INFORME DE MONITOREO Y SEGUIMIENTO RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Corte 31de Diciembre

OFICINA ASESORA DE PLANEACIÓN
2024

ALCALDÍA MAYOR DE BOGOTÁ D.C.
JARDÍN BOTÁNICO DE BOGOTÁ
BOGOTÁ

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 muestra el seguimiento a los riesgos identificados de Seguridad Digital, lo anterior con el fin de contribuir a la toma de decisiones basados en la gestión de los riesgos, 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.

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

SIGLA	DEPENDENCIA / OFICINA	PROCESO
CD	Control Disciplinario	CDI –Control Disciplinario Interno
TEC	Gestión de la Tecnología	TEC- Gestión de la Tecnología
SG	Secretaría General	FCR Gestión de Recursos Financieros GTH Gestión del Talento Humano
SC	Subdirección Científica	GEN Generación de Conocimiento
STO	Subdirección Técnica Operativa	APL Aplicación del Conocimiento

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

Se mantiene la Gestión del Riesgo de Seguridad Digital de acuerdo con los lineamientos impartidos en la Política de Administración del Riesgo, la cual fue 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”. 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.

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

[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

3. MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL.

Con el fin de dar cumplimiento a los lineamientos en materia de administración del riesgo, en una primera etapa se realizó una valoración de activos de seguridad digital y posteriormente una identificación riesgos asociados a los activos críticos en términos de disponibilidad, confidencialidad e integridad de la información de los procesos, producto del ejercicio se procedió a realizar la matriz; Mapa de Riesgos Sistema Seguridad de la Información y finalmente se estructuraron los controles con los cuales se dará tratamiento. En el ejercicio del 2022 se realizó la valoración de los riesgos de los 16 procesos, se identificaron 56 Riesgos en total asociados a los procesos relacionados en el reporte del segundo cuatrimestre del 2023.

A continuación del Monitoreo y seguimiento Primer Cuatrimestre - Riesgos de SDI 31 de agosto 2023, se evidencio el ajuste a la tabla N. 1, que compone la Matriz de Riesgos de Seguridad Digital de la entidad y se cambia la distribución de la siguiente manera:

Tabla N.1 Relación de riesgo identificados

No Riesgo	PROCESO	DESCRIPCION DEL RIESGO CAUSA INMEDIATA+CAUSA RAIZ)
R1	TEC- Gestión de la Tecnología	por ataques cibernéticos debido a la ejecución de código malicioso, malware, Ransomware o cualquiera de sus derivadas.
R2	TEC- Gestión de la Tecnología	por ataques cibernéticos debido a la ejecución de código malicioso, malware, Ransomware o cualquiera de sus derivadas.
R3	TEC- Gestión de la Tecnología	por ataques cibernéticos debido a la ejecución de código malicioso, malware, Ransomware o cualquiera de sus derivadas.
R4	TEC- Gestión de la Tecnología	por ataques cibernéticos debido a la ejecución de código malicioso, malware, Ransomware o cualquiera de sus derivadas.
R5	TEC- Gestión de la Tecnología	por ataques cibernéticos debido a la ejecución de código malicioso, malware, Ransomware o cualquiera de sus derivadas.
R6	TEC- Gestión de la Tecnología	por ataques cibernéticos debido a la ejecución de código malicioso, malware, Ransomware o cualquiera de sus derivadas.
R7	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R8	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R9	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R10	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R11	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R12	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones

No Riesgo	PROCESO	DESCRIPCION DEL RIESGO CAUSA INMEDIATA+CAUSA RAIZ)
R13	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R14	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R15	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R16	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R17	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R18	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R19	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R20	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R21	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R22	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R23	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R24	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones
R25	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o fallas de operación de los controles técnicos establecidos debido al no monitoreo de los controles establecidos
R26	TEC- Gestión de la Tecnología	por modificación indebida de los registros ingresados debido al acceso no autoriza al aplicativo y la base de datos que contiene los registros.
R27	OAP - Oficina Asesora de Planeación	por modificación indebida de los registros ingresados debido al acceso no autoriza al aplicativo y la base de datos que contiene los registros.
R28	SG - Secretaría General	Por indisponibilidad o perdida de la integridad de los datos debido a la modificación de los registros almacenados o daños para lectura.

No Riesgo	PROCESO	DESCRIPCION DEL RIESGO CAUSA INMEDIATA+CAUSA RAIZ)
R29	SG - Secretaría General	Por indisponibilidad o perdida de la integridad de los datos debido a la modificación de los registros almacenados o daños para lectura y edición en el documento.
R30	CD – Control Disciplinario	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R31	SC - Subdirección Científica	Por indisponibilidad o perdida de la integridad de los datos debido a la modificación de los registros almacenados o daños para lectura y edición en el documento.
R32	STO - Subdirección Técnica Operativa	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R33	CD – Control Disciplinario	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R34	CD – Control Disciplinario	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R35	CD – Control Disciplinario	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R36	CD – Control Disciplinario	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R37	TEC- Gestión de la Tecnología	por modificación indebida de los registros ingresados debido al acceso no autorizado al aplicativo y la base de datos que contiene los registros
R38	TEC- Gestión de la Tecnología	por modificación indebida de los registros ingresados debido al acceso no autorizado al aplicativo y la base de datos que contiene los registros
R39	TEC- Gestión de la Tecnología	por indisponibilidad de acceso a recursos locales, onpremise e Internet debido a afectaciones de tipo físico, lógico o ambiental
R40	TEC- Gestión de la Tecnología	por uso indebido de privilegios y/o contraseñas comprometidas debido a la ausencia de medidas de protección en el momento de configurar la autenticación y administración de sesiones.
R41	SG - Secretaría General	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R42	SG - Secretaría General	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R43	SG - Secretaría General	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R44	SG - Secretaría General	Por perdida de la integridad de la información registrada debido a la modificación no autorizada de la información registrada por el titular de los datos

No Riesgo	PROCESO	DESCRIPCION DEL RIESGO CAUSA INMEDIATA+CAUSA RAIZ)
R45	SG - Secretaría General	Por perdida de la integridad de la información registrada debido a la modificación no autorizada de la información registrada por el titular de los datos
R46	CD – Control Disciplinario	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R47	CD – Control Disciplinario	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R48	CD – Control Disciplinario	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R49	SG - Secretaría General	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R50	SC - Subdirección Científica	Por indisponibilidad o perdida de la integridad de los datos debido a la modificación de los registros almacenados o daños para lectura y edición en el documento
R51	STO - Subdirección Técnica Operativa	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R52	STO - Subdirección Técnica Operativa	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R53	STO - Subdirección Técnica Operativa	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R54	STO - Subdirección Técnica Operativa	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R55	STO - Subdirección Técnica Operativa	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos
R56	STO - Subdirección Técnica Operativa	Por perdida de la confidencialidad de la información registrada debido a la divulgación no autorizada de la información registrada por el titular de los datos

Para el tercer cuatrimestre de 2023, se cuenta con 56 Riesgos con relación al cierre de la vigencia anterior con un riesgo repetido. Sin embargo, en el segundo cuatrimestre se ajustaron los riesgos correspondientes a la Oficina Asesora de Planeación y se asignaron a Gestión de la Tecnología, dado que cuando se realizó la identificación, Sistemas pertenecía a la Oficina Asesora de Planeación y se ajustó la matriz con aprobación de sistemas a quien corresponde la acción de control.

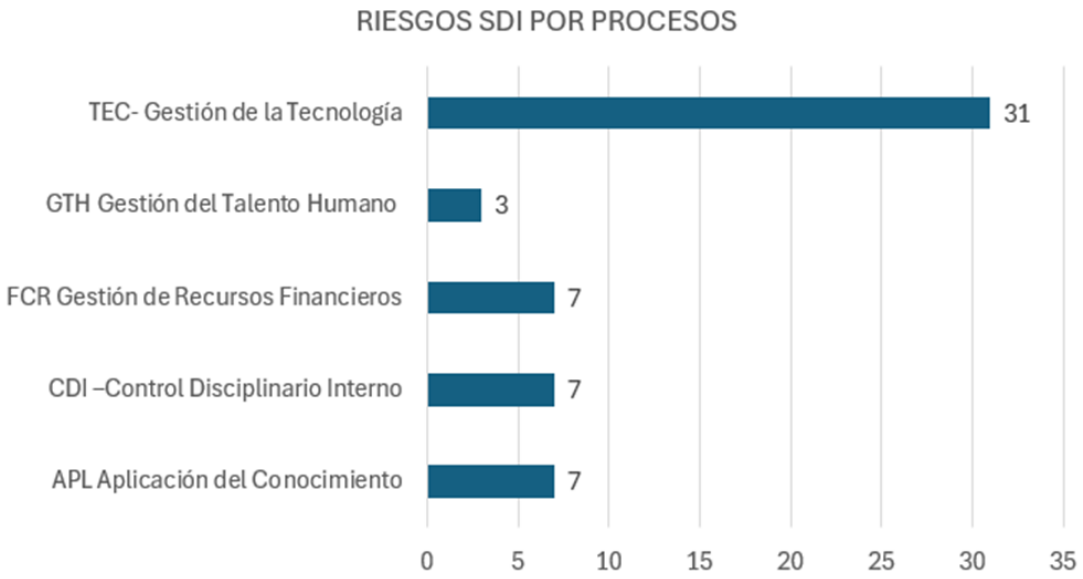


Ilustración 1 Riesgos SDI por proceso

	RIESGO INHERENTE DEL PROCESO		RIESGO RESIDUAL DEL PROCESO	
Sumatoria de riesgos Extremos	0	0%	0	0%
Sumatoria de riesgos altos	54	96%	28	50%
Sumatoria de riesgos moderados	2	4%	26	46%
Sumatoria de Riesgos bajos	0	0%	2	4%
Total	56	100%	56	100%

Tabla 1 Comportamiento de Riesgo

Los riesgos identificados son altos debido a su naturaleza y criticidad, en el desarrollo los controles aplicados para mitigar los riesgos pasan a riesgos moderados pero no es su totalidad dado que hay riesgos que seguirán altos teniendo en cuenta que si se llega a materializar por factores externos ajenos al control establecido tendrán un impacto alto, es importante seguir con la implementación de los controles de manera constante que mitiguen los riesgos de seguridad digital.

4. RESULTADOS DEL SEGUNDO SEGUIMIENTO DE LOS RIESGOS DE SD

Para realizar el seguimiento se revisaron las matrices por proceso y se evidenciaron las siguientes observaciones por cada riesgo de seguridad digital identificados.

No ACTIVO /RIESGO	ACTIVO	PROCESO	OBSERVACIONES/RECOMENDACIONES SEGUNDO SEGUIMIENTO
122/R1 123/R2 124/R3 125//R4 126/R5 127/R6	Servidor ESXi Host vmWare Servidor ESXi Host vmWare Servidor ESXi Host vmWare Servidor ORACLE Base de Datos Servidor SRAPLSICAPITAL Servidor BASE DE DATOS	TEC- Gestión de la Tecnología	Los activos de seguridad digital identificados están relacionados los servidores (hardware) que corresponden a la administración y gestión del proceso de TEC- Gestión de la Tecnología. De las acciones realizadas para mitigar los riesgos el proceso TEC ha avanzado en el cumplimiento dl cronograma de mantenimiento preventivo el cual es esencial para proteger la seguridad informática al mantener los sistemas actualizados, prevenir ataques y asegurar que los usuarios estén informados y preparados para enfrentar posibles amenazas El equipo de soporte con corte al mes de diciembre de 2023 ha realizado los mantenimientos correspondientes a las siguientes áreas: Planeación - 100%, Jurídica - 100%, Educativa - 100%, Participación - 100%, Comunicaciones - 100%, Técnica - 100%, Secretaria General - 100%, Vivero - 100%, Control Interno - 100%, Almacén - 100%, Control Interno Disciplinario - 100% Se encuentra pendiente la finalización de las siguientes áreas: Científica - 50%, Arborización - 75% y Herbario - 50% Las evidencias de la ejecución de los mencionados mantenimientos se encuentran en el Cronograma mantenimientos preventivos Repositorio con evidencia de mantenimientos realizados en carpeta de TEC Dado que durante la vigencia 2023 el equipo de soporte y administración de la infraestructura se encontró con la actualización del conjunto de los diferentes procedimientos institucionales de TI, y la ejecución de varios proyectos como la adquisición e implementación switch, la implementación de la herramienta automática para la generación de backup, la migración del aplicativo SI CAPITAL al servicio de nube pública de Oracle, no fue posible la ejecución de mantenimiento de los servidore a lo programado inicialmente, de tal forma que se ha reprogramado su ejecución para la vigencia 2024. y se han realizado la reposición tecnológica a equipos priorizados en conformidad a las necesidades de las áreas mejorando las condiciones para el desarrollo de las funciones y obligaciones en cumplimiento de metas. De igual manera se han realizado la gestión de eventos y alerta de seguridad a través de la mesa de ayuda, de manera preventiva con el fin de mitigar los riesgos a los que se exponen las entidades el estado se entre reporte de Incidentes de 2023

No ACTIVO /RIESGO	ACTIVO	PROCESO	OBSERVACIONES/RECOMENDACIONES SEGUNDO SEGUIMIENTO
129/R07 130/R08 131/R09 132/R10 133/R11 134/R12 135/R13 136/R14 137/R15 138/R16 139/R17 140/R18 141/R19 142/R20 143/R21 144/R22 145/R23 146/R24 147/R25	Switch Core Slave CORE_JBB Switch SW_AVROJAS_1 Switch SW_AVROJAS_3 Switch SW_AVROJAS_2 Switch SW_ARBORIZACION_1 Switch SW_ARBORIZACION_2 Switch SW_EDUCATIVA_1 Switch SW_EDUCATIVA_2 Switch SW_ADMINISTRATIVA_1 Switch SW_ADMINISTRATIVA_2 Switch SW_CIENTIFICA_1 Switch SW_CIENTIFICA_2 Switch SW_RENATURALIZACION Switch SW_SISTEMAS Switch SW_CENTRO_EVENTOS Switch SW_AULA Switch SW_HERBARIO_2 Switch SW_HPE Wireless Controller WC_JBB	TEC- Gestión de la Tecnología	Los activos de seguridad digital identificados están relacionados los equipos activos Switches de red (hardware), que corresponden a la administración y gestión del proceso de ***TEC- Gestión de la Tecnología***, de igual manera el riesgo identificado es el mismo y la acción de mitigación es la misma por lo cual en riesgo debería ser uno solo que aplica para los 18 activos identificados. En relación al avance de las acciones ejecutadas para mitigar los riesgos se realizó la actualización del Switches Con un proceso de contratación celebrado y asignado con contrato N° JBB-CTO-1021-2023-contratista - SOFTSECURITY S.A.S. con el objeto: Adquirir los switches de Interconexión de red para la comunicación Entre las diferentes áreas de la sede principal del jardín botánico de Bogotá el cual fue ejecutado y cuenta con la evidencia de implementación y configuración mejorando la infraestructura y con las nuevas tecnologías mitigando riesgos por obsolescencia y contando con una mejor configuración se seguridad.
165/R26	Factory	TEC- Gestión de la Tecnología	En el seguimiento de los avances de este riesgo se verifica la actualización del instructivo de autenticación de doble factor, y adicionalmente se realiza seguimiento a las cuentas que tienen habilitado este método de autenticación. A través del documento TEC.PR.07. I.02 Instructivo Autenticación de Doble Factor y configuración en la infraestructura tecnológica y se cuenta con el Informe_validanción_Implemetacion_MFA y fortaleciendo la transferencia de conocimiento.
168/R27	SRV aplicación Central de Cuentas	TEC- Gestión de la Tecnología	El activo de seguridad digital identificado está relacionado con el aplicativo se central de cuentas el cual está configurado en los servidores de la entidad, pero la administración se hace desde la Secretaria General y no está configurado con el directorio activo los que genera un riesgo en el control de acceso, como medida preventiva desde la secretaria se envía correo con el fin de sensibilizar en el cambio de la contraseña de usuario. Así mismo desde tecnología se realiza la administración de la infraestructura.
207/R37 210/R38 211/R39 213/R40	SI CAPITAL aplicativo Correo Red VPN	TEC- Gestión de la Tecnología	Los riesgos identificados relacionados con las aplicaciones, con el fin de realizar el mitigar afectación que pueda presentarse por control de acceso se realiza gestión de usuario activos e inactivos de igual forma durante este periodo se realizó la configuración por parte del equipo de sistemas de las diferentes políticas dentro del Firewall y reporte de monitoreo de usuarios que tienen habilitado el acceso a VPN, dentro del directorio activo. Así mismo se cuenta con las copias de seguridad de SI capital para mitigar riesgos por perdida de información
197/R30 198/R33 202/R34 203/R35	Expedientes Disciplinarios Correspondencia IR Y ER Notificación Comunicación	CDI –Control Disciplinario Interno	Los activos de seguridad digital identificados están relacionados a los expedientes disciplinarios y la documentación asociada al mismo, por lo cual deja un solo seguimiento un solo riesgo que aplica para los 8

No ACTIVO /RIESGO	ACTIVO	PROCESO	OBSERVACIONES/RECOMENDACIONES SEGUNDO SEGUIMIENTO
292/R36 293/R46 297/R47			activos de información identificados. de evaluación y seguimiento, para este periodo se cuenta con la actualización de la matriz peticiones ocasionales de los investigados la cual se guarda en el repositorio del área de igual forma se cuenta con la sección del contrato JBB-CTO-139-2023 para no impactar la falta del personal en el área. De igual forma cuenta con su repositorio seguro de información gestionado.
268/R28	Relación de Cuentas por Cobrar y Pagar	FCR Gestión de Recursos Financieros	Los activos de seguridad digital identificados con Tesorería, Contabilidad, Talento Humano y la documentación asociada a los mismos, por lo cual teniendo en cuenta que los riesgos son de información se dejó la información el repositorio de copias de información centralizado para la mitigación del riesgo y mantiene la cultural de guardarla información en le repositorio correspondiente.
277/R29	Conciliaciones Bancarias		
248/R41	Consignaciones y transferencias bancarias		
261/R42	Estado diario de tesorería		
262/R43	Conciliación bancaria		
279/R44	Conciliaciones de Nomina		
280/R45	Conciliación Cuenta Única Distrital - SHD		
303/R49	Liquidación y pagos de obligaciones del personal	GTH Gestión del Talento Humano	
315/R31 316/R50	Seguimientos y Reportes de la Subdirección Científica	GEN Generación de Conocimiento	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.
692/R32	Cartera de georreferenciación plantaciones	APL Aplicación del Conocimiento	Los activos de seguridad digital identificados en el aplicativo SIGAU - Jardín Botánico de Bogotá (jbb.gov.co), están relacionados con la información contenida en el mismo y en los tableros de control. Adicional a lo anterior se identifica que en “Descripción de la Acción, basado en el análisis de causas” se relaciona la misma para todas y se realiza ajuste con el enlace asignado y se identifica el riesgo R32 y R56 responde al mismo control por lo cual se hace un solo análisis para el mismo riesgo.
687/R51	registro de árboles talados SIGAU		
688/R52	registro bloqueo y traslado de árboles SIGAU		
689/R53	Registro verificación modificación o novedades SIGAU		
690/R54	Registro de solicitud de áreas geográficas		
691/R55	Descarga y registro de actividades		
692/R56	Cartera de georreferenciación plantaciones		

Tabla 2 Seguimiento y observaciones a riesgos

5. RECOMENDACIONES FINALES

- Realizar el ejercicio de revisión y actualización de riesgos de seguridad digital, relacionado los controles al estándar ISO27002, que permita menorar la mitigación de riesgos que se encuentran en nivel alto.

- Realizar las mesas de trabajo con los procesos para el levamiento de activos en conformidad con el proceso SDI.PR.02 Gestión de Activos de Información, para todos los procesos con el fin de verificar la criticidad de seguridad digital como resultado se cuenta con SDI_PR_02_F_01_Identificación_y_clasificación_de_activos_de_información, actualizada como insumo para realizar la gestión de riesgos a los activos críticos de los procesos asociados y se consideraron los activos que corresponden a hardware, software, servicios, espacios físicos y personas. Continuar por parte de la segunda línea de defensa la asesoría y acompañamiento a los procesos en materia de gestión del riesgo de seguridad digital, conforme a los lineamientos de la Política de Administración del Riesgo, que permita la mejora constante y ajuste de los mapas de riesgos de seguridad digital de los procesos de la entidad, revisando tanto el diseño como la ejecución del control para evitar que el riesgo se materialice y se permita el cumplimiento de los objetivos del proceso.

- Actualizar, revisar y monitorear por parte de la Oficina Asesora de Planeación a través de oficial de seguridad las acciones incluidas en la Matriz Institucional de Riesgos de seguridad digital por parte de la primera línea de defensa, con el fin de atender oportunamente las causas que dieron origen a los riesgos identificados, así como su probabilidad e impacto, con el fin de evitar que se materialicen

6. CONCLUSIONES

- Con la actualización del procedimiento de proceso SDI.PR.02 Gestión de Activos de Información realizada en su versión 2, el cuan se ejecutó el levantamiento de activos para todos los procesos JBB, con el resultado de la criticidad en Seguridad Digital, ca partir de este levantamiento se realizará el análisis de riesgo a los críticos con el fin de implementar acciones alineada a los controles que se mitiguen los riesgos asociados.

- De las actividades propuesta en la mitigación e riesgos podemos concluir que se deben seguir trabajando en migrar la información de repositorios personales de OneDrive de los contratistas o funcionarios de dependen de cuentas particulares a la cuentas institucionales, sin embargo se refleja que se adopta esta buena práctica.

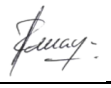
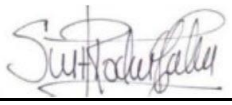
- En relación la infraestructura tecnológica de han presentado avance importantes como la implementación de código doble factor para el control de acceso en confidencialidad de la cuentas, falta vincular a los sistemas de información de los cuales no tiene la

administración la infraestructura tecnológica del área de sistemas, así mismo se han identificado la adquisición de equipo activos y de cómputo con los cuales se realiza una renovación tecnológica con el fin de contar con nuevas tecnologías que brinden seguridad y mitigar las vulnerabilidades por actualizaciones no aplicadas. Igualmente con los dos proyectos de los contratos JBB-CTO-1091-2023 con objeto “adquirir e implementar una solución de almacenamiento de datos de respaldo y el licenciamiento de una herramienta de backup on-premise para fortalecer la estrategia seguridad de la información, recuperación ante desastres y continuidad (DRP) DEL Jardín Botánico De Bogotá y contrato 1021 de 2023 con el objeto contractual "Adquirir los switches de interconexión de red para la comunicación entre las diferentes áreas de la sede principal del Jardín Botánico De Bogotá " y el cambio del antivirus institucional se logra contar con herramientas con las cuales puedan mitigar los riesgos de seguridad digital.

- 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, el cual se encuentra en siguiente enlace:

  Seguimiento a Riesgos evidencias

	Nombre	Firma	Fecha
Aprobado por:	José Alberto Amaya González Jefe Oficina Asesora de Planeación		23-01-2024
Revisado por:	José Alberto Amaya González Jefe Oficina Asesora de Planeación		23-01-2024
Elaborado por:	Catherine Suárez Rodríguez Contratista Oficina Asesora de Planeación		20-01-2024
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			