CORVIVIENDA
HÁBITAT• SOCIEDAD• AMBIENTE

GUÍA DE IMPLEMENTACIÓN

Política Seguridad Digital

2022-2023

Oficina Asesora de Planeación
Gestión Tic

Versión 1

Salvemos Juntos a Cartagena

Tabla de Contenido

Introducción 1

La **GUÍA DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL** es la declaración general que representa la posición de la administración del Fondo de Vivienda de Interés Social y Reforma Urbana Distrital de Cartagena CORVIVIENDA, con respecto a la protección de los activos de información que soportan los procesos de la entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus Políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la Gestión de la Seguridad de la Información.

El artículo 133 de la Ley 1753 de 2015, por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un Nuevo País", integró en un solo Sistema de Gestión los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad, previstos en las Leyes 489 de 1998 y 872 de 2003, respectivamente, los cuales deberán articularse con el Sistema de Control Interno consagrado en la Ley 87 de 1993 y en los artículos 27 al 29 de la Ley 489 de 1998, generando así el Modelo Integrado de Planeación y Gestión MIPG.

En cumplimiento a lo estipulado en el Modelo Integrado de Planeación y Gestión MIPG, el cual es un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos , con integridad y calidad en el servicio, incorpora la **POLÍTICA DE SEGURIDAD DIGITAL** en el marco de la ***3ra. Dimensión: Gestión con Valores para Resultados*** y la implementación de la política se hará a través de la adopción e implementación del ***Modelo de Gestión de Riesgos de Seguridad Digital.***

[1]*Párrafo extraído de Decreto 1499 del 2017*

2 Objetivo de la guía

La presente **GUÍA DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL** busca fortalecer las capacidades institucionales para la Identificación, gestión, tratamiento y mitigación de los riesgos de ***Seguridad Digital*** en las actividades institucionales en el entorno digital, en un marco de cooperación, colaboración y asistencia con los grupos de valor y grupos de interés.

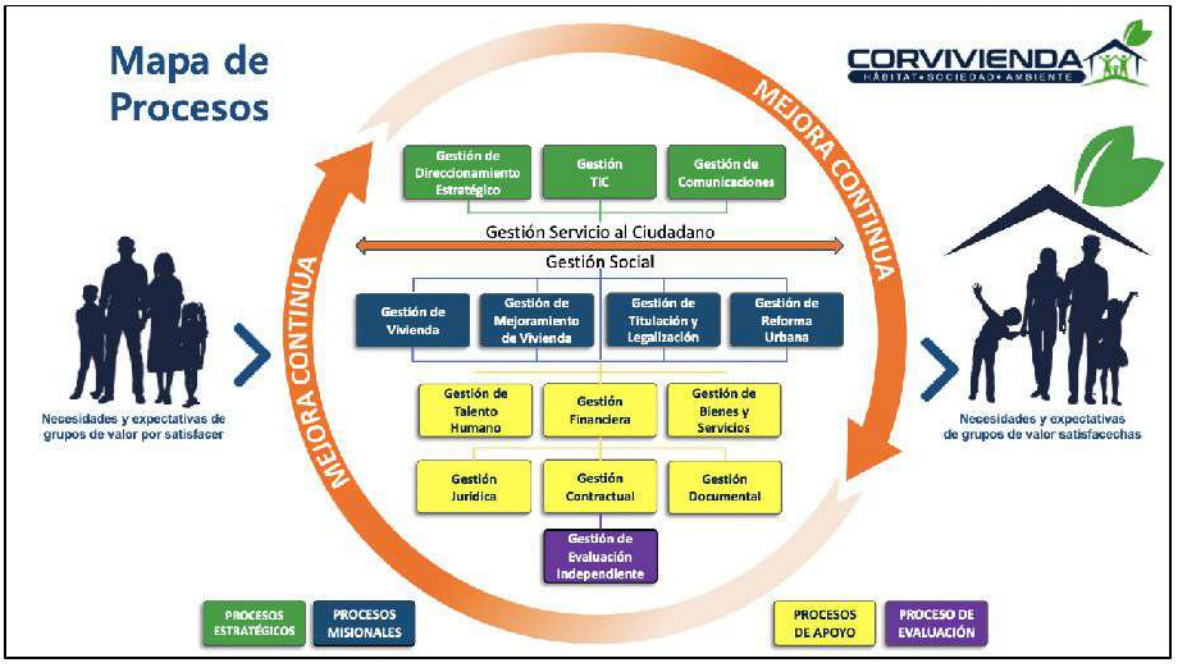
La implementación de la política por parte del Fondo de Vivienda de Interés Social y Reforma Urbana Distrital de Cartagena CORVIVIENDA, se hará a través de la adopción e implementación del ***Modelo de Gestión de Riesgos de la Seguridad Digital.***

La política está liderada a nivel nacional por el Ministerio de Tecnologías de la Información y Comunicaciones y la Secretaria de Transparencia de la Presidencia de la República, y al interior de la entidad por el ***Proceso Estratégico: Gestión TIC*** (Tecnología de la Información y Comunicaciones) de la ***Oficina Asesora de Planeación,*** con el acompañamiento del Comité Institucional de Gestión y Desempeño.

Alcance de la guía 3

Con la expedición del Decreto 1499 de 2017 y el Manual Operativo de MIPG, se debe elaborar e implementar la **POLÍTICA DE SEGURIDAD DIGITAL** en cada una de las entidades públicas, como parte integral de la ***Dimensión: Gestión con Valores para Resultados***, en este sentido, CORVIVIENDA y bajo el liderazgo del ***Proceso de Gestión TIC,*** establece en ella los lineamientos para garantizar la seguridad y la privacidad de la información, a través de la implementación de la presente política, procedimientos e instrumentos de medición que permitan establecer controles en todos los sistemas de información. Cabe anotar que las medidas establecidas requieren del liderazgo de todas las dependencias responsables de la emisión de la información.

Esta **GUÍA DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL,** designó como responsable de la Seguridad Digital y de la Seguridad de la Información en la entidad, al ***Proceso Estratégico Gestión TIC*** de la ***Oficina Asesora de Planeación.***



Teniendo en cuenta lo anterior, se plantean los Roles, Funciones y Responsables de la **Guía de implementación de la Política de Seguridad Digital.**

Dimensión de MIPG	Rol	Función	Responsable
Dimensión 3 Gestión con Valores para Resultados / Seguridad Digital	Líder de la Política de Seguridad Digital.	Emitir los manuales, guías, procedimientos y la metodología de seguimiento y evaluación para la implementación de la Política de Gobierno Digital, en la entidad.	Oficina Asesora de Planeación Líder Proceso Gestión TIC
	Responsable Institucional de la Política Seguridad Digital.	Responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Seguridad Digital. Debe garantizar el desarrollo integral de la política al interior de sus entidades, entendiendo que esta es un eje transversal y apalancador de su gestión interna, que apoya el desarrollo de las políticas de gestión y desempeño institucional.	Oficina Asesora de Planeación Líder Proceso Gestión TICS
Dimensión 6 Gestión del Conocimiento y la Innovación / Gestión del Conocimiento y la Innovación	Responsable de orientar la Implementación de la Política Seguridad Digital.	Orientar la implementación y operación de todas las políticas del Modelo Integrado de Planeación y Gestión -MIPG (entre las que se encuentra seguridad Digital); debe articular todos los esfuerzos institucionales, recursos, metodologías y estrategias para el desarrollo de las políticas del MIPG y en esta medida, lograr que Gobierno Digital se desarrolle articuladamente con las demás políticas en el marco del sistema de gestión de la entidad. Aprobar y verificar del cumplimiento de las políticas y procedimientos de seguridad y privacidad de la información. Hacer que los miembros del Gabinete sean conscientes de la criticidad de los activos de información para el desarrollo de los procesos de la Alcaldía Distrital de Cartagena de Indias. Divulgar las responsabilidades de seguridad y privacidad de la información de la Alcaldía Distrital de Cartagena de Indias con base en los lineamientos del MSPI.	Comité Institucional de Gestión y Desempeño Líder Proceso Gestión TICS
	Otros roles e instancias importantes	Estas instancias deben actuar en coordinación con el Comité Institucional de Gestión y Desempeño para la toma de decisiones. Liderar y apoyar de mejora continua para la aplicación del MSPI al interior de la dependencia a cargo. Alineación de	Nivel Directivo Decretarios, Asesores, Directores y Jefes de Oficina.

Dimensión de MIPG	Rol	Función	Responsable
		los objetivos de la dependencia para que su cumplimiento este apoyado por el MSPI. Asignar y verificar el cumplimiento de las funciones y responsabilidades de seguridad y privacidad de la información para los roles definidos en la dependencia a cargo.	

4 Descripción de la Política

La **GUÍA DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL,** busca fortalecer las capacidades de la entidad para identificar, gestionar y mitigar los riesgos de seguridad digital en las actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia que permita gestionar la confidencialidad e integridad.

Esta política la componen los siguientes elementos direccionadores, que determinan su implementación:

Fuente: Creación propia

Marco conceptual 5

DATOS: Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Entidad.

EJEMPLO: archivo de Word "listado de personal.docx".

IMPACTO: Resultado de un incidente de seguridad de la información.

INCIDENTE: Según [ISO IECTR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INFORMACIÓN: es un activo, esencial para las actividades de una organización.

INSTALACIONES: Son todos los lugares en los que se almacenan o utilizan los sistemas de información.

EJEMPLO: Oficina Pagaduría.

INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

INVENTARIO DE ACTIVOS: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance de la Política de Seguridad Digital, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de julio de 2007.

ISO 19011: Guía de utilidad para el desarrollo de las funciones de auditor interno.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

ISO IECTR 13335-3: Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

ISO IECTR 18044: Guía de utilidad para la gestión de incidentes de seguridad de la información.

ITIL IT INFRASTRUCTURE LIBRARY: Marco de gestión de los servicios de tecnologías de la información.

LEGALIDAD: El principio de legalidad o primacía de la ley, es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

LISTA DE CHEQUEO: apoyo para el auditor con los aspectos a revisar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo.

MEDIDA CORRECTIVA: Medida de tipo reactivo orientada a eliminar, minimizar o mitigar la causa y consecuencias de una no conformidad.

MEDIDA PREVENTIVA: Medida de tipo proactivo orientada a prevenir potenciales no conformidades.

MSPI: Modelo de seguridad y privacidad de la información.

NO REPUDIO: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PERSONAL: Son todos los funcionarios de la Entidad, el personal subcontratado, aprendices, practicantes y peticionarios, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la Entidad.

PLAN DE CONTINUIDAD DEL NEGOCIO (BUSSINES CONTINUITY PLAN): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

PLAN DE TRATAMIENTO DE RIESGOS (RISK TREATMENT PLAN): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

POLÍTICA: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

POLÍTICA DÉ ESCRITORIO DESPEJADO: La política de la empresa que indica a los funcionarios, contratista y demás colaboradores de la Entidad, que deben dejar su escritorio libre de cualquier tipo de información que puede ser usada para perjudicar a la entidad.

POLÍTICA DE SEGURIDAD: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO IEC27002:20005): intención y dirección general expresada formalmente por la Dirección.

PROCEDIMIENTO: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico.

RIESGO: Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

RIESGO RESIDUAL: Según [ISO IEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

SEGREGACIÓN DE TAREAS: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

SEGURIDAD DE LA INFORMACIÓN: Según [ISO IEC27002:2005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

TERCEROS: Toda persona natural o jurídica que tenga una relación directa o indirecta con la Entidad Mayor de Cartagena de Indias. Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de la Entidad, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Entidad y a quienes se les otorga un nombre de usuario y una clave de acceso.

VALORACIÓN DE RIESGOS: Según [ISO IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

VULNERABILIDAD: Según [ISO IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

Marco de referencia 6

CONSTITUCIÓN POLÍTICA DE COLOMBIA 1991. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

LEY 23 1982 Derechos de Autor.

LEY 527 1999 Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

LEY 594 2000 Reglamentada parcialmente por los Decretos Nacionales 4124 de 2004, 1100 de 2014. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones.

LEY 603 2000 Esta ley se refiere a la protección de los derechos de autor en Colombia. El software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

LEY 962 2005 Simplificación y Racionalización de Trámite. Atributos de seguridad en la información electrónica de entidades públicas.

LEY 1150 2007 Seguridad de la información electrónica en contratación en línea.

LEY 1266 2008 Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

LEY 1273 2009 Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado "de la protección de la información y de los datos"-y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

LEY 1341 2009 Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

LEY 1474 2011 Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.

7 Herramientas de Implementación

Para la correcta implementación de l**a GUÍA DE IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD DIGITAL,** el Fondo de Vivienda de Interés Social y Reforma Urbana Distrital de Cartagena CORVIVIENDA tendrá como punto de partida los documentos y herramientas que proporciona el Departamento Administrativo de Función Pública a través de su Página Web:

https://www.funcionpublica.gov.co/web/mipg

https://www.funcionpublica.gov.co/web/mipg/autodiagnostico Gobierno Digital - Gobierno Digital (gobiernoenlinea.gov.co)

https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MGRSD/#:~:text=El%20Modelo%20de%20Gesti%C3%B3n%20de,econ%C3%B3micas%20en%20el%20entorno%20digital%20

https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

8 Implementación de la Política

En la presente matriz se detallan las actividades a desarrollar para la implementación y seguimiento de la **POLÍTICA DE SEGURIDAD DIGITAL.**

ACTIVIDADES PARA LA IMPLEMENTACIÓN DE LA POLÍTICA

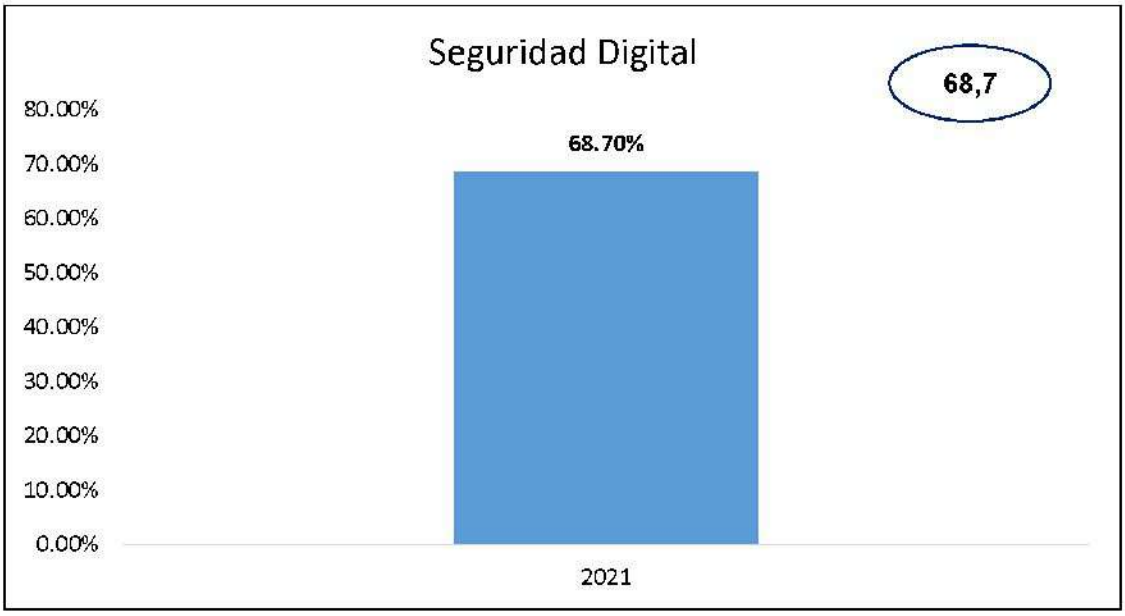
Categorías	Actividad de Gestión	Estrategias por Desarrollar	Producto Esperado	Políticas con la que Interactúa	Responsables	Periodicidad
Modelo de Seguridad y Privacidad de la Información SPI	El Modelo de Seguridad y Privacidad de la Información, busca contribuir al incremento de la transparencia en la Gestión Pública, promoviendo el uso de las mejores prácticas de seguridad de la Información como base de la aplicación del concepto de Seguridad Digital.	Consta de cinco (5) fases: 1. Diagnóstico 2. Planeación 3. Implementación 4. Evaluación de desempeño 5. Mejora continua	Modelo de Seguridad y Privacidad de la Información Plan Estratégico de Seguridad y Privacidad de la Información Etapa de Diagnóstico: Plan de Cierre de Brechas	Gobierno Digital	Gestión TIC	Anual
Plan de Mitigación de Riesgos y Privacidad de la Información	En cumplimiento al decreto 612 del 2018 por el cual se fijan directrices que entre otras incluye la definición de una metodología de gestión del riesgo enfocada a procesos, que le permita identificar, evaluar, tratar y dar seguimiento a los riesgos de seguridad de la información.	Matriz de Riesgos de Seguridad y Privacidad de la Información.	Estructurar el Documento con la metodología para Identificación, clasificación y valoración de activos de información. Elaborar la Matriz con la identificación, valoración y clasificación de activos de información. Elaborar Matriz de Riesgos	Gobierno Digital Transparencia, acceso a la información pública y lucha contra la corrupción	Gestión TIC	Trimestral

Categorías	Actividad de Gestión	Estrategias por Desarrollar	Producto Esperado	Políticas con la que Interactúa	Responsables	Periodicidad
Políticas de Seguridad y Privacidad de la Información	El manual de Política de Seguridad y Privacidad de la información está contenido en un documento de alto nivel que incluye la voluntad de la Alta Dirección de la Entidad para apoyar la implementación del Modelo de Seguridad y Privacidad de la Información.	Elaborar el Documento del diagnóstico y análisis de vulnerabilidades Construir Documento con la Política de Seguridad de la Información. Elaborar el Manual con las políticas y procedimientos de seguridad y privacidad de la información.	Manual de Políticas de Seguridad y Privacidad de la Información Procedimientos de Seguridad y Privacidad de la Información.	Gobierno digital Fortalecimiento Organizacional y Simplificación de Procesos	Gestión TIC	Anual
Política de Seguridad Digital MIPG	Lineamientos generales para la implementación de la Política de acuerdo con los lineamientos del MinTIC.	Elaborar, implementar y realizar seguimiento continuo a la Política de Seguridad Digital.	Guía de implementación de la política y plan de acción de ejecución	Gobierno digital Fortalecimiento Organizacional y Simplificación de Procesos	Gestión TIC	Trimestral

Actividades con Potencial Mejoramiento 9

Los resultados obtenidos en el Formulario Único de Reportes y Avances de Gestión FURAG por la **POLÍTICA DE SEGURIDAD DIGITAL** para la vigencia 2021 fue del **68,7%.**

Los resultados dejan entre ver que es importante generar acciones que fortalezcan la política y a la vez acciones que mantengan los resultados FURAG obtenidos, lo que va a permitir el cierre de brecha en la política.



Con el fin de mejorar el puntaje obtenido en el FURAG-2021, es necesario implementar las actividades de gestión que la misma herramienta FURAG nos sugiere para avanzar y que se deben desarrollar con el fin de lograr el cierre de brecha de la política y el mantenimiento de las actividades que se encuentran en desarrollo.

Categoría	Actividades de Gestión	Producto esperado	Responsables	Fecha de entrega de productos
Plan de Mitigación del Riesgo	Incorporar el análisis del contexto interno y externo de la entidad dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.	Un Capítulo en donde se Incorpore el análisis del contexto interno y externo de la entidad dentro de la política de administración de riesgos establecida por la alta dirección y el comité institucional de coordinación de control interno.	Profesional Universitario	31/12/2022

Categoría	Actividades de Gestión	Producto esperado	Responsables	Fecha de entrega de productos
Plan de Mitigación del Riesgo	Fomentar la promoción de los espacios para capacitar a los líderes de los procesos y sus equipos de trabajo sobre la metodología de gestión del riesgo con el fin de que sea implementada adecuadamente entre los líderes de proceso y sus equipos de trabajo, por parte del comité institucional de coordinación de control interno.	Elaborar una Campaña o capacitación referente a los riesgos de seguridad informática	Profesional Universitario	31/12/2022
Plan de Mitigación del Riesgo	Establecer una periodicidad para la ejecución de los controles, por parte de los líderes de los programas, proyectos, o procesos de la entidad y en coordinación con sus equipos de trabajo, al momento de diseñar los controles.	Un Cronograma para ejecución de los controles	Profesional Universitario	31/12/2022
Plan de Mitigación del Riesgo	Divulgar oportunamente la actualización de los mapas de riesgos de la entidad.	Publicación de mapa de riesgos en el sitio web con fecha de publicación	Profesional Universitario	31/12/2022
Modelo de Seguridad y Privacidad de la Información (MSPI)	Realizar un diagnóstico de seguridad y privacidad de la información para la vigencia, mediante la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI).	Un informe de diagnóstico de seguridad y privacidad de la información para la vigencia, mediante la herramienta de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI).	Profesional Universitario	31/12/2022
Políticas de Seguridad y Privacidad de la Información	Definir y documentar procedimientos de seguridad y privacidad de la información, aprobarlos mediante el comité de gestión y desempeño institucional, implementarlos y actualizarlos mediante un proceso de mejora continua.	un procedimiento de seguridad	Profesional Universitario	31/12/2022

Categoría	Actividades de Gestión	Producto esperado	Responsables	Fecha de entrega de productos
Modelo de Seguridad y Privacidad de la Información (MSPI)	Elaborar el inventario de activos de seguridad y privacidad de la información de la entidad, clasificarlo de acuerdo con los criterios de disponibilidad, integridad y confidencialidad, aprobarlo mediante el comité de gestión y desempeño institucional, implementarlo y actualizarlo mediante un proceso de mejora continua.	Un inventario que contenga las características descritas en la acción de mejora	Profesional Universitario	31/12/2022
Plan de Mitigación del Riesgo	Implementar el plan de tratamiento de riesgos de seguridad de la información.	Plan de tratamiento de riesgos implementado	Profesional Universitario	31/12/2022
Política de Seguridad Digital	Utilizar la información de caracterización de los grupos de valor para definir sus estrategias de servicio al ciudadano, rendición de cuentas, trámites y participación ciudadana en la gestión.	Un informe de caracterización de los grupos de valor	Profesional Universitario	31/12/2022
Plan de Mitigación del Riesgo	Definir el direccionamiento estratégico teniendo en cuenta los lineamientos para la gestión del riesgo (Política de Riesgo).	Establecer el direccionamiento estratégico dentro de la política de seguridad digital	Profesional Universitario	31/12/2022
Plan de Mitigación del Riesgo	Establecer directrices en la planeación institucional tomando en cuenta los resultados de la evaluación de la gestión de riesgos.	Informe de recomendaciones y/o sugerencias	Profesional Universitario	31/12/2022
Plan de Mitigación del Riesgo	Establecer directrices en la planeación institucional tomando en cuenta los resultados de la evaluación de la gestión de riesgos.	Informe de recomendaciones y/o sugerencias	Profesional Universitario	31/12/2022

Categoría	Actividades de Gestión	Producto esperado	Responsables	Fecha de entrega de productos
Plan de Mitigación del Riesgo	Fortalecer las capacidades en seguridad digital de la entidad a través de su participación en las jornadas de socialización y promoción del uso del modelo de gestión de riesgos de seguridad digital convocadas por el Ministerio de Tecnologías de la Información y las Comunicaciones.	Participar al menos en una jornada de capacitación convocada por MinTic	Profesional Universitario	31/12/2022
Política de Seguridad Digital	Fortalecer las capacidades en seguridad digital de la entidad estableciendo convenios o acuerdos con otras entidades en temas relacionados con la defensa y seguridad digital.	Convenio / acuerdo / contrato con entidad en temas de defensa y seguridad digital	Profesional Universitario	31/12/2022
Plan de Mitigación del Riesgo	Adelantar acciones para la gestión sistemática y cíclica del riesgo de seguridad digital en la entidad tales como registrarse en el CSIRT Gobierno y/o ColCERT.	Enlace a sitio web	Profesional Universitario	31/12/2022
Política de Seguridad Digital	Establecer objetivos específicos de seguridad de la información, aprobarlos mediante la alta dirección y medir su nivel de cumplimiento mediante los indicadores definidos para tal fin.	Objetivos Específicos e indicadores	Profesional Universitario	31/12/2022
Política de Seguridad Digital	Establecer roles y responsabilidades específicos de seguridad de la información, aprobarlos mediante la alta dirección, actualizarlos de acuerdo con las necesidades de la entidad y actualizarlos mediante un proceso de mejora continua.	Definición de roles	Profesional Universitario	31/12/2022

Categoría	Actividades de Gestión	Producto esperado	Responsables	Fecha de entrega de productos
Política de Seguridad Digital	Hacer campañas de concientización en temas de seguridad de la información de manera frecuente y periódica, específicas para cada uno de los distintos roles dentro de la entidad.	Campañas de concientización en temas de seguridad de la información de manera frecuente y periódica, específicas para cada uno de los distintos roles dentro de la entidad.	Profesional Universitario	31/12/2022

VERSIÓN	FECHA	DESCRIPCION CAMBIOS DE CONTENIDO
1.0	16/11/2022	Elaboración del documento.

CORVIVIENDA
HÁBITAT • SOCIEDAD • AMBIENTE

FONDO DE VIVIENDA DE INTERES SOCIAL Y REFORMA URBANA DISTRITAL - CORVIVIENDA

Salvemos Juntos a Cartagena

Página web: www.corvivienda.gov.co

Teléfono: 301 479 3336

Redes Sociales: @corviviendacartagena

Dir: Manga 3ª Avenida, Calle 28 #21-62 | **Email:** atencionalusuario@corvivienda.gov.co