podrán contemplar la implementación de modelos basados en las siguientes técnicas (Pisoni, Molnár, & Tarcsi, 2023):

Análisis de Causalidad

Esta técnica busca establecer una relación de causa y efecto entre diferentes variables. En lugar de simplemente correlacionar datos, el análisis de causalidad intenta determinar si un cambio en una variable produce un cambio en otra.

Utilidad para el ejercicio de vigilancia y control fiscal:

- Identificar las causas subyacentes de irregularidades en contratos, pagos o gastos. Por ejemplo, si se observa un aumento inusual en los pagos a un contratista específico, se puede analizar si existen factores causales como conflictos de interés, colusión o falta de control interno.
- Determinar si la implementación de nuevas políticas o regulaciones ha tenido el efecto deseado en términos de reducción de la corrupción o mejora de la eficiencia.
- Identificar los factores que influyen en la duración de los procesos de auditoría, para proponer mejoras y reducir tiempos.

Técnicas comunes:

- **Modelos de ecuaciones estructurales:** Permiten analizar relaciones causales complejas entre múltiples variables.
- **Análisis de series de tiempo**: Se utilizan para identificar patrones causales en datos históricos.

- **Experimentos naturales:** Aprovechan eventos externos (como cambios en la legislación) para evaluar sus efectos causales.

Análisis Predictivo

El análisis predictivo utiliza datos históricos y modelos estadísticos para predecir eventos futuros.

Utilidad para el ejercicio de vigilancia y control fiscal:

- Identificar transacciones o patrones de gasto que se desvían de lo normal, lo que podría indicar posibles irregularidades.
- Evaluar el riesgo de fraude o corrupción en diferentes áreas de la administración pública.
- Predecir la demanda de servicios públicos para verificar la asignación de los recursos de manera más eficiente.

Técnicas comunes:

- **Aprendizaje automático:** Algoritmos como árboles de decisión, redes neuronales y bosques aleatorios se utilizan para construir modelos predictivos.
- **Series de tiempo:** Se emplean para predecir variables como el gasto público o el número de denuncias.

Análisis Prescriptivo

Más allá de la predicción, ofrece recomendaciones sobre las mejores acciones a tomar en función de los resultados del análisis.

Utilidad para el ejercicio de vigilancia y control fiscal:

- Sugerir las mejores opciones para investigar denuncias, asignar auditores o tomar medidas correctivas.
- Evaluar el impacto de diferentes decisiones políticas o de gestión para generar recomendaciones para la priorización y programación de la planeación distrital.
- Identificar las tareas que pueden automatizarse para mejorar la eficiencia y reducir el error humano.

Técnicas comunes:

- **Optimización matemática:** Se utiliza para encontrar la solución óptima a problemas complejos.
- **Simulación:** Permite modelar sistemas complejos y evaluar diferentes escenarios.

7. Herramientas recomendadas para el Gobierno de Datos

Existen varias herramientas que son ampliamente utilizadas en el desarrollo del Gobierno de Datos para facilitar la gestión, el control y la implementación de políticas y procesos relacionados con los datos en una organización. Algunas de estas herramientas recomendadas son:

Collibra: Es una plataforma de Gobierno de Datos líder en el mercado que ofrece una variedad de soluciones para la gestión de datos, incluyendo catálogos de datos, metadatos, gestión de calidad de datos, gestión de políticas y cumplimiento, y más.

Informatica Axon: Axon es una solución de gestión de metadatos y Gobierno de Datos que ayuda a las organizaciones a establecer políticas, normas y procesos para la gestión y el control de los datos. También proporciona capacidades de automatización y seguimiento para garantizar el cumplimiento de las políticas de datos.

IBM InfoSphere Information Governance Catalog: Esta herramienta de IBM ofrece un catálogo de datos centralizado que permite a las organizaciones gestionar y compartir metadatos, definir políticas de datos, realizar análisis de impacto de datos y asegurar la calidad de los datos.

Dataiku Data Governance: Dataiku ofrece una plataforma de Gobierno de Datos que permite a las organizaciones definir y gestionar políticas de datos, identificar y gestionar datos sensibles, gestionar el acceso a los datos y garantizar la conformidad con las regulaciones de privacidad y seguridad.

Alation Data Catalog: Alation es una plataforma de catálogo de datos que ayuda a las organizaciones a descubrir, catalogar y colaborar en torno a los datos. Ofrece capacidades de búsqueda inteligente, recomendaciones de conjuntos de datos relevantes, colaboración y Gobierno de Datos.

Informatica Data Quality: Esta herramienta proporciona capacidades avanzadas para la gestión de la calidad de los datos, incluyendo la identificación, limpieza, estandarización y enriquecimiento de datos, así como la monitorización y mejora continua de la calidad de los datos.

SAP Data Intelligence: SAP Data Intelligence es una plataforma de Gobierno de Datos que permite a las organizaciones gestionar y gobernar sus datos de manera efectiva. Ofrece capacidades de catalogación de datos, gestión de metadatos, integración y transformación de datos, calidad de datos y más.

Talend Data Catalog: Talend ofrece una solución de catalogación de datos que permite a las organizaciones descubrir, catalogar y gestionar sus datos de manera centralizada. La herramienta ofrece capacidades de búsqueda y descubrimiento de datos avanzadas, colaboración, gestión de metadatos y Gobierno de Datos.

Microsoft Azure Purview: Azure Purview es una plataforma de Gobierno de Datos en la nube que ofrece capacidades de catalogación de datos, gestión de metadatos, Gobierno de Datos y cumplimiento de regulaciones y normativas. Permite a las organizaciones descubrir, entender y gobernar sus datos de manera efectiva.

8. Procedimiento de uso de datos

8.1 Datos maestros y datos críticos

8.1.1 Datos maestros

Los datos maestros son de carácter fundamental debido a que generan información central para la entidad. Esto se debe a que representan los elementos clave sobre los cuales se construye y operan los procesos, suelen ser estructurados y están bien definidos, actuando como la base sobre la cual se gestionan todas las operaciones y decisiones.

La calidad y precisión de los datos maestros son cruciales, ya que cualquier error o inconsistencia en ellos puede afectar negativamente a múltiples áreas de la entidad, por lo tanto, es común implementar procesos de gestión de datos para asegurar que los datos maestros sean confiables, actualizados y consistentes.

Para la Contraloría de Bogotá, los datos maestros son aquellos esenciales para la continuidad de la entidad, proteger estos datos es crucial para evitar interrupciones en la atención a los ciudadanos y usuarios, fallas legales, errores en sistemas dependientes y fugas de información.

Los datos considerados como maestros son:

a) Datos de auditoría.
b) Datos financieros y presupuestales.
c) Datos de planeación, control y seguimiento.
d) Datos de investigaciones internas y externas.
e) Datos de contratos y proveedores.
f) Datos personales de empleados y ciudadanos.

Estos datos son esenciales para el funcionamiento adecuado de la entidad y su divulgación indebida o compromiso podría tener graves repercusiones en la integridad de las operaciones y la confianza pública. Por lo tanto, es crucial protegerlos adecuadamente mediante medidas de seguridad y cumplimiento normativo.

8.1.2 Datos críticos

Pueden incluir datos maestros, pero también otros tipos de datos que son necesarios para llevar a cabo las operaciones diarias, como datos de transacciones, datos de análisis, etc. Los datos maestros se centran en las actividades clave, mientras que los datos críticos abarcan un espectro más amplio de información.

Los datos maestros proporcionan una base sólida para la gestión de la información, mientras que los datos críticos son aquellos que son necesarios para llevar a cabo las tareas específicas de una organización.

No todos los datos críticos son datos maestros, ya que pueden incluir otros tipos de información además de los datos de las entidades clave.

Los datos considerados como críticos son:

a) Datos de auditoría del proceso de Vigilancia y Control Fiscal
b) Datos de los procesos de Responsabilidad Fiscal
c) Datos de investigaciones internas y externas.
d) Datos de los sistemas de información institucionales (aplicativos)
e) Bases de datos obtenidas de fuentes externas oficiales como Registraduría Nacional del Servicio Civil, SECOP, DIAN, Cámaras de Comercio, RUES, entre otros.

Sin perjuicio de lo definido en el presente manual, la entidad debe elaborar el catálogo de datos donde se realice la clasificación de datos maestros y críticos.

8.2 Ciclo de vida de los datos

La gestión del ciclo de vida del dato es un proceso indispensable para alcanzar el aprovechamiento de los datos dispuestos en la infraestructura de datos del Estado. El ciclo de vida de los datos de la Contraloría de Bogotá está integrado por diferentes fases como se muestra en la siguiente figura:

Ilustración 8 Ciclo de vida del dato



Fuente: Elaboración propia - DIAGNÓSTICO SCD E INFRAESTRUCTURA DE DATOS

El ciclo de vida de los datos describe el recorrido que sigue un conjunto de datos desde su creación hasta su eliminación o archivo. Cada fase del ciclo de vida de los datos es fundamental para garantizar la calidad, integridad y valor de la información. Un ciclo de vida de los datos bien gestionado permite a las organizaciones tomar decisiones más informadas, mejorar la eficiencia operativa y obtener una ventaja competitiva. A continuación, se detallan la descripción del proceso que ocurre en cada fase:

Tabla 6 Descripción del ciclo de vida de los datos

FASE CICLO DE VIDA	DESCRIPCIÓN
Creación	Los datos pueden provenir de diferentes fuentes, estructuradas, no estructuradas o fuentes secundarias como las redes sociales. De igual manera, son diversos los formatos en que se encuentra los datos, por ejemplo, pdf, jpg, docx, xml, txt, json, csv, png, entre muchos otros. Los datos suelen ser creados usualmente de las siguientes formas: • Adquisición de datos ya existentes que se han producido fuera de la organización. • Entrada manual de nuevos datos por parte del personal dentro de la organización. • Captura de datos generados por dispositivos utilizados en varios procesos de la organización.
Procesamiento	En la etapa de procesamiento debe contemplar las siguientes tareas: • Limpieza de datos en la que un conjunto de datos se limpia y se transforma de su forma sin procesar a algo más accesible y utilizable. También se conoce como corrección de datos. • Compresión de datos en la que los datos se transforman en un formato que se puede almacenar de manera más eficiente.

FASE CICLO DE VIDA	DESCRIPCIÓN
	• Cifrado de datos en el que los datos se traducen a otra forma de código para protegerlos de problemas de privacidad. • Calidad de los datos en los procesos de obtención y procesamiento de datos, donde principalmente se aplican las políticas y controles establecidos en el diseño, con el propósito de determinar cuáles datos son utilizables. Además de las tareas mencionadas, existen muchas otras como, por ejemplo, cuando se toma un formulario impreso y se digitaliza, también puede considerarse una forma de procesamiento de datos.
Almacenamiento	El almacenamiento y operaciones incluyen el diseño, la implementación y el soporte de los datos almacenados para maximizar su valor, utilizando tanto formatos como repositorios que busquen el equilibrio entre disponibilidad y coste de almacenamiento, según los distintos escenarios de consulta, por ejemplo, diferenciando datos de alta demanda o disponibilidad de otros que no se consultan frecuentemente. Comúnmente el almacenamiento se realiza mediante la creación de bases de datos o conjuntos de datos. Estos conjuntos de datos pueden almacenarse en la nube, en servidores locales o utilizando otras formas de almacenamiento físico como discos duros magnéticos o de estado sólido, memorias o cintas magnéticas, entre otros.
Intercambio	A medida que se requieren datos de fuentes secundarias, generados por otros actores del ecosistema de datos útiles para la toma de decisiones, la planificación, la optimización de operaciones, entre otros, existe una mayor presión para compartir también datos generados. Los datos compartidos pueden ayudar a mejorar las decisiones, ya que las organizaciones pueden obtener una vista más completa de los impactos que sus decisiones han tenido con base en las contribuciones de nuevos conjuntos de datos de una variedad más amplia de fuentes, tanto internas como externas. Esta capacidad de compartición de datos debe estar soportada en una capa de interoperabilidad y haciendo uso de un estándar de lenguaje común de intercambio.
Uso y análisis de datos	Durante la fase los datos se utilizan para respaldar las actividades de la organización. Los datos se pueden ver, procesar, modificar y guardar. Se debe mantener un registro de auditoría para todos los datos críticos, con el propósito de garantizar que todas las modificaciones que se realicen a los datos sean completamente rastreables y auditables. Los datos también pueden estar disponibles para exponer a otros actores del ecosistema de datos que se encuentren fuera de la organización. El análisis de datos se refiere a procesos que intentan obtener información significativa a partir de datos sin procesar. Los analistas y científicos de datos utilizan diferentes herramientas y estrategias para realizar estos análisis. Algunos de los métodos más utilizados incluyen modelado estadístico, algoritmos, inteligencia artificial, minería de datos y aprendizaje automático.

FASE CICLO DE VIDA	DESCRIPCIÓN
Archivo y preservación	El archivado de datos hace referencia a la copia de datos en un entorno donde se almacenan en caso de que se necesiten nuevamente en un ambiente de producción, así mismo también incluye la eliminación de estos datos de todos los entornos de producción activos. Un archivo de datos es un lugar donde se almacenan los datos, pero donde no se realiza mantenimiento o uso general. Si es necesario, los datos se pueden restaurar a un entorno en el que se puedan utilizar. Dado que el volumen de datos archivados crece inevitablemente, si bien es posible que desee guardar todos los datos de manera indefinida, los costos de almacenamiento pueden incentivan la destrucción de los datos que ya no se requieren. Por otro lado, es posible que se disponga de datos de uso limitado a una ventana de tiempo o a hasta /durante la ocurrencia de un suceso. La destrucción o depuración de datos es la eliminación de cada copia de un elemento de datos de una organización.
Reutilización	Reutilizar significa usar datos que originalmente fueron recopilados para otro fin o propósito. La reutilización de datos también se puede llamar análisis secundario

Fuente: Elaboración propia - DIAGNÓSTICO SCD E INFRAESTRUCTURA DE DATOS

Tabla 7 Ejes ciclo de vida del dato

EJE	DESCRIPCIÓN	FASE RELACIONADA
Archivado de datos históricos.	Se realiza el traslado de datos a sistemas de almacenamiento de bajo costo y eliminación o archivo de acuerdo con las políticas.	Almacenamiento, Eliminación/Archivo
Enmascaramiento de entornos.	Implica la transformación de datos para proteger la privacidad y uso en entornos de prueba, de esta manera, se realizar el enmascaramiento coherente entre los datos sensibles, generados y procesados por los diferentes sistemas de la entidad, teniendo en cuenta las políticas de seguridad, privacidad y datos abiertos; establecidos por el Estado Colombiano.	Procesamiento, Uso
Reducción de entornos	Reducción del tamaño de los datos a través de compresión y eliminación de datos redundantes y entornos no productivos, para disminuir el coste IT asociado.	Almacenamiento, Eliminación/Archivo
Generación de datos de prueba.	Creación de datos sintéticos o basados en datos reales para pruebas, soporte a la resolución de incidencias o externalización de los entornos de desarrollo.	Creación, Procesamiento

Fuente: Elaboración propia

8.3 Catálogo de datos

El catálogo de datos es un inventario detallado y organizado de todos los activos de información que posee la entidad. Este inventario funciona como un directorio que facilita la búsqueda, el acceso y la comprensión de los datos, independientemente de su formato o ubicación.

La Ley 1712 de 2014, ha impulsado la creación y el uso de catálogos de datos como herramienta fundamental porque permite a los ciudadanos conocer qué información posee el Estado y acceder a ella de manera más fácil y rápida. De igual manera facilita la reutilización de los datos por parte de investigadores, emprendedores y otros ciudadanos, fomentando la innovación y el desarrollo.

A un nivel interno, el catálogo de datos ayuda a organizar, gestionar y controlar sus activos de información de forma más eficiente, lo cual repercute en la mejora de la toma decisiones, teniendo en cuenta que facilita proporcionar la información confiable y actualizada para respaldar la toma de decisiones basadas en datos.

Un catálogo de datos de la Contraloría de Bogotá, deberá estar coordinado con los procedimientos y directrices relacionados con la gestión documental institucional. En este sentido, deberá incluir la siguiente información como mínimo:

- **Metadatos:** Datos que describen otros datos, como el nombre del conjunto de datos, su descripción, el formato, la fecha de creación, la frecuencia de actualización, etc.
- **Ubicación:** Donde se encuentran almacenados los datos.
- **Contacto:** Quien es el responsable de los datos y a quién dirigirse para obtener más información.
- **Licencia de uso:** Las condiciones bajo las cuales se pueden utilizar los datos.

Se recomienda realizar una revisión anual del catalogo de datos para asegurar su actualización y alineación con los instrumentos de gestión documental.

8.4 Datos abiertos

Los datos abiertos, definidos como información pública en formatos accesibles y reutilizables bajo licencia abierta, están regulados en Colombia por la Ley 1712 de 2014. Esta ley establece que los datos primarios en formatos estándar deben estar disponibles para todos los ciudadanos sin restricciones, con el fin de fomentar su reutilización y la creación de servicios derivados.

La Contraloría de Bogotá como entidad pública está obligada a divulgar datos abiertos, salvo excepciones relacionadas con información clasificada o reservada. De esta manera, la entidad debe mantener actualizados y publicados cada uno de los conjuntos de datos abiertos y los activos de información con el fin de que los ciudadanos tengan siempre disponible la información.

Los formatos aceptados para publicar datos abiertos son:

- CSV (Valores Separados por Coma): Es un tipo de documento de texto plano para representar datos tabulados en columnas separadas por comas (o punto y coma) y filas separadas por saltos de línea.

- XML (Lenguaje Etiquetado Extensible): es el estándar utilizado para el intercambio de información estructurada entre diferentes plataformas
- RDF (Infraestructura para Descripción de Recursos): es un lenguaje de propósito general para representar información en la web, es una de las tecnologías esenciales para la web semántica.
- RSS (Sindicación Realmente Sencilla): es un formato basado en XML para la ordenación de contenidos de páginas web actualizados frecuentemente (noticias, blogs o podcasts).
- JSON (Notación de objetos Javascript): es un formato simple y ligero para el intercambio de datos, de fácil lectura e interpretación por las personas y sencillo para ser analizado y generado por las máquinas
- ODF (Formato de Documento Abierto para Aplicaciones Ofimáticas): es un formato de fichero estándar para el almacenamiento de documentos ofimáticos.
- WMS (Servicio Web de Mapas): es un servicio definido por el OGC (Open Geospatial Consortium) que produce mapas de datos referenciados espacialmente, de forma dinámica a partir de información geográfica.
- WFS (Servicio Web de características): es un servicio estándar, que ofrece una interfaz de comunicación que permite interactuar con los mapas servidos por el estándar WMS.

Además, la entidad debe seguir los siguientes lineamientos, los cuales establecen directrices específicas sobre la gestión y el uso de los datos. Entre ellos, destacan:

- **Guía de Estándares de Calidad e Interoperabilidad**: Ofrece orientación y buenas prácticas para desarrollar estrategias de apertura de datos que cumplan con los principales estándares de calidad e interoperabilidad.
- **Marco de Arquitectura Empresarial**: Principal instrumento para implementar la Arquitectura TI de Colombia y facilitar la Política de Gobierno Digital.
- **Marco de Interoperabilidad**: Define lineamientos y recomendaciones para el intercambio eficiente de información entre entidades del Estado.
- **Estándar de Información**: Definido por el Estado colombiano para intercambiar información entre organizaciones, facilitando el entendimiento en los procesos de intercambio.
- **Guía de Anonimización**: Orienta a las entidades del Sistema Estadístico Nacional sobre el proceso de Anonimización de bases de datos provenientes de registros administrativos y operaciones estadísticas.

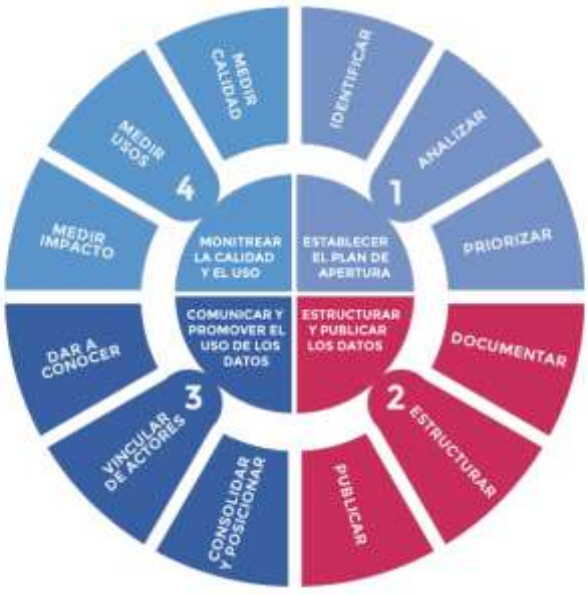
- **Lineamientos Técnicos para la Producción y Gestión de Información Geográfica**: Proporciona un marco de normas técnicas para consolidar la información geográfica de las entidades del Estado bajo una estructura estándar.

Los nuevos conjuntos de datos abiertos que se requieran publicar, deberán ser revisados y presentados en los términos que defina el Comité del Gobierno de Datos, con el fin de establecer una ruta técnica mediante la cual se garantice el cumplimiento de los requerimientos para la publicación y difusión.

Es competencia del nivel estratégico del Gobierno de Datos, desarrollar estrategias que promuevan en las diferentes áreas misionales y de apoyo, la identificación, producción y actualización de nuevos conjuntos de datos para publicar en el portal oficial de Datos Abiertos.

De acuerdo con la Guía para el uso y aprovechamiento de los Datos Abiertos en Colombia[4]: "Establecer un ciclo para el proceso de apertura, mejora y uso de datos abiertos permite que los actores del ecosistema definan acciones a tomar en cada una de las fases estratégicas de este ciclo: construcción de plan de apertura, estructuración, comunicación y monitoreo. La buena implementación y seguimiento a estas actividades redundará en calidad de datos y, por tanto, en usos de impacto. Adicionalmente es un proceso recurrente, que debe presentarse con una vigencia definida, como recomendación este ciclo se planea y ejecuta cada dos años."

Ilustración 9 Ciclo de vida de los datos abiertos



Fuente: Elaboración propia

[4] Tomado de: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://herramientas.datos.gov.co/sites/default/files/Guia%20de%20Datos%20Abiertos%20de%20Colombia.pdf

Cada conjunto de datos abiertos definidos por la Contraloría de Bogotá, deberá contar con el desarrollo de cada una de las etapas del ciclo de vida de los datos abiertos presentado.

9. Consideraciones finales

- Todos los proyectos de la entidad que tengan relación con datos, deben aplicar los principios, políticas y lineamientos definidos en por el Gobierno de Datos Institucional.
- Con el fin de mejorar los servicios tecnológicos focalizados en entregar y gestionar los datos de manera correcta por parte de la entidad y para la entidad, se debe asegurar la coordinación con los lineamientos y políticas establecidas por el Gobierno de Datos Institucional.
- Se debe continuar asegurando la preservación de la confidencialidad de la información, lo cual implica implementar medidas efectivas de seguridad y control para proteger los datos institucionales.
- Garantizar los recursos adecuados es fundamental para mantener y mejorar continuamente las políticas del gobierno de datos, lo que incluye la capacitación del personal, la adquisición de tecnología y la realización de auditorías periódicas. Estas acciones garantizarán la integridad y eficacia del Gobierno de Datos Institucional, fortaleciendo así la capacidad de la organización para cumplir con sus objetivos y responsabilidades de manera sostenible.

Bibliografía

DAMA. (s.f.). *DMBoK - Data Management Body of Knowledge.* Obtenido de https://www.dama.org/cpages/body-of-knowledge

DNP. (17 de abril de 2018). *www.dnp.gov.co.* Obtenido de https://www.dnp.gov.co/LaEntidad_/subdireccion-general-prospectiva-desarrollo-nacional/direccion-desarrollo-digital/Paginas/documentos-conpes-infraestructura-de-datos.aspx

Función Pública. (2023). Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www1.funcionpublica.gov.co/documents/28587410/34112007/2023-03-21_Manual_operativo_mipg_5V.pdf/dbe560cc-e81d-bd7b-b23f-075184e029c6?t=1679509602732

Haider, K. (24 de abril de 2024). *Astera.* Obtenido de https://www.astera.com/es/type/blog/data-quality/

IBM. (17 de julio de 2023). *www.ibm.com.* Obtenido de https://www.ibm.com/es-es/topics/data-storage

IBM. (3 de julio de 2024). *www.ibm.com.* Obtenido de https://www.ibm.com/es-es/topics/data-governance

IBM. (17 de octubre de 2024). *www.ibm.com.* Obtenido de https://www.ibm.com/es-es/topics/data-architecture

Microsoft. (s.f.). *https://azure.microsoft.com/.* Obtenido de https://azure.microsoft.com/es-es/resources/cloud-computing-dictionary/what-is-data-integration

MinTIC. (30 de diciembre de 2014). Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cvc.gov.co/sites/default/files/2018-10/G.Inf_.06%20Guia%20Tecnica%20-%20Gobierno%20del%20dato%20V1%202014-Dic-30.pdf

MinTIC. (30 de diciembre de 2014). Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.cvc.gov.co/sites/default/files/2018-10/G.Inf_.02%20Guia%20Tecnica%20base%20de%20informacion%20V1%202014-Dic-30.pdf

MinTIC. (2022). Obtenido de chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gobiernodigital.mintic.gov.co/692/articles-238196_recurso_1.pdf

MinTIC. (s.f.). *gobiernodigital.mintic.gov.co.* Obtenido de https://gobiernodigital.mintic.gov.co/portal/Iniciativas/Datos-abiertos/

Pisoni, G., Molnár, B., & Tarcsi, A. (29 de noviembre de 2023). Técnicas de gestión del conocimiento y análisis de datos para empresas financieras basadas en datos. *Revista de economía del conocimiento, 15*, 13374–13393,. Obtenido de https://link.springer.com/article/10.1007/s13132-023-01607-z#citeas

PowerData. (19 de marzo de 2016). *blog.powerdata.es.* Obtenido de https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/que-son-los-metadatos-y-cual-es-su-utilidad

Puig, D., & Mañes, J. (29 de julio de 2021). *datos.gob.es. .* Obtenido de https://datos.gob.es/es/blog/el-potencial-uso-de-la-metodologia-de-dama-en-la-gestion-de-los-datos-abiertos

SDNA Digital. (s.f.). *www.sdnadigital.com.* Obtenido de https://www.scribbr.es/citar/generador/folders/4RhOWmCBNm0TBmw99OT6gv/lists/32zlFx6Yfn5nDPUwo84HBh/

Sicex. (12 de septiembre de 2022). *sicex.com.* Obtenido de https://sicex.com/blog/tipos-de-analitica-de-datos/

Universitat de Valencia. (s.f.). *ww.uv.es/cibisoc/tutoriales.* Obtenido de https://www.uv.es/cibisoc/tutoriales/trabajo_social/22_las_fuentes_de_informacin.html

Control de cambios

Versión	Descripción de la modificación
1.0	Primera versión 2024

Anexos.

Anexo 1. Matriz RACI

Actividad/Responsabilidad	Comité de Gobierno de Datos	Director de Datos	Equipo de Datos	Admón. de Datos	Admón. de Seguridad y Privacidad	Líder de Datos	Gestor Tecnológico de Datos	Analista de Datos	Gestor Técnico de Datos
Definir políticas y lineamientos estratégicos	R	A	C	I	I	I	I	I	I
Revisar y aprobar los planes y proyectos	R	C	C	I	I	I	I	i	I
Gestión de recursos para estrategias	A	R	C	I	I	I	I	I	I
Coordinación de actividades del Gobierno de Datos	I	R	A	C	I	C	I	I	I
Supervisión de la calidad de los datos	I	C	R	R	C	A	I	C	C
Implementación de modelos de datos empresariales	I	I	I	R	C	A	I	C	I
Análisis y generación de informes	I	I	I	I	I	C	I	R	C
Gestión y protección de datos	I	I	I	C	R	I	A	I	I
Monitoreo de cumplimiento de políticas	I	I	R	C	C	A	C	I	I
Determinar las estrategias de divulgación de las decisiones tomadas.	A	R	I	I	I	I	I	I	I
Elaborar documentos para procesos de intercambio de datos con fuentes externas	I	A	R	I	I	I	I	I	I
Asegurar confidencialidad, integridad y disponibilidad de información	I	I	I	I	I	R	I	I	I
Definir el flujo de datos en los procesos y los sistemas de información	I	I	I	I	I	A	I	I	R
Diseño de estrategias de analítica de datos	I	I	I	C	C	R	C	R	I