INFORME DE MONITOREO Y SEGUIMIENTO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Corte 30 de abril

Oficina Asesora de Planeación - SDI

2024

BOGOTÁ
ALCALDÍA MAYOR DE BOGOTÁ D.C.
JARDÍN BOTÁNICO

1. INTRODUCCIÓN

En el entendido que la gestión del riesgo es un proceso liderado por la Alta Dirección de la Entidad y es ejecutado por los servidores y funcionarios propendiendo por una adecuada administración y tratamiento de los mismos, así como, un aseguramiento razonable con respecto al logro de los objetivos y metas trazadas; mediante el presente informe se da conocer las actividades realizadas de Gestión de Riesgos de Seguridad de la Información – Digital, así como el resultado del tratamiento de riesgos oficializado en SDI.PR.02.F.03 Mapa de Riesgos Sistema Seguridad de la Información-Digital por procesos del Jardín Botánico de Bogotá durante el periodo comprendido entre el 1 de enero y el 30 de abril de 2024, lo anterior con el fin de contribuir a la toma de decisiones basados en la gestión de los riesgos JBB, enfocados en la planificación y aplicación de acciones para minimizar la materialización de estos y a su vez modificar aquellas condiciones o situaciones generadoras de pérdidas económicas o reputacionales, en el marco de la Política de Administración del Riesgo de la entidad y cumpliendo con el esquema de las líneas de defensa..

El Jardín Botánico de Bogotá en su estructura por procesos, identifico para tratamiento de riesgos de seguridad digital de conformidad con los activos críticos enmarcados en disponibilidad, integridad y confidencialidad, de los riesgos asociados para los siguientes procesos de la siguiente forma:

Número	Código	Proceso	Dependencia / Oficina
1	APL.C	Aplicación del Conocimiento	Subdirección Técnica Operativa
2	APR.C	Apropiación del Conocimiento	Subdirección Educativa y Cultural
3	CDI.C	Control Disciplinario Interno	Oficina de Control Disciplinario Interno
4	DOC.C	Gestión Documental	Secretaría General
5	DYP.C	Direccionamiento y Planeación Estratégico	Oficina Asesora de Planeación
6	ECM.C	Evaluación, Control y Mejora	Oficina de Control Interno
7	FCR.C	Gestión de Recursos Financieros	Secretaría General
8	FIS.C	Gestión de Recursos Físicos	Secretaría General
9	GCO.C	Comunicaciones	Secretaría General
10	GCT.C	Gestión Contractual	Secretaría General
11	GEN.C	Generación de Conocimiento	Subdirección Científica
12	GTH.C	Gestión del Talento Humano	Secretaría General
13	JUR.C	Jurídico	Oficina Jurídica
14	SAC.C	Servicio al Ciudadano	Secretaría General
15	SDI.C	Seguridad de la Información	Oficina Asesora de Planeación
16	TEC.C	Gestión de la Tecnología	Secretaría General

Tabla 1 Procesos JBB

2. POLÍTICA DE ADMINISTRACIÓN DEL RIESGO EN EL JARDÍN BOTÁNICO DE BOGOTÁ JOSÉ CELESTINO MUTIS - JBB.

Para el desarrollo del presente informe se aplica lo establecido en la Política de Administración del Riesgo en su versión 5 oficializada el pasado 29 de diciembre de 2023, adoptada mediante resolución 501 del 29 de diciembre de 2023 “Por medio de la cual se actualiza la Política de Administración del Riesgo en el Jardín Botánico de Bogotá “José Celestino Mutis”. Se destaca que la gestión efectuada durante el primer cuatrimestre permite dar continuidad al cumplimiento de los lineamientos establecidos en la política antes mencionada, esta a su vez adopta lo indicado en la “Guía para la Administración del Riesgo y el diseño de controles en entidades públicas” versión 6, emitida por el Función Pública – FP en diciembre de 2022, en ese sentido, en la metodología para la gestión integral del riesgo en el JBB, se relacionaron los lineamientos para la formulación e implementación de la gestión de riesgos de seguridad de la información que se puedan presentar en el desarrollo de la gestión de la entidad están fundamentados en el Anexo 4. “Lineamientos para la gestión de riesgos de seguridad digital en

entidades públicas”[1]. Como resultado se dio alcance al diligenciamiento del Mapa de Riesgos Sistema Seguridad de la Información-Digital.

Por lo anterior, el presente informe está elaborado en atención a lo establecido en la política, para realizar el seguimiento de las acciones propuestas alineadas a la identificación, valoración y aplicación de controles asociados a los riesgos de seguridad digital identificados en los procesos.

3. MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL.

Con el fin de dar cumplimiento a los Lineamientos riesgos de seguridad de la información, se articula la Política de Operación para la administración del riesgo en el Jardín Botánico José Celestino Mutis, realizando un ajuste documental desde el proceso SDI elaborando el Manual SDI.PR.02.M.01 Gestión de Riesgos de Seguridad de la Información - Digital con la modificación de la Matriz SDI.PR.02.F.03 Mapa de Riesgos Sistema Seguridad de la Información-Digital, aprobadas y publicadas, lo que generó que las mesas de trabajo para la identificación de riesgos por proceso se realizaran posteriormente.

Para el primer cuatrimestre, se realizaron las mesas de trabajo con base en la matriz de Identificación y clasificación de activos de información del 2023, para los procesos de Generación del Conocimiento, Aplicación del Conocimiento, Control Disciplinario Interno, Evaluación, Control y Mejora, Gestión de recursos financieros, Gestión de la Tecnología, Gestión del Talento Humano y Seguridad de la Información con los siguientes riesgos identificados:

	Aplicación del Conocimiento	Control Disciplinario Interno	Evaluación, Control y Mejora	Generación del Conocimiento	Gestión de la Tecnología	Gestión de recursos financieros	Gestión del Talento Humano	Seguridad de la Información
Riesgos	3	3	2	5	9	3	1	0

Ilustración 1 Riesgos por Proceso a corte Abril.

En la primera etapa se realizó el 50% del análisis por procesos con 26 riesgos identificados, quedando pendiente 8 procesos por analizar para el 30 de junio del 2024, esta etapa se dio por el cambio de procedimiento y del instrumento de análisis que ahora pertenece al proceso Seguridad de la Información- SDI, lo que llevó a realizar socializaciones antes realizar el diligenciamiento con la responsabilidad de apoyo del Oficial de Seguridad de la Oficina de Planeación.

A continuación, se encuentran relacionados los 26 riesgos del análisis realizado de los 8 procesos, Riesgos de SDI con corte a 30 de abril 2024:

Proceso	Referencia	Nombre de Activo	Tipo de activo	Descripción del Riesgo
Generación del Conocimiento	GENR1	Disco Duro - Copia de respaldo Herbario	Hardware (Equipos y Redes de Comunicación)	Posibilidad de pérdida Disponibilidad y Posibilidad de pérdida de Integridad Por Hurto de medios o documentos o Debido a Almacenamiento sin protección

[1] https://www.funcionpublica.gov.co/documents/418548/34316316/Anexo+4+Lineamientos+para+la+Gestion+del+Riesgo+de++Seguridad+Digital+en+Entidades+P%C3%BAblicas+-+Gu%C3%ADa+riesgos+2018.pdf/1ce5099d-c5e5-8ba2-00bc-58f801d3657b

Proceso	Referencia	Nombre de Activo	Tipo de activo	Descripción del Riesgo
Generación del Conocimiento	GENR2	Documentación de Seguimientos y Reportes de la Subdirección Científica	Información	Posibilidad de pérdida Disponibilidad y Posibilidad de pérdida de Integridad Por Fallas humanas Debido a Deficiencia en la autorización de permisos de la información o Debido a Ausencia de validación de autenticación de la información
Generación del Conocimiento	GENR3	Profesional Subdirección científica que administra bases de datos y aplicaciones	Recurso Humano	Posibilidad de pérdida Disponibilidad y Posibilidad de pérdida de Integridad, Por La información puede ser accedida por personal no autorizado , Debido a Ausencia del personal
Generación del Conocimiento	GENR4	Imágenes del Herbario	Información	Posibilidad de pérdida Disponibilidad y Posibilidad de pérdida de Integridad Por Pérdida de información o Debido a Ausencia de copias de respaldo o backups de la información
Generación del Conocimiento	GENR5	Base de datos Subdirección científica	Información	Posibilidad de pérdida de Integridad Por Pérdida de información o Debido a Ausencia de copias de respaldo o backups de la información
Aplicación del Conocimiento	APLR1	Base de Datos del Sistema de Información FACTORY)	Información	Posibilidad de pérdida de Integridad Por Fallas humanas o Debido a Manejo manual de la información
Aplicación del Conocimiento	APLR2	Sistema de información SIGAU y aplicación móvil ArbolApp	Software	Posibilidad de pérdida de Confidencialidad Por Falsificación de derechos o Debido a Gestión deficiente de las contraseñas
Aplicación del Conocimiento	APLR3	Información del Sistema de información SIGAU y aplicación móvil ArbolApp	Información	Posibilidad de pérdida de Integridad Por Fallas humanas o Debido a Manejo manual de la información

Proceso	Referencia	Nombre de Activo	Tipo de activo	Descripción del Riesgo
Control Disciplinario Interno	CDIR1	Información asociada a Control disciplinario interno (Disciplinario Ordinario y Disciplinario Verbal , Preservación del Orden Interno y Expediente disciplinario)	Información	Posibilidad de pérdida Disponibilidad y Posibilidad de pérdida de Integridad Por Fallas humanas Debido a Retraso en la entrega de información por parte del personal o Debido a Manejo manual de la información
Control Disciplinario Interno	CDIR2	Información asociada a Expedientes Disciplinarios	Información	Posibilidad de pérdida de Integridad Por Pérdida de información Debido a Ausencia de copias de respaldo o backups de la información
Control Disciplinario Interno	CDIR3	Archivo físico de información de Control Disciplinario Interno	Infraestructura Física	Posibilidad de pérdida de Confidencialidad y Posibilidad de pérdida de Integridad Por Destrucción de equipos o de medios Debido a Ausencia de protección física de la edificación, puertas y ventanas
Evaluación, Control y Mejora	ECMR1	Token físico de firma digital Contraloría Bogotá	Hardware (Equipos y Redes de Comunicación)	Posibilidad de pérdida Disponibilidad Por Hurto de medios o documentos Debido a Falta de cuidado en la disposición final o Debido a Almacenamiento sin protección
Evaluación, Control y Mejora	ECMR2	OneDrive y correo de Contratista y/o funcionario	Información	Posibilidad de pérdida Disponibilidad Por Fallas humanas Debido a Retraso en la salida de información de los sistemas
Gestión de recursos financieros	FCRR1	Información relacionada con Identificar, clasificar y reconocer, los hechos económicos de la Entidad para la emisión de estados financieros	Información	Posibilidad de pérdida de Confidencialidad y Posibilidad de pérdida de Integridad Por Fallas humanas Debido a Manejo manual de la información

Proceso	Referencia	Nombre de Activo	Tipo de activo	Descripción del Riesgo
Gestión de recursos financieros	FCRR2	Información relacionada con tesorería de Extractos bancarios Estado diario de tesorería	Información	Posibilidad de pérdida de Confidencialidad y Posibilidad de pérdida de Integridad Por Fallas humanas Debido a Manejo manual de la información
Gestión de recursos financieros	FCRR3	Token físico de firma digital tesorería y presupuesto	Hardware (Equipos y Redes de Comunicación)	Posibilidad de pérdida Disponibilidad Por Hurto de medios o documentos Debido a Almacenamiento sin protección
Gestión del Talento Humano	GTHR1	Documentación Asociada Procedimiento: Liquidación y pagos de obligaciones del personal	Información	Posibilidad de pérdida de Confidencialidad y Posibilidad de pérdida de Integridad Por Fallas humanas Debido a Manejo manual de la información
Gestión de la Tecnología	GTER1	Servicio de Correo electrónico Institucional	Organizacionales	Posibilidad de pérdida de Confidencialidad y Posibilidad de pérdida Disponibilidad , Por Error en el uso o Por Incumplimiento en el mantenimiento del sistema de información , Debido a Respuesta inadecuada de mantenimiento de servicio o Debido a Ausencia de políticas sobre el uso del correo electrónico
Gestión de la Tecnología	GTER2	Servicio de Servicios de Internet - RED /VPN	Organizacionales	Posibilidad de pérdida Disponibilidad y Posibilidad de pérdida de Integridad , Por Incumplimiento en el mantenimiento del sistema de información o , o Debido a Respuesta inadecuada de mantenimiento de servicio
Gestión de la Tecnología	GTER3	Sistemas de Información Administrados por TEC	Software	Posibilidad de pérdida Disponibilidad , Por Manipulación del software o Debido a Ausencia de control de cambios eficaz

Proceso	Referencia	Nombre de Activo	Tipo de activo	Descripción del Riesgo
Gestión de la Tecnología	GTER4	Información asociada al Registro, monitoreo, medición de la capacidad y desempeño de la Infraestructura de TI.	Software	Posibilidad de pérdida Disponibilidad , Por Manipulación del software o Debido a Ausencia de control de cambios eficaz
Gestión de la Tecnología	GTER5	Servidores Nube Pública (Microsoft Azure)	Hardware (Equipos y Redes de Comunicación)	Posibilidad de pérdida Disponibilidad , Por Incumplimiento en el mantenimiento del sistema de información o Debido a Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento
Gestión de la Tecnología	GTER6	Servidores Nube Privada (On Premise)	Hardware (Equipos y Redes de Comunicación)	Posibilidad de pérdida Disponibilidad , Por Incumplimiento en el mantenimiento del sistema de información o Debido a Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento
Gestión de la Tecnología	GTER7	Aplicaciones / Sistemas de información	Software	Posibilidad de pérdida Disponibilidad y Posibilidad de pérdida de Integridad , Por Manipulación del software o Debido a Ausencia de copias de respaldo o backups de la información
Gestión de la Tecnología	GTER8	Base de datos TEC	Información	Posibilidad de pérdida de Integridad , Por Pérdida de información o Debido a Ausencia de copias de respaldo o backups de la información
Gestión de la Tecnología	GTER9	Datacenter	Hardware (Equipos y Redes de Comunicación)	Posibilidad de pérdida Disponibilidad y Posibilidad de pérdida de Integridad , Por Incumplimiento en el mantenimiento del sistema de información o Debido a Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento

Tabla 2 Relación de Activos con riesgos identificados

Para el primer cuatrimestre de 2024, se cuenta con 26 Riesgos identificados al corte de 30 de abril

del 2024, relacionados según la siguiente ilustración:

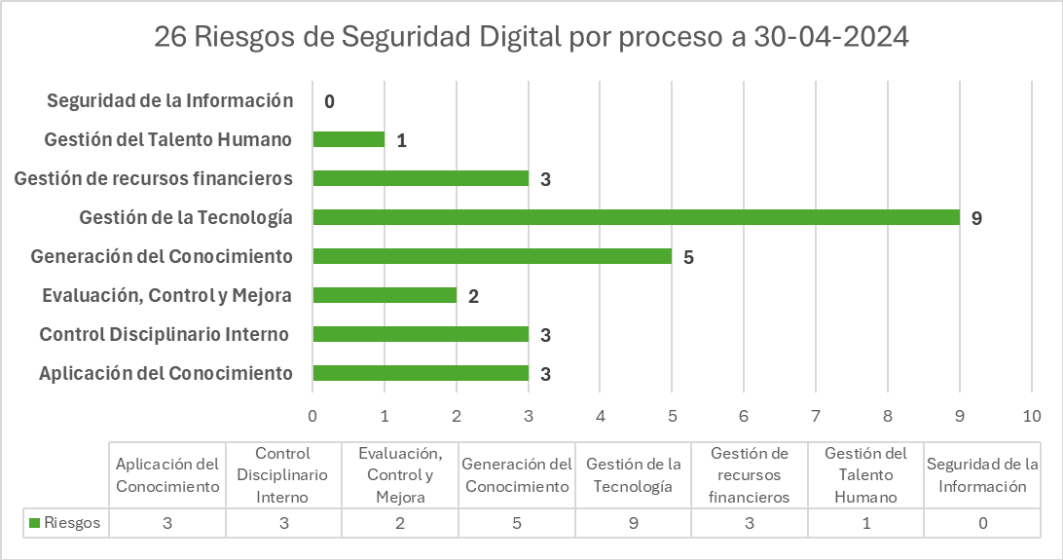


Ilustración 1 Riesgos por 8 Procesos

	RIESGO INHERENTE DEL PROCESO		RIESGO RESIDUAL DEL PROCESO	
Sumatoria de riesgos Extremos	0	0%	0	0%
Sumatoria de riesgos altos	3	12%	0	0%
Sumatoria de riesgos moderados	12	46%	10	38%
Sumatoria de Riesgos bajos	11	42%	16	62%
Total	26	100%	26	100%

Ilustración 2 comportamiento de Riesgo

Con las actividades de riesgos de seguridad digital adoptadas por JBB desde el 2023, se ha mitigado los riesgos relacionados con la seguridad de la información usando el SharePoint como herramienta de gestión en las cuentas institucionales de cada proceso como repositorios de la información, así como, la actualización documental de los procesos, lo que impacta el análisis de riesgos altos identificados, es importante seguir con la implementación de los controles de manera constante que mitiguen los riesgos de seguridad digital.

4. RESULTADOS DEL PRIMER SEGUIMIENTO DE LOS RIESGOS DE SEGURIDAD DIGITAL

Para el primer cuatrimestre dentro del seguimiento quedaron 6 riesgos para el corte de 30 de abril del 2024 de los cuales se recibieron las evidencia correspondientes, no sin antes aclarar que por ser una matriz nueva los controles cambiaron de conformidad al estándar ISO/IEC 27002:2022[2] (Seguridad de la información, ciberseguridad y protección de la privacidad: controles de seguridad de la información), por lo cual para realizar implementación de controles se dejó el seguimiento para el segundo cuatrimestre a los riesgos faltantes. Ver resultados:

[2] https://www.iso.org/es/contents/data/standard/07/56/75652.html

No ACTIVO /RIESGO	ACTIVO	PROCESO	OBSERVACIONES/RECOMENDACIONES SEGUNDO SEGUIMIENTO
GENR2	Documentación de Seguimientos y Reportes de la Subdirección Científica	Generación del Conocimiento	Se asignó un repositorio, el cual corresponde a: “Informes Científicos" y está asociado a la cuenta institucional: "Informes Científica" informescientifica@jbb.gov.co alojado en One576Drive de la cuenta, lo que permite a su vez, contar con la disponibilidad de la información y la confidencialidad de los permisos que son administrados por el área. o Esta la información se actualiza y se relacionadas por vigencias y de acuerdo con la periodicidad correspondiente a la programación aprobada para cada vigencia y en cada vigencia, de acuerdo con lo programado para cada mes. Se envía como soporte, la evidencia del repositorio asignado con la generación de carpetas para la vigencia, disgregadas por mes. Por favor, revisar el soporte contenido en la Carpeta: C1_RD_Soportes. o La Subdirección Científica dispuso de un administrador de repositorio de la cuenta "Informes científica" <informescientifica@jbb.gov.co>, quien concede los permisos de la carpeta correspondiente, realiza el monitoreo de la información generada y controla el acceso para la integridad de la información. Se cuenta con la captura de pantalla de administración de OneDrive en permisos de acceso, así como los correos de envío y recepción de solicitud de la creación de los enlaces para que cada coordinador asignado, realice el cargue de la información de acuerdo con los tiempos establecidos, evitando así, la modificación de la información una vez reportado el informe y a su vez, garantizando que, la información reportada corresponde con los soportes aportados. Se envía como soporte, la evidencia de los correos con la solicitud de la creación de los enlaces y la respuesta con los enlaces disgregadas por mes. Por favor, revisar el soporte contenido en la Carpeta: C2_RD_Soportes.
GENR3	Documentación de Seguimientos y Reportes de la Subdirección Científica	Generación del Conocimiento	Documento acta de inicio o copia de contrato donde se tiene la continuidad de profesional que administra bases de datos y aplicaciones en la Subdirección Científica Se evidencia la contratación del personal por medio del JBB-CTO-208-2024 ACTA DE INICIO-1

CDIR1	Información asociada a Control disciplinario interno (Disciplinario Ordinario y Disciplinario Verbal, Preservación del Orden Interno y Expediente disciplinario)	Control Disciplinario Interno	Diligenciar el Formato donde se relaciona la gestión del expediente, así como las Relación de respuestas a los investigados y donde se gurda la información correspondiente en el repositorio correspondiente
FCRR1	Información relacionada con Identificar, clasificar y reconocer, los hechos económicos de la Entidad para la emisión de estados financieros	Gestión de recursos financieros	Realizar el resguardo de la Información relacionada con las Conciliaciones y la Cuentas por Cobrar y Pagar con el fin de verificar la calidad de los datos y la integridad de la información Para el primer cuatrimestre se cuenta la relación de copia de seguridad de : 1.Relación de Estado financieros 2.Relación de Conciliaciones bancarias Extractos bancarios 3 Conciliación CUD y definitivos movimientos estado publico
FCRR2	Información relacionada con tesorería de Extractos bancarios Estado diario de tesorería	Gestión de recursos financieros	Realizar el resguardo de la Información relacionada con tesorería de Extractos bancarios Estado diario de tesorería 1.Relación de Extractos bancarios 2.Relación de Estado diario de tesorería-
GTHR1	Documentación Asociada Procedimiento: Liquidación y pagos de obligaciones del personal	GTH Gestión del Talento Humano	Cargue de información de los documentos asociados a la Conciliación Cuenta Única Distrital - SHD en el repositorio MIPG - reportes riesgos de seguridad digital.

Tabla 3 Seguimiento y observaciones a riesgos

5. RECOMENDACIONES FINALES

- Realizar el ejercicio de revisión y actualización de riesgos de seguridad digital, para los 8 procesos pendientes al 30 de junio del 2024.
- Como segunda línea de defensa la Oficina Asesora de Planeación a través de oficial de seguridad deberá revisar el cumplimiento de los controles establecidos alineados al estándar IS0 27002, que evitan o reducen los riesgos de seguridad digital en JBB.
- Los procesos deben seguir generando la cultura de generar copias de información y repositorios institucionales y no en los OneDrive personal.

6. CONCLUSIONES

- Con la actualización del procedimiento de proceso SDI.PR.02 Gestión de Activos de Información realizada en su versión 3, del cual se ejecutó el levantamiento de activos para todos los procesos JBB, adicionalmente se actualizo el Manual SDI.PR.02.M.01 Gestión de Riesgos de Seguridad de la Información - Digital con la modificación del Matriz SDI.PR.02.F.03 Mapa de Riesgos Sistema

Seguridad de la Información-Digital con la cual se realiza la identificación y análisis de riesgo por proceso con la propuesta de controles del estándar ISO27002 de seguridad que mitiguen los riesgos asociados.

- De las actividades propuestas en la mitigación de riesgos podemos concluir que se debe seguir trabajando en migrar la información de repositorios personales de OneDrive de los contratistas o funcionarios de dependen de cuentas particulares a las cuentas institucionales, como buena práctica.

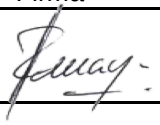
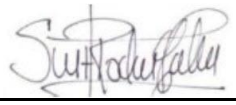
- En relación la infraestructura tecnológica se deja el seguimiento para el segundo cuatrimestre dado que los cambios de los procedimientos se están implementado y que se deben realizar acciones alineadas al cumplimiento de los controles de seguridad que son un deber del estándar de seguridad.

- No se recibió notificación de la materialización de algún riesgo por parte de la primera línea de defensa quien es la responsable de informar a la segunda línea.

- Se evidencia el cargue de evidencias lo cual queda sujeto a la evaluación de parte de la tercera línea de defensa, información que puede ser consultada en el siguiente enlace: Seguimiento a Riesgos evidencias

Cordialmente;

JOSÉ ALBERTO AMAYA GONZÁLEZ
Jefe Oficina Asesora de Planeación
e-mail: jamaya@jbb.gov.co

	Nombre	Firma	Fecha
Aprobado por:	José Alberto Amaya González Jefe Oficina Asesora de Planeación		24-05-2024
Revisado por:	Jina Paola González Coordinadora MIPG		24-05-2024
Elaborado por:	Catherine Suárez Rodríguez Contratista Oficina Asesora de Planeación		24-05-2024
Los arriba firmantes declaramos que hemos revisado el presente documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y, por lo tanto, bajo nuestra responsabilidad, lo presentamos para la firma del. Jefe Oficina Asesora de Planeación