MEMORANDO

Fecha: 22 de septiembre de 2023

PARA: **CLAUDIA ALEXANDRA PINZON OSORIO**
Subdirectora Científica

GERMÁN DARÍO ÁLVAREZ LUCERO
Subdirector Técnico Operativo

TANIA ELENA RODRIGUEZ ANGARITA
Subdirectora Educativa y Cultural

AURA ELVIRA GÓMEZ MARTINEZ
Secretaria General

CAMILO ANDRÉS ORTIZ MOTTA
Jefe Oficina Jurídica

JESÚS MATEO MÁRQUEZ GARAY
Jefe Oficina Control Disciplinario Interno

OSCAR JAVIER HERNANDEZ SERRANO
Jefe Oficina de Control Interno

DE: **JOSE ALBERTO AMAYA GONZÁLEZ**
Jefe Oficina Asesora de Planeación

ASUNTO: Monitoreo y seguimiento Segundo Cuatrimestre - Riesgos de Seguridad De la Información - SDI 31 agosto 2023.

Cordial saludo

La Oficina Asesora de Planeación a través del proceso de Seguridad de la Información – SDI, dando cumplimiento a los lineamientos establecidos por el Departamento Administrativo de la Función Pública en la Guía para la administración del riesgo y el diseño de controles en entidades públicas V5, se permite remitir el monitoreo y seguimiento a los Riesgos de Seguridad de la Información del JBB-JCM correspondiente al segundo cuatrimestre de la vigencia 2023.

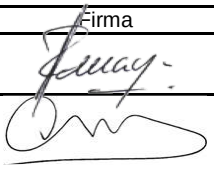
Cualquier inquietud con gusto será atendida.

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

Cordial saludo.

JOSÉ ALBERTO AMAYA GONZÁLEZ
Jefe Oficina Asesora de Planeación

Anexos: Formato DYP.PR.07. F.05. Mapa de Riesgos Sistema Seguridad de la Información

	Nombre	Firma	Fecha
Aprobado por:	José Alberto Amaya González Jefe Oficina Asesora de Planeación		22-09-2023
Revisado por:	Gustavo Olaya F. Contratista Oficina Asesora de Planeación		22-09-2023
Elaborado por:	Catherine Suárez Rodríguez Contratista Oficina Asesora de Planeación		22-09-2023
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			

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

Informe de Monitoreo y Seguimiento Riesgos de Seguridad de la Información

Corte a 31de agosto

Jardín Botánico de Bogotá - José Celestino Mutis

Oficina Asesora de Planeación

2023

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

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[1].

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, 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
OAP	Oficina Asesora de Planeación	DYP Direccionamiento y Planeación
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 en su versión 4, la cual fue adoptada mediante resolución 363 del 21 de octubre de 2022 “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 riesgos de seguridad de la información, fundamentado en la aplicación del Anexo 4. “Lineamientos para la gestión de riesgos de seguridad digital en entidades públicas”[2] y como resultado se dio alcance al diligenciamiento del Mapa de Riesgos Sistema Seguridad de la Información.

[1] https://jbb.gov.co/documentos/planeacion/2022/octubre/Politica_Riesgos_JBB.pdf
[2] 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

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

3. MATRIZ DE RIESGOS DE SEGURIDAD DIGITAL.

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.

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 identificaron riesgos asociados a los activos críticos en términos de disponibilidad, confidencialidad e integridad de la información de los procesos, producto del ejercicio En el ejercicio del 2022, se realizó la valoración de los riesgos de seguridad de la información y se estructuraron los controles con los cuales se dará tratamiento en la matriz; "*Mapa de Riesgos Sistema Seguridad de la Información", donde se identificaron 56 riesgos para los proceso seleccionados.*

Con base en los resultados del monitoreo y seguimiento del Primer Cuatrimestre de riesgos de SDI 30 abril 2023, se realizó 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 asignación del riesgo que correspondía al proceso DYP y fue asignado previo conocimiento de sistemas a TEC- Gestión de la Tecnología de la siguiente manera:

Tabla 1 Relación de riesgo identificados

No Riesgo	PROCESO	DESCRIPCION DEL RIESGO CAUSA INMEDIATA+CAUSA RAIZ-2022)
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.

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

No Riesgo	PROCESO	DESCRIPCION DEL RIESGO CAUSA INMEDIATA+CAUSA RAIZ-2022)
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
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

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

No Riesgo	PROCESO	DESCRIPCION DEL RIESGO CAUSA INMEDIATA+CAUSA RAIZ-2022)
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.
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

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

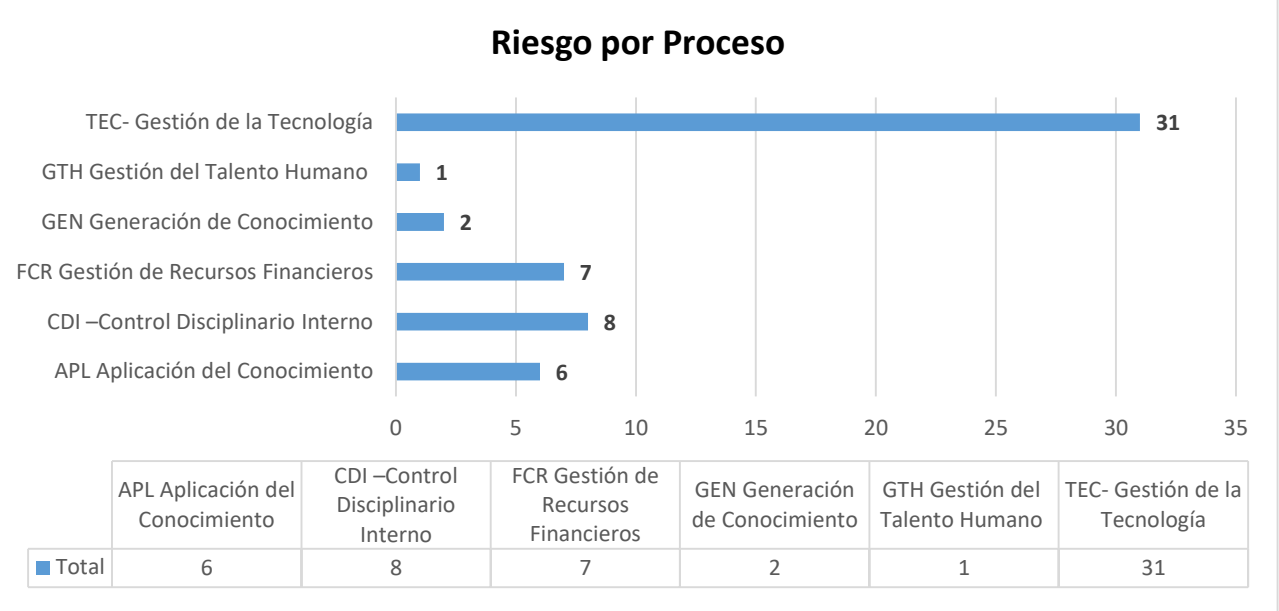
No Riesgo	PROCESO	DESCRIPCION DEL RIESGO CAUSA INMEDIATA+CAUSA RAIZ-2022)
R37	TEC- Gestión de la Tecnología	por modificación indebida de los registros ingresados debido al acceso no autorizado al aplicativo y la base de datos que contiene los registros
R38	TEC- Gestión de la Tecnología	por modificación 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
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

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

No Riesgo	PROCESO	DESCRIPCION DEL RIESGO CAUSA INMEDIATA+CAUSA RAIZ-2022)
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 segundo cuatrimestre de 2023, se mantiene la cantidad de Riesgos con relación al cierre de la vigencia anterior. Es importante mencionar que se hace un ajuste de asignación de proceso a los riesgos correspondientes a DYP Direccionamiento y Planeación los cuales quedan relacionados al proceso de TEC-Gestión de la Tecnología, dado que cuando se realizó la identificación, Sistemas pertenecía a la Oficina Asesora de Planeación por lo cual se ajustó para este informe y se presenta en riesgos por proceso así:

Ilustración 1 Riesgos SD por proceso



Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

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, esta actividad tiene un avance del 9% de los 381 equipos proyectados, teniendo en cuenta que se han presentado dificultades por los diversos traslados por obra civil a 5 edificaciones, así mismo, a través de la coordinación se ha dado prioridad a la recepción de equipos nuevos durante el mes de agosto de 2023 y se han realizado la reposición tecnológica a equipos priorizados en conformidad a las necesidades de la áreas, mejorando la 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 envidos por los entes de control 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. Para el mantenimiento preventivo de los servidores se están ejecutando esta actividad y para el próximo cuatrimestre de tendrán los resultados representados.

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

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 el 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 Switch Core a la última versión, sin embargo, algunos de los switches de la entidad no pueden ser actualizados debido a que su infraestructura es obsoleta. Por lo anteriormente mencionado se realizó un proceso de contratación celebrado y asignado con contrato N° JBB-CTO-1021-2023-contratista -SOFTSECURITY S.A.S, que tiene por 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 vence el 22 de octubre del 2023.
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. En el cumplimiento de la actividad se realiza la actualización del documento TEC.PR.07.I.02 "Instructivo Autenticación de Doble Factor" y se desarrollan las actividades relacionadas en el mismo para las cuentas de toda la entidad y se elabora un Informe validación Implementación MFA.
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 lo 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 y de igual manera desde tecnología se realiza la administración de la infraestructura.

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

No ACTIVO/RIESGO	ACTIVO	PROCESO	OBSERVACIONES/RECOMENDACIONES SEGUNDO SEGUIMIENTO
207/R37 210/R38 211/R39 213/R40	SI CAPITAL aplicativo Correo Red VPN	TEC- Gestión de la Tecnología	Para los riesgos identificados relacionados con las aplicaciones, con el fin de mitigar la 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.
197/R30 198/R33 202/R34 203/R35 292/R36 293/R46 297/R47 298/R48	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 se deja un solo seguimiento a riesgos que aplica para los 8 activos de información identificados. la evaluación y seguimiento, para este periodo esa relacionada 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.
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. Así mismo esta con el usuario de Secretaria General como propietario de la información.
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	Los activos de seguridad digital identificados con Subdirección Científica están relacionados con la copia de información en el repositorio del área para mitigar el riesgo de pérdida de integridad de la información, se deja un solo análisis riesgo asociado a los dos activos identificados.
692/56	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
687/R51	registro de árboles talados SIGAU		
688/R52	registro bloqueo y traslado de árboles SIGAU		
689/R53	Registro verificación modificación o novedades SIGAU		

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

No ACTIVO/RIESGO	ACTIVO	PROCESO	OBSERVACIONES/RECOMENDACIONES SEGUNDO SEGUIMIENTO
690/R54	Registro de solicitud de áreas geográficas		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 elimina dejando el R56.
691/R55	Descarga y registro de actividades		

Tabla 2 Seguimiento 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 desde la Oficina asesora de Planeación a través del Oficial de seguridad con los procesos para el levantamiento 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

- En el ejercicio de análisis de riesgos identificar los activos que corresponden a hardware, software, servicios, espacios físicos y personas para todos los procesos.

- 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 en su versión 4 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.

- Continuar con la revisión y monitoreo 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 próximo cuatrimestre se realizará el levantamiento de activos para todos los procesos JBB, con el resultado de la criticidad en Seguridad Digital, 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.

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071

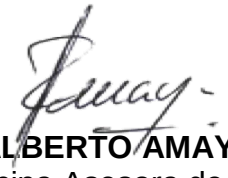
- Con las actividades propuesta en la mitigación de los procesos en la matriz de riesgos, podemos concluir que se deben contar con repositorios asignados a las cuentas de cada área y no de OneDrive de los contratistas o funcionarios que dependen de cuentas particulares, de igual manera se ha avanzado en la implementación de código doble factor para el control de acceso en confidencialidad de la cuentas, es importante mencionar que se deben 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.

- 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:

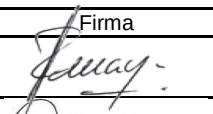
  Seguimiento a Riesgos evidencias

Cordialmente;



JOSE ALBERTO AMAYA GONZALEZ
Jefe Oficina Asesora de Planeación

Anexos: Formato DYP.PR.07. F.05. Mapa de Riesgos Sistema Seguridad de la Información

	Nombre	Firma	Fecha
Aprobado por:	José Alberto Amaya González Jefe Oficina Asesora de Planeación		22-09-2023
Revisado por:	Gustavo Olaya F. Contratista Oficina Asesora de Planeación		22-09-2023
Elaborado por:	Catherine Suárez Rodríguez Contratista Oficina Asesora de Planeación		22-09-2023
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			

Av cll 63 # 68-95
Teléfono: 437 7060
www.jbb.gov.co
Código Postal: 111071