INFORME AVANCE PLAN TECNOLÓGICO

1. ACTIVIDADES POR SEDES

Con el fin de fortalecer la plataforma tecnológica de la entidad se adelantaron las siguientes actividades discriminadas por sede:

✓ **SEDE COLEGIO DE LA CGR**

- Se fortalecieron las políticas de navegación y de accesos a la información en las salas de sistemas.
- Se extendió la cobertura de la red inalámbrica del Colegio de la CGR, con la instalación de dos AP y la redistribución de los existentes.
- Actualización del firewall CHECKPOINT.
- Contratación del servicio del software de gestión académica para el colegio de la CGR, bajo la modalidad de outsourcing.

✓ **SEDE CENTRO MÉDICO**

- Se extendió la cobertura de la red inalámbrica del Centro médico, cubriendo los tres pisos de la sede.
- Actualización del firewall CHECKPOINT.
- Ajuste de la red de datos con la segmentación de la red de datos.
- Ajuste del software para implementar un esquema de seguridad y disponibilidad más robusto que el que se venía manejando.
- Actualización de las políticas de acceso y distribución de información.

✓ **SEDE ADMINISTRATIVA**

- Estudio de vulnerabilidades mediante análisis GAP de las tres sedes;
- Ajuste del mapa de riesgos existente.
- Configuración de navegación segura de dominio para los aplicativos: ALFANET, CREDITO Y CARTERA, SOFTWARE DE GESTIÓN MÉDICA y PORTAL INSTITUCIONAL.

- Reinstalación de tres servidores conforme se ajusta la infraestructura de la sede administrativa.

- Ajuste de la cobertura inalámbrica en la sede administrativa e instalación de servicios sobre servidores CENTOS.

- Ajuste de las políticas del dominio FBSCGR.LOCAL.

- Aumento de la capacidad de los correos de la entidad y aseguramiento de la información manejada en el correo.

- Configuración de la herramienta de análisis de tráfico para la sede administrativa

- Centralización de la nube de información del FBS en las unidades organizativas

- Optimización del acceso a la información en las áreas de:

    - Atención al usuario
    - Crédito
    - Cesantías

- Automatización de las copias de respaldo y salvaguarda de información en las áreas de Cesantías, atención al usuario.

- Centralización de la información de archivo digital para el archivo de la entidad.

✓ **DATACENTER EXTERNO**

Se adelantaron actividades de reforzamiento de seguridad web, escritorios remotos y optimización de aplicaciones. Todo esto con el fin de mitigar los intentos de accesos a la información que se presentan.

Se ha optimizado las actividades con la modificación de servidores Microsoft a servidores Linux, con el fin de asegurar la correcta protección de la información.

El tamaño de las bases de datos ha aumentado el tiempo de generación de los backup´s de aplicaciones, por lo cual se ha requerido de un escalamiento de servicios para asegurar el acceso a la información. Se ha realizado el proceso conllevando dos días de exportación de máquinas, por esta razón la actividad se debe realizar ya sea fuera de horario laboral o los días sábados y domingos para mitigar la indisponibilidad de aplicaciones.

2. ACTIVIDADES GENERALES

- **Actividades de seguridad:** Se reforzó la plataforma tecnológica en el DATACENTER externo, la mitigación de ataques alcanzo una eficiencia del 95%, las reglas configuradas y el monitoreo sobre el tráfico de red en las aplicaciones externas permitió llevar a cero los ingresos no autorizados, se ha tenido un 5% de

indisponibilidad debido a tareas propias de accesos y mantenimiento de las plataformas.

- **Índice de transparencia y acceso a la información,** Se diligencio y actualizo el formulario de la Procuraduría. El portal institucional se adecuo a los requerimientos establecidos por la norma de la ITA.

- **Políticas de acceso a la información y protección de datos,** se presentó la política de seguridad y manejo de datos de la entidad, a nivel de información y masificación se envió mediante correo electrónico y se socializo en las pantallas de los equipos como mensaje de bienvenida para el uso y autorización de acceso a los servicios tecnológicos del FBS para sus funcionarios. Se incrementó el nivel de seguridad para blindar los datos y asegurar una mayor calidad de los mismos. Está pendiente la realimentación de las medidas de seguridad implementadas para el manejo de datos de la entidad.

- **Accesibilidad,** este trabajo se adelantó con la ayuda y gestión del área de atención al usuario, cesantías, crédito y servicios misionales, se habilitaron accesos y masificación de formularios mediante el uso de las herramientas de Google. Con el ajuste del módulo de PQRD´s de la entidad se estandarizo a los requerimientos solicitados por la política de gobierno digital y a los requerimientos internos planteados por los usuarios finales.

- **Política de Gobierno Digital,** Se inició el año 2019 con un avance de migración del 37% a la fecha se ha subido a un 70% según plantilla de evaluación provista por el sitio de evaluación del MINTIC, a la fecha es necesario migar la medición a la MIPG conforme la respuesta del asesor del MINTIC y la apertura de la herramienta de evaluación del FURAG.

- **Renovación tecnológica,** Se adelantaron todos los procesos de contratación planteados y los equipos se ingresaron al inventario

3. RESULTADO ANÁLISIS GAP

Anexo A de referencia	Título de control	Descripción del control	Función	Status	Hallazgos
A.5	Políticas de seguridad de la información				
5.1	Directrices de la Dirección en seguridad de la información.				
5.1.1	Conjunto de políticas para la seguridad de la información	Existe un documento. Más se requiere su actualización a la nueva plataforma		MD	Está documentado, se pone en práctica pero falta la formalización
5.1.2	Revisión de las políticas para la seguridad de la información	No se ha realizado la revisión por parte de la alta gerencia		MD	Está documentado, se pone en práctica pero falta la formalización
A.6	Aspectos Organizativos De La Seguridad De La Información				
6.1	Organización interna.				
6.1.1	Asignación de responsabilidades para la segur. de la información	No existe una designación formal de estas responsabilidades		RD	El control está diseñado pero no se ajusta a la norma
6.1.2	Segregación de tareas			RD	No se realiza mediante medios convencionales
6.1.3	Contacto con las autoridades			RD	No está establecido
6.1.4	Contacto con grupos de interés especial			MD	
6.1.5	Seguridad de la información en la gestión de proyectos.	No existe		MD	
6.2	Dispositivos para movilidad y teletrabajo.				
6.2.1	Política de uso de dispositivos para movilidad			RD	
6.2.2	Teletrabajo	En formulación		RD	Aunque existe una política del estado Colombiano, en la entidad no se ha establecido el proceso, ni mucho menos los controles
A.7	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS				
7.1	Antes de la contratación.				
7.1.1	Investigación de antecedentes			MD	Depende de recursos humanos y no se tiene claridad si se hace o no
7.1.2	Términos y condiciones de contratación.			MD	Depende de recursos humanos y no se tiene claridad si se hace o no
7.2	Durante la contratación				
7.2.1	Responsables de gestión			D	
7.2.2	Concienciación, educación y capacitación en seguridad de la información.			RD	No está establecido
7.2.3	Proceso disciplinario			RD	Depende de jurídica y no se tiene claridad si se hace o no
7.3	Cese o cambio de puesto de trabajo.				
7.3.1	Cese o cambio de puesto de trabajo.			RD	No se hace

A.8	Gestión de activos				
8.1	Responsabilidad sobre los activos				
8.1.1	Inventario de activos.			MD	
8.1.2	Propiedad de los activos			MD	
8.1.3	Uso aceptable de los activos.			MD	El control se diseñó, se aplica pero no se alinea con la norma
8.1.4	Devolución de activos.			MD	no se utiliza
8.2	Clasificación de la información				
8.2.1	Directrices de clasificación.			RD	El control se diseñó y aplica, pero no está ajustado del todo con la norma
8.2.2	Etiquetado y manipulado de la información			RD	El control se diseñó y aplica, pero no está ajustado del todo con la norma
8.2.3	Manipulación de activos			RD	El control se diseñó y aplica, pero no está ajustado del todo con la norma
8.3	Manejo de los soportes de almacenamiento				
8.3.1	Gestión de soportes extraíbles			RD	
8.3.2	Eliminación de soporte			PNP	no se hace
8.3.3	Soportes físicos en transito			RD	no se hace seguimiento
A.9	Control de accesos				
9.1	Requisitos de negocio para el control de accesos.				
9.1.1	Política de control de accesos			MD	
9.1.2	Control de acceso a las redes y servicios asociados.			MD	
9.2	Gestión de acceso de usuario.				
9.2.1	Gestión de altas/bajas en el registro de usuarios.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma
9.2.2	Gestión de los derechos de acceso asignados a usuarios.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma
9.2.3	Gestión de los derechos de acceso con privilegios especiales.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma
9.2.4	Gestión de información confidencial de autenticación de usuarios.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma
9.2.5	Revisión de los derechos de acceso de los usuarios.			RD	
9.2.6	Retirada o adaptación de los derechos de acceso			MD	Falta formalizar la política
9.3	Responsabilidades del usuario				

9.3.1	Uso de información confidencial para la autenticación			MD		
9.4	Control de acceso a sistemas y aplicaciones.					
9.4.1	Restricción del acceso a la información.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma	
9.4.2	Procedimientos seguros de inicio de sesión.			MD		
9.4.3	Gestión de contraseñas de usuario.			MD		
9.4.4	Uso de herramientas de administración de sistemas.			MD		
9.4.5	Control de acceso al código fuente de los programas.			NA (Not Applicable)		
A.10	Cifrados					
10.1	Controles criptográficos					
10.1.1	Política de uso de los controles criptográficos			RD	No se trabaja controles criptográficos	
10.1.2	Gestión de claves			RD	No se trabaja controles criptográficos	
A.11	Seguridad física y ambiental					
11.1	Áreas seguras					
11.1.1	Perímetro de seguridad física.			MD		
11.1.2	Controles físicos de entrada.			MD		
11.1.3	Seguridad de oficinas, despachos y recursos.			MD	Hasta ahora están conformando el equipo que maneja la seguridad de oficinas	
11.1.4	Protección contra las amenazas externas y ambientales.			MD		
11.1.5	El trabajo en áreas seguras.			MD		
11.1.6	Áreas de acceso público, carga y descarga			MD		
11.2	Seguridad de los equipos					
11.2.1	Emplazamiento y protección de equipos.			RD		
11.2.2	Instalaciones de suministro.			RD		
11.2.3	Seguridad del cableado.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma	
11.2.4	Mantenimiento de los equipos.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma	
11.2.5	Salida de activos fuera de las dependencias de la empresa.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma	
11.2.6	Seguridad de los equipos y activos fuera de las instalaciones.			RD		

11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.			RD	no hay un proceso establecido para esto	
11.2.8	Equipo informático de usuario desatendido.			RD		
11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla			MD		
A.12	SEGURIDAD EN LA OPERATIVA					
12.1	Responsabilidades y procedimientos de operación					
12.1.1	Documentación de procedimientos de operación.			PNP	No existe	
12.1.2	Gestión de cambios.			RD		
12.1.3	Gestión de capacidades.			RD		
12.1.4	Separación de entornos de desarrollo, prueba y producción			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma	
12.2	Protección contra código malicioso					
12.2.1	Controles contra el código malicioso			RD		
12.3	Copias de seguridad					
12.3.1	Copias de seguridad de la información			MD		
12.4	Registro de actividad y supervisión					
12.4.1	Registro y gestión de eventos de actividad.			MD		
12.4.2	Protección de los registros de información.			RD	no se ha establecido	
12.4.3	Registros de actividad del administrador y operador del sistema.			RD	no hay seguimiento ni control ni procedimiento	
12.4.4	Sincronización de relojes			MD	No se realiza formalmente	
12.5	Control de software en explotación					
12.5.1	Instalación del software en sistemas en producción			MD		
12.6	Gestión de la vulnerabilidad técnica					
12.6.1	Gestión de las vulnerabilidades técnicas.			MD		
12.6.2	Restricciones en la instalación de software			MD		
12.7	Consideraciones de las auditorías de los sistemas de información					
12.7.1	controles de auditoría de los sistemas de información			MD		
A.13	Seguridad en las telecomunicaciones					

13.1	Gestión de la seguridad en las redes					
13.1.1	Controles de red.			MD	Hasta ahora van a comenzar su formulación	
13.1.2	Mecanismos de seguridad asociados a servicios en red.			MD		
13.1.3	Segregación de redes			MD		
13.2	Intercambio de información con partes externas					
13.2.1	Políticas y procedimientos de intercambio de información.			RD		
13.2.2	Acuerdos de intercambio.			RD		
13.2.3	Mensajería electrónica.			RD		
13.2.4	Acuerdos de confidencialidad y secreto.			RD	No están formalizados a pesar de que existe un documento. Solo en contadas ocasiones los trabajan	
A.14	Adquisición, desarrollo y mantenimiento de sistemas					
14.1	Requisitos de seguridad de los sistemas de información					
14.1.1	Análisis y especificación de los requisitos de seguridad.			MD		
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas			MD		
14.2	Seguridad en los procesos de desarrollo y soporte					
14.2.1	Política de desarrollo seguro de software.			RD	No existe	
14.2.2	Procedimientos de control de cambios en los sistemas.			RD	No existe	
14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo			RD	No existe	
14.2.4	Restricciones a los cambios en los paquetes de software.			MD		
14.2.5	Uso de principios de ingeniería en protección de sistemas.			MD		
14.2.6	Seguridad en entornos de desarrollo.			RD	No existe	
14.2.7	Externalización del desarrollo de software.			MD	No existe	
14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.			RD		
14.2.9	Pruebas de aceptación.			RD		
14.3	Daños de prueba					
14.3.1	Protección de los datos utilizados en pruebas			MD		
A.15	RELACIONES CON SUMINISTRADORES					

15.1	Seguridad de la información en las relaciones con suministradores				
15.1.1.	Política de seguridad de la información para suministradores.			RD	
15.1.2	Tratamiento del riesgo dentro de acuerdos con suministradores			RD	
15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones			RD	
15.2	Gestión de la prestación del servicio por suministradores				
15.2.1	Supervisión y revisión de los servicios prestados por terceros.			RD	
15.2.2	Gestión de cambios en los servicios prestados por terceros			RD	
A.16	Gestión de incidentes de seguridad de la información				
16.1	Gestión de incidentes de seguridad de la información y mejoras				
16.1.1	Responsabilidades y procedimientos.			MD	
16.1.2	Notificación de los eventos de seguridad de la información.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma
16.1.3	Notificación de puntos débiles de la seguridad.			MD	
16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma
16.1.5	Respuesta a los incidentes de seguridad.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma
16.1.6	Aprendizaje de los incidentes de seguridad de la información.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma
16.1.7	Recopilación de evidencias			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma
A.17	Aspectos de seguridad de la información dentro de la continuidad del negocio				
17.1	Continuidad de la seguridad de la información				
17.1.1	Planificación de la continuidad de la seguridad de la información			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma
17.1.2	implantación de la continuidad de la seguridad de la información.			RD	
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información			RD	
17.2	Redundancias				
17.2.1	Disponibilidad de instalaciones para el procesamiento de la información			RD	
A.18	Cumplimiento				
18.1	Cumplimento de los requisitos legales y contractuales				
18.1.1	Identificación de la legislación aplicable.			MD	

18.1.2	Derechos de propiedad intelectual (DPI).			MD	Hay un control que no cumple con las normas. Debe ser rediseñado
18.1.3	Protección de los registros de la organización.			MD	
18.1.4	Protección de datos y privacidad de la información personal.			MD	El control se realiza, pero falta su documentación formal. Está alineado con la norma y las leyes y políticas existentes en el país
18.1.5	Regulación de los controles criptográficos			RD	no existe
18.2	Revisiones de la seguridad de la información				
18.2.1	Revisión independiente de la seguridad de la información.			RD	no existe
18.2.2	Cumplimiento de las políticas y normas de seguridad.			RD	no existe
18.2.3	Comprobación del cumplimiento			RD	no existe

Cantidad	Códigos Status	Significado	%	Contribución %
1	**D**	El control se documentó e implementó	100	**1%**
61	**MD**	El Control se lleva a cabo y el proceso debe ser documentado para asegurar la repetitividad del proceso y mitigar los riesgos.	90	**54%**
48	**RD**	El control no cumple las normas y debe ser rediseñado para cumplir con las normas	50	**43%**
2	**PNP**	El proceso no está en su lugar / no implementado. (Control requeridos ni documentado ni implementado)	0	**2%**
0	**NA (Not Applicable)**	El control no es aplicable para la empresa ni para el negocio		**0%**
112				

Como resultado de los análisis y actividades adelantadas se tiene:

1. Es necesario desagregar las actividades de seguridad, manejo de información, soporte, infraestructura, administración de software y avances TIC´s en varias designaciones.
2. Se requiere entrara a reconfigurar en la sede Colegio de la CGR la red y las políticas con el fin de asegurar una mejor operación de los equipos.
3. Fortalecer el uso de la gestión electrónica de documentos
4. Fortalecer el almacenamiento, gestión de información y manejo de las copias de seguridad de los archivos contenidos en los discos duros de los equipos de la entidad.
5. Fomentar el conocimiento del manejo responsable de la información por parte de los usuarios finales, esto con el fin de mitigar la pérdida de datos o la modificación de los mismos.

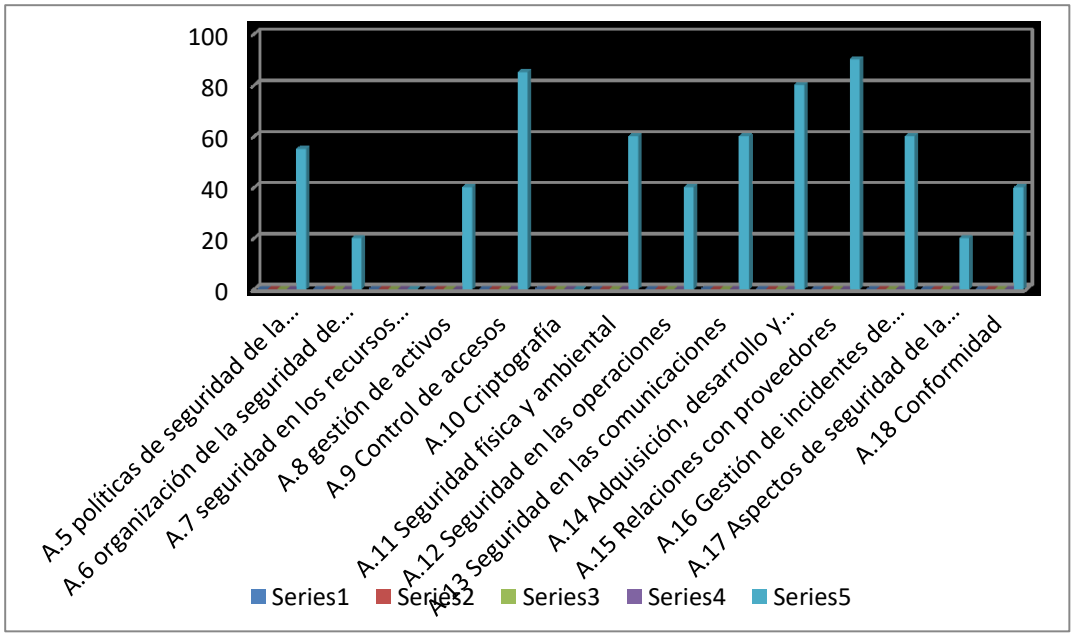
Se ha establecido el siguiente esquema para el manejo de aplicaciones en aras de asegurar la disponibilidad de la información y la continuidad de procesos

APLICACIÓN	ÁREA QUE LA REQUIERE	ADMINISTRADOR OPERATIVO	ADMINISTRADOR SEGURIDAD	DIRECCIÓN ENCARGADA DE SU MANTENIMIENTO Y POLITICAS	ADMINISTRADOR POLITICA DE MANEJO DE DATOS	RESPONSABLE TRATAMIENTO DE DATOS
Crédito y cartera	Crédito y cartera	Profesionales crédito y cartera	Profesional sistemas	Director Administrativo y financiero	Director Administrativo y financiero	La entidad (funcionarios que registran y hacen proceso de información) Contratistas y terceros con relación contractual vigente
ALFANET	Atención al usuario	Técnico de atención al usuario	Profesional sistemas	Director Administrativo y financiero	Director Administrativo y financiero	La entidad (funcionarios que registran y hacen proceso de información) Contratistas y terceros con relación contractual vigente
Nomina	Talento Humano	Profesional Talento Humano	Profesional sistemas	Director Administrativo y financiero	Director Administrativo y financiero	La entidad (funcionarios que registran y hacen proceso de información) Contratistas y terceros con relación contractual vigente
Portal institucional	Dirección de desarrollo	Profesional comunicaciones	Profesional sistemas	Directora de Desarrollo y Bienestar	Director Administrativo y financiero	La entidad (funcionarios que registran y hacen proceso de información) Contratistas y terceros con relación contractual vigente
Gestión médica	Centro médico	Profesional centro Médico	Profesional sistemas	Directora de Desarrollo y Bienestar	Director Administrativo y financiero	La entidad (funcionarios que registran y hacen proceso de información) Contratistas y terceros con relación contractual vigente
Gestión académica	Colegio de la CGR	Rectora Colegio CGR	Profesional sistemas	Directora de Desarrollo y Bienestar	Director Administrativo y financiero	La entidad (funcionarios que registran y hacen proceso de información) Contratistas y terceros con relación contractual vigente
Coolocation	Dirección administrativa y financiera	Director administrativo y financiero	Profesional sistemas	Director Administrativo y financiero	Director Administrativo y financiero	La entidad (funcionarios que registran y hacen proceso de información) Contratistas y terceros con relación contractual vigente

4. CUMPLIMIENTO DE NORMA ISO 27001:2013

GRÁFICA RADIAL CONTROLES ANEXO A 27002:2013

GRÁFICO DE BARRAS PORCENTAJE CUMPLIMIENTO DOMINIOS



Se detecta una falla sobre la gestión de los activos y los controles de seguridad a nivel de acceso, el valor sobre recursos humanos se encuentra en cero, debido a la falta de una herramienta efectiva de evaluación de este ítem.

Se detecta que los pilares de seguridad, integridad y disponibilidad a nivel de hardware se encuentran cubiertos conforme las revisiones y resultados presentados. A nivel de software se encuentran en proceso de mejora para blindar más las aplicaciones.

El componente Humano tiene una baja puntuación, es necesario socializar las políticas del FBS sobre el manejo de los recursos tecnológicos. Es necesario se incluya capacitaciones a los funcionarios sobre el manejo de la seguridad de información ya que en la actualidad no es conocido o adoptado por los funcionarios en sus actividades diarias.

Los procedimientos en la entidad no hacen uso de la transversalidad y en especial el manejo del flujo de la información contenida en los aplicativos.
La gestión de los documentos físicos y electrónicos debe ser reforzada ya que a la fecha se presenta un proceso de adaptación al uso de las herramientas con sus consecuencias.

No se hace uso y gestión adecuados de la seguridad de información, el nivel de integridad de los datos que se manejan fuera de aplicaciones es muy bajo ya que es posible el intercambio no autorizado de la misma y no existe una cultura definida en los funcionarios sobre el manejo responsable de dicha información.

La entidad cuenta con todo su software debidamente licenciado, cumpliendo con la legislación de derechos de autor que rige a las entidades públicas.

5. DETALLE DE GESTIÓN TIC

Licencias	1	Objetivo misional de seguridad	Actualización y/o actualización de licencias	renovación del licenciamiento del antivirus,	Software mcafee sobre motor mysql	Licencia renovada	Producción	Plan de compras Recursos propios
Licencias	1	Mejoramiento de la infraestructura tecnológica del FBS	Actualización y/o actualización de licencias	Renovación de licenciamiento del sistema firewall	Software checkpoint	Licencia renovada	Producción	Plan de compras Recursos propios
Licencias	1	Mejoramiento de la infraestructura tecnológica del FBS	Actualización y/o actualización de licencias	Renovación de licenciamiento del sistema vmware	software Vmware	Licencia renovada	Producción	Plan de compras Recursos propios
Licencias	200	Mejoramiento de la infraestructura tecnológica del FBS	Actualización y/o actualización de licencias	Upgrade de licenciamiento de correo electrónico	Plataforma de correos gmail enterprise	Licencia renovada	Producción	Plan de compras Recursos propios
Equipos	5	Mejoramiento de la infraestructura tecnológica del FBS	Adquisición de hardware	Adquisición de impresoras de alto volumen		Equipos adquiríos	Instaladas	Plan de compras Recursos propios
Equipos	4	Mejoramiento de la infraestructura tecnológica del FBS	Adquisición de hardware	Adquisición de video BEAMS		Equipos adquiríos	Asignados	Plan de compras Recursos propios
Equipos	1	Mejoramiento de la infraestructura tecnológica del FBS	Adquisición de hardware	Adquisición de impresora de etiquetas		Equipos adquiríos	Adquirida	Plan de compras Recursos propios

6. ANALISIS DE RIESGOS

		Determinación de Controles existentes		Matriz de análisis de Riesgos			
	RIESGOS	¿EXISTE ALGUN CONTROL?	¿ES LO MÁS APROPIADO?	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO	TRATAMIENTO SUGERIDO
A	Incumplimiento de los acuerdos establecidos en los pliegos de contratación por parte de los proveedores y contratistas.	SI	Si, ya que existe un supervisor experto en el área para revisar el cumplimiento de los acuerdos establecidos.	5	5	25	Ejecución de los Acuerdos de Nivel de Servicios o las sanciones contempladas en la ley 80 referente a contratación estatal, Se realiza la mitigación del riesgo.
B	Demoras en la gestión por parte de la administración en los trámites requeridos por el área de sistemas.	SI	Se ajustó el manual y se ha dado celeridad a los procesos	5	5	25	Aplicabilidad del manual de contratación de la entidad, Se realiza la mitigación del riesgo.
C	Aumento de la cartera morosa.	SI	Se hace seguimiento en el área de cartera con el fin de realizar su recuperación y disminuir este índice.	3	5	15	Ejecución de las cláusulas a los morosos con el fin de recuperar esta cartera. Se realiza la mitigación del riesgo, esta actividad corresponde al área financiera y al grupo de cartera de la entidad.
D	Disminución de los aportes entregados por los funcionarios.	SI	No, porque no se puede aplicar un control sobre el manejo de los aportes que cada funcionario quiera entregar.	3	5	15	Redistribución de fondos de funcionamiento. Se realiza la mitigación del riesgo.
E	Robo de información por parte de los funcionarios.	SI	Se encuentra bloqueado la copia de cd y dvs, la información del sistema financiero se encuentra restringida a registro y acceso, más sin embargo el acceso por usb se encuentra habilitado, por lo tanto se vulnera la seguridad de la información al momento que los funcionarios se llevan los datos para continuar con su trabajo fuera de las instalaciones de la entidad.	10	7	70	Restricción de los medios de almacenamiento mediante bloqueos de periféricos. Revisión de la información substraída con el fin de determinar las implicaciones del robo. Se realiza la mitigación del riesgo con el ajuste de los sistemas de dominio y antivirus con el fin de implementar restricciones de dispositivos USB y la presentación de políticas de manejo de la información generada, entregada y manipulada en la entidad.
F	Traslado de archivos en medios extraíbles	NO		10	7	70	Instalación de software de monitoreo de los equipos y bloqueo de accesos a USB, Se realiza la mitigación del riesgo.

G	Substracción de equipos.	SI	Se realiza la revisión y solicitud de autorizaciones por parte de la empresa de vigilancia contratada por la entidad.	3	5	15	Revisión del sistema de cámaras de seguridad y registro de acceso con el fin de determinar la ruta por la cual los equipos fueron retirados de las instalaciones, con base en esta información identificar a los implicados con el fin de aplicar las correspondientes medidas. Se realiza la mitigación del riesgo.
H	Terremotos	NO		3	10	30	Se transfiere el riesgo. Mediante las pólizas de seguros.
I	Tormentas eléctricas.	NO		5	5	25	De acuerdo con la intensidad empezar la secuencia de apagado de equipos con el fin de evitar daños en la infraestructura de comunicaciones como en los equipos del FONDO DE BIENESTAR SOCIAL DE LA CGR. Se realiza la mitigación del riesgo.
J	Incendios.	SI	Existen sistemas de prevención y detectores en las sedes.	5	5	25	Se realizó la solicitud a la administración para contratar la implementación de sistema de aviso y extinción de incendios. Se realiza la mitigación del riesgo con la solicitud que se dirigió a la gerencia de la entidad y la dirección administrativa y financiera.
K	Caída de los servidores	SI	Se realiza el registro de los eventos en el formato de operación de los servidores y se hace la corrección del evento, si es de hardware se adelanta el trámite de solicitud de soporte al contratista de mantenimiento y si es de software se realiza la revisión y el debido a acompañamiento por parte del proveedor de las aplicaciones montadas en los servidores	3	10	30	Utilizar el protocolo de mantenimiento referente al proceso de respaldo en cuanto a caída de servidores. Se realiza la mitigación del riesgo a través de la contratación de empresas de apoyo tanto para los sistemas Windows, Linux, bases de datos y demás sistemas implementados en los servidores.
L	Ataques de virus, troyanos, gusanos y spyware.	SI	Se actualiza el antivirus y se mantienen parchados los sistemas a través de las consolas	5	5	25	Dependiendo de la severidad del ataque y la vulnerabilidad de los sistemas ejecutar rutinas de contención y utilización de antivirus con el fin de eliminar la infección o realizar su contención hasta lograr eliminarla de los equipos. Se realiza la mitigación del riesgo.
M	Caídas de la rede de datos	SI	Se ha ajustado la topología de las redes con el fin de optimizar el servicio	3	3	9	Revisión del plano lógico de la red de datos y diseñar los correctivos para solventar la falla en la transmisión de datos. Se realiza la mitigación del riesgo.

N	Desbalanceo de las cargas de la red eléctrica.	SI	No, porque no hay un sistema de monitoreo en la red eléctrica y se realizan reasignación de personal y áreas sin contar con el estudio previo de distribución de cargas.	5	5	25	Identificar la fuente del desbalanceo de cargas y redistribuirlas a fin de evitar caídas en el sistema. De presentarse caídas iniciar la secuencia de encendido para identificar la fuente del desbalanceo y corregirlo mediante el balanceo de cargas sobre el tablero eléctrico. Se realiza la mitigación del riesgo.
O	Desactualización de manuales y planes de contingencia	SI	Si, con el seguimiento a través de la herramienta MIPG se asegura la actualización y validación de las contingencias	5	5	25	Revisión de los procesos e identificación de las falencias de los manuales y los planes de contingencia de cada proceso con el fin de asegurar la continuidad del negocio, de no existir ni el manual ni el plan de contingencia este debe ser desarrollado. Se realiza la mitigación del riesgo.
P	Sabotaje a la red.	SI		5	5	25	Identificar la procedencia del sabotaje, determinar si es a nivel lógico o físico, si es a nivel lógico realizar el seguimiento del tráfico a través del software de monitoreo e identificar los alcances del sabotaje con base en estos alcances determinar la acción a tomar. Si es a nivel físico realizar la investigación debida para identificar a las personas implicadas y determinar la acción a ser tomada. En cualquier caso, se debe realizar un análisis para determinar las acciones correctivas para evitar futuros sabotajes. Se realiza la mitigación del riesgo.
Q	Descontento de los funcionarios	NO		5	5	25	Realizar reuniones de concertación e identificar las causas y posibles fuentes de desconcierto para tomar medidas correctivas, que pueden ir desde la modificación de funciones hasta el nivel de investigación interna con sus debidas implicaciones. Se realiza la mitigación del riesgo.

R	Penetración indebida	SI	Se registra a través del acceso de firewall y con políticas de auditoria sobre los recursos compartidos del servidor.	5	5	25	Identificar el punto de acceso y determinar el grado de complicidad de los diversos funcionarios, con base en estos hechos realizar el proceso de investigación interna con las debidas implicaciones que esto conlleva, paralelamente se debe dar parte a las autoridades y entes de control, para identificar a los participantes en la acción y realizar el debido proceso legal, de igual forma se debe identificar las intenciones de dicha acción. Se debe verificar si el acceso fue consecuencia de un punto de acceso desprotegido y corregir dicha situación. Se realiza la mitigación del riesgo.
S	Cambio de las actividades establecidas en el manual de procesos.	NO		3	3	9	Se debe realizar el ajuste de las normas de seguridad a las nuevas actividades, de ser necesario se deben ajustar las normas de seguridad a actividades o procesos nuevos. Se realiza la mitigación del riesgo.
T	Pérdida de la información almacenada tanto en medio físico como en medio magnético y óptico.	SI	A través de la consola antivirus, generación de backups y atención de solicitudes de recuperación.	5	5	25	Identificar la causa y de ser posible la restauración de la información de las copias de seguridad. Se realiza la mitigación del riesgo.
U	Falta de compromiso de los funcionarios responsables de las áreas en las cuales se utilizan los sistemas de información de la entidad	NO		5	10	50	Se debe adelantar reuniones de concientización sobre la importancia del manejo adecuado de la información e identificar las posibles falencias en los procesos y determinar la responsabilidad de los funcionarios en el proceso, se mitiga este riesgo.
V	Comunicaciones informales sobre el manejo y acceso a la información sin la debida documentación requerida ni el registro pertinente	NO		5	10	50	Se debe realizar el registro de toda información proveniente desde y hacia las áreas con el fin de poder medir la trazabilidad existente. Se debe realizar el registro en el sistema de gestión documental o a través de correos electrónicos, se mitiga este riesgo.
W	Manejo indebido de los backup generados	SI	Las copias de respaldo se almacenan en discos externos y en la nube del FBS, el manejo se encuentra restringido a determinados funcionarios	5	5	25	Se generará un documento para el manejo de los backup´s de igual manera se realizará las pruebas de eficiencia y se verificará la salvaguarda de dichas copias de respaldo, se mitiga el riesgo.

X	Ingreso por parte de los funcionarios a páginas web no autorizas	SI	Se realiza un seguimiento de las páginas no autorizadas, más sin embargo hace falta definir la acción pertinente al momento de presentarse reiteración en el acceso de páginas web o contenido no autorizado o con contenido no relevante para el desarrollo de las actividades al interior de la entidad.	5	5	25	Se aplican bloqueos a través del sistema firewall y sistema antivirus, de persistir el acceso indebido se procederá con el informe de esta situación a la dirección administrativa y financiera de la entidad, se mitiga ese riesgo.
Y	Ejecución de software portable en la red de la entidad	SI	Existen restricciones desde las GPO implementadas en la red y en el sistema antivirus de la entidad. Más sin embargo hace falta definir la acción pertinente al momento de presentarse reiteración en la ejecución de aplicativos portables.	5	5	25	Se bloquea el acceso y ejecución de medios portables. Se mitiga este riesgo.
Z	Préstamo indebido de contraseñas token´s	SI	El control del uso de este elemento toke´n o certificado de firma digital se encuentra asignado mediante acuerdo firmado por el funcionario ante la empresa certificadora. De existir algún fallo o vulnerabilidad en este uso la responsabilidad recae enteramente en el funcionario que tiene asignado el toke´n o certificado de firma digital.	5	5	25	Como responsabilidad de los usuarios finales de los toke´s, contraseñas cuentas de usuarios se realizara un comunicado para dar a conocer los riesgos del préstamo y las implicaciones que conlleva esta actividad, se mitiga el riesgo.
AA	Debilidad en las contraseñas del aplicativo ALFANET	SI	Se ajustó la seguridad del aplicativo para mitigar este riesgo	5	5	25	
AB	El sistema ALFANET no se está utilizando por parte de los funcionarios de la entidad	SI	Mediante correos electrónicos y memorandos se realiza el seguimiento al uso de dicha aplicación.	5	5	25	Se solicita a los funcionarios que manejan el sistema ALFANET la realización de capacitaciones y talleres de utilización del aplicativo con el fin de implementar las políticas de cero papel al interior de la entidad y sus sedes externas.
AC	La clasificación por organigrama dentro del aplicativo ALFANET no ha sido alimenta de forma adecuada	SI	Se ha realizado el cargue de información	5	5	25	Se solicita al administrador del aplicativo ALFANET el registro correcto de las dependencias y los niveles de accesos requeridos, se mitiga este riesgo.
AD	Falta de avance en la implementación en la estrategia de Gobierno en Línea	SI	Se evalúa mediante uso de la herramienta MIPG	5	5	25	Solicitar a los Lideres de GEL y las profesionales de cada grupo el avance de las actividades estipuladas, Este riesgo se Mitiga.

AE	Falta de personal de apoyo, No hay suficiente personal en el área de sistemas, esto implica una exceso en carga laboral de la persona del área,	NO		10	10	100	Solicitar un mayor número de personal para el área de sistemas, Este riesgo se Mitiga.
AF	Manejo de información descentralizada	NO		10	10	100	Verificar la aplicabilidad de la norma de usabilidad e igualdad tecnológica contemplada en GEL
AG	Aplicativo del Centro médico, sin una persona a cargo que tenga los conocimientos tanto de sistemas de información como manejo de aplicativos de salud y atención a pacientes	SI	Se ha descentralizado el uso de la aplicación y mediante el contrato de soporte se ha ajustado el esquema de solicitudes y modificaciones del mismo	5	10	50	Es necesario aplicar la normatividad vigente en cuento a la implementación de GEL en la entidad
AH	No existe una diferenciación en cuanto administración manejos, operatividad y funcionalidad de los aplicativos	NO		10	10	100	Es necesario establecer el nivel de jerarquías y responsabilidades en los aplicativos, se recomienda el cumplimiento de la NTC/ISO 27000 y sus subseries
AI	Centralización sobre el área de sistemas de los procedimientos, referentes en los aplicativos de la entidad	NO		10	10	100	No existe un documento que defina los roles administrativos, operativos, funcionales, auditoria ni manejo de la información, la centralización sobre una única persona va en contra de las normas vigentes en la actualidad, de igual manera es un alto riesgo mantener en una sola persona todo el control de los aplicativos

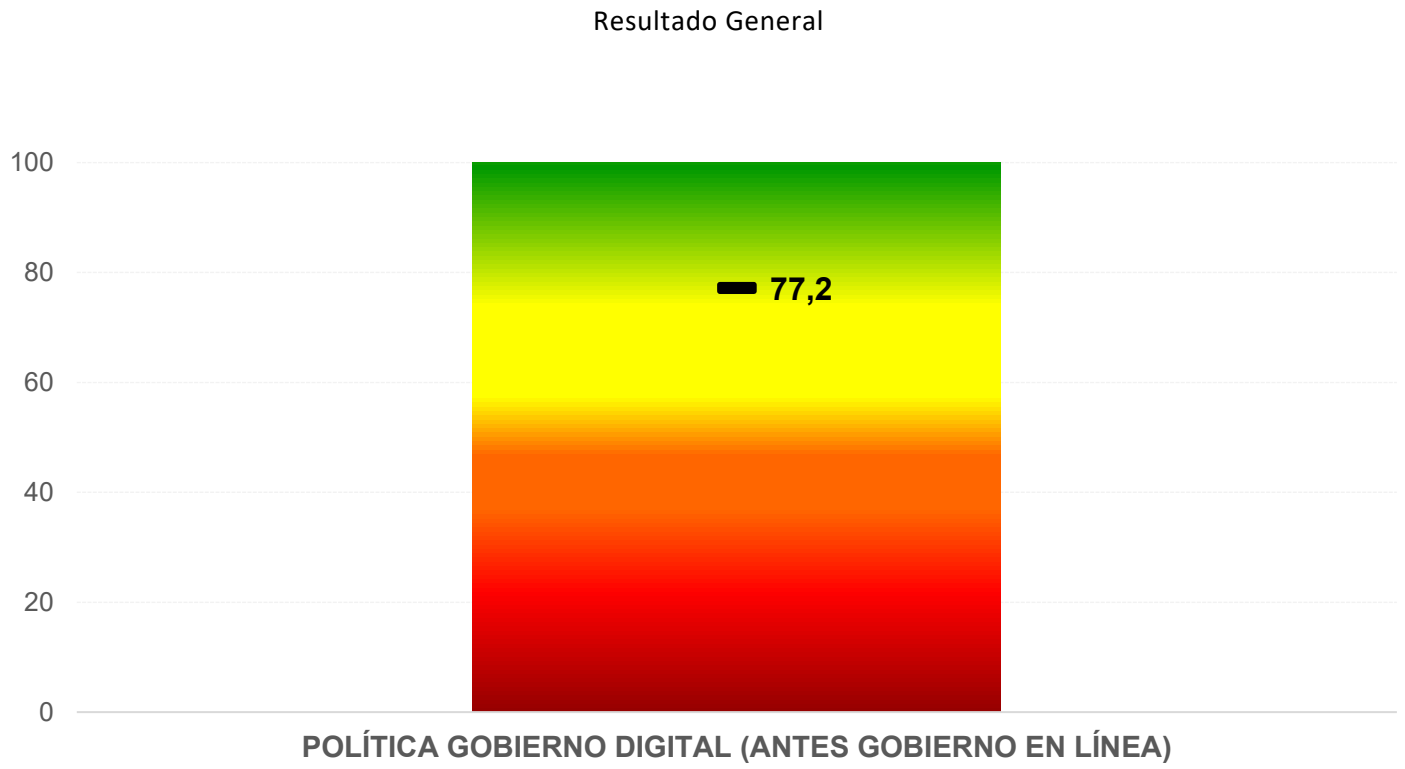
7. INVENTARIO DE INFORMACIÓN FONDO DE BIENESTAR SOCIAL DE LA CGR

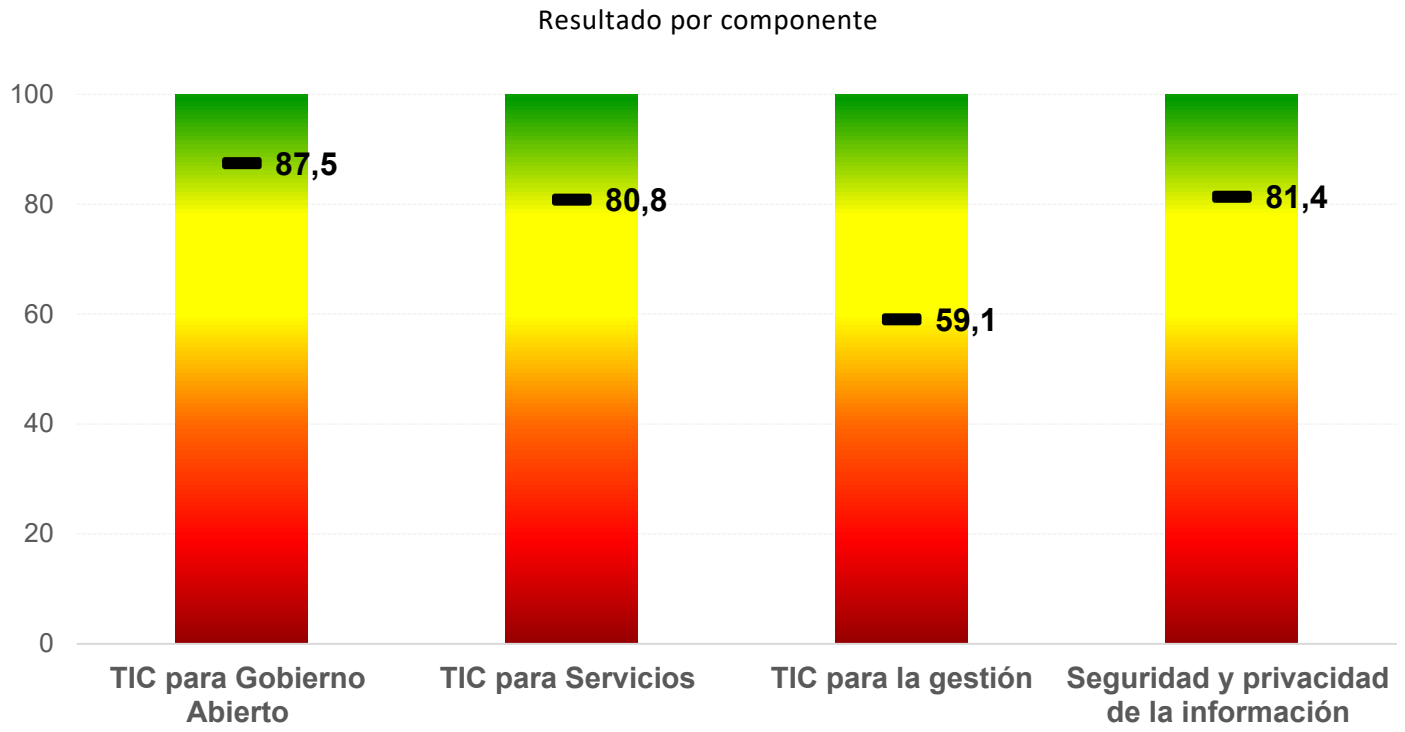
Nombre de la información	Descripción	Área responsable de la información	Tipología de información	Ámbito geográfico	Idioma	Fuente primaria	Evidencia de solicitud	Tipo de información/ origen	Frecuencia de generación de la información	Formato	Frecuencia de actualización
Portal Institucional - PORTAL	El portal de Internet del Fondo de Bienestar Social de la Contraloría General de la Republica de forma fácil e integrada, el acceso a una serie de recursos y de servicios relacionados con la Entidad. Incluye: enlaces a las aplicaciones que se administran dentro del Fondo, foros, documentos información misional y demás ; está dirigido resolver necesidades de información especifica	Oficina de Comunicaciones	Servicios y Beneficios	Nacional e Internacional	español / Ingles	Fuente primaria	Estado - Contraloría - Ciudadanía	Digital	Diaria	pdf, doc,xls,csv,wms,zip,Html, css,Java scrip	Quincenal
INTRANET	La intranet del Fondo de Bienestar Social de La Contraloría General de la Republica es el sitio web que ofrece a los funcionarios de la Entidad, información de manera fácil e íntegra, permitiendo el acceso a una serie de recursos y de servicios relacionados con la Entidad. Temas de	Oficina de Comunicaciones	Institucional y de Interés para los funcionarios	Nacional	Español	Fuente primaria	Funcionarios de la Entidad	Digital	Diaria	pdf, doc,xls,csv,wms,zip,Html, css,Java scrip	Diaria

	interés a los funcionarios										
Correo electrónico	Servicio de red que permite a los usuarios enviar y recibir correos electrónicos	Oficina de Sistemas e Informática	Oficial	Nacional e Internacional	Español	Fuente primaria	Servicio	Digital	Permanente	Texto	Permanente
Plan Estratégico	Almacena el avance de las acciones asociadas al Plan de Acción del FBS	Oficina de Planeación	Gestión	Nacional	Español	Fuente primaria	Administrativa	Manual - Documento Físico	Trimestral	XLS	Trimestral
PMI	Plan de Mejoramiento Institucional PMI - Almacena el avance de las actividades que buscar mitigar los hallazgos encontrados por los diferentes entes que nos realizan auditoria y que se plasman en un plan de mejoramiento	Oficina de Planeación	Gestión	Nacional	Español	Fuente primaria	Entidad Pública	Documento Físico / Manual	Mensual	XLS	Mensual
Plan de Manejo de riesgos	Almacena el avance de las actividades que buscan mitigar los riesgos encontrados y que hacen parte del manejo de riesgo institucional	Oficina de Control Interno: Realiza el seguimiento; el registro lo realizan cada dependencias responsables de la actividad	Gestión	Nacional	Español	Fuente primaria	Administrativa	Documento Físico / Manual	Mensual	XLS	Mensual
Alfanet	Sistema de Gestión Documental: Es un sistema lógico que permite radicar documentos recibidos, registrar documentos enviados, realizar trámites, gestión, archivo y consulta de los documentos	Atención Al Usuario	Documental	Nacional	Español	Fuente primaria	Interna / Externa	Físico / Digital	Diaria	TIF, pdf, excel, word	Automatico
Normograma	Almacena la información sobre la normatividad que rige a la Entidad	Oficina de Planeación	Gestión	Nacional	Español	Fuente primaria	Interna / Externa	Documento Físico / Manual	Mensual	doc/txt	Mensual

SICME	Sistema Integrado de Control de Calidad - Control de Documentos Internos del Sistema de Control de Calidad	Oficina de Planeación	Gestión	Nacional	Español	Fuente primaria	Interna / Externa	Documento Físico / Manual	Mensual	doc/txt	Mensual
Boletín Ingresos y Egresos	Sistema de apoyo al FBS para el control de los ingresos y egresos diarios. Apoyo al proceso contable	Dirección Administrativa y Financiera	Gestión	Nacional	Español	Fuente primaria	Entidad Pública	Documento Físico / Manual	Cada Hora	Bases de Datos	Diaria
Portal - Sitio WEB	Es el aplicativo donde muestra los servicios y beneficios ofrecidos por el FBS a los funcionarios	Sistemas	Gestión	Nacional	Español	Fuente primaria	Entidad Pública	Audiovisual	Semanal	HTML	Semanal
SIGEP	Aplicativo para la administración del sistema de talento Humano de la planta de personal del FBS	Talento Humano	Talento Humano	Nacional	Español	Fuente primaria	Interna / Administrativa	Documento Físico / Digital	Diaria	pdf, papel, archivos planos	Diaria
PQR	Sistema de Información que permite registrar las solicitudes de quejas, derechos de petición, denuncias, etc	Atención Al Usuario	Gestión	Nacional	Español	Fuente primaria	PQR	Digital / Físico	Diaria	Bases de Datos	Diaria
TAO	Aplicativo para la gestión de créditos y cartera	Dirección Administrativa y Financiera	Gestión	Nacional	Español	Fuente primaria	Interna / Administrativa	Digital	Diaria	Bases de Datos	Diaria

8. AVANCE POLITICA GOBIERNO DIGITAL




Resultado por componente
100
80
60
40
20
0
87,5
80,8
59,1
81,4
TIC para Gobierno Abierto
TIC para Servicios
TIC para la gestión
Seguridad y privacidad de la información