BOGOTÁ | CAJA DE LA VIVIENDA POPULAR

MEMORANDO

Al contestar cite estos datos:
Radicado No.: **202211200132203**
Fecha: 02-12-2022

PARA: **JUAN CARLOS LÓPEZ LÓPEZ**
Director General

LUZ YAMILE REYES BONILLA
Jefe Oficina de Tecnologías de la Información y Comunicaciones TIC

MARÍA MERCEDES MEDINA OROZCO
Directora Administrativa De Gestión Corporativa Y CID

GLORIA MARINA CUBILLOS MORALES
Subdirectora Administrativa

CATALINA MARGARITA NAGY PATIÑO
Jefe Oficina Asesora de Planeación

DE: **DIANA CONSTANZA RAMIREZ ARDILA**
Asesora de Control Interno

ASUNTO: Informe Final - Auditoria de Evaluación del grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Caja de la Vivienda Popular - CVP, conforme a lineamientos MINTIC e ISO 27001-2013

Respetados Doctores, reciban un cordial saludo,

En cumplimiento del Plan Anual de Auditorías de la vigencia 2022, adjunto presentamos el informe final de la Evaluación del grado de implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) de la Caja de la Vivienda Popular - CVP, conforme a los lineamientos establecidos MINTIC e ISO 27001-2013.

Como resultado general de la auditoría practicada y según la escala de valoración de efectividad de controles definida para el anexo 1 de la norma técnica ISO 27001:2013, se puede concluir que el Modelo de Privacidad y Seguridad de la Información adoptado en la

Calle 54 No. 13-30
Código Postal: 110231, Bogotá D.C.
PBX: (60-1) 3494550 - (60-1) 3494520
FAX:(60-1) 310 5583
www.cajaviviendapopular.gov.co
soluciones@cajaviviendapopular.gov.co

Caja de Vivienda Popular alcanza actualmente un nivel de implementación del 71% y se clasifica como GESTIONADO, lo cual significa que buena parte de los controles se monitorean y se miden de manera que es posible tomar medidas de acción cuando se detecta que los procedimientos y/o actividades no funcionan eficientemente.

El informe adjunto contempla el resultado y análisis de las observaciones recibidas en respuesta al informe preliminar mediante comunicaciones No. 202211600123143 del 16 de noviembre de 2022 por parte la Oficina TIC y No. 202217200124503 del 18 de noviembre de 2022 por parte la Subdirección de Gestión Administrativa.

Es preciso manifestar que el análisis y respuesta frente a las catorce (14) observaciones y tres (3) Oportunidades de mejora formuladas se encuentran dirigidas así:

Proceso de Gestión de Tecnologías de la información y las Comunicaciones.

- Oportunidades de mejora 1,2,3
- Observaciones: 1,2,3,4,5,6,7,8,9,10,11,12,13 y 14

Proceso Gestión del Talento Humano

- Observaciones: 2 y 3

Proceso Gestión Adquisición de Bienes y Servicios:

- Observación: 2

Procesos de Servicio a la Ciudadanía

- Observaciones: 3

Proceso Gestión Administrativa:

- Observación: 6

Asimismo, existen veintitrés (23) recomendaciones que la Asesoría de Control Interno realiza de carácter preventivo con el propósito de que sean analizadas e incorporadas en la gestión y mejora de los procesos.

Calle 54 No. 13-30
Código Postal: 110231, Bogotá D.C.
PBX: (60-1) 3494550 - (60-1) 3494520
FAX:(60-1) 310 5583
www.cajaviviendapopular.gov.co
soluciones@cajaviviendapopular.gov.co

Finalmente, cabe señalar que la Asesoría de Control Interno mediante esta oficialización del informe final solicita que dentro de los ocho (8) días hábiles siguientes remita los formatos 208-CI-FT-15 Formulación de Plan de Mejoramiento y 208-CI-FT-16 Formato de análisis causal a los correos electrónicos: jsarmientop@cajaviviendapopular.gov.co y dramireza@cajaviviendapopular.gov.co.

Agradecemos nuevamente la colaboración y disposición prestada en todo momento por los funcionarios de su (s) dependencia (s) para el desarrollo de este proceso auditor.

Cordialmente,

DIANA CONSTANZA RAMÍREZ ARDILA
Asesora de Control Interno
dramireza@cajaviviendapopular.gov.co

Anexos: Informe Final de auditoría (PDF)
Herramienta Evaluación MSPI CVP (Excel)

Proyectó: Javier Alfonso Sarmiento Piñeros – Contratista CTO-696-2022 Asesoría de Control Interno
Revisó: Diana Constanza Ramírez Ardila – Asesora de Control Interno

Calle 54 No. 13-30
Código Postal: 110231, Bogotá D.C.
PBX: (60-1) 3494550 - (60-1) 3494520
FAX:(60-1) 310 5583
www.cajaviviendapopular.gov.co
soluciones@cajaviviendapopular.gov.co

1. **OBJETIVO:** Evaluar el Sistema de Gestión de la Seguridad de la Información implementado en la Caja de la Vivienda Popular - CVP, conforme a lineamientos del Modelo de Seguridad y Privacidad de la información - MSPI del Ministerio de Tecnologías de la Información las Comunicaciones y la Norma Técnica ISO 27001:2013.

2. **ALCANCE:** Cubre la implementación del Sistema de Gestión de Seguridad de la Información al corte de 31 julio de 2022.

3. **PERIODO DE EJECUCIÓN:** Inicio 16 de agosto y finalización 11 de octubre de 2022.

4. **EQUIPO AUDITOR:** Diana Constanza Ramírez Ardila – Auditor Líder, Asesora de Control Interno
Javier Alfonso Sarmiento Piñeros- Auditor Contratista Asesoría Control Interno CTO 696-2022

5. **CRITERIOS DE AUDITORIA:**

   - Conpes 3995 julio de 2020 – Política Nacional de Confianza y Seguridad Digital.
   - Decreto 1008 de 2018 - Política de Gobierno Digital.
   - Modelo de Seguridad y Privacidad de la Información V4 – febrero 2021.
   - Guía Metodológica de Pruebas de Efectividad – MSPI G1.
   - Guía para la Gestión y Clasificación de Activos de Información – MSPI G5.
   - Marco de Ciberseguridad del NIST[1].
   - Procedimientos GTIC – CVP.

6. **METODOLOGÍA DE TRABAJO:** La Asesoría de Control Interno (en adelante ACI) dando cumplimiento al Plan Anual de Auditorías vigencia 2022, planificó el desarrollo de la auditoria con radicado 202211200085333 cuyo propósito consistió en evaluar el grado de implementación del Modelo de Seguridad y Privacidad de la Información en adelante (MSPI) de la Caja de la Vivienda Popular - CVP, conforme a lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones y la Norma Técnica ISO 27001-2013.

   Para realizar la evaluación fueron contempladas tres (3) perspectivas principales:

   La primera, consistió en evaluar la efectividad de los controles definidos en la norma ISO 27001:2013 para catorce (14) dominios puntuables en componentes administrativos y técnicos en el marco del Modelo de Seguridad y Privacidad MSPI.

   La segunda, se enfocó en determinar el nivel de madurez del Modelo de Seguridad y Privacidad de la Información implementado en la Caja de Vivienda Popular – CVP.

   La tercera perspectiva buscó identificar una línea base para la CVP frente a las mejores prácticas en ciberseguridad definidas por el NIST, alrededor de cinco (5) funciones básicas (Detectar, Identificar, Responder, Recuperar y Proteger) acorde a los lineamientos de la política nacional de confianza y seguridad digital Conpes 3995[2].

---

[1] Instituto Nacional de Estándares y Tecnología de Estados Unidos

[2] Define medidas para desarrollar la confianza digital a través de la mejora la seguridad digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías – julio de 2020.

La herramienta empleada para emitir la valoración cuantitativa y cualitativa corresponde al *"instrumento de evaluación MSPI"* creado por el Ministerio de Tecnologías de la Información y las Comunicaciones en adelante MINTIC el cual es usado para identificar el nivel de madurez en la implementación de MSPI y el cual define la siguiente escala para valoración de controles:

Tabla de Escala de Valoración de Controles ISO 27001:2013 ANEXO A		
Descripción	**Calificación**	**Criterio**
No Aplica	N/A	No aplica.
Inexistente	0	*Total, falta de cualquier proceso reconocible.*
Inicial	20	*Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo*
Repetible	40	*Los procesos y los controles siguen un patrón regular*
Efectivo	60	*Los procesos y los controles se documentan y se comunican.*
Gestionado	80	*Los controles se monitorean y se miden.*
Optimizado	100	*Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas.*

Fuente: Herramienta evaluación MSPI

A continuación, se presentan los rangos de calificación para los dominios.

Tabla de rangos de Calificación de Dominios		
Descripción	**Calificación**	**Criterio**
Inexistente	0	*Total, falta de cualquier proceso reconocible.*
Inicial	1 A 20	*Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo*
Repetible	21 A 40	*Los procesos y los controles siguen un patrón regular*
Efectivo	41 A 60	*Los procesos y los controles se documentan y se comunican.*
Gestionado	61 A 80	*Los controles se monitorean y se miden.*
Optimizado	81 A 100	*Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas.*

Fuente: Herramienta evaluación MSPI

La evaluación de los criterios se desarrolló tomando como base el análisis de las evidencias solicitadas y las entrevistas de auditoria programadas con la Líder y equipo de trabajo del proceso de Tecnologías de la Información y las Comunicaciones.

Como valor agregado la ACI contrastó los resultados actuales con la evaluación 2021 adelantada por la Alta Consejería TIC con el fin de identificar los criterios en los cuales se evidencia avance y también aquellos que suponen emprender acciones de mejora por encontrarse rezagados.

7. CONCLUSIONES:

Como resultado de la auditoría practicada y según la escala de valoración de efectividad de controles definida para el anexo 1 de la norma técnica ISO 27001:2013, se puede concluir que el Modelo de Privacidad y Seguridad de la Información adoptado en la Caja de Vivienda Popular alcanza actualmente un nivel de implementación del 71% y se clasifica como GESTIONADO, lo cual significa que buena parte de los controles se monitorean y se miden de manera que es posible tomar medidas de acción cuando se detecta que los procedimientos y/o actividades no funcionan eficientemente.

A continuación, se presenta la conclusión por cada una de las perspectivas:

7.1 Perspectiva evaluación de la efectividad de los controles definidos en la norma ISO 27001:2013 en la Entidad:

Se evidenció que ocho (8) de los dominios evaluados (57%) incrementaron su calificación respecto a la evaluación 2021, resaltando que tres (3) de ellos subieron de nivel pasando de Gestionado a Optimizado en el caso del dominio A6 “Organización de la seguridad de la Información” y “A16 Gestión de Incidentes de la seguridad de la información” lo cual significa que las buenas prácticas se siguen y automatizan. Por otra parte, el dominio A8 “Gestión de Activos” incrementó su nivel de Efectivo a Gestionado lo cual significa que los controles se monitorean y además se mide el cumplimiento de los procedimientos.

	Evaluación de Efectividad de controles					
No.	DOMINIO	Calificación Actual	Evaluación Alta Consejeria TIC - Semestre II - 2021	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL ACTUAL	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2021
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	81	65	100	OPTIMIZADO	GESTIONADO
A.8	GESTIÓN DE ACTIVOS	62	54	100	GESTIONADO	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	85	75	100	OPTIMIZADO	GESTIONADO

Fuente: Herramienta evaluación MSPI 2022 CVP

Por otra parte, se identificaron (2) dominios del sistema que bajaron de nivel “A7. Seguridad de los recursos humanos” y “Aspectos de seguridad de la Información de la gestión de la Continuidad del Negocio” y el dominio “A10 Criptografía” que es el dominio con más baja puntuación.

	Evaluación de Efectividad de controles					
No.	DOMINIO	Calificación Actual	Evaluación Alta Consejeria TIC - Semestre II - 2021	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL ACTUAL	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2021
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	77	83	100	GESTIONADO	OPTIMIZADO
A.10	CRIPTOGRAFÍA	20	0	100	INICIAL	INEXISTENTE
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	37	64	100	REPETIBLE	GESTIONADO
	PROMEDIO EVALUACIÓN DE CONTROLES	**71**	**69**	**100**	GESTIONADO	GESTIONADO

Fuente: Herramienta evaluación MSPI 2022 CVP

7.2 Nivel de madurez del Modelo de Seguridad y Privacidad de la Información implementado en la Caja de Vivienda Popular – CVP:

Se evidenció un avance del 53% en el desarrollo del ciclo PHVA del Modelo de Seguridad y Privacidad de la Información implementado en la CVP que corresponde a un nivel de madurez “Administrado” lo cual significa que la mayoría de los controles han sido documentados, aprobados, implementados y actualizados permitiendo establecer la efectividad de los mismos.

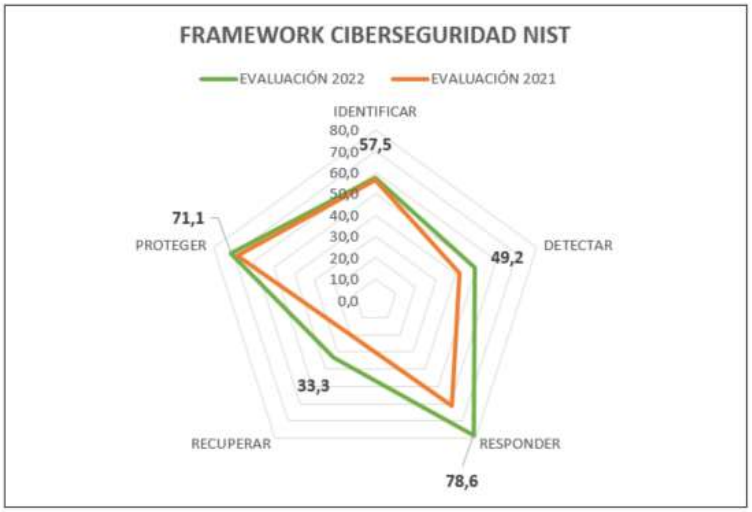
Año	AVANCE PHVA		
	COMPONENTE	% de Avance Actual Entidad	% Avance Esperado
2022	Planificación	35%	40%
	Implementación	3%	20%
	Evaluación de desempeño	7%	20%
	Mejora continua	8%	20%
TOTAL		53%	100%

Fuente: Herramienta evaluación MSPI 2022 CVP

7.3 Línea de base para la CVP frente a las mejores prácticas en ciberseguridad definidas por el NIST:

El nivel de adopción de buenas prácticas de ciberseguridad definidas por el NIST en la CVP se estima en 58% un avance de 9 puntos frente al 49% obtenido en la evaluación 2021. Sobresale la puntuación de las funciones RESPONDER y PROTEGER cuyos porcentajes respectivamente fueron 78% y 71%. Sin embargo, para las funciones DETECTAR y RECUPERAR, la puntuación obtenida es inferior al 50%. Esta valoración se puede explicar por el bajo desempeño identificado en los Dominios del sistema “A.10 Criptografía”, y “A.17 Aspectos de la Seguridad de la Información de la continuidad del negocio”. A continuación

FUNCIÓN	EVALUACIÓN 2022	EVALUACIÓN 2021
IDENTIFICAR	57,5	56,5
DETECTAR	49,2	41,5
RESPONDER	78,6	61,4
RECUPERAR	33,3	20,0
PROTEGER	71,1	68,0
	58,0	**49,5**



Fuente: Elaboración propia

8. DESARROLLO Y RESULTADOS DE LA AUDITORÍA:

A continuación, se presentan los aspectos observados, recomendaciones formuladas y oportunidades de mejora planteadas, producto de las pruebas desarrolladas de acuerdo con los objetivos de auditoria, las cuales tienen como propósito principal contribuir al fortalecimiento de la gestión, operación y control del Modelo de Seguridad y Privacidad de la Caja de Vivienda Popular.

8.1 Objetivo 1: Evaluar efectividad de los controles de seguridad de la información ISO 27001:2013 Anexo A.

Prueba: Evaluar el cumplimiento de los catorce (14) dominios del anexo A de la Norma ISO 27001:2013, utilizando la Herramienta EvaluacionMSPI.xlsx del MINTIC mediante técnicas:

- Entrevistas con el o los profesionales de gestión TIC encargados de infraestructura y Profesional de la construcción del MSPI.
- Verificación de los documentos soportes requerido en la solicitud de información inicial.
- Entrevistas con funcionarios y o contratistas de los procesos que componen la CVP.

Luego de realizar la evaluación de efectividad de los controles contemplados en el anexo A de la norma ISO 27001:2013, se obtuvieron los siguientes resultados generales por cada uno de los dominios objeto de revisión:

	Evaluación de Efectividad de controles					
No.	DOMINIO	Calificación Actual	Evaluación Alta Consejeria TIC - Semestre II - 2021	Calificación Objetivo	EVALUACIÓN DE EFECTIVIDAD DE CONTROL ACTUAL	EVALUACIÓN DE EFECTIVIDAD DE CONTROL 2021
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	100	100	100	OPTIMIZADO	OPTIMIZADO
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	81	65	100	OPTIMIZADO	GESTIONADO
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	77	83	100	GESTIONADO	OPTIMIZADO
A.8	GESTIÓN DE ACTIVOS	62	54	100	GESTIONADO	EFECTIVO
A.9	CONTROL DE ACCESO	93	100	100	OPTIMIZADO	OPTIMIZADO
A.10	CRIPTOGRAFÍA	20	0	100	INICIAL	INEXISTENTE
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	59	53	100	EFECTIVO	EFECTIVO
A.12	SEGURIDAD DE LAS OPERACIONES	74	75	100	GESTIONADO	GESTIONADO
A.13	SEGURIDAD DE LAS COMUNICACIONES	78	73	100	GESTIONADO	GESTIONADO
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	93	97	100	OPTIMIZADO	OPTIMIZADO
A.15	RELACIONES CON LOS PROVEEDORES	60	50	100	EFECTIVO	EFECTIVO
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	85	75	100	OPTIMIZADO	GESTIONADO
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	37	64	100	REPETIBLE	GESTIONADO
A.18	CUMPLIMIENTO	79	71	100	GESTIONADO	GESTIONADO
	PROMEDIO EVALUACIÓN DE CONTROLES	**71**	**69**	**100**	GESTIONADO	GESTIONADO

Fuente: Herramienta evaluación MSPI 2022 CVP

A continuación, se detallan los aspectos relevantes en la revisión específica de cada dominio:

8.1.1 Dominio A5 - Política de Seguridad de la Información:

Mediante revisión documental y verificación se evaluó:

- La definición de los objetivos y alcance de la política.
- Si la política está alineada con la estrategia y objetivos de la entidad.
- Si la política está aprobada y socializada al interior de la entidad por la alta dirección.
- Si la política de seguridad de la información se revisa en intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.

Para emitir esta calificación se tuvo en cuenta la actualización de la política de Seguridad de la Información que quedó formalizada mediante resolución 2319 del 25 de noviembre de 2022.

8.1.2 8.1.1 Dominio A6 - Organización de la Seguridad de la Información:

Mediante revisión documental y entrevista se validó:

- Si los roles y responsabilidades frente a la ciberseguridad han sido establecidos.
- Si los roles y responsabilidades de seguridad de la información han sido coordinados y alineados con los roles internos y las terceras partes externas.
- Si son los roles y responsabilidades son claros para la detección de incidentes.

Observación No 1:

No se evidencia el establecimiento de un lineamiento que especifique procedimentalmente como se protege la información almacenada o procesada en dispositivos móviles y el acceso a servicios de TI desde los mismos.

La anterior situación incumple el control A.6.2.1 anexo A de la Norma ISO 27001:2013 *"(…) Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles. (…)*".

Recomendaciones:

El proceso de Tecnologías de la Información y las Comunicaciones:

1. Ajustar y solicitar la inclusión de la política de dispositivos móviles a SGC, según lo acordado en sesión extraordinaria de Comité de Institucional de Gestión y Desempeño desarrollado el 4 de agosto de 2022.

8.1.3 Dominio A7 - Seguridad de los Recursos Humanos:

Mediante el desarrollo de entrevistas y revisión documental se buscó determinar cómo la entidad asegura que los contratistas:

- Estén debidamente informados sobre sus roles y responsabilidades de seguridad de la información, antes, durante y después de que se les otorgue el acceso a información o sistemas de información confidenciales.
- Se les suministran las directrices que establecen las expectativas de seguridad de la información de sus roles dentro de la Entidad.

Fue seleccionada una muestra del 10% de los contratistas con vinculación hasta septiembre del año en curso, el muestreo aplicado fue aleatorio estratificado. Finalmente, la muestra se compuso en la siguiente proporción:

DEPENDENCIA	CONTRATISTAS
DIRECCIÓN DE GESTIÓN CORPORATIVA Y CID	2
DIRECCIÓN DE REASENTAMIENTOS	6
DIRECCIÓN JURÍDICA	1
OFICINA ASESORA DE PLANEACIÓN	1
OFICINA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	1
SUBDIRECCIÓN FINANCIERA	1
TOTAL GENERAL	**12**

Fuente: Elaboración propia

En promedio, el tiempo de vinculación de los contratistas seleccionados fue de 2 años, por lo cual llama la atención que solo el 11% afirma conocer que en la CVP existe una política de Seguridad de la Información y solo el 44% manifiesta haber participado en capacitaciones o formaciones relacionadas con seguridad de la información. A continuación, se detallan los resultados por pregunta:

Pregunta	SI	NO
¿Usted conoce si el la CVP existe una politica de seguridad de la información?	11%	89%
¿Usted sabe donde esta ubicada la politica de seguridad de la información?	33%	67%
¿Usted ha sido informado(a) sobre sus roles y responsabilidades de seguridad de la información, antes de que se les otorgue el acceso a información o sistemas de información confidenciales?	89%	11%
¿Usted ha participado en capacitaciones o formaciones de seguridad de la información en la entidad? ¿Cuales?	44%	56%
¿Usted ha firmado un acuerdo o compromiso de confidencialidad de la información?	22%	78%

Fuente: Elaboración propia

Observación No 2:

No se evidencia en el formato *"Contrato de Prestación de Servicios Profesionales y/o Apoyo a la Gestión 208-Dgc-Ft-82 V6*" el establecimiento de obligaciones generales relacionadas con las responsabilidades de los contratistas frente a la Seguridad de la Información.

La anterior situación incumple el control A.7.1.2 anexo A de la Norma ISO 27001:2013 *"(…) Los acuerdos contractuales con empleados y contratistas, deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información. (…)*".

Recomendaciones:

A los procesos de Adquisición de Bienes y Servicios (Dirección Corporativa) y en conjunto con el Proceso de Tecnologías de la Información y las Comunicaciones:

1. Incluir como responsabilidad General en los contratos de Prestación de Servicios Profesionales la referencia a la política de Seguridad de la Información de la CVP.

2. Todos los contratistas con acceso a información sensible deben firmar acuerdos de confidencialidad o de no divulgación antes de que tengan los permisos para acceder a dicha información.

A la Dirección Corporativa líder del Proceso de Servicio al Ciudadano y como Oficial de Protección de Datos Personales en conjunto con el Proceso de Tecnologías de la Información y las Comunicaciones como Oficial de Seguridad de la Información:

3. Realiza la clasificación de la información sensible, partiendo del instrumento INVENTARIO Y CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN 208-TIC-Ft-21 en su versión más reciente que incluye una columna para identificar si el activo contiene datos personales.

Gestión de Talento Humano (Subdirección Administrativa)

4. Los empleados con acceso a información sensible deben firmar acuerdos de confidencialidad o de no divulgación antes de que tengan los permisos para acceder a dicha información.

Observación No 3:

En revisión del Plan Institucional de Capacitación – PIC de la CVP 2022 no se evidencia la inclusión de temas de capacitación, socialización y/o sensibilización relacionados con Seguridad de la Información.

La anterior situación incumple el control A.7.2.2 anexo A de la Norma ISO 27001:2013 *"(…) Todos los empleados, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo. (…)*".

Recomendaciones:

Al proceso de Tecnologías de la Información y las Comunicaciones y Gestión de Talento Humano (Subdirección Administrativa):

1. Incluir en el PIC el abordaje de conceptos generales de Seguridad de la Información que resalten la importancia del conocimiento y el cumplimiento de las obligaciones aplicables de seguridad de la información contenida en las políticas, normas, contratos etc.

2. Incluir los procedimientos básicos de GTIC además responsabilidad de los funcionarios y contratistas de sus propias acciones u omisiones en la protección de la información.

8.1.4 Dominio A8 – Gestion de Activos:

Mediante revisión documental se verificó el inventario de los activos de información de la CVP para la vigencia 2022 esta identificación la hace cada Proceso de la CVP y es consolidada por GTIC. Se evidencia actualización periódica del inventario en formato 208-Tic-Ft-21 Inventario y Clasificación de Activos de Información V5 de manera consistente desde el año 2018 de manera anual.

Oportunidad de mejora 1:

Para la vigencia 2022 se evidencia el desarrollo de sesiones de socialización para el diligenciamiento del inventario de activos de información. Sin embargo, se considera pertinente que este formato lo acompañe un instructivo para su diligenciamiento.

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones:

1. Generar un instructivo para el diligenciamiento del Inventario y Clasificación de activos de Información el cual especifique cada variable dentro de la matriz, más aun teniendo en cuenta que se incluyó una nueva variable en formato 208-Tic-Ft-21 Inventario y Clasificación de Activos de Información V6.

8.1.5 Dominio A9 – Control de Acceso:

Mediante revisión documental y entrevista se evaluaron:

- La coherencia entre los derechos de acceso y las políticas de clasificación de información de los sistemas y redes.
- La legislación pertinente y cualquier obligación contractual concerniente a la limitación del acceso a datos o servicios.
- La gestión de los derechos de acceso en un entorno distribuido y en red.
- La separación de los roles de control de acceso, (solicitud de acceso, autorización de acceso, administración del acceso).

Observación No 4:

Se observa que la Política de Seguridad de la Información vigente 208-TIC-Mn-07 V2 en el numeral *"10.4. Gestión de la seguridad de las redes"* hace mención general de las consideraciones a tener en cuenta para asegurar la protección de la información en redes y la protección de la infraestructura de soporte. Sin embargo, en la documentación normalizada del proceso GTIC no se evidencia un lineamiento que contenga el detalle procedimental y controles establecidos para mantener la disponibilidad de los servicios de red.

La anterior situación incumple el control A.9.1.2 anexo A de la Norma ISO 27001:2013 *"(…) Se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente. (…)*".

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones:

1. Documentar el detalle procedimental para la gestión de seguridad de las redes, ya sea en la versión propuesta de Manual de Políticas de Seguridad de la Información para aprobación del Comité Institucional de Gestión y Desempeño o en un procedimiento independiente.

8.1.6 Dominio A10 - Criptografía:

Mediante revisión documental y entrevista se evaluó:

- El enfoque de la dirección con relación al uso de controles criptográficos en toda la organización, incluyendo los principios generales bajo los cuales se deben proteger la información de la CVP.
- Si se ha realizado una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido.

Observación No 5:

Se observa que la Política de Seguridad de la Información vigente 208-TIC-Mn-07 V2 en los numerales *"7.10 Desarrollo y Mantenimiento de Software", "10.5.1. Políticas y procedimientos de intercambio de información"* se mencionan aspectos relacionados con la necesidad de implementar controles criptográficos. Sin embargo, en la documentación normalizada del proceso GTIC no se evidencia una valoración de riesgos, que identifique el nivel de protección requerida en los procesos de la CVP.

La anterior situación incumple los siguientes controles:

A.10.1.1 anexo A de la Norma ISO 27001:2013 *"(…) Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. (…)*".

A.10.1.2 anexo A de la Norma ISO 27001:2013 *"(…) Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida. (…)*".

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones:

1. Realizar una valoración de riesgos, que identifique el nivel de protección requerida, teniendo en cuenta el tipo, fortaleza y calidad del algoritmo de encriptación requerido.

2. Elaborar un lineamiento que contenga el detalle procedimental y los controles criptográficos según las necesidades de los procesos en toda la organización.

3. Evaluar la pertinencia de implementar un sistema de gestión de llaves basado en normas, procedimientos y métodos seguros para generación, recuperación, respaldo y eliminación de llaves.

8.1.7 Dominio A11 - Seguridad física y del entorno:

Mediante revisión documental y entrevista se evaluó:

- Si se han definido perímetros de seguridad, y si se usan para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.
- La pertinencia de los controles establecidos para los equipos desatendidos.
- El establecimiento de directrices de escritorio limpio.

Observación No 6:

No se evidencia una identificación integral de perímetros de seguridad física que tenga en cuenta los requisitos de seguridad de los activos dentro del perímetro y la aplicación de una valoración de riesgos.

La anterior situación incumple los siguientes controles:

A.11.1.1 anexo A de la Norma ISO 27001:2013 *"(…) Se debe definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información. (…)*".

A.11.1.2 anexo A de la Norma ISO 27001:2013 *"(…) Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado. (…)*".

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones – Gestión Administrativa:

1. Definir los perímetros de seguridad, y los controles de seguridad física aplicables.
2. Actualizar/revisar lineamientos para el trabajo en áreas seguras.

8.1.8 Dominio A12 - Seguridad de las Operaciones:

Mediante revisión documental y entrevista se evaluó:

- Si se controlan los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
- El seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
- La separación los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
- La ejecución de copias de respaldo de la información, del software e imágenes de los sistemas, y su puesta a prueba regularmente de acuerdo con la política de copias de respaldo aceptada.

Observación No 7:

En revisión de los procedimientos "208-Tic-Pr-07 Administración de Copias de Seguridad y Restauración" Y "208-Tic-Pr-05 Administración de la plataforma de Antivirus V2" se observa que están relacionados con el aseguramiento de la integridad y disponibilidad de los datos y sistemas de información de la CVP. Sin embargo, no se consideran suficientes para afirmar que se realiza un seguimiento riguroso a la demanda de recursos tecnológicos y proyección de los requisitos sobre capacidad futura.

La anterior situación incumple el control A.12.1.3 anexo A de la Norma ISO 27001:2013 *"(…) Para asegurar el desempeño requerido del sistema se debe hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura. (…)*".

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones.

1. Generar un lineamiento para la gestión de la demanda de capacidad tecnológica de la CVP.

Observación No 8:

En revisión de la documentación vigente del SGC del proceso GTIC no se observa una versión vigente del manual de políticas de seguridad de la información que establezca las políticas complementarias y el detalle procedimental para la gestión de la seguridad y privacidad de la información en la Caja de la Vivienda Popular – CVP.

La anterior situación incumple el control A.12.1.1 anexo A de la Norma ISO 27001:2013 *"(…) Los procedimientos deben estar documentados y estar disponibles. (…)".*

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones.

1. Solicitar el control e inclusión de la versión revisada del manual de políticas de seguridad de la información de la CVP.

8.1.9 Dominio A13 - Seguridad de las Comunicaciones:

Mediante revisión documental y entrevista se evaluó:

- La pertinencia de las políticas, procedimientos y controles para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
- La pertinencia de los acuerdos sobre transferencia de información.

Observación No 9:

Se observa que la Política de Seguridad de la Información vigente 208-TIC-Mn-07 V2 en el numeral *"10.5.1. Políticas y procedimientos de intercambio de información"* señala: "(…) *Se establecerán*

procedimientos y controles formales para proteger el intercambio de información a través del uso de elementos de comunicación. (…)". Sin embargo, en revisión de la documentación normalizada del proceso de GTIC no se evidencia algún procedimiento / lineamiento que especifique los controles que aplican en la transferencia de información.

La anterior situación incumple el control A.13.2.1 anexo A de la Norma ISO 27001:2013 *"(…) Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación. (…)*".

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones

1. Generar un procedimiento que tenga en cuenta los controles pertinentes para hacer transferencia segura de información entre la organización y las partes externas.

8.1.10 Dominio A14 - Adquisición, desarrollo y Mantenimiento de Sistemas:

Mediante revisión documental y entrevista se evaluaron:

- La inclusión de elementos de seguridad de la Información en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
- Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se establecen programas de prueba para aceptación y criterios de aceptación relacionados.

Observación No 10:

En revisión de los soportes allegados no se evidencia la inclusión de requisitos de seguridad de la información y de protección de datos personales en el diseño (Lista de verificación de requisitos de Seguridad de la Información) de las etapas que componen el sistema misional de la CVP.

La anterior situación incumple lo establecido en documento normalizado 208-Tic-In-02 Lineamientos Construcción Sistemas de Información CVP V2 *"(…) 5. METODOLOGIA PARA GESTIONAR CICLO DE VIDA DE LOS SISTEMAS DE INFORMACIÓN…. Lista de verificación para la etapa de planeación, diligencia por el arquitecto de software de la CVP o quién haga sus veces. Consultar anexo: Formato Lista de verificación de Seguridad Sistemas de Información (…)*".

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones

1. Generar los artefactos establecidos en la gestión del ciclo de vida de los sistemas de información para el Sistema Misional de la CVP.

8.1.11 Dominio A15 - Relaciones con los Proveedores:

Mediante revisión documental y entrevista se evaluó:

- Seguridad de la información en las relaciones con los proveedores.

Para esta revisión fue seleccionado el proveedor ETB y se analizó el periodo de junio a agosto de la presente vigencia, se aportaron soportes que dan cuenta de un seguimiento de forma consistente una vez por mes, mediante reunión entre el personal de soporte de ETB y el enlace de GTIC con el fin de revisar la gestión de casos y disponibilidad de los servicios contratados. Se recomienda hacer extensivo este seguimiento con los demás proveedores.

8.1.12 Dominio A16 - Gestión de Incidentes de la Seguridad de la Información:

Mediante revisión documental y entrevista se evaluaron:

- Las responsabilidades de gestión, para asegurar que los siguientes procedimientos se desarrollan y comunican adecuadamente dentro de la organización:
- los procedimientos para la planificación y preparación de respuesta a incidentes;
- los procedimientos para seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad de la información.
- los procedimientos para el manejo de evidencia.
- los procedimientos para la valoración y toma de decisiones sobre eventos de seguridad de la información y la valoración de debilidades de seguridad de la información.

En revisión de documento *208-Tic-Pr-13 Gestión de Incidentes de Seguridad de la Información V1* se identifica que contienen los elementos necesarios para el reporte de eventos de seguridad de la información y la destinación de canales de gestión apropiados para el reporte.

Oportunidad de Mejora 2:

En entrevista con el equipo de GTIC se afirma que durante la vigencia 2022 no se han presentado incidentes de seguridad. En este sentido, se recomienda socializar periódicamente a los funcionarios y contratistas el procedimiento para identificación y reporte de incidentes de seguridad.

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones:

1. Solicitar la inclusión en el Plan Institucional de Capacitación conceptos generales y canales para el reporte de incidentes de seguridad de la Información.

8.1.13 Dominio A17- Aspectos de la Seguridad de la Información de la continuidad del negocio:

Mediante revisión documental y entrevista se evaluó:

- BIA (Análisis de Impacto al Negocio)
- BCP (Plan de Continuidad del Negocio)
- DRP (Plan de recuperación de Desastres).

Se observa el establecimiento de un plan de trabajo de 4 meses y se verifico el cumplimiento de las actividades planteadas para el mes de septiembre mediante la revisión de los soportes BIA Táctico: Evaluación de criticidad de procesos y actividades de la entidad, BIA Operativo: Identificación de requerimientos mínimos de operación e Identificación de riesgos de interrupción.

Fuente: Plan de Trabajo BIA – BCP- DRP GTIC 2022

8.1.14 Dominio A18 - Cumplimiento:

Mediante revisión documental y entrevista se evaluó:

- Actualización del normograma GTIC.
- Revisión independiente de la seguridad de la información
- Ejecución de pruebas de seguridad técnicas por o bajo la supervisión de personal autorizado, apoyado en herramientas automáticas o con revisiones manuales realizadas por especialistas.

Oportunidad de Mejora 3:

Se evidencia la ejecución de escaneos automatizados de seguridad a nivel de host y de servicios de red a través de la herramienta NESSUS lo cual constituye un insumo importante para la elaboración de un plan de remediación de las vulnerabilidades detectadas. Sin embargo, se considera pertinente retomar la realización de pruebas de seguridad enfocadas en los sistemas de información por parte de personal especializado.

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones:

1. Realizar pruebas de seguridad por parte de personal especializado priorizando aquellos sistemas de información que son sensibles para la operación de la CVP.

8.2 Objetivo 2: Evaluar el avance de los componentes del modelo de operación SGSI - MSPI (PHVA).

Prueba: Mediante revisión documental y entrevistas con el equipo GTIC, se buscó establecer el nivel de madurez de SGSI de la CVP mediante la valoración de los avances reportados en aspectos técnicos y administrativos para los componentes de planificación, implementación, evaluación de desempeño y mejora continua que hacen parte del ciclo PHVA a continuación, se presentan los resultados por componente:

8.2.1 Planificación:

Mediante revisión documental y entrevista se evaluó:

- Plan de Seguridad y Privacidad de la Información
- Alcance de MSPI
- Roles y responsabilidades
- Tratamiento de riesgos

Observación No 11:

En revisión del documento controlado "208-TIC-Mn-08 - Plan de Seguridad y Privacidad de la Información V3" se observa que las actividades planteadas para cubrir la implementación del MSPI se programaron para ejecutarse durante la vigencia 2021 actualmente se evidencia que el 54% de las actividades y productos se encuentran pendientes o en proceso de ejecución.

La anterior situación incumple lo establecido en la sección 8. Planificación de la Guía de Implementación MSPI V4 *"(…) Determinando los límites y la aplicabilidad del MSPI en el marco del modelo de operación por proceso de la Entidad. Determinando a qué procesos y recursos tecnológicos se realizará la implementación del MSPI. (…)*".

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones.

1. Actualizar el Plan de Seguridad y Privacidad de la Información para la vigencia 2023.

Observación No 12:

En revisión de la documentación del SIG, no se evidencia la definición de alcance del MSPI (Modelo de Seguridad y Privacidad de la Información) donde la CVP identifique las partes interesadas y los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.

La anterior situación incumple los siguientes criterios:

- Punto 7.1.3 Definición del alcance del MSPI de la Guía de Implementación MSPI V4 numeral *"(…) Determinando los límites y la aplicabilidad del MSPI en el marco del modelo de operación por proceso de la Entidad. Determinando a qué procesos y recursos tecnológicos se realizará la implementación del MSPI. (…)*".
- Numeral 4.1 de la Norma ISO 27001:2013 *"(…) Aspectos internos y externos…. La organización debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito. (…)*".
- Numeral 4.2 de la Norma ISO 27001:2013 *"(…) a. Se debe determinar las partes interesadas que son pertinentes al SGSI; b. Se debe determinar los requisitos de las partes interesadas. (…)*".

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones

1. Documentar los límites y la aplicabilidad del MSPI para establecer su alcance teniendo en cuenta los requisitos 4.1 y 4.2 de la Norma ISO 27001:2013.

8.2.2 Implementación:

Mediante revisión documental y entrevista fueron evaluados:

- Control operacional
- Controles establecidos
- Indicadores de gestión MSPI

Observación No 13:

No se evidencia el establecimiento de indicadores de Gestión de Seguridad de la Información que permitan efectuar mediciones precisas de la efectividad y eficiencia del Sistema de Gestión de Seguridad de la Información implementado en la CVP, estos indicadores son insumo importante del componente de mejora continua.

La anterior situación incumple lo establecido en la sección 9. Evaluación del desempeño de la Guía de Implementación MSPI V4 *"(…) Es importante que las Entidades conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo establece el MIPG. (…)*".

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones.

1. Documentar indicadores de Gestión del Modelo de Seguridad y Privacidad de la Información tomando como base la sección "*11.5 Guía Indicadores Gestión de Seguridad de la Información" del documento Guía de Implementación MSPI V4"*.

8.2.3 Evaluación de desempeño:

Mediante revisión documental y entrevista se evaluaron:

- Plan de seguimiento, evaluación y análisis del MSPI
- Auditoría Interna y evaluación del plan de tratamiento de riesgos

Observación No 14:

No se evidencia el establecimiento un plan de seguimiento, evaluación y análisis del Modelo de Seguridad y Privacidad de la Información implementado en la CVP que permita monitorear el avance o rezago en la gestión de la Seguridad de la Información de la entidad.

La anterior situación incumple lo establecido en la sección 9. Evaluación del desempeño de la Guía de Implementación MSPI V4 *"(…) Es importante que las Entidades conozcan de manera permanente los avances en su gestión, los logros de los resultados y metas propuestas, para la implementación del modelo habilitador de la Política de Gobierno Digital. Para tal fin es importante establecer los tiempos, recursos previstos para el monitoreo, desempeño, resultados y aceptación de estos en el comité de gestión institucional y desempeño, como lo establece el MIPG. (…)*".

Recomendaciones:

El proceso de Gestión de Tecnologías de la información y las Comunicaciones.

1. Documentar plan de seguimiento, evaluación y análisis del documento se sugiere tomar como referencia los anexos de la Guía de Implementación MSPI V4.

8.2.4 Mejora continua:

Mediante revisión documental y entrevista se evaluaron:

- Plan de seguimiento y evaluación MSPI y Auditoria interna

Se hizo revisión de los Planes Anuales de Auditoria de las vigencias 2019, 2020, 2021 y 2022 con el objetivo de determinar si la CVP ha realizado seguimiento continuo para optimizar procesos o controles y mejorar el nivel de madurez del MSPI. A continuación, el total de trabajos programados con relación al componente tecnológico:

Fuente: Elaboración Propia

De la anterior gráfica es posible afirmar que la CVP ha triplicado el número promedio de trabajos de auditoria con énfasis en el componente tecnológico a partir de la vigencia 2022.

En revisión especifica del Plan anual de Auditorias para la vigencia 2022 se identifican seis (6) auditorias/seguimientos relacionados con el Componente Tecnológico y que abordan temas transversales a la Implementación del Modelo de Seguridad y Privacidad de la Información. A corte de la presente evaluación se evidencia el cumplimiento del 100% de la auditorias planeadas en este componente.

DENOMINACIÓN DEL TRABAJO	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	ESTADO
Auditoría Evaluación a la Implementación de estándares publicación sede electrónica y web: Resolución 1519 de 2020 Anexo 2,3 y 4		■	■										CUMPLIDA
Seguimiento Cumplimiento Normas de Derechos de Autor			■										CUMPLIDA
Auditoria_Evaluación de Cumplimiento Protección de Datos Personales					■	■	■						CUMPLIDA
Auditoria_Evaluación a la Implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)								■	■	■			CUMPLIDA
Auditoria_Proceso Gestión Tecnología de la Información y las Comunicaciones										■	■		PROGRAMADA
Auditoria_Plan Estratégico de Tecnologías PETI												■	PROGRAMADA

Fuente: Plan Anual de Auditorias 2022

Se considera pertinente realizar auditoria al MSPI dos (2) evaluaciones, en primer y segundo semestre para la vigencia 2023.

8.3 Objetivo 3: *Identificar la línea de base frente a las mejores prácticas en ciberseguridad definidas por el NIST para la CVP.*

Prueba: Mediante revisión documental y entrevistas con el equipo GTIC técnico, se identificaron varias recomendaciones que aportan como línea de base frente a las mejores prácticas en Ciberseguridad (NIST) de acuerdo con las siguientes cinco (5) funciones principales:

8.3.1 Identificar:

Para la función identificar se recomienda documentar:

- Las amenazas internas y externas de ciberseguridad de la CVP.
- Los impactos potenciales en la entidad y su probabilidad, partiendo del análisis BIA y el BCP que se encuentra en desarrollo en la entidad.

8.3.2 Detectar:

En términos generales se evidenció que la red de datos institucional es monitoreada para detectar eventos potenciales de ciberseguridad a partir de la ejecución de herramientas automatizadas de detección de vulnerabilidades como NESSUS. Sin embargo, se recomienda tener en cuenta los siguientes aspectos:

- Correlación de datos de eventos.
- Estimación de impacto de los eventos.
- Definición de umbrales de alerta de los incidentes.

Se sugiere hacer monitoreo del ambiente físico para detectar eventos potenciales de ciberseguridad esta recomendación tiene relación directa con la observación 7 del presente informe.

8.3.3 Responder:

Se sugiere que los planes de respuesta a incidentes estén coordinados con las partes interesadas, ejemplo: Alta Consejería TIC.

Se recomienda integrar en la versión actualizada del procedimiento de Gestión de incidentes de seguridad lo establecido en el *Artículo 9 "Gestión de incidentes de seguridad digital*" de la resolución 500 de MINTIC marzo de 2021.

8.3.4 Recuperar:

Esta función está directamente relacionada con el trabajo que adelanta el proceso GTIC en el desarrollo de los documentos BIA (Análisis de Impacto al Negocio), BCP (Plan de Continuidad del Negocio) y DRP (Plan de recuperación de Desastres) cuya finalización se espera para diciembre del año en curso se recomienda tener en cuenta los siguientes aspectos:

- Incorporar las lecciones aprendidas en los planes de recuperación.
- Definir tiempos de actualización para las estrategias de recuperación.

8.3.5 Proteger:

Se observa que los procesos de protección son continuamente mejorados, a la fecha se encuentra en ejecución oportuna la acción 39 del plan de mejoramiento por procesos GTIC *"Semestralmente el delegado por el Jefe Oficina de Tecnologías de la Información y las Comunicaciones, debe revisar previamente los documentos que sean generados y/o actualizados por los diferentes responsables de los servicios de TI. Se revisará de manera previa todos los documentos que sea generados y/o actualizados por los responsables de los servicios de TI de acuerdo al Nomograma de la Oficina TIC*"

9. **Plan de Mejoramiento:** Producto de la evaluación practicada y resultado del análisis del informe final el proceso de Gestión de Tecnología de la Información y Comunicaciones, Gestión del Talento Humano y Gestión Administrativa definirán las acciones de mejora dirigidas a subsanar y prevenir, las catorce (14) observaciones identificadas, en un plan de mejoramiento que será sujeto de seguimiento por parte de la Asesoría de Control Interno para asegurar su cumplimiento.

10. Criterios de clasificación de conceptos derivados de la auditoría.

Tipo de observación	Descripción
Observación	Incumplimiento de un criterio de auditoria normas, procedimientos internos, resolución que pueden materializar un riesgo.
Oportunidad de mejora	Sin implicar un incumplimiento normativo o de procedimientos internos, es susceptible de mejora el proceso.

11. Firmas

Elaborado:	Revisado	Aprobado
Firmado digitalmente por Javier Alfonso Sarmiento Piñeros DN: C=CO, OU=CVP, O=CVP, CN=Javier Alfonso Sarmiento Piñeros, E=jsarmientop@cajaviviendapopular.gov.co Razón: Soy el autor de este documento Ubicación: Bogotá	RAMIREZ ARDILA DIANA CONSTANZA Firmado digitalmente por RAMIREZ ARDILA DIANA CONSTANZA	RAMIREZ ARDILA DIANA CONSTANZA Firmado digitalmente por RAMIREZ ARDILA DIANA CONSTANZA
Equipo Auditor **Nombre y Cargo:** Javier Alfonso Sarmiento Piñeros Contrato CVP-696-2022	**Auditor Líder** **Nombre y cargo:** Diana Constanza Ramírez Ardila – Asesora de Control Interno	**Nombre y cargo:** Diana Constanza Ramírez Ardila – Asesora de Control Interno
Fecha: 2-12-2022	**Fecha: 6-12-2022**	**Fecha: 6-12-2022**