ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE VÍCTIMAS DE BOGOTÁ (SIVIC BOG)

JULIÁN EMIR PARRA GARZÓN

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ-CUNDINAMARCA
AGOSTO-2023

ESTADO ACTUAL DE LA SEGURIDAD INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE VÍCTIMAS DE BOGOTÁ (SIVIC BOG)

JULIÁN EMIR PARRA GARZÓN

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Eduard Mantilla Torres
Tutor de Curso

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ-CUNDINAMARCA
AGOSTO-2023

NOTA DE ACEPTACIÓN

Firma del presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá, agosto de 2023

DEDICATORIA

Con todo el amor dedico este trabajo a mi esposa que me ha brindado un apoyo fundamental en todo mi proceso de formación, a mi hijo que con su alegría y motivación me acompaña en cada etapa de mi vida. A mi madre y padre, por siempre acompañarme y ser mi apoyo durante todo este tiempo. Así mismo, agradezco infinitamente a mis Hermanos que con sus palabras me hacen sentir orgulloso de lo que soy.

AGRADECIMIENTOS

Agradezco a la Universidad Nacional Abierta y a Distancia UNAD, que me ha brindado la oportunidad de estudiar y laborar y mostrar los conocimientos aprendidos en la institución también al cuerpo docente que me ha acompañado y evidenciado mi proceso de cambio. Sin el apoyo no hubiese alcanzado mis metas.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

OACDVPR: Oficina Alta Consejería para los Derechos de las Víctimas la Paz y la Reconciliación.

ACTIVO DE INFORMACIÓN: Conocimiento o información que tiene valor para el individuo u organización.

AHI: Ayuda Humanitaria Inmediata.

AMENAZAS: Causa potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

AUTENTICACIÓN: la seguridad informática brinda la posibilidad de validar la identidad y datos a través de la autenticación.

BASES DE DATOS: Colección organizada de información estructurada, o datos, típicamente almacenados electrónicamente en un sistema de computadora.

CIFRADO: método para proteger la información mediante la transformación de los datos en una forma ilegible.

CONFIDENCIALIDAD: Los usuarios autorizados son los que pueden acceder a los datos, recursos e información de un sistema.

DISPONIBILIDAD: Los recursos, datos e información deben estar disponibles para los usuarios cuando los requieran.

FIREWALL: un sistema de seguridad que controla el acceso a una red y protege contra ataques externos.

INTEGRIDAD: Sólo los usuarios autorizados pueden ser capaces de modificar los datos de un sistema.

ISO/IEC 27001: Es la norma principal de la serie y contiene los requisitos del SGSI.

PHISHING: un método para engañar a los usuarios para que revelen información confidencial, como contraseñas o números de tarjetas de crédito.

POLÍTICA DE SEGURIDAD: un conjunto de reglas y procedimientos para garantizar la seguridad de una organización.

SIVIC BOG: Sistema de Información de Víctimas de Bogotá.

SGSI: Sistema de Gestión de seguridad de la información.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Riesgo de Seguridad Digital: Combinación de amenazas y vulnerabilidades en el entorno digital, este riesgo puede afectar de sobremanera la economía nacional, la construcción armónica del territorio o debilitar objetivos económicos y sociales.

VÍCTIMAS: “Todas las personas que individual o colectivamente hayan sufrido daños dentro del marco del Conflicto Armado Interno, a partir del primero de enero de 1985”.

VPN: Red Privada Virtual.

RESUMEN

La oficina alta consejería para los derechos de las víctimas, la paz y la reconciliación la cual hace parte de la secretaría general de la alcaldía Mayor de Bogotá, cuenta con un programa específico para tratar los datos susceptibles de la población víctima del conflicto armado interno colombiano reportados en la ciudad de Bogotá, en este sistema se puede encontrar información personal y familiar, servicios otorgados, encuesta PAS (documento que permite otorgar las ayudas humanitarias inmediatas), direcciones, teléfonos, entre otros datos. Durante la emergencia mundial por el COVID19, la entidad ha tenido que implementar el teletrabajo para los funcionarios, afrontando los riesgos que conlleva la virtualidad, al igual que ha incrementado la seguridad informática para garantizar un uso adecuado de la información manejada por el personal que trabaja en los Centros de Encuentros (Centros de atención a Víctimas del distrito) en la presencialidad y desde sus casas. La confidencialidad y manejo de la informacion está a cargo de los funcionarios del área de sistemas en conjunto con la oficina de las tecnologías de la información y las comunicaciones de la secretaria, asi mismo este equipo estan enfocados en la implementación sistemática y la promoción de estrategias que brinden seguridad de los datos recaudados; el presente documento, pretende realizar una prueba de vulnerabilidades del sistema de víctimas de Bogotá, enseguida realizar un análisis de la criticidad de las vulnerabilidades detectadas para definir posibles mitigaciones.

Palabras Claves: OACDVPR, confidencialidad, disponibilidad, integridad, SIVIC BOG, Vulnerabilidades.

ABSTRACT

The High Counselling Office for Victims' Rights, Peace and Reconciliation, which is part of the General Secretariat of the Mayor's Office of Bogotá, has a specific program to process sensitive data of the victim population of the Colombian internal armed conflict. reported in the city of Bogotá, in this system you can find personal and family information, services provided, PAS survey (document that allows immediate humanitarian aid to be granted), addresses, telephone numbers, among other data. During the global emergency due to COVID19, the entity has had to implement teleworking for officials, facing the risks that virtually entails, as well as increasing computer security to guarantee adequate use of the information handled by working personnel. in the Meeting Centers (Victim Care Centers of the district) in person and from their homes.

The confidentiality and management of information is in charge of the officials of the systems area in conjunction with the information and communications technologies office of the secretary. Likewise, this team is focused on the systematic implementation and promotion of strategies. that provide security of the data collected; This document aims to carry out a vulnerability test of the Bogotá victim system, then carry out an analysis of the criticality of the detected vulnerabilities to define possible mitigations.

Keywords: OACDVPR, confidentiality, availability, integrity, SIVIC BOG, vulnerabilities.

INTRODUCCIÓN

La seguridad informática, comprende un sistema de control manejado por los empleados que utilizan los diferentes recursos de información presentada en datos obtenidos por diferentes fuentes identificando y mitigando posibles vulnerabilidades, riesgos de perdida de la misma, bajo los pilares de confidencialidad, integridad y disponibilidad de la información. Los procedimientos de seguridad que debe implementar al OACDVPR es alta debido al alto flujo de informacion y datos que día a día obtiene, restando las posibilidades de tener perdidas o infiltración de datos susceptibles o privados de las personas atendidas en el centro.[1(*)]

Esta monografía pretende proporcionar una descripción general de la situación de seguridad, realización de una prueba de vulnerabilidades del sistema de información de víctimas de Bogotá, así mismo, dar las recomendaciones para minimizar los impactos que generan los riesgos de seguridad, donde se requiere un análisis, monitoreo, seguimiento y mejoras de los procesos involucrando los activos informáticos, evitando ataques cibernéticos que puedan ocasionar grandes pérdidas de información.

Una vez detectadas las vulnerabilidades en el sistema de información de víctimas de Bogotá – SIVIC BOG, su objetivo es dar recomendaciones para obtener un sistema de información con seguridad robusta a cualquier tipo de ataque, garantizando un modelo de negocio estable, disminuyendo posibles vulnerabilidades bridando herramientas mínimas que ayuden detectar y prevenir posibles ataques, ya que hay elementos y acciones que no son consecuentes con el manejo de la gravedad de la amenaza.

[1(*)] Entendiendo que las vulnerabilidades se presentan en un complejo de situaciones incluyendo las ofimáticas y las malas prácticas con el software y hardware.

Es de suma importancia documentar claramente la identificación, diagnósticos y tratamientos a la variedad de vulnerabilidades y riesgos involucrados en el sistema de información de víctimas de Bogotá, con el propósito de garantizar la seguridad considerada como el activo más importante de esta entidad.

1. DEFINICIÓN DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

Bogotá como muchas otras ciudades principales del territorio colombiano, recibe diariamente población víctima del conflicto armado interno, esto ha hecho que en la ciudad se hayan implementado diferentes sistemas que proporcionen información relevante de las víctimas en el territorio, también debido a lo establecido en la ley de víctimas y restitución de tierras, Ley 1448 de 2011, que estipula que "los municipios receptores deben contar con un sistema amplio de recolección de información de las víctimas para su caracterización, identificación y ubicación para las respectivas ayudas"[2(*)], contemplando que las ayudas no solo dependen de los entes territoriales sino también del estado en general quien debe propender y garantizar las correspondientes ayudas a la población que ha vivido el flagelo de la violencia en Colombia.

El volumen de información es alto, según en datos encontrados en el sistema de "Terridata del Departamento Nacional de Planeación", en un reporte a 2017, Bogotá había recibido 571.537 Víctimas del Conflicto Armado[3]; indicando que las ciudades receptoras deben tener un sistema robusto que guarde los datos de la población Víctima que ingresa y declara, sobra decir que la información es bastante susceptible e importante debido que la población en esta condición puede estar amenazada o en peligro.

En la distribución institucional del distrito: la entidad a cargo de la atención a las Víctimas es la Alta consejería para los derechos de las víctimas, la paz y la

---

[2(*)] Ministerio del Interior y de Justicia, Ley de víctimas 1448 del 10 junio de 2011, Bogotá, Agencia Presidencial para la Acción Social y la Prosperidad Social-ACCIÓN SOCIAL. 2011. P 48.

[3] Departamento Nacional de Planeación. Sitio WEB Colombia. https://terridata.dnp.gov.co/index-app.html#/comparaciones..

reconciliación, encargada de ejecutar la política pública de atención a la población víctima y de dar cumplimiento a lo estipulado por la Ley de Víctimas y restitución de Tierras 1448 de 2011, por tanto, debe, contemplar todos los aspectos que atañen a las ayudas, reparación, retorno entre otras a las víctimas del conflicto.

El mundo, ha pasado por varias pandemias y enfermedades, ejemplo de ellas es pandemia denominada Covid-19 o SARS 2 lo cual después de 2 años, incrementó el cuidado en casa y el distanciamiento social, atendiendo a los cuidados establecidos por la OMS, las instituciones se vieron en la necesidad de implementar estrategias en los equipos; En Bogotá, en algunas entidades distritales se ha implementado el teletrabajo, cuidando a los funcionarios que se encuentran con problemas de salud y propendiendo por el cuidado de la salud individual y de la familia.

Es preocupante el manejo adecuado que se le está dando a la información, el cuidado de la misma por los funcionarios que diariamente acceden a las bases de datos del SIVIC BOG[4(*)], por esto, es importante evidenciar como los funcionarios encargados de la seguridad de la informacion estan blindando y salvaguardando la informacion restando cada vez más, las probabilidades de riego o perdida de la informacion.

[4(*)] Actual sistema de información manejados por la Alta consejería, denominado SIVIC BOG- sistema de información de víctimas de Bogotá-, el cual ha canalizado toda la información referente a las víctimas, su núcleo familiar, ubicación actual, número de ayudas y tipos de ayudas entregadas, encuesta PAS, herramienta que sirve para otorgar o no la ayuda humanitaria inmediata entre otras funcionalidades.

1.2. FORMULACIÓN DEL PROBLEMA

Teniendo en cuenta lo anterior surge el siguiente interrogante:

¿Cómo determinar el estado actual de la seguridad de la información del sistema de información de víctimas de Bogotá (SIVIC BOG), para la prevención de incidentes cibernéticos?

2. JUSTIFICACIÓN

Este trabajo cobra relevancia porque pretende evidenciar cómo se están manejando los datos depositados en el sistema SIVIC BOG y cómo éste resguarda la información susceptible, contemplando el trabajo remoto o desde casa en momentos de pandemia o aislamiento: determinando si esta información es tratada con los requerimientos de integridad, confidencialidad y disponibilidad.

Los datos de la población víctima, son susceptibles no solo por ser información personal como nombres y apellidos, sino también por tratarse de datos de ubicación, que indica contacto de personas víctimas, familias y comunidades. Los datos representan la identidad de los sujetos, caracterización de las familias, contacto de las víctimas, entre otros.

En contexto, El centro Nacional de Memoria Histórica[5] menciona que las víctimas del país son producto de una guerra escalada y perdurable, en un conflicto que lleva más de 60 años y que ha dejado daños irreparables en la población en varios aspectos: psicológicos, sexuales, físicos, comunitarios, sociales etc., como lo documentan varios informes mencionando que: “las víctimas han sido afectadas en la búsqueda constante del restablecimiento de derechos. Personas que han huido de la crisis humanitaria”.

Así, los funcionarios de la alta consejería para los derechos de las víctimas la Paz y la reconciliación – ACDVPR, han sido designados por la entidad para promover la garantía y protección de los derechos de las víctimas en Bogotá.

[5] “Centro Nacional de Memoria histórica. ¡BASTA YA! COLOMBIA: MEMORIAS DE GUERRA Y DIGNIDAD. Bogotá, 2013. P 28-50”.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Evaluar el estado actual de la seguridad de la información del sistema de información de víctimas de Bogotá (SIVIC BOG) y brindar recomendaciones de ciberseguridad para la prevención de incidentes y ataques cibernéticos.

3.2. OBJETIVOS ESPECÍFICOS

- Describir el funcionamiento el sistema de información de víctimas de Bogotá (SIVIC BOG) y las acciones de responsabilidad con el manejo de la información de los funcionarios de atención a las víctimas.

- Elaborar un diagnóstico para la identificación de los riesgos, amenazas y vulnerabilidades en la seguridad de la información ocasionado por errores humanos, físicos o lógicos del sistema SIVIC BOG.

- Proponer recomendaciones de ciberseguridad para la protección y seguridad de la información, enfocadas en la prevención de incidentes y ataques cibernéticos.

4. MARCO REFERENCIAL

4.1. MARCO TEÓRICO

Las Naciones Unidas, tras la segunda guerra Mundial, evidenció que bastantes personas quedaron desprotegidas, abandonadas y sin territorio, en su momento se denominaron: “Refugiados, persona con un fundado temor de ser perseguida a causa de su raza, religión, nacionalidad, pertenencia a un determinado grupo social u opinión política; y que al encontrarse fuera del país de su nacionalidad no puede o no quiere, debido a ese temor, acogerse a la protección de su país”[6] pero en el año 1972 las Naciones unidas ve y entiende la necesidad de aclarar los conceptos que ya no era solo el de refugiado, sino de desplazado externo y desplazado interno: “Los desplazados internos, son: “las personas o grupos de personas que han sido forzadas u obligadas a abandonar sus hogares o lugares de residencia habitual, para evitar los efectos de conflictos armados, situaciones de violencia generalizada, violaciones de derechos humanos o desastres naturales o causados por la acción humana, y que no han cruzado fronteras reconocidas internacionalmente”[7].

Con este término definido, aunque fuese por las entidades internacionales se evidencio que en américa latina había procesos de desplazamiento masivos e individuales, denotando que el problema en común era la disputa del territorio, factores económicos y políticos, y que Colombia era uno de los países con mayor desplazamiento en el continente producto de la disputa del estado y grupos insurgentes y paraestatales[8].

El gobierno colombiano, tras varios reportes de violaciones al derecho internacional humanitario y a los derechos humanos, reconoce que las “víctimas se convertían

[6] RUIZ Nubia. El desplazamiento forzado en Colombia: una revisión histórica y demográfica. México. urbanos vol.26 no.1. 2011.
[7] Ibíd.
[8] Ibíd.

todas en población desplazada” despojadas de sus territorios, aunque los hechos reales que desencadenaron en los actos victimizantes no se podían determinar a menos que se devolvieran los entes judiciales a leer las declaraciones o a solicitar rendir declaración. El impacto de la guerra en los diferentes aspectos de la vida no se podía medir y en consecuencia no se brindaba una adecuada atención y orientación, y las ayudas podían llegar a ser insuficientes o deficientes porque se remitían a dar un soporte económico o de resguardo por un tiempo corto solo para el desplazado y lo demás concerniente al rezago de la guerra, y reforzando la idea de un Estado paternalista.[9]

Tras esta evidencia clara, solo hasta la presidencia de Juan Manuel Santos en el 2011, dijo en Tumaco (Nariño), durante el lanzamiento del Plan Troya, “en Colombia hace rato hay conflicto armado”. Así lo mencionaron varios medios de comunicación[10].

Este paso que dio la política colombiana[11(*)] fue vital para la construcción actual de la ley de víctimas, la cual posibilitó que las personas afectadas por éste conflicto fueran reconocidas como tal, se prestó una atención reparativa y re constitutiva, se establecieron procesos de diálogo y concertación entre víctimas y victimarios, se asumieron compromisos expresos por los entes territoriales receptores, permitió una judicialización especializada para victimarios quienes a través de la narración de las acciones delictivas se comprometieron a diferentes tipos de reparación a las víctimas.

---

[9] Centro de Memoria Histórica, Óp. Cit., p 80.

[10] Anónimo. “¿Qué significa el reconocimiento del conflicto armado por parte del Gobierno? 2011”. sección de política. Bogotá.

[11(*)] Desde la jurisprudencia se trataba el tema del conflicto Interno Armado desde hacía varios años, evidencia de estos son las sentencias de ley que salieron posterior a la ley 387 de 1997 siendo la más representativa la sentencia de ley T-025 de 2004.

Inicia la Alta Consejería para los Derechos de las Víctimas la Paz y la Reconciliación, inscrita a la secretaría General del Distrito. En la cual, actualmente, trabajan personas, motivadas por la consecución de un único fin: la Paz y la reconciliación de un problema que atañe a todos los colombianos; las y los funcionarios pueden acceder al sistema de víctimas SIVIC donde se deposita información relevante de las personas y sus familias, entre otros[12(*)]. Los encargados de este manejo y acceso son el personal del área de las TICs de la ACDVPR.

El SIVIC BOG está en cabeza en la dependencia, pero esto no exime que otras áreas de la ACDVPR requieran información, a diferentes requisitos exigidos por otros entes gubernamentales y también solicitudes expresas de las víctimas, por ejemplo: las y los funcionarios de asistencia y atención, las personas encargadas de brindar atención psicosocial; área de divulgación; área de estrategia; área misional; área de seguimiento y evaluación; área de gestión para la estabilización socioeconómica; observatorio de víctimas; las y los funcionarios del centro de memoria histórica; participación; reparación integral; funcionarios de las demás entidades que hagan articulación con la ACDVPR para brindar atenciones integrales entre otros. Considerando que las medidas tomadas por el departamento de las TICs son funcionales, pero ante la solicitud de la información de tantas instituciones y personas puede llegar a ser insuficiente en términos de seguridad informática.

En un informe realizado en 2015 a la oficina de las TICs, evidenciaron el manejo de un equipo de infraestructura para los contratos con operador que brinda internet, cableado estructurado, licencias, mesas de ayuda para las dependencias de la secretaría general en la alcaldía mayor de Bogotá, administrar servidores de la entidad por medio de máquinas virtuales VmWare, VirtualBox entre otros, o

[12(*)] El sistema SIVIC es creado por la ACDVPR, administrado por la oficina de las TIC de la ACDVPR, a mediados del año 2013.

directamente instalado con sistemas operativos estables como centOS, Ubuntu server, Windows server.

Adicional mencionaba que realizaban backups diarios a sus servidores y bases de datos, backups en cinta mensualmente, monitoreo de red con Nagios, agente de antivirus Trend Micro OfficeScan, reglas de firewall con forticlient, Metasploit y Netposse para pentesting, administración de directorio activo de la entidad, administración de licencias de correo, office y aplicaciones.

En cuanto a la seguridad y privacidad de la información: “se asume con responsabilidad e idoneidad su rol, existe evidencia del desarrollo de actividades necesarias para la identificación y clasificación de los activos de información y la aplicación de controles de confidencialidad, integridad y disponibilidad bajo un entorno de mejora continua en el ciclo PHVA (Planear, Hacer, Verificar, Actuar)” [13(*)]

El teletrabajo que se fortaleció con el momento coyuntural por el que atravesó la sociedad, la pandemia del coronavirus; varias empresas y entidades se sometieron a los cambios pese a no estar preparados adecuaron y lograron que los equipos de trabajo se ajustarán a la nueva realidad; El nuevo panorama trajo consigo preocupaciones acerca de la protección y resguardo de la información, creó pasos para conectarse desde otras redes esperando garantizar las medidas seguras para conectarse desde canales propios como VPN que permitieron el acceso de información, uso del computador institucional y en dado caso el personal, solicitando que el equipo contará con antivirus vigente, debidamente actualizado y sin programas considerados piratas.

[13(*)] Secretaria General, Alcaldía mayor de Bogotá, informe de gestión y resultados 2015, disponible en: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://secretariageneral.gov.co/sites/default/files/documentos_ppi/2022-08/cbn-1090_informe_gestion_y_resultados_2015_0.pdf

Es probable que de no seguir estas recomendaciones se podría adquirir un malware o ataque que se transfiriera e infectara el software de la entidad. Dentro de las políticas de seguridad era importante reconocer los parámetros de seguridad que se implementaron para evitar o minimizar vulnerabilidades.

4.2. MARCO CONCEPTUAL

Alta Consejería para el Derecho de las Víctimas la Paz y la Reconciliación: fue creada en el año 2012, en búsqueda de la atención de las víctimas en la ciudad, está representada en espacios físicos: El Centro de Memoria paz y Reconciliación o los centros de para la Paz y la integración local de víctimas del conflicto armado interno; éstos se crean a raíz de la implementación y ejecución de la ley de víctimas 1448 de 2011. A través de esta entidad se marcó el comienzo del proceso de autorreconocimiento y reconocimiento social del conflicto armado interno en el país y de las personas afectadas directa o indirectamente por este flagelo social. No sobra mencionar que antes ya existían espacios físicos para la atención a la población, pero solo se contemplaba el hecho victimizante del desplazamiento y por tanto la ayuda prestada por el distrito contaba solo con albergue o mercado, para atender coyunturalmente una crisis de carácter estructural.

Seguridad Informática: Es un conjunto de procesos tecnológicos y prácticas que blindan la informacion obtenida a través de datos depositados en los sistemas informáticos, respaldándola y cuidándola de posibles ataques o vulnerabilidades, reduciendo ataques físicos o lógicos a los que pueda estar expuesta.[14]

[14] Baca Urbina, Gabriel. Introducción a la seguridad informática. En: "https://www.google.com.co/books/edition/Introducci%C3%B3n_a_la_seguridad_inform%C3%A1tic/IhUhDgAAQBAJ?hl=es&gbpv=1&dq=que+es+la+seguridad+informatica&printsec=frontcover". Primera edición E-book. 2016.

Seguridad de la información: Son procesos organizados orientados a la aplicación de buenas prácticas y metodologías para cuidar la informacion. Controla el uso de la adecuado de la misma.[15].

ISO/IEC 27001: Norma que contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en el año 2002 y ha sido actualizada. Aunque su aplicación no es obligatoria, si es importante argumentar la no aplicabilidad de la misma[16].

Instrumento de Evaluación MSPI: Esta herramienta identifica el nivel de madurez en la seguridad y Privacidad de la Información, a través de controles técnicos y administrativos al interior de las Entidades Públicas.

Escaneo de vulnerabilidades: Son técnicas y herramientas automatizada para los análisis de los sistemas y servicios, se identifica el uso de manuales que describen las vulnerabilidades de los hosts y atributos de estos, por ejemplo, sistemas operativos, aplicaciones, detección e identificación de redes y puertos abiertos, servicios de red, versiones de software anticuadas, parches faltantes y configuraciones erróneas, entre otros. Además, valida el cumplimiento o las desviaciones de la política de seguridad de una organización, y se comparan con vulnerabilidades existentes recopiladas en las bases de datos de los escáneres de vulnerabilidades. NIST (2008) SP 800-115.

4.3. MARCO HISTÓRICO

[15] Vega Briceño, Edgar. Seguridad de la Información. En: "https://books.google.com.co/books?id=nx4uEAAAQBAJ&printsec=frontcover&dq=que+es+la+seguridad+de+la+informaci%C3%B3n&hl=es&newbks=1&newbks_redir=1&sa=X&ved=2ahUKEwjg4az0qbn-AhW7ZzABHSpOBxgQ6AF6BAgJEAI" Primera edición 3Ciencias. 2021.

[16] ISO27000.es, «ISO 27000.es,». En: "https://www.iso27000.es/iso27000.html"

El conflicto armado colombiano ha sido un flagelo que ha vivido el territorio durante algo más de 60 años, sus comienzos con exactitud son desconocidos pero están asociados directamente a la propiedad privada, el narcotráfico, el microtráfico y la disputa territorial, la pobreza, factores políticos y sociales entre otros a raíz de ello bastante población sobre todo de la periferia colombiana se ha tenido que desplazar despojados y desarraigados de sus tierras a entornos que no siempre fueron y son los más amigables principalmente por lo desconocidos, "Dicho fenómeno se agudizó a principios de la década de 1990, generando un flujo de población que llegó principalmente a las ciudades intermedias, y posteriormente las áreas urbanas han seguido recibiendo corrientes de población procedentes de regiones rurales o semirrurales"[17]. En Colombia el desplazamiento ha perdurado en el tiempo y aunque ha cambiado de actores y se ha recrudecido por periodos, el enfrentamiento y la disputa continúa existiendo y siendo la causal de estos desplazamientos.

Según Nubia Ruiz en su revisión histórica, menciona que la desigualdad en la tenencia de la tierra y en la baja o nula participación política incrementaron los niveles de violencia, "subsidiados en posterioridad por narcotráfico, el narcoterrorismo, la lucha revolucionaria, la guerra fría y contra el terrorismo".

-Los grupos armados han justificado el uso de la violencia al considerarla un método efectivo para cambiar la sociedad, con la intención de que los cambios no sean vistos como ilegales. Así, la ruptura provocada por la desigualdad, el uso de la violencia y la lucha por el poder han caracterizado las dinámicas sociales y políticas en Colombia desde la fundación de la República (siglo XIX) hasta nuestros días. -[18]

[17] RUIZ Nubia. El desplazamiento forzado en Colombia: una revisión histórica y demográfica. Estudios demográficos. En "http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0186-72102011000100141". urbanos vol.26 no.1 México ene./abr. 2011.

[18] Ibíd. Pág. 46

En el siglo XIX se institucionalizó el Partido Conservador y Liberal de Colombia. “El primer sistema se caracterizó por un programa continuo de flujos políticos y sociales destinados a proteger los intereses de los ricos; Mientras el segundo se presentó como una alternativa reformista que protegía los intereses de los comerciantes y grupos sociales menos favorecidos (…)”. “(…) El conflicto entre los dos poderes se manifestó en 54 guerras civiles: 14 entre conservadores contra liberales, 2 entre liberales contra conservadores, 38 entre conservadores y conservadores, y liberales contra liberales. El enfrentamiento final estalló en lo que se conoció como el período de violencia”.[19]

4.4. ANTECEDENTES O ESTADO ACTUAL[20]

Bogotazo

En Colombia a principios de siglo XX, se presentó en Bogotá la muerte de un caudillo lo cual incendio las plazas de mercado y la ciudad de Bogotá en general, la lucha política era el sustrato para una guerra y hechos de violencia desatados en esa época. Jorge Eliecer Gaitán líder político asesinado en 1948, mostro la radicalización a nivel distrital, municipal y nacional ya que este periodo de violencia se extendió por el territorio nacional.

Frente Nacional

[19] Ibíd. Pág. 47
[20] Todo este capítulo fue extraído de: Mediedo. María; Samper José María; Cipriano de Mosquera Tomas. Orígenes de los Partidos Políticos en Colombia. Biblioteca Básica colombiana. 1978, Editorial Andes. Pág. 205 al 238.

Dado este periodo de violencia y con el principal móvil que era el poder y la política en 1956 se firma Tratado de Benidorm, España en que las partes (Conservadores y Liberales) se pusieron de acuerdo para rotarse la gobernanza del país por periodos de tiempo, ante esta situación surgieron movimientos de oposición como: el Movimiento Revolucionario Liberal (MRL), el Movimiento Obrero Independiente Revolucionario (MOIR) y Alianza Nacional Popular (ANAPO).

Este acuerdo tuvo vigencia hasta 1974 y después de ese periodo Colombia tuvo varias reformas que estuvieron presentes hasta el año 1990, como: Reforma Agraria, las nuevas disposiciones que se le otorgaba al ejército y la policía en aras de apaciguar los levantamientos sociales entre otras. También hubo una creciente especulación de precios y una inflación que marco un hito en la historia.

Fuerzas Armadas Revolucionarias de Colombia - Ejército del Pueblo (FARC - Ejército del Pueblo): este grupo armado al margen de la ley se fundó en 1964 en el departamento del Tolima en el municipio de Gaitana, conocido como Marquetalia, las ideas fundacionales eran respaldar al campesino y representarlo distribuyendo en equidad lo que realmente le pertenecía.

Ejército de Liberación Nacional de Colombia (ELN): nace influenciado del movimiento revolucionario cubano bajo el ideal de la lucha de clases y la teología de la liberación en Latino América, una de sus ideales era y es el control político, económico y social (manejo de poderes) a nivel local y
nacional.

Ejército Popular de Liberación Nacional (EPL): nace en 1966 con una fuerte influencia del marxismo y leninismo, pero como fiel expositor de estas dos corrientes ideológicas el modelo político comunista y de extrema izquierda en Colombia.

Movimiento 19 de abril (M-19): Movimiento enfocado en la ruralidad y la democracia basada en los DDHH, se crea en 1974 y es artífice en la construcción de la constitución de 1991.

Paramilitarismo nace de la privatización de la guerra en búsqueda de la protección de campesinos hacendados amenazados o que querían resguardar sus tierras, es un grupo de extrema derecha. Son agentes paraestatales.

Fuerzas de seguridad: Estas son las fuerzas naturales de los gobiernos. Avaladas jurídicamente y legalmente, formadas en pro de la protección de la ciudadanía y de los colombianos. Participa también en los combates contra grupos al margen de la ley.

Narcotráfico "En la década de 1990, Colombia se convirtió en el mayor productor de hoja de coca del planeta" Según Rafael Pardo en su libro (La historia de las guerras). Esto se complejiza con la participación del gobierno y Las FARC-EP en diferentes sectores del país, acrecentando un conflicto armado promovido por la tenencia de la tierra y ahora por los corredores estratégicos para la venta interna y externa de la droga.

Crimen organizado Durante las décadas de 1970 y 1980, los carteles de la droga se concentraron en lagunas ciudades, generando personas que cuidaban intereses particulares y aparecieron nuevos grupos armados más pequeños, que se denominaba criminales organizados y a medida que se extingue uno grupo nace otro siempre al margen de la droga.

4.5. MARCO CIENTÍFICO O TECNOLÓGICO

Como se evidencio en el recorrido histórico hubo y hay variedad de actores participes en los escalonamientos de violencia en Colombia como: partidos políticos, los movimientos insurgentes, fuerzas paramilitares, narcotráfico entre otros, ocasionando grandes catástrofes a la población que se caracteriza principalmente por pertenecer históricamente a poblaciones vulneradas y violentadas, así como a minorías étnicas, raciales, pueblos indígenas etc.

Según el informe "¡Basta ya! Del Centro de Memoria Histórica, publicado en 2013, señala que: entre 1958 y 2012, el conflicto mató a 40.787 combatientes y 177.307 civiles. El número de personas desaparecidas de 1981 a 2010 fue de 25.000, el número de secuestros fue de 27.023 y el número de asesinatos de 150.000. De esta cifra final, el 38,4% fue responsabilidad de los paramilitares, el 16,8% de guerrillas y el 10,1% de Fuerza Pública", asi mismo, "el Anuario Procesos de Paz 2015 de la Escuela de Cultura de Paz destaca: en 40 años de conflicto interno, 39.000 colombianos han sido víctimas de secuestros, con una tasa de impunidad del 92%. El 37% de los secuestros fueron realizados por las FARC-EP y el 30% por el Ejército de Liberación Nacional. El anuario señala que bajo el Programa de Datos de Conflictos de Uppsala (UCDP), hay al menos 1,000 muertes relacionadas con batallas anualmente"[21]. La sociedad civil fuera de las áreas de conflictividad también ha sido afectada por el conflicto armado como éste. Las mujeres, los afrodescendientes y las comunidades indígenas, entre otros, juegan un papel importante en las reivindicaciones cívicas. Desde 1998 (año de creación del Consejo Nacional de Paz), han contribuido al diálogo de paz, atendiendo las peticiones ante todos los actores.

[21] "Centro Nacional de Memoria histórica. ¡BASTA YA! COLOMBIA: MEMORIAS DE GUERRA Y DIGNIDAD". Bogotá, Colombia.2013, pág. 45 -56

4.6. MARCO LEGAL

“Constitución Política de Colombia”	Artículos 12, 13, 15, 20, 21, 22, 23, 44, entre otros. Se destacan a manera de ejemplo Art. 12, en el cual se establece que: “Nadie será sometido a desaparición forzada, a torturas ni a tratos o penas crueles, inhumanos o degradantes”. “el Art. 15, menciona: todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (...)”; en el Art. 20 expone: “Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Estos son libres y tienen responsabilidad social. Se garantiza el derecho a la rectificación en condiciones de equidad. No habrá censura”.
Ley 387 de 1997	Plantea la protección y atención a la población en situación de desplazamiento y dictamina las acciones a aplicar por las instituciones para

	velar, propender y garantizar la estabilidad socioeconómica.
Ley de víctimas 1448 de 2011	"Por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno y se dictan otras disposiciones". Entre ellos Ayudas Humanitarias, Atención y Asistencia, Reparación y Restitución. Art. 3, el cual dispone: "**VÍCTIMAS:** Se consideran víctimas, para los efectos de esta ley, aquellas personas que individual o colectivamente hayan sufrido un daño por hechos ocurridos a partir del 1º de enero de 1985, como consecuencia de infracciones al Derecho Internacional Humanitario o de violaciones graves y manifiestas a las normas internacionales de Derechos Humanos, ocurridas con ocasión del conflicto armado interno." Art. 4, el cual establece "**DIGNIDAD**: El fundamento axiológico de los derechos a la verdad, la justicia y la reparación, es el respeto a la integridad y a la honra de las víctimas. Las víctimas serán tratadas con consideración y respeto, participarán en las decisiones que las afecten, para lo cual contarán con información, asesoría y acompañamiento necesario y obtendrán la tutela efectiva de sus derechos en virtud del mandato constitucional, deber positivo y principio de la dignidad".

Ley 1581 de 2012 de Habeas data	Orienta la protección de datos personales dispuesta en base de datos, autorizada por las personas.
-CONPES 3995-	Política Nacional de Confianza y Seguridad Digital, vinculación a la sociedad colombiana implementando metodologías orientadas al uso de nuevas tecnologías.
-Ley 1273 de 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".
“Decreto 2758 de 2012”	“Por el cual se modifica la estructura del Ministerio de Defensa Nacional y se dictan otras disposiciones. Se le encarga a la Dirección de Seguridad Pública y de Infraestructura, la función de implementar políticas y programas que mantengan la seguridad pública y protejan la infraestructura, diseñar el plan estratégico sectorial en materia de ciberseguridad y ciberdefensa”.
“Decreto 2573 de 2014 Gobierno en Línea”	“Por el cual se establecen los lineamientos generales, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones”
“Decreto 1008 de 2018”	"Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del

	libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"

Tabla 1. Marco Legal

5. DESCRIPCIÓN DEL FUNCIONAMIENTO DEL: “SISTEMA DE INFORMACIÓN DE VÍCTIMAS DE BOGOTÁ” (SIVIC BOG)

El sistema SIVIC BOG se encuentra articulada con el sistema VIVANTO el cual (como muchas otras) es una herramienta informática de la nación que consigna datos susceptibles de la población víctima del país, y allí se encuentran principalmente los números de registros únicos asignados a las familias o individuos tras su declaración y posterior reconocimiento, se procede a las ayudas y servicios que tiene la nación en responsabilidad con ellos. La articulación entre distrito y nación ha permitido que las víctimas puedan acceder de forma más oportuna a los diferentes servicios que se ofrecen en las diferentes entidades distritales.

Este sistema ha logrado mejorar la eficiencia, debido a las soluciones informáticas en el WEB SERVICE entre entidades optimizando los tiempos de atención y respuesta. Esta herramienta cuenta con un módulo de gestión del conocimiento con un prototipo llamado” AVANTI” que integra la visualización, compilación y control de calidad para manejar datos estadísticos relevantes para la población en general, los cuales sirven entre otras para atender problemas estructurales o coyunturales por parte de las entidades; incrementar y potenciar la participación en la construcción de la política pública de víctimas y la interrelaciona entre cada una de las entidades.

La UARIV, cuenta con nodos creados para la atención a las Víctimas, manejan un Web Service dentro del sistema de información de víctimas (SIVIC BOG) para consultar directamente si la persona es víctima, también deben tener participación las entidades públicas del nivel distrital y nacional, por ejemplo: “Uno de estos nodos es el Nodo de vivienda, el cual se orienta a facilitar el flujo de información para el acceso o mejoramiento de vivienda de interés rural o urbana, para población víctima del conflicto, así como a la caracterización, diagnóstico, planeación e

implementación de las acciones que conduzcan al goce efectivo de los derechos de las víctimas. El Distrito se vinculó a este nodo con la participación de la Secretaría Distrital del Hábitat, la Caja de Vivienda Popular y la Alta Consejería para los Derechos de las Víctimas, la Paz y la Reconciliación. De las acciones a desarrollar, se pretende que las víctimas se beneficien con servicios y trámites más eficientes frente al derecho a la vivienda y las entidades pertenecientes puedan tomar mejores decisiones basadas en datos." [22]

En el año 2015 el sistema SIVIC BOG fue ganador del tercer puesto del premio ExcelGEL , premio que otorga el ministerio de las TICs a las entidades públicas que contribuyen al desarrollo del gobierno electrónico del país y promueven el beneficio de los ciudadanos y durante el tiempo de vigencia del este sistema ha sido reconocido por múltiples organizaciones nacionales e internacionales por el beneficio que ha prestado a la población víctima y la promoción de la información para entidades públicas y órganos privados que trabajan con la población víctima, propiciando que la información se encuentre de una forma organizada, rápida y veraz. En esta ocasión también presentaron proyectos de éxito de Europa y América[23].

[22] "Ministerio de vivienda ciudad y territorio MVCT- Plan nacional de construcción y mejoramiento de vivienda social rural-PNVISR", república de Colombia, Bogotá 2021. pág. 92, Disponible en: "chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.minvivienda.gov.co/sites/default/files/2021-08/plan-nacional-de-construccion-y-anexo-a-cronograma.pdf"

[23] Secretaria General, Alcaldía mayor de Bogotá, informe de gestión y resultados 2015, disponible en: "chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://secretariageneral.gov.co/sites/default/files/documentos_ppi/2022-08/cbn-1090_informe_gestion_y_resultados_2015_0.pdf"

5.1. ROLES DE DEL SISTEMA DE INFORMACIÓN DE VÍCTIMAS DE BOGOTÁ (SIVIC-BOG)

En la actualidad el SIVIC BOG cuenta con 10 roles asignados según las necesidades de trabajo y de información que se solicita de parte de la entidad por parte de los funcionarios que trabajan en los centros de encuentro CLAVs, tales como:

Administrador: Este perfil es asignado por el área del observatorio de víctimas junto a los ingenieros de sistemas: ellos son los responsables de la infraestructura y arquitectura tecnológica, gestionan los usuarios, perfiles, roles y permisos, realizan mantenimientos a las bases de datos, backups, actualizaciones, reportes, almacenamiento, planificación y deben estar pendientes de cubrir las necesidades de los usuarios e implementar medidas de seguridad.

Consultas: Este perfil se habilita a los funcionarios de la ACDVPR, ellos pueden visualizar los datos registrada dentro del sistema de información, obteniendo información específica, generar informes y realizar análisis, tales como; identificaciones, núcleo familiar, registro único de víctima, ayudas humanitarias inmediatas entregadas por el distrito, entre otras.

Representación jurídica: Perfil asignado junto al de consultas a los Abogados de la ACDVPR quienes son los encargados de representar a las víctimas para la compensación por daños físicos, emocionales y económicos. Registran en el sistema de información los actos administrativos generados, ayudan a redactar los derechos de petición, acompañamiento a las víctimas para solicitud de servicios de orden nacional y distrital como las ayudas humanitarias inmediatas,

también es asignado a las personas que entregan Ayuda Humanitaria Inmediata (AHÍ).

Asistencia y atención: Perfil asignado junto al de consultas a los funcionarios que brindan atención psicosocial en la entidad, suelen ser profesionales con formación en psicología, trabajo social, enfermería o relacionado con carreras de educación social, ellos registran las atenciones y acompañamientos de los servicios a las víctimas en el sistema de información, identificando las necesidades de las víctimas y abren el abanico para la oferta que ofrece la ACDVPR y el Distrito en general a encontrar recursos y servicios para satisfacer sus necesidades, apoyo emocional a las personas, promoviendo la inclusión y la equidad social.

Entrega AHÍ: Perfil asignado junto al de consultas a los funcionarios encargadas de la entrega de AHI (en este equipo también están las personas que hacen atención psicosocial: ya que ellos en su atención hacen un reconocimiento de necesidades enmarcadas en lo establecido por la ley 1448 de 2011 de acuerdo a lo mencionado en el título III, capítulo III Artículo 63 referente a la Ayuda Humanitaria Inmediata). Recolectar y procesar la información en el sistema sobre la ubicación del cual fueron desplazados, la declaración y magnitud de los hechos victimizantes, necesidades de la población afectada. Verificación de la información de las diferentes bases de datos proveniente de una variedad de fuentes, como agencias gubernamentales, organizaciones no gubernamentales (ONG) y medios de comunicación.

Coordinar la distribución de las ayudas humanitarias a las personas que necesitan ayuda y garantizar que ésta llegue a las personas adecuadas, dejando el registro en el sistema de manera eficiente y efectiva, para poder dar seguimiento y evaluación de las entregas humanitarias, garantizando la recopilación de datos sobre la cantidad de ayuda que se ha entregado, a quién

se ha entregado y si la ayuda está satisfaciendo las necesidades de las personas afectadas.

Coordinador: Este perfil se asigna junto al de consultas a los coordinadores que se encuentran en cada una de las unidades de atención a las víctimas y cada uno de los coordinadores de los equipos internos de la OACDVR. Es responsable de supervisar las entregas de las ayudas humanitarias inmediatas desde el sistema, aprobando y/o desaprobando los bonos entregados por el equipo de trabajo; coadyuva en la implementación de nuevos recursos y servicios, de ayuda humanitaria inmediata, y demás servicios que se entregan en la oficina de atención.

Bonos: El perfil se asigna junto al de consultas, usado por los coordinadores de los equipos y los funcionarios de entrega de AHÍ y Psicosociales (esto debido que dentro de la estrategia de AHÍ se cuenta con ayudas como; albergue, pago de arriendos o Bonos de Emergencia) también este perfil lo usan los ingenieros de sistemas ya que ellos también colocan a disponibilidad los bonos en el sistema cuando se requieren (el procedimiento es el siguiente se destina mensualmente un número determinado de bonos pero hay meses donde los bonos asignados por unidad no son suficientes es el equipo de sistemas el encargado de)y equipo de ingenieros de sistemas para el cargue de bonos que se realiza periódicamente dependiendo de la disponibilidad de presupuesto.

Depuración: Se habilita para los ingenieros de Sistemas de la OACDVPR quienes buscan la precisión de los datos. La depuración es un proceso que se lleva a cabo para identificar errores en los datos de forma manual, y poder corregir los errores realizando una actualización, seguido de una limpieza de bases, este proceso debe estar debidamente documentado para que puedan ser rastreados y resueltos en el futuro.

GESE: Este perfil se asigna junto al de consultas y habilitado para los funcionarios encargados de generar estrategias de estabilización socioeconómica en común acuerdo con las víctimas y evidenciando las necesidades; este equipo se articula con el SENA abordando una variedad de factores como: educación, salud, infraestructura, empleo, protección social etc.

Básico: Este perfil es solo para que puedan consultar datos como nombres, apellidos de las víctimas, este perfil está asignado a todos los funcionarios de la OACDVPR que están en atención y sólo requieren consultas básicas, no tienen permisos para realizar modificaciones.

Participación: Este perfil se asigna junto al de consultas, habilitado para el grupo de funcionarios que trabajan en territorio, realizando acompañamiento a las víctimas, apoyando y asistiendo a las personas que han sufrido un daño contra su integridad, también a los servidores que asisten a las mesas distritales de víctimas.

Estos perfiles están distribuidos en aproximadamente 50 funcionarios que trabajan en los ocho Centros de Encuentro existentes en el distrito:

Figura 1. Tomado de: https://victimasbogota.gov.co/print/166

En revisión de los contratos de las personas que trabaja en la ACDVPR y en atención a la población víctima, no se evidencia mención alguna de los criterios de confidencialidad y manejo de la información lo cual es preocupante por el volumen y confidencialidad de información, los permisos que se generan según los roles y el teletrabajo. Pese a la existencia de unos manuales de usuario para el uso adecuado de la herramienta estas capacitaciones son importantes para el manejo de la confidencialidad, integridad y disposición de los datos registrados en el sistema de información y no se han realizado nuevamente en este año siendo necesarias ya que en la entidad se ha generado niveles alto de rotación del talento humano.

6. IDENTIFICACIÓN DE LOS RIESGOS, AMENAZAS Y VULNERABILIDADES EN EL SISTEMA SIVIC- BOG.

El objetivo principal es dar a conocer las debilidades relativas a la seguridad, señalar que los riesgos, amenazas y vulnerabilidades presentes en la interrelación de sistemas de informacion y los que estan bajo otros componentes de la organización, como son: las personas, los procesos, los procedimientos, las políticas y controles de seguridad. Por ello, al elaborar un análisis de seguridad de la información se debe tener en cuenta los siguientes aspectos:

1). Identificación activos de información, es decir, los datos o sistemas necesarios para las operaciones de la organización.
2). Evaluar los riesgos como: acceso no autorizado, modificación, supresión, robo, etc.
3). Identificación de amenazas como: los ataques informáticos, fugas de información, espionaje industrial, etc.
4). Evaluación de las vulnerabilidades y/o debilidades de seguridad en hardware, software, falta de políticas de seguridad, falta de capacitación del personal, etc.
Así los riesgos identificados deben priorizarse en función de su impacto potencial en la entidad y la probabilidad de que no ocurran, ejecutando acciones necesarias para mitigarlas. Las aplicaciones de dichas medidas están sujetas al nivel de la criticidad real de cada vulnerabilidad.

FACTOR DE RIESGO		
Factor de Riesgo	**Descripción**	**COMBINACIÓN**
Factores Externos	Condiciones que afectan el proceso y son causadas por	Los factores externos son factores que tienen un

	factores externos, fuera del control de la entidad.	impacto directo o indirecto en el proceso, haciéndolos incontrolables.
Infraestructura	Una variedad de posesiones materiales que ayudan en la ejecución de la organización y sus operaciones particulares.	Conjunto de recursos físicos que ayudan a la organización, y específicamente al proceso, a funcionar.
No Aplica	La línea de activos de información y la agrupación de activos de información, como Etapas y Grupos, son indistinguibles.	No Aplica- Si la línea de activos de información está relacionada con la agrupación de activos de información, como Etapas y Grupos.
Personas	Personas físicas involucradas en la ejecución directa o indirecta del proceso.	El personal de la organización involucrado en la ejecución o realización del proceso.
Procesos	Conjunto de acciones y deberes esenciales para la ejecución del proceso.	Interacción de procesos y tareas requeridas para ejecutar el proceso.
Tecnología	Un grupo de dispositivos que pueden influir directa o indirectamente en el proceso.	Instrumentos tecnológicos que interviene de forma directa o indirecta que contribuyen al proceso.

Tabla 2. Factores de Riesgo.

Vulnerabilidad	Descripción
Acceso no autorizado/desbloqueo sin autorización y forzado del documento/archivo	Acceso no permitido/desbloqueo sin autorización o realizado de manera forzada por terceros del documento/archivo a través de herramientas utilitarias y de sistema.
Suplantación de puntos de acceso	Cuando un delincuente cibernético manipula o administra un punto de acceso de ordenadores como anzuelo y confundir a los usuarios con una auténtica red WLAN.
Alta Rotación de personal / Ausencia de la persona a cargo (enlace-gestor a cargo)	Una rotación de personal constante dentro de una empresa, suele tener ausencia operativa para el desarrollo de actividades que apliquen acciones o procedimientos dentro de una Entidad.
Envenenamiento ARP	Es un actor malicioso que envía mensajes de ARP falsificados a una red. Para permitir interceptar, modificar o incluso bloquear el tráfico de una red y sus dispositivos conectados a ella.
Broken Access Control	Puede ocurrir cuando se presenta una falla o ausencia de un mecanismo de control de acceso, permitiendo que un usuario pueda ingresar a uno de los recursos que se encuentren fuera de sus grupos o roles asignados, esto podría dar acceso no autorizado a funcionalidades con privilegios e ingreso datos clasificados de los que generalmente no tenga permisos.

Cross-Site Request Forgery	Se requiere el envío de una solicitud HTTP falsa por parte del navegador de una víctima autenticada, llevándolo al engañado para que use accidentalmente sus credenciales, involucrándolo en una actividad o induciéndolos a que el usuario realice acciones que ellos no tienen intención de llevar a cabo, para alterar el servidor web. Al explotar la vulnerabilidad, el atacante puede manipular las solicitudes que la aplicación reconoce como legítimas.
"Instalaciones por defecto de sistemas y aplicaciones"	Las instalaciones predeterminadas de programa rápidamente y tener todas sus funciones instaladas sin requerir mucho esfuerzo por parte del administrador. La vulnerabilidad de estos scripts y otros ejemplos los hace vulnerables a ataques o recopilación de información por parte del atacante.
Inyección	Datos falsos enviados mediante un jQuery o consulta que pueden provocar fallas de inyección, como las que se encuentran en SQL, OS y LDAP. En el que se puede engañar al intérprete para que utilice los datos hostiles del atacante.
No Aplica	Cuando no existe la aplicabilidad de una vulnerabilidad.
Redirecciones no validadas	Los navegadores web son utilizados frecuentemente para redireccionar a otros tipos de sitios web, sin depender de información confiable cambian la página de destino, con el

	objetivo de que los usuarios caigan en los mensajes de phishing o en unos de sus malwares, para acceder a páginas no autorizadas, sin la validación adecuada.
Referencia Directa Insegura a Objetos	El acto de exponer una referencia interna al centro de implementación, a modo de archivo, directorio o base de datos, da como resultado la definición de objetos "directos". Las referencias se pueden explotar para obtener acceso a datos clasificados, sin ningún control de acceso (Riesgos de seguridad de aplicaciones OWAPS).
Cross-Site Scripting	Una aplicación al recibir información que no es de confianza, la envía de vuelta al navegador web sin la validación y codificación adecuadas, encuentra problemas XSS. Permitiendo a los atacantes ejecutar scripts en el navegador de la víctima, secuestrar sesiones de usuario, destruir sitios web o redirigir a los usuarios a un sitio malicioso (Riesgos de seguridad de aplicaciones OWAPS).
Utilización de componentes con vulnerabilidades conocidas	La mayoría de dispositivos están compuestos de componentes como bibliotecas, marcos, entre otros módulos de software, funcionan con privilegios completos. Un ataque a un componente vulnerable puede provocar una gran pérdida de información y fallas significativas dentro de un servidor. Las aplicaciones que utilizan o incluyen

	componentes con vulnerabilidades conocidas obstruye la protección de la aplicación, aumentando el potencial o la vulnerabilidad en posibles ataques y consecuencias (OWAPS Application Security Risks).
“Vulnerabilidades de los programas (software)”	Las falencias en el código pueden provocar un funcionamiento incorrecto, sin ningún impacto previsto en la integridad o funcionalidad de los datos del usuario.

Tabla 3. Descripción de vulnerabilidades.

Causa / Amenaza	DESCRIPCIÓN
Abuso de privilegios de acceso	Se refiere a los usuarios que hacen uso inadecuado de la red y “abusan” de los privilegios que tienen los perfiles. .
Acceso no Autorizado	El atacante explota los recursos de sistema de identificación sin previa autorización.
Alteración o modificación de la informacion	Manipulación involuntaria/Intención de obtener una ventaja o causar daño/Ingreso sensibilizado de datos inexactos, con la intención de obtener una ventaja o resultar perjudicado. En ocasiones, las modificaciones pueden no ser intencionadas, lo que dificulta la consolidación y presentación de la información.
Ataque de virus sofisticados	Sucede cuando un firewall u otro sistema de antivirus no está respaldado o actualizado para los ataques sofisticados, aunque se consideran sistemas de respaldo no es suficiente, y cada máquina debe contar con su propio software de antivirus.

Ataques en la base datos	El firewall no puede impedir la ejecución de programas a los que se accede a través de protocolos, que a menudo tienen errores.
Ataques internos de seguridad en el perímetro de la organización	Los ataques informáticos y los robos de información son perpetrados con mayor frecuencia por el personal de la organización o intrusos.
Ataques que se pueden dar sin pasar por el cortafuegos	Los colaboradores de la entidad pueden acceder a los ordenadores a través de un módem sin ser bloqueados por los filtros establecidos por el firewall. Estas a menudo se denominan "puerta trasera" porque permiten la entrada a la red sin pasar por el firewall principal.
Ausencia de aplicación documental	Cuando los documentos no cumplen con los tres pilares de la seguridad informática.
Avería de origen físico o lógico	Fallos del programa y/o mal funcionamiento del equipo. Podría deberse a un mal funcionamiento original o a algo que sucede en el sistema.
Agotamiento de recursos y cargas del sistema	Sucede cuando no hay recursos adecuados para sobrellevar cargas de trabajo.
Afectaciones por temperatura y/o humedad	Adaptación del entorno no es óptima, lo que resulta en límites de trabajo de los equipos superiores a la media debido a niveles excesivos de calor, frío y humedad.
Configuración de Seguridad Incorrecta	Para garantizar la seguridad, es necesario tener seguros los equipos y sus funcionalidades como: los marcos, el servidor de aplicaciones, el servidor web, base de datos y la plataforma. Es necesario definir,

	implementar y mantener todas estas configuraciones ya que generalmente no son seguras por defecto. Mantener la última versión de todo el software, incluidas sus bibliotecas de códigos, es parte de este proceso. Esto es importante. Vulnerabilidades de seguridad en aplicaciones OWAPS.'
Contaminación mecánica	La presencia de vibraciones, polvo y suciedad.
Corrupción de la información	Objetos alterados intencionalmente para generar daños o beneficios.
Suspensión del suministro eléctrico	La terminación de la electricidad.
Daño de la información	Ausencia de información, con la intención de obtener algo que hacer a cambio.
Deterioro por agua	Los daños causados por el agua pueden resultar de inundaciones, produciendo agotamiento de recursos del sistémicos.
Deterioro del almacenamiento de informacion por el tiempo	Durante el transcurso del tiempo los elementos de hardware se deterioran.
Desastres industriales	La actividad humana también puede provocar desastres como explosiones o colapsos provocados por productos industriales.
Expansión de malware	Infecciones virales, spyware, troyanos entre otros.
Expansión de software dañino	Difusión no invasiva de virus, spyware entre otros.
Uso indiscreto de información	Sucede cuando se da informacion de parte de un humano o la maquina a personas ajenas a la

	organización y esta es utilizada mal intencionadamente.
Errores de configuración	La digitación de datos incorrectos en la configuración.
Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos de mantenimiento o controles para mejorar el equipo que permitan su uso más allá de su duración designada.
Errores de mantenimiento / actualización de programas (software)	Es cuando fallan las actualizaciones de código y los programas con defectos sean funcionales después de la reparación del fabricante.
Fallos en la monitorización	Documentación defectuosa de las operaciones: documentación inadecuada, errores de documentación incompleta, fechas de registros inexactas, imprecisiones,
Errores de usuarios	Malas conductas cometidas por personas al utilizar servicios, datos u otros métodos.
Errores del administrador	Errores cometidos por los responsables de instalar y operar.
Indagación mal intencionada de usuarios	Usando una computadora o dispositivo desatendido, el tráfico inalámbrico puede ser monitoreado por un invitado (u otra parte), contratista o empleado sin que el usuario objetivo lo sepa.
Error en los servicios de comunicaciones	No permitir la transferencia de datos de un lugar a otro. también puede deberse a la destrucción, la detención o simplemente la incapacidad de atender el tráfico.

Falta de transferencia adecuada y/u oportuna del conocimiento	La ausencia de documentación o descripción de la dinámica interna de trabajo, de los roles y responsabilidades del equipo de trabajo que compone cada proceso relacionado con los temas a cargo y/o designados.
Fuego	Un incendio puede potencialmente consumir recursos del sistema.
Indisponibilidad del personal	Las ausencias no planificadas, los disturbios públicos y las enfermedades pueden provocar indisponibilidad del personal.
Ingeniería social	Abuso de las personas, por realizar actividades para un tercero.
Manipulación de la configuración	La configuración y el cuidado del administrador son esenciales para casi todos los activos, incluidos los privilegios de acceso, los flujos de actividad, el registro y el enrutamiento.
Manipulación de programas	La reelaboración deliberada de los programas, en un esfuerzo por obtener algún beneficio indirecto cuando alguien autoriza a utilizarlos.
Pérdida de Autenticación y Gestión de Sesiones	Las funciones de autenticación y gestión de sesiones en las aplicaciones con frecuencia se implementan incorrectamente, lo que puede poner en riesgo contraseñas, claves, disponibilidad de tokens de sesión u otras fallas de implementación. (Riesgos de seguridad de aplicaciones OWAPS).
Phishing	Un modelo de abuso informático conocido como phishing o robo de identidad implica el uso de técnicas de ingeniería social para obtener

	información confidencial, a menudo contraseñas y otros detalles.
Redirecciones y reenvíos no validados	Enviar datos incorrectos a personas o procesos.
Repudio	Negación posterior de acciones o compromisos asumidos en el pasado. La negación de la originalidad es la negación de que alguien esté enviando o recibiendo un mensaje. Dejar de recibir un mensaje o comunicación a través de recepción implica rechazarlo. Denegar la entrega negándose a recibir un mensaje para entregarlo a otra persona.
Robo	La prestación de servicios deja de estar disponible debido al robo de equipos.
Sesiones de cuentas de secuestro	En las redes inalámbricas, los usuarios pueden intentar iniciar sesión con una conexión HTTPS/SSSL segura para evitar el secuestro de la sesión, lo que puede implicar el envío de cookies o texto sin cifrar que pueden exponer al usuario a posibles vulnerabilidades sin previo aviso.
Identidad Suplantada	Cuando un humano se hace pasar por un usuario legítimo, el perpetrador usa para su propio beneficio los privilegios adquiridos.
Uso indebido de la Información	La información con uso distinto del apropiado de la misma como parte de deberes laborales o derechos sobre un sistema asociado.
Wardriving and warchalking	Localizar puntos de acceso a redes inalámbricas, mientras se conduce por la ciudad y se utiliza un portátil con identificación de redes inalámbricas para

	detectar señales. Una vez que localizan una puerta de enlace a la red inalámbrica elegida, los individuos marcan la ubicación con tiza de identificación e informan a otros intrusos mediante un acto de "warchalking". Esto se conoce como violación o piratería.

Tabla 4. Descripción de Causas o Amenazas.

RIESGOS EN LA SEGURIDAD DIGITAL, SEGURIDAD DE LA INFORMACIÓN Y PRIVACIDAD DE LA INFORMACIÓN		
Riesgos	**Descripción**	**Combinación**
NO APLICA	No se ha encontrado ningún tipo de amenaza o riesgo.	Cuando no se evidencia ningún riesgo que aplique en el sistema.
CIBER ESTRÉS O CIBER FATIGA	Se refiere a efectos dañinos causados por el agotamiento de nuevas o constantes renovaciones en la tecnología que se enfrentan día a día. Estos cambios en tan corto tiempo pueden fatigar y dificultar la adaptación de herramientas digitales, teniendo un impacto negativo.	Esto conlleva a que los usuarios puedan descuidar su ciberseguridad, ya que pueden compartir información que usualmente no comparten.
CIBER PIRÁMIDES	Es un esquema que tiene como propósito es atraer la atención de personas que	Los copartícipes suelen ser víctimas de hurto de identidad o fraude

	refieran unos a otros, teniendo como objetivo de generar beneficios adicionales.	financiero. Los participantes pueden ser llevados a compartir información personal, lo que puede conllevar a transgresiones de la privacidad.
SUPLANTACIÓN DE IDENTIDAD DIGITAL O SPOOFING	Es el acto que una persona suplanta a otra, para llevar a cabo actividades pícaras, que pueden afectar la reputación, o materializando fraudes a través de redes sociales, correo y líneas telefónicas.	Las personas suelen ser víctimas de robo de identidad, compartir la información adicional sin darse cuenta, daños en la reputación personal y fraude financiero.
CARDING	Es el uso ilegítimo de la información financiera, extraída por tarjetas perdidos, robadas, a través de sitios comprometidos de pago, incluso de personal de una tienda que logre tomar los datos, mediante una u otra manera.	los usuarios usualmente pueden ser víctimas de robo de identidad o fraude financiero.
DEEPFAKES	Suelen ser imágenes, videos o audios, puede reemplazar la cara o voz de una persona por otra, a través de inteligencia artificial para crear	Pueden ser víctimas de imágenes, videos, entre otros métodos de falsificación creados, por ejemplo, un actor o personaje que aparezca un

	información falsa o solicitando información con fines de estafas, entre otros tipos de mal uso.	video falso de contenido sexual, con escenas de películas o series, dando información falsa o solicitando información con fines de estafas.
DOXING	Es la abreviación informal DOCS – de documentos, compila información de un objetivo, sea persona u organización, a través de técnicas que incluyen búsquedas en las bases de datos de acceso público, redes sociales, Ingeniería social y vulneración de sistemas y se utiliza para extorsionar a persona natural o jurídica en la Web.	Cualquier persona puede ser víctima de la compilación de información de las bases de datos públicos, redes sociales e ingeniería social y de sistemas vulnerados.
FAKE NEWS O NOTICIAS FALSAS	Las noticias falsas circulan a gran velocidad, a través redes sociales y medios de comunicación como: prensa, radio, televisión y cuyo objetivo es la desinformación, estafar o hacer alguna broma.	Los usuarios suelen caer en noticias falsas, dan información que no deben dar y caen en estafas.

Riesgos de Seguridad de la Información	Descripción	Combinación
RANSOMWARE	El ciberdelincuente tiene la capacidad de bloquear un dispositivo, a través de malware ubicado remotamente, el cual encripta todo el dispositivo, quitándole el control de toda la información y datos almacenados, lanzando una ventana emergente solicitando rescate, generalmente en moneda virtual (bitcoins, por ejemplo).	Cualquier usuario puede ser víctima de un malware, con tan solo un clic.
ATAQUES DE MALWARE	Tiene como objetivo infiltrarse o dañar un sistema de información. Tiene una gran variedad de software hostil, intrusivo y molesto.	Los usuarios por su gran variedad de malware, puede ser víctima y vulnerado sin darse cuenta.
FUGA O PÉRDIDA DE LA INFORMACIÓN	Pérdida de los datos/información al interior de(los) proceso(s) por no generar la información que se solicita/requiera/reporta/entrega en los tiempos	La pérdida de los datos/información al interior de(los) proceso(s) por no generar la información que se solicita/requiera/reporta/entrega en los tiempos

	establecidos a las dependencias definidas	establecidos a las dependencias definidas
DISPONIBILIDAD	La información debe encontrarse siempre a disposición de quienes deban acceder a ella, ya sean personas, procesos o aplicaciones.	La cualidad o condición de la información debe estar a disposición de quienes deban acceder a ella, ya sean personas, procesos o aplicaciones.
Riesgos de Privacidad de la Información	**Descripción**	**Combinación**
FUGA O PÉRDIDA DE LA INFORMACIÓN	Es un suceso en el que la información queda exhibida físicamente o digitalmente, a personas no autorizadas, que puede ser ocasionado por descuidos internos o externos de una empresa, originado por posible malware, spyware o phishing.	Puede ser causado por ciberdelincuentes, brechas de seguridad de una empresa sea por descuidos de un proveedor, un tercero o errores humanos, provocando posibles pérdidas financieras, mala reputación o problemas legales.
INADECUADO TRATAMIENTO DE DATOS PERSONALES	La gestión incorrecta de los datos personales, uso negligente, exposición o perdida de los mismos, suelen ser ignoradas las medidas de seguridad técnicas, administrativas y personales, causando	El uso no adecuado de la información que identifica a las personas, lo que repercute en una violación de los derechos constitucionales. Explosión de información que afecta el

	daños irreparables a la privacidad, dignidad y honor de las personas.	ámbito de la vida personal de un individuo.
INGENIERÍA SOCIAL	Es la práctica para obtener información confidencial a través de la manipulación psicológica de usuarios legítimos, suelen usar los investigadores privados, criminales, o ciberdelincuentes, para obtener información, para obtener acceso o privilegios en un sistema de información, que les permitan realizar algún acto que perjudique o exponga a la persona u organismo comprometido a riesgo o abusos.	La pérdida de privacidad y confidencial a través de la manipulación de usuarios legítimos, permitiendo dar acceso sin darse cuenta, como claves de redes o dispositivos, seguridad de la empresa o personal.
INTERRUPCIÓN EN EL FLUJO DE DATOS	Cuando ocurre la pérdida o interrupción de comunicación, entre los dispositivos y el transporte de información, como fallos o problemas de red, software, hardware o ciberataques de delincuentes.	La interrupción puede ser causado por daños en el servicio de internet, fallas en el servidor, causando pérdidas financieras, productividad o reputación de una empresa.

PÉRDIDA DE LA CONFIDENCIALIDAD	Es sensible la violación o pérdida de la propiedad de la información, su divulgación puede tener un gran impacto en una persona, entidad o proceso no autorizados.	La consecuencia en una empresa puede tener gran impacto legal, información sensible, pérdida de clientes, daños personales, entre otros.
PÉRDIDA DE LA INTEGRIDAD	La información personal comprometida, suelen ser por errores humanos, o ataques dirigidos directo o indirectamente, siendo manipulada, alterada por personas o procesos no autorizados.	Los usuarios suelen ser comprometidos sus datos personales, en un ciberataque dirigido directa o indirectamente a una organización.
PHISHING	Ataque de suplantación de identidad o simplemente suplantador, a través de mensajes de texto, correo, teléfono, usando ingeniería social, caracterizado por intentar adquirir información personal de forma fraudulenta.	Las personas no se dan cuenta en ocasiones que están siendo víctimas de un ciberdelincuente entregando la información personal o de una empresa sin darse cuento trayendo pérdidas financieras y legales.

Tabla 5. Riesgos de seguridad de la informacion y privacidad de la informacion

TIPO DE ACTIVOS	DESCRIPCIÓN

Base de Datos	Los datos personales que contengan nombre y docuemnto se deben tipificar como base de datos.
Claves Criptográficas	Garantiza los mecanismos criptográficos. **Ejemplo:** Claves de Cifrado de canal, certificados digitales, claves de autenticación entre otros.
Datos / Información	Depositados en equipos o servidores que brindan soporte de la informacion guardada en ficheros y posterior transferido por medios de transmisión de informacion **Ejemplos:** Matrices de roles y privilegios, Credenciales (Contraseñas), Copias de Respaldo, Ficheros, Datos de Gestión Interna entre otros.
Hardware / Infraestructura	Medios que soportan los servicios de la entidad, pueden almacenar datos de forma temporal o permanente y soportan la ejecucion de aplicaciones y trasmisión de datos. **Ejemplos:** Módems, Dispositivos Biométricos, Servidores de Impresión, Soporte de la Red (Network), Access Point, entre otros.
Instalaciones	Lugar donde se encuentra el hardware y software y allí se procesa los sistemas de informacion.
Recurso Humano	Personas con los conocimientos y capacidades para pueden desarrollar tareas especificas y son considerados activos de informacion.

Redes de Comunicaciones	Instalaciones de comunicación con servicios de terceros o contratados por la misma organización y son encargados de transportar la informacion. **Ejemplo:** Red Local (LAN), Internet, Radio Comunicaciones, Red Digital (RDSI), entre otros.
Servicios	Funciones que suplen alguna necesidad de la organización o de las personas naturales. **Ejemplo:** Gestión de Privilegios, transferencia de ficheros, intercambio electrónico de datos entre otros.
Software / Aplicaciones Informáticas	Procesan la informacion, posterior de la gestión y análisis, logrando asi la prestación de los servicios. . **Ejemplos:** Servidor de Terminales, Cliente de Correo Electrónico, Desarrollo In House, Sistemas de Gestión de Bases de Datos (dbms) entre otros.
Soportes de Información / Dispositivos móviles	Se refiere a los dispositivos de almacenamiento físicos o no que permiten albergar informacion durante periodos largos. **Ejemplo:** Discos, Discos Virtuales, Almacenamiento en Red (san), Memorias USB, CDROM, DVD, Cinta Magnética (tape), Tarjetas de Memoria, Tarjetas Inteligentes, Material Impreso, Microfilmaciones.

Tabla 6. Tipos de Activos.

IDENTIFICACIÓN DEL ACTIVO					
Id. Activo	**NOMBRE DEL ACTIVO DE INFORMACIÓN**	**DESCRIPCIÓN / FINALIDAD DEL ACTIVO DE INFORMACIÓN**	**MEDIO DE CONSERVACIÓN O SOPORTE**	**RESPONSABLE DE PRODUCCIÓN**	**DESCRIPCIÓN DE LA CLASIFICACIÓN O RESERVA PARCIAL**
DRI-001	Carpeta por Sujeto de Reparación Colectiva	Información correspondiente a la gestión y articulación interinstitucional para la implementación y seguimiento de PIRC.	Documento Digital y/o Documento Físico	OACDVR	N/A
DRI-002	Matriz de Seguimiento y Monitoreo	Información de gestión y seguimiento realizada por las	Documento Electrónico	OACDVR	N/A

	Reparación Colectiva	líneas de Reparación Colectiva en cumplimiento de medidas acordadas con los sujetos.			
OACPVR-003	Folios de Casos de Restitución de Tierras (Casos Activos)	Archivos de los casos de acompañamiento de la OACPVR en el proceso de Restitución de Tierras	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.
OACPVR-004	Matriz de Casos de Restitución de Tierras (Casos Activos)	Base de datos con los casos en procesos de Restitución de Tierras con	Documento Electrónico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.

		acompañamiento de la OACPVR			
OACPVR-005	Folios de Casos de Restitución de Tierras (Casos Inactivos)	Archivos de los casos de acompañamiento de la OACPVR	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.
OACPVR-006	Matriz de Casos de Restitución de Tierras (Casos Inactivos)	Base de datos de casos en procesos de Restitución de Tierra con acompañamiento de la OACPVR	Documento Electrónico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.
OACPVR-007	Carpeta respuestas entes de control y entidades externas	Histórico de respuestas y soportes brindadas y recepcionadas por entes de control.	Documento Electrónico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.

OACPVR-008	Formato único de declaración de solicitud de ingreso al registro único de víctimas SNARIV	Declaración de hechos victimizantes y evidencia del registro en la UARIV	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.
OACPVR-009	Documento de identificación - Víctima	Documento público de identidad del ciudadano que solicita AHÍ.	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.
OACPVR-010	Reporte consulta en el sistema de información Vivanto	Consulta de la vigencia de la declaración ante ministerio público	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.
OACPVR-011	Resolución de entrega de ayuda humanitaria inmediata	Acto administrativo del otorgamiento o negación de los componentes de	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información

		Ayuda Humanitaria Inmediata			
OACPVR-012	Notificación personal	Notificación personal del acto administrativo de entrega de AHÍ.	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.
OACPVR-013	Recurso de reposición	Solicitud para imponer recurso administrativo.	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información
OACPVR-014	Resolución que resuelve el recurso de reposición	Acto administrativo del otorgamiento o negación de AHÍ.	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.
OACPVR-015	Recurso de apelación	Documento posterior al recurso de reposición	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.

OACPVR-016	Resolución que resuelve el recurso de apelación	Acto administrativo l recurso de apelación de AHÍ.	Físico	OACDVR	Se define la clasificación TOTAL y Reserva de la Información.
OACPVR-017	Memorandos Electrónicos	Establecer una comunicación interna	Documento Electrónico	OACDVR	Clasificación parcial los Datos Laborales, serán anónimos.
OACPVR-018	SIVIC	SIVIC.	Documento Electrónico	DRP (Dirección Reparación Integral)	Clasificación parcial los Datos Laborales, serán anónimos.
OACPVR-019	URCUNINA BD	Base de Datos SIVIC	Documento Electrónico	DRP	Clasificación parcial los Datos Laborales, serán anónimos.
OACPVR-020	AVANTI	Sistema que mide el cumplimiento de indicadores y	Documento Electrónico	OACDVR	N/A

		metas de la OACPVR			
OACPVR-021	AVANTI BD	Base de Datos del Sistema para el cumplimiento de indicadores y metas de la OACPVR	Documento Electrónico	OACDVR	N/A
OACPVR-022	Boletines	Documentos que aportan al análisis de la política pública con un enfoque de derechos humanos y procesos de Paz, memoria y reconciliación.	Documento Digital y/o Documento Electrónico	OACDVR	N/A

OACPVR-023	Fichas	Recopila datos cuantitativos sobre las Victimas en el distrito: condiciones de vida y percepciones ciudadanas.	Documento Digital y/o Documento Electrónico	OACDVR	N/A
OACPVR-069	Planilla control de ingreso y salida funcionarios	Contiene el registro de ingreso y salida de los funcionarios administrativos.	Documento Digital y/o Documento Físico	OACDVR	N/A
OACPVR-070	Documentos de Política Pública	Documentos generados por la ACDVPR el PAD y Documento Informe nueve de Abril	Documento Digital y/o Documento Electrónico	OACDVR	N/A

OACPVR-071	Micro sitio Web Observatorio Distrital de Víctimas	Sitio Web que visualiza la información obtenida del centro de Observatorio Distrital de Víctimas.	No es aplicación web y/o APP	Oficina de Alta Consejería de Paz, Víctimas y Reconciliación	No aplica
OACPVR-072	Página Web Víctimas Bogotá	Repositorio donde se evidencian las actividades ejecutadas y proyectadas por la Oficina Alta Consejería de Paz, Víctimas y Reconciliación	No Aplica por ser aplicación web y/o APP	OACDVR	N/A
DPR-028	Actas Consejo Distrital de Paz, Reconciliación	Deposita información sobre reuniones	Documento Electrónico y/o Físico	ACDVPR (Dirección de Paz y	N/A

	Convivencia y Transformación de Conflictos	ordinarias y extraordinarias del Concejo Distrital de Paz, Reconciliación Convivencia y Transformación de Conflictos		Reconciliación) ACDVPR	
DPR-029	Funcionamiento Consejo Distrital de Paz, Reconciliación Convivencia y Transformación de Conflictos	Organización y operación del Consejo Distrital de Paz, Reconciliación Convivencia y Transformación de Conflictos	Documento Electrónico y/o Documento Físico	ACDVPR	N/A
DPR-030	Asistencia Sesiones y reuniones del	Compromisos y mesas de trabajo para organización	Documento Físico	ACDVPR	N/A

	Consejo Distrital de Paz, Reconciliación Convivencia y Transformación de Conflictos	y operación del Consejo Distrital de Paz, Reconciliación Convivencia y Transformación de Conflictos			
DPR-031	“Mesa Intersectorial de implementación del Acuerdo de Paz para Bogotá.”	Actas de reuniones de la “Mesa Intersectorial para la implementación del Acuerdo de Paz para Bogotá”.	Documento Electrónico y/o Documento Físico	ACDVPR	N/A
DPR-032	Reuniones Intersectoriales para la implementación del Acuerdo de Paz para Bogotá.	Organización y operación de la “Mesa Intersectorial para la implementación	Documento Electrónico y/o Documento Físico	ACDVPR	N/A

		del Acuerdo de Paz para Bogotá.”			
DPR-033	Reuniones Mesa Intersectorial para la implementación del Acuerdo de Paz para Bogotá.	Mesas de trabajo para organizar y operar en las “Mesa Intersectorial para la implementación del Acuerdo de Paz para Bogotá.”	Documento Físico	ACDVPR	N/A
DPR-034	Boletín No 1 Dirección de Paz y Reconciliación.	Reflexiones sobre Paz en Bogotá.	Documento Digital y/o Físico	ACDVPR	N/A

DPR-035	Correos electrónicos de la Dirección de Paz y Reconciliación	Se relacionan los correos siguientes correos electrónicos: 1.secretariatecnicaconsejodepaz@alcaldiabogota.gov.co, referente al Consejo Distrital de Paz 2.pdetbr@alcaldiabogota.gov.co Sitio donde se compila información de los programas con enfoque territorial. PDET-BR 3.mesa.intersectorial@alcaldiabogota.	No es aplicación web y/o APP	ACDVPR	N/A

		gov.co Correo electrónico envió y recibo de información sobre la mesa Intersectorial. 4.dirpazreconciliacion@alcaldiabogota.gov.co Correo electrónico en el cual se registra la información digital del equipo de trabajo			
DPR-036	Actas de equipo	Documentos para seguimiento de acciones y exposición de metas y proyectos:	Documento Electrónico y/o Documento Físico	ACDVPR	N/A

		1. Equipo PDET 2. Equipo Reincorporación. 3.Equipo Reconciliación. 4. Equipo Sistema Integral de Paz.			
DPR-037	Asistencia reuniones equipo	Asistencia a las reuniones para seguimiento de lo registrado en el acta de equipo.	Documento Electrónico y/o Documento Físico	ACDVPR	N/A
DRI-038	Carpeta prevención	Carpeta que contiene todas las actas de: 1. mesas técnicas con conceptos.	Documento Electrónico	ACDVPR	N/A

DRI-039	Plan de Contingencia para la Atención y Ayuda Humanitaria Inmediata en Bogotá D.C.	Instrumento técnico apoyado en el Plan de Acción Distrital y este propende por fortalecer la respuesta del ente territorial para atender de manera eficaz y eficiente a la población víctima.	Documento Digital y/o Documento Físico	DRI (Dirección Reparación Integral)	N/A
OACPVR-040	Carpeta digital Actas Subcomités Temáticos	"Información correspondiente al desarrollo de los cinco (5) Subcomités Temáticos: 1. Asistencia y	Documento Digital y/o Documento Físico	OACDVR	N/A

		Atención 2. Reparación Integral 3. Prevención, Protección y Garantías de no Repetición 4. Memoria, Paz y Reconciliación 5. Sistemas de Información"			
OACP VR-041	Carpeta digital Actas CDJT	Actas reuniones ordinarias y extraordinarias del CDJT	Documento físico y/o digital.	OACDVR	N/A
OACP VR-042	“Plan de Acción Distrital (PAD): matriz e informes	“Información correspondiente al Plan de Acción Distrital (PAD):	Documento físico y/o digital.	OACDVR	N/A

	de seguimiento trimestral.”	documentos descriptivos, matrices e informes de seguimiento “			
DRI-043	Correos electrónicos de la DRI	“Correos de la DRI seguimientodri@alcaldiabogota.gov.co: Correo electrónico del equipo de seguimiento a la operación de la Dirección de Reparación Integral psicosocial@alcaldiabogota.gov.co: Correo electrónico	Documento Electrónico	DRI	Datos confidenciales y anonimizados para proteger la información de NNA.

		del equipo psicosocial de la Dirección de Reparación Integral ppgnr@alcaldiabogota.gov.co: Correo electrónico del equipo de prevención y protección".			
DCMPR-97	Página web CMPR	Proponer exponer a la ciudadanía un espacio para conocer las actividades ejecutadas y proyectadas por el equipo del "Centro	No es aplicación web y/o APP	DCMPR (Dirección Centro de Memoria, Paz y Reconciliación)	N/A

		de Memoria, Paz y Reconciliación".			
DCMPR-045	Autorización para la Participación de Niños, Niñas o Adolescentes en Procesos, Eventos o Actividades del "Centro De Memoria, Paz y Reconciliación"	autorizaciones para la participación de los NNA en las actividades del CMPR, (Incluye autorización de uso de imagen)	Documento Físico	DCMPR	N/A
DCMPR-046	Solicitud visitas guiadas Centro de Memoria, Paz y Reconciliación	Formato de Visita guiada a las instalaciones del CMPR	Documento Físico	DCMPR	N/A

DCMPR-047	Permiso de exhibición de piezas en el CMPR.	Formato de autorización para exhibir las piezas en el CMPR.	Documento Físico	DCMPR	N/A
DCMPR-048	“Actas de Donación o Canje de Recursos Bibliográficos”	“Donación o Canje de Recursos Bibliográficos”	Documento Físico	DCMPR	N/A
OACPVR-049	Acta Comité de Autocontrol	Actas del comité de autocontrol	Documento Digital y/o Físico	OACDVR	N/A
OACPVR-050	Oficio	Documento enviado o a y recibido de carácter externo o interno.	Documento Digital y/o Físico	OACDVR	N/A

DRI-051	Herramienta de reconocimiento de garantías a la participación de las víctimas	Datos de asistencia de los 24 delegados y delegadas de las mesas de participación de víctimas y registro de hechos victimizantes.	Base de Datos Automatizada	DRI	Se mantiene la información de forma anónima.
DRI-052	Matriz de caracterización de espacios de participación	Contiene datos sobre la normatividad, composición y funcionamiento de los espacios de participación en la ACDVPR.	Documento Electrónico	DRI	Se mantiene la información de forma anónima por la protección de datos.

DRI-053	“Matriz de incidencia de los espacios de participación”	Contiene las acciones de seguimiento semestral de participación de las victimas teniendo en cuenta las dificultades y logros en los espacios.	Documento Electrónico	DRI	N/A
DR I-054	“Matriz de reconocimiento de garantías a la participación efectiva de las víctimas”	Contiene los datos de los y las delegadas de las mesas de participación.	Documento Electrónico	DRI	N/A
DRI-055	Actas de reunión de las “mesas de	Información de las reuniones de las mesas de enfoque	Documento Electrónico	DRI	N/A

	participación de víctimas”	étnico y diferencial de Mujeres.			
DRI-056	Evidencia de reunión de las mesas de participación de víctimas	Compilado de fotos y actas de las reuniones de las mesas de participación.	Documento Electrónico	DRI	N/A
	Informe de gestión de espacios para la participación	Documento de rendición de cuentas de los espacios para la participación de las víctimas.	Documento Electrónico	DRI	N/A
DRI-057	Asistencia en las mesas de participación de víctimas por parte	Listados de asistencia de los 24 delegados y delegadas de las	Documento Físico	DRI	Se mantiene la información anónima debido a la protección de datos.

	de los y las delegadas.	mesas de participación.			
DCMPR-058	Visitas guiadas y recorridos pedagógicos	Documento de solicitud de visita guiada del CMPR.	Documento Físico	DCMPR	N/A
OACPVR-059	Recurso Humano de la OACPVR.	Servidores OACPVR.	Documento Físico	DCMPR	N/A
DCMPR-060	Recurso Humano de la DCMPR.	Servidores DCMPR.	Documento Físico	DCMPR	N/A
DPR-061	Recurso Humano de la ACDVPR	Servidores ACDVPR	Documento Físico	DCMPR	N/A
DRI-062	Recurso Humano de la DRI	Servidores DRI	Documento Físico	DCMPR	N/A

DCMPR-063	Acta	Documento en el que depositan información sobre las articulaciones y gestiones realizadas.	Documento Físico	DCMPR	N/A
DCMPR-064	Registro de Asistencia	Asistencia a las acciones en articulación o gestión realizadas.	Documento Físico	DCMPR	N/A
DCMPR-065	Evidencias de reunión	Soportes a las acciones de articulación o gestión realizadas.	Documento Físico	DCMPR	N/A
DCMPR-066	Acta préstamo de espacios	Documentos diligenciados por parte de quienes organizan los eventos en el	Documento Físico	DCMPR	N/A

		marco de las acciones planteadas en el plan de trabajo.			
DCMPR-067	Asistencia de los eventos realizados.	Eventos en CMPR–con necesidad de llevar asistencia.	Documento Físico	DCMPR	N/A
DCMPR-068	Encuesta Satisfacción préstamo espacios	Formatos que son diligenciados por los organizadores de eventos en CMPR - como evidencia de la implementación de acciones	Documento Físico	DCMPR	N/A
DCMPR-069	“Encuesta de satisfacción Visitas guiadas”	Documentos diligenciados de forma cuantitativa y	Documento Físico	DCMPR	N/A

		cualitativa para valorar la visita guiada.			
DCMPR-070	“Registro de Asistencia a visitas guiadas”	Documentos diligenciados por los asistentes a las visitas guiadas.	Documento Físico	DCMPR	N/A
DCMPR-071	Solicitud de permiso para el registro fílmico o fotográfico de las actividades.	Documento diligenciado por la persona que solicita el registro fílmico o fotográfico por parte del CMPR.	Documento Físico	DCMPR	N/A
DCMPR-072	“Registro de control interno préstamo de material bibliográfico”	Solicitud de consulta de material bibliográfico del CMPR	Documento Físico	DCMPR	N/A

DCMPR-073	“Consentimiento informado para la recolección de información testimonial”	recolección de información testimonial de las acciones realizadas en el marco de los planes de trabajo del CMPR.	Documento Físico	DCMPR	N/A

Tabla 7. Inventario de Activos de información OACPVR

Valor	CONFIDENCIALIDAD	Valor	INTEGRIDAD	Valor	DISPONIBILIDAD
5. Crítico	La divulgación sin autorización que se ve relacionada en el activo logrando impactar de forma negativa en el SGAMB.	**5. Crítico**	La pérdida de la exhaustividad se refleja negativamente en el SGAMB. poca o nula seguridad de la	**5. Crítico**	No hay disponibilidad del activo reflejándose negativamente el SGAMB.

	El impacto es considerable dañando la reputación de la entidad.		información perjudicando la toma de decisiones genera eventos que propenden al error ocasionando pérdidas importantes de información.		Gasto de tiempo 5 días aproximadamente para recuperar la información perdida / Disponible al menos el 99% del Tiempo.
4. Alto	La divulgación sin autorización que se ve relacionada en el activo logrando impactar en varios procesos de forma negativa en el SGAMB. El tratamiento de la	**4. Alto**	La pérdida de la exhaustividad se refleja en varios procesos en el SGAMB. Perdida considerable de	**4. Alto**	Poca disponibilidad del activo, reflejado negativamente en el SGAMB en uno o varios procesos. Gasto de aproximadamente 1

	información de forma desconsiderada y sin autorización puede arriesgar la información y a la entidad / puede afectar otras dependencias, procesos o activos de información.		información y toma retrasada de decisiones estratégicas, riesgos de seguridad, bajos niveles de protección.		día en recuperar la información/ Disponible al menos el 70% del Tiempo.
3. Medio	La divulgación no autorizada es reflejada de forma negativa pero leve al proceso. Se podría afectar el resultado al no estar autorizado para acceder a la información, y aunque ya fue procesada aún puede interferir en la toma de	**3. Medio**	La inexactitud de la información impacta levemente el proceso. impacta en decisiones pequeñas del proceso. se podrían ocasionar	**3. Medio**	La no disponibilidad del activo puede perjudicar el proceso. la recuperación de información es menor a 1 semana / Disponible al menos el 30% del tiempo.

	decisiones poniendo en riesgo el proceso/ podría aplicar a otros procesos o activos de información.		perdidas de información		
2. Bajo	La divulgación no permitida de información impacta de forma baja el proceso. Se podría afectar el resultado al no estar autorizado para acceder a la información, y aunque ya fue procesada aún puede interferir en la toma de decisiones poniendo en riesgo el proceso / podría continuar afectando otros procesos.	**2. Bajo**	La inexactitud de la información impacta de forma baja el proceso. aún hay perdida de información lo cual puede perjudicar procesos menores.	**2. Bajo**	La no disponibilidad del activo impacta de forma baja en el proceso. Para recuperar la información no se debe superar la semana y se debe volver a procesar la información del activo / Disponible al menos el 30% del tiempo.

1. Mínimo	La divulgación no permitida de información impacta de mínimamente el proceso. Al acceder sin las autorizaciones correspondientes el riesgo es mínimo y no afectaría el proceso/ El riego no afectara otros procesos.	**1. Mínimo**	La inexactitud de la información afectara de forma mínima el proceso. La información perdida no representa pérdida significativa y se puede fácilmente reconstruir o recuperar.	**1. Mínimo**	La no disponibilidad del activo y mínima en el proceso. Para recuperar o reconstruir la información no se debe superar la semana y se debe volver a procesar la información del activo / Disponible al menos el 30% del tiempo.

Tabla 8. Valores de Confidencialidad, Integridad y Disponibilidad en los Activos de Información

CLASIFICACIÓN DEL ACTIVO					
Id. Activo	**CONFIDENCIALIDAD** **1. Mínimo** **2. Bajo** **3. Medio** **4. Alto** **5. Critico**	**INTEGRIDAD** **1.Mínimo** **2.Bajo** **3.Medio** **4.Alto** **5.Critico**	**DISPONIBILIDAD** **1. Mínimo** **2. Bajo** **3. Medio** **4. Alto** **5. Critico**	**VALOR TOTAL DEL ACTIVO:** **A:** Alto **C:** Critico **M:** Medio **B:** Bajo	**CLASIFICACIÓN DE LA INFORMACIÓN:** **IPC:** Información Publica Clasificada **IPR:** Información Publica Reservada **IP:** Información Publica
DRI-001	**3**	**4**	**3**	**M**	**IPC**
DRI-002	**3**	**4**	**3**	**M**	**IPC**
OACPV R-003	**5**	**3**	**3**	**A**	**IPR**
OACPV R-004	**5**	**3**	**3**	**A**	**IPR**

OACPV R-005	**5**	**3**	**3**	**A**	**IPR**
OACPV R-006	**5**	**3**	**3**	**A**	**IPR**
OACPV R-007	**2**	**2**	**2**	**M**	**IPC**
OACPV R-008	**5**	**3**	**3**	**A**	**IPR**
OACPV R-009	**3**	**3**	**3**	**M**	**IPC**
OACPV R-010	**5**	**3**	**3**	**A**	**IPR**
OACPV R-011	**5**	**3**	**3**	**A**	**IPR**
OACPV R-012	**5**	**3**	**3**	**A**	**IPR**
OACPV R-013	**5**	**3**	**3**	**A**	**IPR**
OACPV R-014	**5**	**3**	**3**	**A**	**IPR**

OACPV R-015	**5**	**3**	**3**	**A**	**IPR**
OACPV R-016	**5**	**3**	**3**	**A**	**IPR**
OACPV R-017	**3**	**2**	**2**	**M**	**IPC**
OACPV R-018	**3**	**4**	**4**	**A**	**IPR**
OACPV R-019	**3**	**4**	**4**	**A**	**IPR**
OACPV R-020	**3**	**4**	**3**	**M**	**IPC**
OACPV R-021	**3**	**4**	**3**	**M**	**IPC**
OACPV R-022	**3**	**2**	**3**	**M**	**IPC**
OACPV R-023	**3**	**2**	**3**	**M**	**IPC**
OACPV R-069	**1**	**2**	**3**	**M**	**IPC**

OACPVR-070	**2**	**2**	**3**	**M**	**IPC**
OACPVR-071	**2**	**2**	**3**	**M**	**IPC**
OACPVR-072	**2**	**2**	**3**	**M**	**IPC**
DPR-028	**3**	**3**	**3**	**M**	**IPC**
DPR-029	**2**	**2**	**2**	**M**	**IPC**
DPR-030	**1**	**1**	**1**	**B**	**IP**
DPR-031	**3**	**3**	**3**	**M**	**IPC**
DPR-032	**2**	**3**	**2**	**M**	**IPC**
DPR-033	**1**	**1**	**1**	**B**	**IP**
DPR-034	**3**	**2**	**3**	**M**	**IPC**

DPR-035	**3**	**3**	**3**	**M**	**IPC**
DPR-036	**1**	**3**	**2**	**M**	**IPC**
DPR-037	**1**	**1**	**1**	**B**	**IP**
DRI-038	**3**	**2**	**2**	**M**	**IPC**
DRI-039	**1**	**1**	**2**	**B**	**IPC**
OACPVR-040	**3**	**3**	**3**	**M**	**IPC**
OACPVR-041	**3**	**3**	**4**	**M**	**IPC**
OACPVR-042	**1**	**4**	**4**	**M**	**IPC**
DRI-043	**3**	**3**	**3**	**M**	**IPC**
DCMPR-97	**1**	**1**	**3**	**M**	**IPC**
DCMPR-045	**4**	**2**	**3**	**M**	**IPC**

DCMPR-046	**3**	**2**	**3**	**M**	**IPC**
DCMPR-047	**3**	**2**	**3**	**M**	**IPC**
DCMPR-048	**1**	**2**	**3**	**M**	**IPC**
OACPVR-049	**3**	**3**	**3**	**M**	**IPC**
OACPVR-050	**1**	**2**	**2**	**M**	**IPC**
DRI-051	**5**	**4**	**4**	**A**	**IPC**
DRI-052	**4**	**3**	**3**	**M**	**IPC**
DRI-053	**2**	**3**	**2**	**M**	**IPC**
DRI-054	**5**	**4**	**4**	**A**	**IPR**
DRI-055	**3**	**3**	**3**	**M**	**IPC**
DRI-056	**3**	**3**	**3**	**M**	**IPC**
	2	**3**	**3**	**M**	**IPC**
DRI-057	**5**	**5**	**4**	**C**	**IPR**
DCMPR-058	**2**	**2**	**2**	**M**	**IPC**

OACPVR-059	**3**	**2**	**2**	**M**	**IPC**
DCMPR-060	**3**	**2**	**2**	**M**	**IPC**
DPR-061	**3**	**2**	**2**	**M**	**IPC**
DRI-062	**3**	**2**	**2**	**M**	**IPC**
DCMPR-063	**4**	**3**	**3**	**M**	**IPC**
DCMPR-064	**2**	**3**	**2**	**M**	**IPC**
DCMPR-065	**4**	**3**	**4**	**A**	**IPR**
DCMPR-066	**2**	**3**	**2**	**M**	**IPC**
DCMPR-067	**2**	**3**	**2**	**M**	**IPC**
DCMPR-068	**2**	**2**	**2**	**M**	**IPC**
DCMPR-069	**2**	**2**	**3**	**M**	**IPC**

DCMPR-070	**3**	**2**	**2**	**M**	**IPC**
DCMPR-071	**5**	**4**	**4**	**A**	**IPR**
DCMPR-072	**5**	**4**	**5**	**C**	**IPR**
DCMPR-073	**5**	**5**	**4**	**C**	**IPR**

Tabla 9. Clasificación del Activo de Información OACPVR.

El análisis permitirá validar y delimitar visiblemente los niveles de vulnerabilidades que se encuentren en la URL https://sivic.alcaldiabogota.gov.co/Sivic , la protección contra posibles violaciones y ataques involuntarios por parte de piratas informáticos tiene como objetivo garantizar que la infraestructura tecnológica instalada esté actualizada y mantenga los riesgos de integridad. Esto también incluye respaldar y cuidar la confidencialidad de la información en la plataforma.

Riesgo	Vulnerabilidad
Crítico	**9**
Alto	**15**
Medio	**9**
Bajo	**3**
Informativas	**33**
Total	**69**

SEVERITY	CVSS V3.0	PLUGIN	NAME
CRÍTICO	10	58987	PHP Unsupported Version Detection.
CRÍTICO	9.8	133845	Apache Tomcat Low: Multiple Vulnerabilities.
CRÍTICO	9.8	111068	Apache Tomcat Low: Multiple Vulnerabilities.
CRÍTICO	9.8	123828	PHP: Multiple vulnerabilities.
CRÍTICO	9.8	130276	PHP: Remote Code Execution Vulnerability.
CRÍTICO	9.1	123754	PHP: Multiple vulnerabilities.
CRÍTICO	9.1	124763	PHP: Heap-based Buffer Overflow Vulnerability.
CRÍTICO	9.1	125639	PHP: Multiple vulnerabilities.

CRÍTICO	9.1	134162	PHP: Multiple vulnerabilities.
ALTO	7.5	121124	Apache Tomcat: Denial of Service.
ALTO	7.5	126125	Apache Tomcat: DoS.
ALTO	7.5	132418	Apache Tomcat: Privilege Escalation Vulnerability.
ALTO	7.5	138097	Apache Tomcat: DoS.
ALTO	7.5	138574	Apache Tomcat: Multiple Vulnerabilities.
ALTO	7.5	147019	Apache Tomcat: Multiple Vulnerabilities.
ALTO	7.5	144054	Apache Tomcat: Information Disclosure.
ALTO	7.5	140532	PHP: Memory Leak Vulnerability.
ALTO	7.5	135926	PHP: Multiple Vulnerabilities.
ALTO	7.5	138593	PHP: Information Disclosure.
ALTO	7.5	142591	PHP: Multiple Vulnerabilities.
ALTO	7.5	42873	SSL Medium Strength Cipher Suites Supported.
ALTO	7.1	127131	PHP: Multiple Vulnerabilities.
ALTO	7.0	132413	Apache Tomcat: Privilege Escalation.
ALTO	7.0	136807	Apache Tomcat: Remote Code Execution.
MEDIO	6.5	151502	Apache Tomcat: Vulnerability.
MEDIO	6.5	141355	PHP: Multiple Vulnerabilities.
MEDIO	5.3	152183	Apache Tomcat: Vulnerability.
MEDIO	5.3	12085	Apache Tomcat Default Files.
MEDIO	5.3	136741	PHP: Denial of Service (DoS).
MEDIO	5.3	152853	PHP: Email Header Injection.
MEDIO	5.3	134220	Nginx Information Disclosure.
MEDIO	4.3	118036	Apache Tomcat: Open Redirect Weakness.
MEDIO	4.3	141446	Apache Tomcat: HTTP/2 Request Mix-Up.

BAJO	3.7	106712	Apache Tomcat: Insecure CGI Servlet Search Algorithm Description Weakness.
BAJO	3.7	106977	Apache Tomcat: Security Constraint Weakness.
BAJO	3.6	139571	PHP: Use-After-Free Vulnerability.
INFO	N/A	159462	Apache Tomcat: Spring4Shell (CVE-2022-22965) Mitigations
INFO	N/A	39446	Apache Tomcat Detection
INFO	N/A	45590	Common Platform Enumeration (CPE)
INFO	N/A	54615	Device Type
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	11936	OS Identification
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	31422	Reverse NAT/Intercepting Proxy Detection
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported

INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	22964	Service Detection
INFO	N/A	25220	TCP/IP Timestamps Supported
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	62564	TLS Next Protocols Supported
INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	10287	Traceroute Information
INFO	N/A	20108	Web Server / Application favicon.ico Vendor Fingerprinting
INFO	N/A	10386	Web Server No 404 Error Code Check
INFO	N/A	11422	Web Server Unconfigured - Default Install Page Present
INFO	N/A	10302	Web Server robots.txt Information Disclosure
INFO	N/A	106375	nginx HTTP Server Detection

Tabla 10. Vulnerabilidades SIVIC BOG.

7. DESCRIPCIÓN Y RECOMENDACIONES DEL ANÁLISIS DE RIESGOS DE SEGURIDAD INFORMÁTICA ENCONTRADAS EN LA PRUEBA DE VULNERABILIDADES.

Se ejecuto el análisis de riesgos con la herramienta de Nessus, evidenciando en análisis de vulnerabilidades, la existencia de 9 vulnerabilidades críticas, 15 vulnerabilidades de severidad Altas, 9 de severidad Media, 3 de severidad Baja y 35 vulnerabilidades Informativas, para poder mitigar el riesgo en las vulnerabilidades se darán a continuación las recomendaciones que deben tener en cuenta para poder mitigarlas.

En cuanto a las vulnerabilidades de índole informativo, es necesario aclarar que estas vulnerabilidades son difíciles de aprovechar por un delincuente cibernético, impacto el funcionamiento mínimo del sistema, ya que no afecta la disponibilidad o integridad de la infraestructura o el servidor que aloja la aplicación.

7.1. DESCRIPCIÓN Y RECOMENDACIONES PARA VULNERABILIDADES DE SEVERIDAD CRÍTICO:

Detección de versiones no compatibles en PHP

Descripción: Ya no se admite la capacidad de instalar PHP en el host remoto. El proveedor no lanzará nuevos parches de seguridad para el producto debido a la falta de soporte. Es probable que tenga fallos de seguridad.

Recomendación: Cambiar a una versión de PHP compatible con el equipo.

Apache Tomcat Low: Multiple Vulnerabilities.

Descripción: El host remoto tiene instalado Tomcat 7.0.x, 8.x u 8.5.51 antes de la última versión de 9.0.x. Por lo tanto, es vulnerable a diversas vulnerabilidades.

Por la posibilidad de un manejo incorrecto de los encabezados de codificación de transferencia detrás de un proxy inverso, Tomcat es vulnerable a una suplantación de solicitudes HTTP. Un atacante remoto puede aprovechar solicitudes HTTP diseñadas para enviar mensajes HTTP no deseados al back-end. (CVE-2019-17569)

Existe una debilidad en el tráfico de solicitudes HTTP en el código Tomcat debido a un análisis incorrecto de final de línea (EOL) que puede permitir que los encabezados HTTP no legales se analizaran como válidos. Un atacante remoto puede aprovechar de estas solicitudes HTTP diseñadas para enviar mensajes HTTP no deseados al back-end. (CVE-2020-1935)

Existe una falla en la lectura de archivos arbitraria en los protocolos de Apache JServ (AJP) por defecto en la implementación de Tomcat. Un atacante que no esté autenticado de forma remota podría utilizar esto para obtener acceso a archivos que normalmente están bloqueados. Si la instancia de Tomcat es capaz de cargar archivos, la vulnerabilidad podría aprovecharse para ejecutar código desde una ubicación remota. (CVE-2020-1938).

Recomendación: Se debe actualizar a Apache Tomcat a versiones posteriores de 9.0.x.

Apache Tomcat: Multiple Vulnerabilities

Descripción: Se evidencia instalación de Apache Tomcat preliminar a la versión 8.5.32. Consecuentemente, se ve afectado por múltiples vulnerabilidades.

Recomendación: Actualizar a Apache Tomcat versiones posteriores de 9.0.x.

PHP: Multiple Vulnerabilities

Descripción: La versión de PHP del servidor web es anterior a 7.2.16. Por lo siguiente, se ve perjudicado por numerosas vulnerabilidades.

Lecturas no inicializadas en el componente EXIF de PHP debido al mal manejo de los datos en exif_process_IFD_in_MAKERNOTE, y exif_process_IFD_in_TIFF. (CVE-2019-9638, CVE-2019-9639, CVE-2019-9641)

Una lectura no válida en el componente EXIF de PHP debido a un mal manejo de los datos en exif_process_SOFn. (CVE-2019-9640)

Existe una debilidad en la omisión de Access control debido a la forma en que se implementa rename (). Esto podría permitir a los usuarios no autorizados a obtener información de otro modo que no tendría acceso (CVE-2019-9637).

Recomendación: Actualizar a PHP versión 7.2.16 o posterior.

PHP: Remote Code Execution Vulnerability.

Descripción: Se ejecuta en el servidor web PHP versión anterior a 7.3.11. Por lo cual, debe tener afectaciones de vulnerabilidad en la ejecución remota de código por una validación insuficiente en el ingreso del usuario. Un atacante no legitimado puede sacar provecho de esto, mediante de un envío de solicitud esencialmente delineada, para inducir la ejecución de un código arbitrario para infringir la directiva fastcgi_split_path_info.

Recomendación: Actualizar versión de PHP posterior a 7.3.12.

PHP: Multiple Vulnerability.

Descripción: Las versiones de PHP ejecutables de un servidor web anterior a 7.2.17. Tienen afectaciones por múltiples hallazgos en vulnerabilidades:

Preexiste condiciones sobre lectura de búfer establecida en php_ifd_get32s en exif.c.

Existe una condición de desbordamiento de búfer basada en montón en exif_iif_add_value en exif.c como resultado de una comprobación incorrecta de la longitud de entrada.

Recomendación: Actualizar a PHP versión 7.2.17 o posterior.

PHP: Heap-based Buffer Overflow Vulnerability.

Descripción: la versión de PHP que se ejecuta en el servidor web remoto es 7.2.x anterior a 7.2.18. Por lo tanto, se ve afectado por una condición de sobre lectura de búfer basada en montón dentro de _estrndup del exif_process_IFD_TAG en el script exif.c.

Un atacante remoto no autenticado puede aprovechar esto para provocar una condición de denegación de servicio o la ejecución de código arbitrario.

Recomendación: Actualizar a PHP versión 7.2.18 o posterior.

PHP: Multiple Vulnerabilities.

Descripción: Versión de PHP en el servidor web preliminar a 7.2.19. Por lo siguiente, se encuentra afectado por las subsiguientes vulnerabilidades:

Vulnerabilidad no inicializada en gdImageCreateFromXbm debido a que el método sscanf no puede leer un valor hexadecimal. Es posible que un atacante pueda aprovechar este problema para provocar la divulgación de información confidencial. (CVE-2019-11038)

Vulnerabilidad de lectura externamente de los límites en iconv.c: _php_iconv_mime_decode () debido al desbordamiento de enteros.

Es posible que un atacante pueda aprovechar este problema para provocar la divulgación de información confidencial. (CVE-2019-11039)

Situación de desbordamiento de búfer asentada en montón en php_jpg_get16. Un atacante puede aprovecharse de esto provocando un estado de denegación de servicio o la realización de un código arbitrario. (CVE-2019-11040)

Recomendación: Actualizar a php versión 7.2.19 o posterior.

PHP: Multiple Vulnerabilities.

Descripción: PHP de versión anterior a 7.4.3 ejecutados en el servidor web, afectado por diferentes vulnerabilidades:

La función phar_extract_file () está sujeta a una condición de desbordamiento de búfer basado en el montón debido a una terminación inadecuada del bucle. Un atacante remoto, que no esté autenticado, puede utilizar esto para desencadenar una condición de denegación de servicio o ejecutar código arbitrario. (CVE 2020 7061)

Vulnerabilidad de denegación de servicio (DoS) está presente en las funciones de progreso de PHP SessionUpload como resultado de la desreferencia del puntero nulo. El servicio php puede ser deshabilitado por un atacante remoto no autenticado debido a este problema. (CVE 2020 7062)

Todas las personas tienen acceso a los archivos Tar cuando la función buildFromIterator está configurada con un permiso de archivo inseguro. (CVE 2020 7063)

Recomendación: Actualizar PHP a la versión 7.4.3 o superior.

7.2. DESCRIPCIÓN Y RECOMENDACIONES PARA VULNERABILIDADES DE SEVERIDAD ALTA:

Apache Tomcat: Denial of Service.

Descripción: De acuerdo a la instancia de Apache Tomcat se escucha en el host remoto es 8.0.x < 8.0.52, 8.5.x < 8.5.31 o 9.0.x < 9.0.8. Tiene afectaciones en la siguiente vulnerabilidad:

Existe una vulnerabilidad de denegación de servicio (DoS) en Tomcat por manejo incorrecto del desbordamiento en el decodificador UTF-8. Un delincuente remoto no identificado puede aprovecharse de este problema para provocar un bucle infinito en el descodificador, lo que conlleva a un estado de denegación de servicio.

Recomendación: Actualizar Apache Tomcat a la versión 9.0.8 o posterior.

Apache Tomcat: DoS.

Descripción: Versión de Tomcat desactualizada en el host remoto es anterior a 8.5.41. Por el cual puede verse afectada por una vulnerabilidad en el documento informativo de fixed_in_apache_tomcat_8.5.41_security-8.

No se ha encontrado la solución definitiva para CVE-2019-0199, donde no deja de abordar el agotamiento de la ventana de conexión HTTP / 2 en la escritura. Al no poder enviar mensajes a WINDOW_UPDATE para que la conexión (secuencia 0), los usuarios pudieron hacer que los subprocesos del servidor se bloquearan, lo que finalmente provocó el agotamiento de los subprocesos y un DoS. (CVE-2019-10072)

Recomendación: Actualizar a Apache Tomcat versión 8.5.41 o posterior.

Apache Tomcat: Privilege Escalation Vulnerability.

Descripción: Versión del Tomcat desactualizada en el host remoto, anterior a la 8.5.50. Afectado por vulnerabilidad de escalada de privilegios a la que se hace referencia en el aviso 'Corregido en Apache Tomcat 8.5.50'.

Al usar la autenticación FORM había una ventana estrecha donde un atacante podía realizar un ataque de fijación de sesión. La ventana se consideró demasiado estrecha para que un exploit fuera práctico, pero, errando por el lado de la precaución, este problema se ha tratado como una vulnerabilidad de seguridad. (CVE-2019-17563)

Recomendación: Actualizar a Apache Tomcat versión 8.5.50 o posterior.

Apache Tomcat: DoS.

Descripción: La versión de Tomcat se encuentra desactualizada en el host remoto es anterior a 8.5.56. Por lo anterior, puede verse afectado por la vulnerabilidad de denegación de servicio a la que se hace referencia en el documento informativo de

fixed_in_apache_tomcat_8.5.56_security-8. Basándose en el número de versión autoinformado de la aplicación.

Recomendación: Actualizar la versión de Apache Tomcat a 8.5.56 o superior.

Apache Tomcat: Multiple Vulnerabilities

Descripción: El Tomcat instalado en el host remoto es anterior a 8.5.57. Por lo siguiente, tiene diferentes vulnerabilidades como se hace referencia en el aviso de seguridad corregido en Apache Tomcat 8.5.57.

La carga de longitud útil en un marco WebSocket no se validó comedidamente. Las cargas de longitudes útil no podrían ser válidas, desencadena un bucle infinito. Varias solicitudes con carga de longitudes útil no válidas podrían provocar una denegación de servicio (DoS).

(CVE-2020-13935): una conexión directa h2c no libró el procesador HTTP/1.1 posteriormente de la actualización a HTTP/2. Si se ejecutara un número bastante de solicitudes, podría causar una excepción OutOfMemoryException que condujera a una denegación de servicio (DoS). (CVE-2020-13934)

Recomendación: Actualizar versión de Apache Tomcat 8.5.57 o posterior.

Apache Tomcat: Multiple Vulnerabilities

Descripción: La versión de Tomcat se encuentra desactualizada en el host remoto es anterior a 8.5.63. Se evidencia afectación por diferentes vulnerabilidades a las que se hace referencia en el aviso del proveedor.

Cuando se utilizan las versiones de Apache Tomcat a 10.0.0-M4, un ciberdelincuente es capacitado para controlar el contenido y el nombre de un archivo en el servidor configurado para utilizar PersistenceManager con un filestore; PersistenceManager está configurado con sessionAttributeValueClassNameFilter=null (el valor predeterminado a menos que se use un SecurityManager) o un filtro lo suficientemente laxo como para permitir que el objeto proporcionado por el atacante se deserialice; conociendo la ruta de

acceso relativa del archivo desde la ubicación de almacenamiento utilizada por FileStore hasta el archivo sobre el que el atacante tiene control; luego, utilizando una solicitud específicamente diseñada, el atacante podrá desencadenar la ejecución remota de código a través de la deserialización del archivo bajo su control. Tenga en cuenta que todas las condiciones deben ser ciertas para que el ataque tenga éxito. (CVE-2020-9484)

Al responder a las nuevas solicitudes de conexión h2c, las versiones anteriores de Apache Tomcat 10.0.0-M1 duplicar los encabezados de solicitud y una cantidad limitada de cuerpo de solicitud de una solicitud a otra, lo que significa que el usuario A y el usuario B podrían ver los resultados de la solicitud del usuario A. (CVE-2021-25122)

Cuando se usaba Apache Tomcat anteriores a 10.0.0-M1 con un caso de borde de configuración que era muy poco probable que se usara, la instancia de Tomcat seguía siendo vulnerable a CVE-2020-9494. Tenga en cuenta que tanto los requisitos previos publicados anteriormente para CVE-2020-9484 como las mitigaciones publicadas anteriormente para CVE-2020-9484 también se aplican a este problema. (CVE-2021-25329)

Recomendación: Actualizar a Apache Tomcat versión 8.5.63 o posterior.

Apache Tomcat: Information Disclosure.

Descripción: La versión de Tomcat instalada en el servidor es anterior a 8.5.60. se afecta por diferentes vulnerabilidades a las que se hace referencia en el documento informativo de fixed_in_apache_tomcat_8.5.60_security-8.

Al servir recursos a partir de una ubicación en la red utilizando el sistema de archivos NTFS, las versiones de Apache Tomcat 10.0.0-M1 a 10.0.0-M9. Son susceptibles a la divulgación del código fuente JSP en algunas configuraciones. El origen raíz fue la conducta inesperada de la API de JRE File.getCanonicalPath() fue causado por el procedimiento inconsistente de la API de Windows (FindFirstFileW) en algunas situaciones. (CVE-2021-24122)

Al investigar el error 64830 se descubrió que Apache Tomcat 10.0.0-M1 a 10.0.0-M9, puede reutilizar un valor de encabezado de solicitud HTTP de la secuencia preliminar recibida en una conexión HTTP / 2 para la solicitud asociada con la secuencia posterior. Si bien esto probablemente conduciría a un error y al cierre de la conexión HTTP / 2, es posible que la información se filtre entre las solicitudes. (CVE-2020-17527)

Recomendación: Actualizar a Apache Tomcat versión 8.5.60 o posterior.

PHP: Memory Leak Vulnerability.

Descripción: El número de versión auto informado de PHP el cual se ejecuta en el servidor web remoto es anterior a 7.3.21. El cual, se encuentra afectaciones por una vulnerabilidad de pérdida de memoria en el componente LDAP. Un ciberdelincuente remoto no identificado podría aprovechar este problema para provocar una condición de denegación de servicio.

Recomendación: Actualizar versión de PHP 7.3.22 o posterior.

PHP: Multiple Vulnerabilities

Descripción: Según la versión auto informado de PHP ejecutado en el servidor web remoto es anterior a 7.2.30. Está afectado por varias vulnerabilidades:

Existe un error de lectura fuera de los límites en urldecode () debido a comprobaciones de validación de datos incorrectas. Un atacante puede aprovechar esto insertando valores hexadecimales negativos para filtrar los servicios que se encuentran en la memoria antes de la matriz.

Existe una vulnerabilidad de inyección de bytes NULL en shell_exec () y el operador de acento grave debido a una desinfección de datos incorrecta.

Recomendación: Actualizar PHP a la versión 7.2.30 o superior.

PHP: Information Disclosure

Descripción: Según la versión auto informado de PHP ejecutado en el host remoto de Windows es anterior a 7.4.8. Se afecta por una vulnerabilidad de divulgación de información. Se puede engañar a la biblioteca libcurl para que anteponga una parte de la contraseña al nombre del host antes de que lo resuelva, lo que podría filtrar la contraseña parcial a través de la red y a los servidores DNS.

Recomendación: Actualizar PHP a la versión 7.4.9 o superior.

PHP: Multiple Vulnerabilities

Descripción: La versión de PHP auto informado, ejecutado en el servidor web remoto es anterior a la 7.3.24. Está afectada por diferentes vulnerabilidades.

Recomendación: Actualizar PHP a la versión 7.3.24 o posterior.

SSL Medium Strength Cipher Suites Supported (SWEET32)

Descripción: El host remoto admite el uso de cifrados SSL que ofrecen cifrado de nivel medio. Se considera de fuerza media cualquier encriptación que use longitudes de clave de al menos 64 bits y menos de 112 bits, o que use la suite de encriptación 3DES.

Tenga en cuenta que es considerablemente más fácil eludir el cifrado de nivel medio si el atacante está en la misma red física.

Recomendación: Volver a configurar la aplicación afectada si es posible para evitar el uso de cifrados de intensidad media.

PHP: Multiple Vulnerabilities

Descripción: Según su banner, la versión de PHP que se ejecuta en el servidor web remoto es 7.2.x anterior a 7.2.21. Por lo consecuente puede verse afectado por vulnerabilidades de desbordamiento de búfer en las funciones exif_read_data y exif_scan_thumbnail.

Recomendación: Actualizar PHP versión a la 7.2.21 o superior.

Apache Tomcat: Privilege Escalation

Descripción: La versión de Tomcat instalada en el host remoto es anterior a la 8.5.49. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso fixed_in_apache_tomcat_8.5.49_security-8.

Cuando Apache Tomcat está configurado con JMX Remote Lifecycle Listener, un atacante local sin acceso al proceso de Tomcat o a los archivos de configuración puede manipular el registro RMI para realizar un ataque de intermediario para capturar los nombres de usuario y las contraseñas utilizadas. para acceder a la interfaz JMX. Luego, el atacante puede usar estas credenciales para acceder a la interfaz JMX y obtener un control completo sobre la instancia de Tomcat. (CVE-2019-12418)

Recomendación: Actualizar a Apache Tomcat versión 8.5.49 o posterior.

Apache Tomcat: Remote Code Execution

Descripción: La versión de Tomcat instalada en el host remoto es anterior a la 8.5.55. Se encuentra afectado por una vulnerabilidad de ejecución remota de código como se menciona en el aviso fixed_in_apache_tomcat_8.5.55_security-8.

Recomendación: Actualizar Apache Tomcat a la versión 8.5.55 o superior.

7.3. DESCRIPCIÓN Y RECOMENDACIONES PARA VULNERABILIDADES DE SEVERIDAD MEDIO:

Apache Tomcat: vulnerability

Descripción: La versión de Tomcat instalada en el host remoto es 10.0.x <= 10.0.5. Por lo siguiente afecta una vulnerabilidad como se menciona en el aviso fixed_in_apache_tomcat_10.0.6_security-10.

Las consultas realizadas por JNDI Realm no siempre escaparon correctamente de los parámetros. Los valores de los parámetros pueden obtenerse de los datos

proporcionados por el usuario (p. ej., nombres de usuario), así como de los datos de configuración proporcionados por un administrador. En circunstancias limitadas, los usuarios podían autenticarse usando variaciones de su nombre de usuario y/o eludir parte de la protección proporcionada por LockOut Realm. (CVE-2021-30640)
Recomendación: Actualizar a Apache Tomcat a la versión 10.0.6 o superior.

Apache Tomcat Default Files

Descripción: La página de error predeterminada, la página de índice predeterminada, los JSP de ejemplo y/o los servlets de ejemplo se instalan en el servidor Apache Tomcat remoto. Estos archivos deben eliminarse, ya que pueden ayudar a un atacante a descubrir información sobre la instalación o el host remoto de Tomcat.
Recomendación: Elimine la página de índice predeterminada y elimine el JSP y los servlets de ejemplo. Siga las instrucciones de Tomcat u OWASP para reemplazar o modificar la página de error predeterminada.

PHP: Denial of Service (DoS)

Descripción: La versión de PHP auto informado que se ejecuta en el host remoto es anterior a 7.4.6. Por lo tanto, se ve afectado por una vulnerabilidad de denegación de servicio (DoS) en su componente de carga de archivos HTTP debido a que no se limpiaron los archivos temporales creados durante el proceso de carga de archivos. Un atacante remoto no autenticado puede explotar este problema, enviando repetidamente cargas con nombres largos de archivos o campos, para agotar el espacio en disco y causar una condición DoS.
Recomendación: Actualizar a la versión de PHP 7.4.6 o posterior.

PHP: Email Header Injection

Descripción: Según la versión auto informado de PHP que se ejecuta en el servidor web remoto es anterior a la versión 7.3.28.

Por lo tanto, se ve afectado por una vulnerabilidad de inyección de encabezado de correo electrónico, debido a una falla en el manejo adecuado de las secuencias CR-LF en los campos de encabezado. Un atacante remoto no autenticado puede explotar esto, insertando caracteres de avance de línea en los encabezados de correo electrónico, para obtener el control total del contenido del encabezado del correo electrónico.

Recomendación: actualice a la versión de PHP 7.3.28 o posterior.

NGINX: Information Disclosure

Descripción: Según el encabezado de respuesta del servidor, la versión instalada de nginx es anterior a la 1.17.7. Tiene afectación por una vulnerabilidad de divulgación de información.

Recomendación: Actualizar a la versión 1.17.7 o posterior de nginx.

Apache Tomcat: Open Redirect Weakness

Descripción: La versión de Apache Tomcat que se encuentra instalada en el host remoto es anterior a la 8.5.34. Por la cual, está afectado por una vulnerabilidad de redirección abierta.

Recomendación: Actualizar a Apache Tomcat versión 8.5.34 o posterior.

Apache Tomcat: HTTP/2 Request Mix-Up

Descripción: La versión de Apache Tomcat instalada en el servidor web es anterior a 9.0.38. Está, por tanto, afectado por una vulnerabilidad. Si un cliente HTTP/2 excede la cantidad máxima acordada de flujos simultáneos de conexión (en violación del protocolo HTTP/2), posiblemente una solicitud posteriormente ejecutada en esa conexión pueda contener encabezados HTTP, incluidos los pseudo encabezados HTTP/2. - de una solicitud anterior en lugar de los encabezados previstos. Esto puede hacer que los usuarios vean respuestas para recursos inesperados.

Recomendación: Actualizar a Apache Tomcat a la versión 9.0.38 o superior.

7.4. DESCRIPCIÓN Y RECOMENDACIONES PARA VULNERABILIDADES DE SEVERIDAD BAJO:

Apache Tomcat: Insecure CGI Servlet Search Algorithm Description Weakness

Descripción: La versión de Apache Tomcat instalada en el host remoto es la 8.5.24. Se encuentra afectado por una falla que se debe a que el programa contiene una descripción incorrecta para el algoritmo de búsqueda CGI Servlet, lo que puede causar que un administrador deje el sistema en un estado inseguro.

Recomendación: Actualizar a Apache Tomcat versión 8.5.24 o posterior.

Apache Tomcat: Security Constraint Weakness

Descripción: La versión de Apache Tomcat ejecutada en el host remoto es anterior a la 8.5.28. En la cual se encuentra afectada por una falla en las restricciones de seguridad que podría exponer los recursos a usuarios no autorizados.

Recomendación: Actualizar a Apache Tomcat versión 8.5.28 o posterior.

PHP: Use-After-Free Vulnerability

Descripción: Según la versión de PHP auto informado que se ejecuta en el servidor web remoto es anterior a 7.2.33. Por lo cual, es afecta por una vulnerabilidad de uso posterior a la liberación en la función phar_parse debido al mal manejo de la variable actual_alias. Un atacante remoto no autenticado podría explotar este problema eliminando la referencia de un puntero liberado, lo que podría conducir a la ejecución de código arbitrario.

Recomendación: Actualizar a la versión de PHP 7.2.33

7.5. DESCRIPCIÓN Y RECOMENDACIONES PARA VULNERABILIDADES INFORMATIVAS:

Apache Tomcat 8.x < 8.5.78 Spring4Shell (CVE-2022-22965) Mitigations

Descripción: La versión de Apache Tomcat ejecutada en el host remoto es anterior de 8.5.78.

- La implementación simplificada de lecturas y escrituras de bloqueo introducidas en Tomcat 10 y devueltas a Tomcat 9.0.47 en adelante expuso un error de concurrencia de larga data (pero extremadamente difícil de activar) en Apache Tomcat 10.1.0 a 10.1.0-M12, que podrían hacer que las conexiones del cliente compartan una instancia de Http11 que resulte en respuestas, o respuestas parciales, ser recibido por el cliente equivocado. (CVE-2021-43980)

Recomendación: Actualice a Apache Tomcat versión 8.5.78 o posterior.

Apache Tomcat Detection

Descripción: El servidor web remoto es un servidor Apache Tomcat.

Recomendación: Actualice a Apache Tomcat versión 8.5.78 o posterior.

Common Platform Enumeration (CPE)

Descripción: Mediante el uso de la información obtenida de un escaneo de Nessus, este complemento informa que CPE (Common Platform Enumeration) coincide con varios productos de hardware y software que se encuentran en un host.

Tenga en cuenta que, si un CPE oficial no está disponible para el producto, este complemento calcula el mejor CPE posible en función de la información disponible en el escaneo.

Device Type

Descripción: Asentar en el sistema operativo del dispositivo remoto, se puede identificar la naturaleza del mismo, ya sea un enrutador, una computadora de propósito general, entre otros.

HSTS Missing From HTTPS Server

Descripción: El servidor HTTPS remoto no está aplicando HTTP Strict Transport Security (HSTS). HSTS es un encabezado de respuesta opcional que se puede configurar en el servidor para indicar al navegador que solo se comunique a través de HTTPS. La falta de HSTS permite ataques de degradación, ataques de hombre en el medio que eliminan SSL y debilita las protecciones de secuestro de cookies.
Recomendación: Configure el servidor web remoto para usar HSTS.

HTTP Methods Allowed (per directory)

Descripción: Al llamar al método OPCIONES, es posible determinar qué métodos HTTP están permitidos en cada directorio.
Los siguientes métodos HTTP se consideran inseguros:
PONER, BORRAR, CONECTAR, RASTREAR, CABEZA
Muchos marcos y lenguajes tratan 'HEAD' como una solicitud 'GET', aunque sin ningún cuerpo en la respuesta. Si se estableciera una restricción de seguridad en las solicitudes 'GET' de modo que solo los 'usuarios autenticados' pudieran acceder a las solicitudes GET para un servlet o recurso en particular, se omitiría para la versión 'HEAD'. Esto permitió el envío ciego no autorizado de cualquier solicitud GET privilegiada.

Como esta lista puede estar incompleta, el complemento también prueba (si las "Pruebas exhaustivas" están habilitadas o "Habilitar pruebas de aplicaciones web" está configurada en "sí" en la política de análisis) varios métodos HTTP conocidos

en cada directorio y los considera no compatibles si recibe un código de respuesta de 400, 403, 405 o 501.
Tenga en cuenta que el resultado del complemento es solo informativo y no indica necesariamente la presencia de vulnerabilidades de seguridad.

HTTP Server Type and Version

Descripción: Este complemento intenta determinar el tipo y la versión del servidor web remoto, se está ejecutando un servidor web en el host remoto, no se puede ver el tipo y la versión HTTP**.**

Host Fully Qualified Domain Name (FQDN) Resolution

Descripción: No se pudo resolver el nombre de dominio completo (FQDN) del host remoto.

HyperText Transfer Protocol (HTTP) Information

Descripción: Esta prueba brinda información sobre el protocolo HTTP remoto: la versión utilizada, si HTTP Keep-Alive y la canalización HTTP están habilitados, etc. Esta prueba es sólo informativa y no indica ningún problema de seguridad.

OS Identification

Descripción: Usando una combinación de sondas remotas (por ejemplo, TCP/IP, SMB, HTTP, NTP, SNMP, etc.), es posible adivinar el nombre del sistema operativo remoto en uso. A veces también es posible adivinar la versión del sistema operativo.

PHP Version Detection

Descripción: No fue posible obtener el número de versión de la instalación remota de PHP disponible en el servidor web remoto.

Patch Report

Descripción: Al host remoto le faltan uno o más parches de seguridad. Este complemento enumera la versión más reciente de cada parche a instalar para garantizar que el host remoto esté actualizado.

Reverse NAT/Intercepting Proxy Detection

Descripción: NAT es una tecnología que permite a varios ordenadores ofrecer servicios públicos en diferentes puertos a través de la misma dirección IP.

Según los resultados de las huellas dactilares del SO, parece que diferentes sistemas operativos están escuchando en diferentes puertos remotos. Tenga en cuenta que este comportamiento también puede indicar la presencia de un proxy interceptor, un equilibrador de carga o un moldeado de tráfico.

SSL / TLS Versions Supported

Descripción: Este complemento detecta qué versiones SSL y TLS son compatibles con el servicio remoto para cifrar las comunicaciones.

SSL Certificate 'commonName' Mismatch

Descripción: El servicio que se ejecuta en el host remoto presenta un certificado SSL para el cual el atributo 'commonName' (CN) no coincide con el nombre de host en el que se escucha el servicio.

SSL Certificate Information

Descripción: Este complemento se conecta a todos los puertos relacionados con SSL e intenta extraer y volcar el certificado X.509.

SSL Cipher Block Chaining Cipher Suites Supported

Descripción: El host remoto admite el uso de cifrados SSL que operan en modo Cipher Block Chaining (CBC). Estas suites de cifrado ofrecen seguridad adicional sobre el modo Electronic Codebook (ECB), pero tienen el potencial de filtrar información si se usan incorrectamente.

SSL Perfect Forward Secrecy Cipher Suites Supported

Descripción: El host remoto admite el uso de cifrados SSL que ofrecen el cifrado Perfect Forward Secrecy (PFS). Estas suites de cifrado aseguran que el tráfico SSL registrado no se pueda romper en una fecha futura si la clave privada del servidor se ve comprometida.

SSL Root Certification Authority Certificate Information

Descripción: El servicio remoto utiliza una cadena de certificados SSL que contiene un certificado de Autoridad de Certificación raíz auto firmado en la parte superior de la cadena.

Recomendación: Asegúrese de que el uso de este certificado de autoridad de certificación raíz cumpla con las políticas de seguridad y uso aceptable de su organización.

SSL/TLS Recommended Cipher Suites

Descripción: El host remoto tiene puertos SSL/TLS abiertos que anuncian suites de cifrado desalentadas. Se recomienda habilitar solo el soporte para las siguientes suites de cifrado:

TLSv1.3: 0x13,0x01 TLS13_AES_128_GCM_SHA256 0x13,0x02 TLS13_AES_256_GCM_SHA384 0x13,0x03 TLS13_CHACHA20_POLY1305_SHA256TLSv1.2: 0xC0,0x2B ECDHE-ECDSA-AES128-GCM-SHA256 0xC0,0x2F ECDHE-RSA-AES128-GCM-SHA256 0xC0,0x2C ECDHE-ECDSA-AES256-GCM-SHA384 0xC0,0x30 ECDHE-RSA-

AES256-GCM-SHA384 0xCC, 0xA9 ECDHE-ECDSA-CHACHA20-POLY1305 0xCC, 0xA8 ECDHE-RSA-CHACHA20-POLY1305 0x00,0x9E DHE-RSA-AES128-GCM-SHA256 0x00,0x9F DHE-RSA-AES256-GCM-SHA384

Service Detection

Descripción: No pudo identificar el servicio remoto por su banner o mirando el mensaje de error que envía cuando recibe una solicitud HTTP.

TCP/IP Timestamps Supported

Descripción: El host remoto implementa marcas de tiempo TCP, según lo definido por RFC1323. Un efecto secundario de esta característica es que a veces se puede calcular el tiempo de actividad del host remoto.

TLS ALPN Supported Protocol Enumeration

Descripción: El host remoto admite la extensión TLS ALPN. Este complemento enumera los protocolos que admite la extensión.

TLS NPN Supported Protocol Enumeration

Descripción: El host remoto admite la extensión TLS NPN (Negociación del siguiente protocolo de seguridad de la capa de transporte). Este complemento enumera los protocolos que admite la extensión.

TLS Next Protocols Supported

Descripción: Este script detecta qué protocolos anuncia el servicio remoto para ser encapsulados por conexiones TLS.

Tenga en cuenta que Nessus no intentó negociar sesiones TLS con los protocolos que se muestran. El servicio remoto puede estar publicitando falsamente estos protocolos y/o no publicitando otros protocolos compatibles.

TLS Version 1.2 Protocol Detection

Descripción: El servicio remoto acepta conexiones cifradas mediante TLS 1.2.

Traceroute Information

Descripción: Fue posible obtener información de traceroute.

Web Server / Application favicon.ico Vendor Fingerprinting

Descripción: El archivo 'favicon.ico' que se encuentra en el servidor web remoto pertenece a un servidor web popular. Esto se puede usar para tomar las huellas dactilares del servidor web.

Recomendación: Elimine el archivo 'favicon.ico' o cree uno personalizado para su sitio.

Web Server No 404 Error Code Check

Descripción: El servidor web remoto está configurado de manera que no devuelva los códigos de error '404 No encontrado' cuando se solicita un archivo inexistente, tal vez devolviendo en su lugar un mapa del sitio, página de búsqueda o página de autenticación.

Nessus ha permitido algunas contramedidas para esto. Sin embargo, pueden ser insuficientes. Si se produce una gran cantidad de agujeros de seguridad para este puerto, es posible que no todos sean precisos.

Web Server Unconfigured - Default Install Page Present

Descripción: El servidor web remoto utiliza su página de bienvenida predeterminada. Por lo tanto, es probable que este servidor no se use en absoluto o esté sirviendo contenido que está destinado a ser oculto.

Recomendación: Deshabilite este servicio si no lo usa.

Web Server robots.txt Information Disclosure

Descripción: El host remoto contiene un archivo llamado 'robots.txt' que tiene como objetivo evitar que los 'robots' web visiten ciertos directorios en un sitio web con fines de mantenimiento o indexación. Un usuario malicioso también puede usar el contenido de este archivo para conocer documentos confidenciales o directorios en el sitio afectado y recuperarlos directamente o dirigirlos a otros ataques.

Recomendación: Revise el contenido del archivo robots.txt del sitio, use etiquetas Robots META en lugar de entradas en el archivo robots.txt y/o ajuste los controles de acceso del servidor web para limitar el acceso a material sensible.

nginx HTTP Server Detection

Descripción: Se detectó el servidor HTTP nginx mirando el banner HTTP en el host remoto.

8. RECOMENDACIONES DE CIBERSEGURIDAD PARA LA PROTECCIÓN DE LA INFORMACIÓN Y LA SEGURIDAD DEL SISTEMA, ENFOCADAS A LA PREVENCIÓN DE INCIDENTES CIBERNÉTICOS

"Todas las entidades públicas tienen como referencia la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, con derechos reservados por parte del Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC, a través de la estrategia de Gobierno en Línea. Se encuentran todas las políticas, definiciones o contenido relacionado, publicadas en el compendio de las normas técnicas colombianas NTC ISO/IEC 27000 vigentes, así como a los anexos con derechos reservados por parte de ISO/ICONTEC."[24]. El MSPI es un conjunto de prácticas y políticas que buscan proteger los datos y sistemas de información contra amenazas y riesgos de seguridad, establecer políticas y procedimientos claros, proteger los sistemas, recuperar los desastres, realizar copias de seguridad, monitorear y auditar, educar y capacitar al personal, realizar evaluaciones continuas para garantizar la privacidad de los datos personales de los usuarios, es un modelo enfocado en el cumplimiento de tres objetivo cumpliendo los criterios de seguridad de la información. Para lograr estos objetivos se incluye estas medidas:

- Acceso restringido a la información a través de contraseñas, autenticaciones de dos pasos, entre otros.
- Datos encriptados que protejan la información mientras está en circulación o almacenada.
- Registro y monitoreo de los accesos a la información para detectar y prevenir actividades sospechosas.

[24] se pueden consultar en: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/#:~:text=El%20Modelo%20de%20Seguridad%20y,de%20vida%20de%20la%20seguridad

- Concientización y capacitación y de los empleados a cerca de las prácticas de protección y manejo adecuado de la información.
- Implementación de políticas, procedimientos de seguridad y privacidad de la información.
- Realización de auditorías periódicas para analizar la existencia de vulnerabilidades y riesgos de seguridad.

Entre otras recomendaciones:

Actualizar el sistema operativo y las aplicaciones: Los sistemas operativos tienen un mecanismo para instalar actualizaciones de seguridad de forma automática o mecánica. Estos parches de seguridad se lanzan de vez en cuando para combatir amenazas conocidas, mejor rendimiento y deben instalarse. Actualizar sus aplicaciones instaladas a la última versión es tan importante, o más, que lo anterior, ya que a menudo incluyen parches de seguridad. A medida que avanzan las versiones, son más vulnerables al ataque de los ciberdelincuentes que encuentren vulnerabilidades, con casos específicos en algunos Apaches: Tomcat, Java, PHP, Adobe Flash o Reader.

Instalación de antivirus en servidores y computadores: Todos los días se recibe mucha información externa, descargas de archivos y se navega bastante por Internet. Haciendo imperativo que la computadora tenga instalado un programa antivirus que actúe en defensa contra las amenazas. Existe la idea errónea de que las Mac no necesitan un antivirus, pero esto es mito; los ciberdelincuentes utilizan de forma más regular los PC con Windows y prestan menos atención a los Mac, pero también necesitan un software antivirus.

Desconfiar de soportes de información externos: Recibir información en USB, CD, DVD o disco duro externo se debe evitar. Este medio debe manipularse con cuidado y debe analizarse con un software de antivirus antes de ser usado. En el caso de las memorias USB o las unidades de DVD, es importante configurarlas para que no se enciendan o utilicen automáticamente, propendiendo que el usuario decida qué hacer con ellas. Hay malware que infecta la unidad flash USB y se

introduce en la computadora ejecuta automáticamente infectando la computadora. Los sistemas antivirus suelen proteger contra esta amenaza. También es peligroso que nos entreguen una memoria USB desconocida, la usamos en otra computadora y luego la insertamos en nuestro dispositivo. Si es posible, evite usar llaves USB para transferir información de terceros.

Bloquear la computadora desatendida: Cuando nos alejamos del computador por un momento o la persona se encuentra haciendo una atención, es importante bloquearlo. Esta actividad tarda unos segundos y evita que nadie use la computadora mientras estamos lejos o fuera; Si dejamos la computadora funcionando en nuestra ausencia, cualquiera puede robar la información a través de la llave USB, infectar la computadora y/o correo electrónico (luego eliminarlo para retrasar el descubrimiento) y puede eliminar/modificar la información importante.

Usar VPN (red privada virtual): El uso de VPN es una opción que brinda mayor privacidad y seguridad en Internet: Enmascaran la dirección IP del usuario y el tráfico lo redirigen a través de un túnel VPN encriptado. Este nivel de "**sigilo**" proporciona mejoras directas en seguridad contra ataques informáticos, privacidad contra robo de datos y robo de identidad, y otros beneficios adicionales. Cómo proteger identidades en línea, proteger transacciones en línea y compras electrónicas, o asegurar el uso de la red Wifi.

Soluciones de seguridad: Windows incluye la solución de seguridad original de **Windows Defender** como principal protección para los consumidores. Considerar usar la suite de seguridad profesional completa junto con otras herramientas de seguridad como el **firewall**. Los sistemas de encriptación de datos como **BitLocker**, ya que permiten encriptar u "ofuscar" los datos de la computadora para protegerlos de ataques maliciosos, amenazas de robo de datos o la piratería. Si el dispositivo se pierde, es robado o se retira incorrectamente.

Gestor de contraseñas: Las infracciones masivas de seguridad de los servicios de Internet son frecuentes en la actualidad y se expusieron millones de contraseñas. La verdad es que las contraseñas son un método funcional que brinda seguridad

limitada, solo hasta que surjan métodos más avanzados de identificación biométrica mejorada, por tanto, se continuaran usando la regla más importante es tener una contraseña fuerte y diferente para cada sitio. Las contraseñas aleatorias largas evitan los ataques de fuerza bruta; el uso de una contraseña diferente para cada cuenta evita que todas se vean comprometidas a la vez en caso de una violación de datos. Es una buena herramienta para reducir el error humano.

Usar autenticación de dos factores: La autenticación de dos factores (o autenticación de dos pasos) proporciona un nivel adicional de seguridad en los servidores y cuentas de nube entre otras, ya que será más difícil violar los nombres de usuario y las contraseñas. Este servicio está disponible en los principales servicios de Internet y debe usarse. Un código de verificación enviado generalmente al móvil o SMS será el mecanismo para confirmar la identidad de los/las usuario/as, pero agrega seguridad al uso de la contraseña. Este método frustra muchos ataques cibernéticos, especialmente los ataques de "fuerza bruta".

Utilice una conexión a Internet confiable: Al usar computadoras portátiles o tabletas fuera del lugar de trabajo, en ocasiones se utilizan redes Wifi públicas significando un riesgo importante para salvaguardar la información y la entidad. Si se considera necesario conectarse a una Red de Wifi pública, se deberían usar conexiones encriptadas (por ejemplo, usar sitios web cuyas direcciones comienzan con "**https**" en lugar de "http"). Lo ideal es que se utilice el portátil o Tablet con conexión a internet a una red que conozca que sea segura. Aún mejor es utilizar un servicio de **VPN (red privada virtual)** que garantice la privacidad de las comunicaciones mediante el cifrado de todas las conexiones a Internet. Se debe prestar especial atención a estas recomendaciones sobre todo en lugares concurridos como ferias o aeropuertos; los ciberdelincuentes monitorean regularmente las conexiones Wifi.

Un método común utilizado por ellos es crear una red Wifi con el mismo nombre de un restaurante o cafetería cercano de alta capacidad y dejarla disponible de forma

gratuita. A veces se considera Wifi para las instalaciones y se cree que son seguras, en realidad alguien o algo está monitoreando el tráfico a través de esa red Wifi.

Protección del navegador: Todos los navegadores web incluyen funciones de seguridad avanzadas que se deben comprobar: saber si están habilitadas y configuradas. Además, se debe considerar el cifrado de extremo a extremo en sincronización o sandbox (aislamiento de procesos), debemos prestar atención a las advertencias sobre sitios no seguros, verificar las extensiones instaladas porque pueden ser fuente frecuente de malware. Para mejorar la privacidad, no hay nada mejor que usar el modo incógnito, una función que todos los principales proveedores ahora ofrecen: Es una sesión de navegación privada temporal que no comparte datos con otros. El navegador no guarda historial de las páginas WEB consultadas, caché WEB, contraseñas o información de formularios, cookies u otros datos del sitio web, eliminando archivos temporales al finalizar la sesión.

Uso de dispositivos personales en la entidad: Para salvaguardar la información de la entidad se sugiere un uso contralado de la información depositada en los dispositivos personales, se pueden presentar perdida de la información en varios escenarios como: pérdida o robo, uso indebido de las aplicaciones, abandono de la entidad entre otras.

Crear copias de seguridad: Se recomienda crear copias de seguridad para usuarios y profesionales que quieran proteger la información personal y profesional en los equipos, además de ser una tarea de mantenimiento que contribuye a la salud del dispositivo. Las copias de seguridad deben almacenarse en el dispositivo de almacenamiento externo del equipo o en un servicio de almacenamiento en la nube que permita restaurar los datos en caso de un ataque.

Sentido común: La precaución es una de las barreras prioritarias frente al malware, y hay que tener cuidado frente a los ataques de **phishing** o **ransomware** que se pueden prevenir en cuanto llegan estas comunicaciones, debido a que están siendo utilizados de forma negligente por parte del (los) usuario(s).

Evite instalar aplicaciones de sitios web que no sean de confianza; abrir correos electrónicos no deseados o archivos adjuntos de redes sociales o aplicaciones de mensajería; navegar por ciertos sitios web; No utilice sistemas operativos y aplicaciones desactualizadas que contengan vulnerabilidades que los ciberdelincuentes pueden explotar en campañas de malware.

9. CONCLUSIONES

Se explica la importancia del funcionamiento del SIVIC BOG, que funciona dentro de la secretaría general de la alcaldía de Bogotá y su integración con el sistema VIVANTO, herramienta informática de la nación que consigna datos susceptibles de la población víctima del país. La articulación entre distrito y nación para garantizar el acceso oportuno a los servicios distritales y salvaguardar los derechos de los ciudadanos.

1. Se describieron cada uno de los roles asignados en SIVIC BOG, según las necesidades de trabajo y centros de encuentro.
2. Se propusieron recomendaciones de ciberseguridad para salvaguardar la información, con enfoque en incidentes cibernéticos, tal como lo describe la implementación del Modelo de Seguridad y Privacidad de la Información MSPI del Ministerio de TIC. Se encuentran disponibles todas las políticas, definiciones y contenidos relacionados publicados en la NTC ISO/IEC 27000, compendio vigente de Normas Técnicas Colombianas.
3. Se presentaron las tablas de factores de riesgo, descripción de vulnerabilidades, descripción de causas o amenazas, red iberoamericana de innovación y conocimiento científico; riesgos de seguridad digital; seguridad y privacidad de la información; activos; tipos de activos; Activos de información de la OACPVR (incluido su inventario); confidencialidad; integridad; valores de disponibilidad; Vulnerabilidades de SIVIC BOG.

Se presentó información del funcionamiento, riesgos y descripción de los roles definidos dentro del SIVIC BOG, los factores de riesgo, descripción de vulnerabilidades, causas o amenazas, red iberoamericana de innovación y

conocimiento científico, incluyendo riesgos de ciberseguridad, categorías de riesgo de seguridad digital, clases de activos OACPVR, estándares de confidencialidad e integridad y vulnerabilidad de SIVIC BOG, se realizaron análisis de vulnerabilidades dentro de SIVIC BOG, inspeccionar datos de diversas fuentes en busca de posibles vulnerabilidades, comprobando el estado en el que se encuentra cara a posibles ataques e invasiones no autorizadas por parte de delincuentes informáticos, en este sentido se encontraron múltiples vulnerabilidades los cuales 9 son vulnerabilidades de carácter críticas, 15 de vulnerabilidades de carácter altas, 9 vulnerabilidades de condiciones medias, 3 vulnerabilidades de condiciones bajas y 35 vulnerabilidades de carácter informativas, la mayoría de las vulnerabilidades encontradas son por actualizaciones a la últimas versiones de PHP y Apache Tomcat, las cuales se han venido actualizando los parches de seguridad, rendimiento, soporte o nuevas características para los desarrolladores del lenguaje de programación PHP y aplicación Apache Tomcat, también se encontró una vulnerabilidad de criticidad alta de SSL de cifrado a un nivel medio, considerando fácil de eludir por un bandido cibernético que se encuentra dentro de la misma red física. Se realiza la descripción de cada una de las vulnerabilidades encontradas y recomendaciones dadas para el robustecimiento de la seguridad del sistema de información, relevando la importancia de hacer periódicamente las pruebas vulnerabilidades y actualización de los componentes que se utilizan para consolidar la seguridad del SIVIC BOG, con el objetivo de asegurar que la infraestructura tecnológica actualmente en uso se alinee con los estándares de seguridad más exigentes, se busca reducir al mínimo los riesgos relacionados con la integridad, disponibilidad y confidencialidad de los datos de la plataforma.

10. RECOMENDACIONES

La seguridad informática es una preocupación importante para la población en general y organizaciones. En fortalecimiento de la gestión de las tecnologías de la información en el estado, el ministerio de tecnologías de la información y las comunicaciones – MINTIC, tiene publicado el Modelo de Seguridad y Privacidad de la Información (MSPI), como marco de referencia de arquitectura de tecnologías de la información, la guía de Roles y responsabilidades en entidades Públicas para estar acorde con las buenas prácticas de seguridad.

A menudo los funcionarios de la entidad de la alcaldía mayor de Bogotá, en la dependencia de la Alta Consejería para los Derechos de las Víctimas, la Paz y la Reconciliación, manipulan el sistema de información de Bogotá SIVIC BOG desde casa por el Covid-19, manejando información privada o incluso confidencial.

Es prescindible mantener la integridad, la confidencialidad y la disponibilidad de los datos, incluso la completa protección de toda la información considerada personal según la LOPD (Ley Orgánica de Protección de Datos) para evitar el espionaje por parte de personas ajenas. No divulgado, de tal manera que los roles y perfiles sean un conjunto de responsabilidades y derechos que se asignan a los usuarios en dicho sistema para controlar el acceso a los datos y las funciones garantizando la confidencialidad y privacidad de la informacion

Realizar controles de accesos, cifrado de datos y auditorías de seguridad para limitar que cualquier persona tenga acceso a los datos de las víctimas, en dado caso que sea comprometida alguna vulnerabilidad o amenaza.

El MINTIC, tiene publicado el MSPI, como arquitectura de tecnologías de la información, la guía para la Administración del Riesgo y el Diseño, Controles en entidades Públicas, y reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, como:

- Reporte No Crítico.
- Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas.
- Gestión de Incidentes de seguridad de la información
- Indicadores Gestión de Seguridad de la Información.
- Gestión inventario clasificación de activos e infraestructura crítica.
- Formato Reporte de Incidentes - CSIRT Gobierno (Versión 3).
- Documento Maestro MSPI.
- Roles y responsabilidades.

Las cuales se deben tener en cuenta para el orientar la implementación y gestión del ciclo de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), que imparte lineamientos a las entidades públicas y privadas en la implementación de buenas prácticas.

En la prueba de vulnerabilidades al sistema de información de víctimas de Bogotá – SIVIC BOG, se hallaron en su mayoría vulnerabilidades por falta de actualizaciones de parches de seguridad en el software y lenguaje de programación PHP, siendo importante mantener actualizado los sistemas operativos (Windows, OS X, Linux, etc.) incluso el software o programas que se utiliza, con los últimos parches de seguridad. Tan pronto como aparece una vulnerabilidad o un problema de seguridad en el sistema operativo o software, los ciberdelincuentes lo analizan y

encuentran formas rápidas de explotarlo para lograr sus objetivos. Por esta razón se recomienda mantener instaladas las actualizaciones en los sistemas operativos o software instalados y lenguajes de programación, antes de que un programa malicioso pueda aprovechar una vulnerabilidad y dañar, borrar o robar nuestra información, ya que es el activo más importante de una organización.

Es relevante revisar y tener actualizado periódicamente la seguridad de la información, factores de riesgo, vulnerabilidades, causas o amenazas, riesgos de seguridad digital, seguridad de la información y privacidad de la información, tipos de activos, inventario de activos de información OACPVR, valores de confidencialidad, integridad y disponibilidad en los activos de información, clasificación del activo de información OACPVR, vulnerabilidades SIVIC BOG, en los procesos, trámites, sistemas, servicios, infraestructura, los activos de información, preservando la confidencialidad, integridad, disponibilidad y privacidad de los datos.

La mejor manera de estar protegidos ante cualquier tipo de eventualidad en ataques de ciberdelincuentes, es de vital importancia hacer pruebas de vulnerabilidades periódicamente, observar e instalar las actualizaciones realizadas por el proveedor, de esta forma mitigar en lo posible las vulnerabilidades encontradas. El hecho de actualizar y ser consciente de las últimas amenazas de seguridad robustece la seguridad en cualquier sistema de información.

11. DIVULGACIÓN

Las políticas de privacidad y protección de datos personales son un aspecto crucial en el proceso de desarrollo de este trabajo de grado, de acuerdo con las leyes que lo rigen. El presente proyecto de grado será confidencial, en ejercicio de las facultades legales, en especial las conferidas por la Ley 489 de 1998, la Ley 1448 de 2011, Ley 1581 de 2015, y los Decretos 4802 de 2011 y 1083 de 2015, 1074 de 2015 y demás normas concordantes, en donde se publicará un archivo PDF correspondiente al documento final presentado ante los jurados, posterior a la sustentación de este documento.

12. BIBLIOGRAFÍA

Anónimo. “¿Qué significa el reconocimiento del conflicto armado por parte del Gobierno?” *Semana*, sección de política, 4 de mayo de 2011. Disponible en: https://www.semana.com/nacion/articulo/que-significa-reconocimiento-del-conflicto-armado-parte-del-gobierno/239313-3/.

ATEHORTÚA, et al. *Derechos humanos de la población desplazada en Colombia: evaluación de sus mecanismos de protección*. Colección textos de jurisprudencia, Centro editorial Universidad del Rosario, 2005. Disponible en: https://repository.urosario.edu.co/bitstream/handle/10336/12041/Derechos%20humanos%20de%20la%20poblacion%20dessplazada%20en%20Colombia.pdf?sequence=1.

Alcaldía Mayor de Bogotá. *Memoria, Paz y reconciliación: El centro en imágenes.* ISBN: 978-958-717-191-4. 2015. Disponible en: http://www.indepaz.org.co/wp-content/uploads/2017/09/Memoria-paz-y-reconciliaci%C3%B3n.pdf.

Baca Urbina, Gabriel. *Introducción a la seguridad informática*. Primera edición E-book, 2016. Disponible en: https://www.google.com.co/books/edition/Introducci%C3%B3n_a_la_seguridad_inform%C3%A1tic/IhUhDgAAQBAJ?hl=es&gbpv=1&dq=que+es+la+seguridad+informatica&printsec=frontcover.

Centro Nacional de Memoria Histórica. *¡BASTA YA! COLOMBIA: MEMORIAS DE GUERRA Y DIGNIDAD*. Bogotá, Colombia, 2013.

Corte Constitucional. (2004). *Sentencia T-025 de 2004*. Recuperado de

https://www.corteconstitucional.gov.co/relatoria/2004/t-025-04.html.

Departamento Nacional de Planeación. (s.f.). *Terridata*. Recuperado de https://terridata.dnp.gov.co/index-app.html#/perfiles/11001.

Galvis, et al. (2011). *Las víctimas y la justicia transicional.* Washington D.C.: ISBN 978-0-9801271-9-5. Recuperado de http://www.dplf.org/sites/default/files/1285258696.pdf

Gobierno Nacional. (1993). *Diario oficial No 41.120*. Noviembre. Recuperado de https://www.sic.gov.co/sites/default/files/normatividad/Ley_87_1993.pdf.

Ibañez, A. M., & Moya, A. (2007). *La población desplazada en Colombia: Examen de sus condiciones socioeconómicas y análisis de las políticas actuales*. ISBN: 978-958-8025-95-7. Recuperado de https://www.acnur.org/fileadmin/Documentos/Publicaciones/2008/6682.pdf?view=1

iso27000.es. (s.f.). *ISO 27000.es*. Recuperado de https://www.iso27000.es/iso27000.html.

Mediedo, M., Samper, J. M., & Cipriano de Mosquera, T. (1978). *Orígenes de los partidos políticos en Colombia*. Biblioteca Básica Colombiana. Editorial Andes, pp. 205-238.

Mesa Local de Comunicaciones Comunitaria y Alternativa Rafael Uribe. (2015). *Notas en acción*. Noviembre. Recuperado de https://www.notasdeaccion.com/2015/11/bogota-recibe-premio-exce-gel-2015-por.html.

Ministerio del Interior. (2011). *Ley de víctimas y restitución de tierras, 1448 de 2011*. Bogotá, Colombia.

Ministerio de Vivienda, Ciudad y Territorio. (2021). *Plan nacional de construcción y mejoramiento de vivienda social rural (PNVISR).* República de Colombia, Bogotá, p. 92. Recuperado de https://www.minvivienda.gov.co/sites/default/files/2021-08/plan-nacional-de-construccion-y-anexo-a-cronograma.pdf.

Oficina de Control Interno. (2020). *Informe ejecutivo: Auditoría controles generales sistema de información SIVIC BOG - Procesos de asistencia, atención y reparación integral a víctimas del conflicto armado e implementación de acciones de memoria, paz y reconciliación en Bogotá*. Recuperado de https://secretariageneral.gov.co/sites/default/files/control/informe_ejecutivo_auditoria_SIVIC%20BOG.pdf.

Ruiz, N. (2011). *El desplazamiento forzado en Colombia: una revisión histórica y demográfica*. Estudio Demográfico y Urbano, 26(1), México, ene./abr. Recuperado de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0186-72102011000100141.

Secretaría General, Alcaldía Mayor de Bogotá. (2015). *Informe de gestión y resultados 2015*. Recuperado de https://secretariageneral.gov.co/sites/default/files/documentos_ppi/2022-08/cbn-1090_informe_gestion_y_resultados_2015_0.pdf.

Sin autor. (2017). *Las víctimas cuentan, informe 9 de abril*. Alcaldía Mayor de Bogotá, informe de avance de la política pública de asistencia, atención y reparación integral a víctimas de conflicto armado, Colombia. Recuperado de http://observatorio.victimasbogota.gov.co/sites/default/files/documentos/Informe%2

09%20de%20abril%202018%20%282%29_0.pdf.

Sin autor. (s.f.). *Centro de Encuentro para la Paz y la Integración Local de Víctimas del Conflicto Armado Interno*. Recuperado de https://victimasbogota.gov.co/print/166.

Sin autor. (2018). *SIVIC BOG*. Octubre. Recuperado de https://secretariageneral.gov.co/transparencia/informacion-interes/glosario/SIVIC%20BOG.

Sistema Nacional de Atención y Reparación Integral a las Víctimas. (s.f.). *Unidad para la Atención y Reparación a las Víctimas.* Recuperado de https://www.unidadvictimas.gov.co/es/gestion-interinstitucional/sistema-nacional-de-atencion-y-reparacion-integral-las-victimas/77.

Urdinola, P. (2011). *La población desplazada interna: el caso colombiano.* Universidad de Berkeley. Recuperado de https://journals.openedition.org/alhim/525.

Vega Briceño, E. (2021). *Seguridad de la Información.* Primera edición. 3Ciencias. Recuperado de https://books.google.com.co/books?id=nx4uEAAAQBAJ&printsec=frontcover&dq=que+es+la+seguridad+de+la+informaci%C3%B3n&hl=es&newbks=1&newbks_redir=1&sa=X&ved=2ahUKEwjg4az0qbn-AhW7ZzABHSpOBxgQ6AF6BAgJEAI.

VIEWNEXT. (s.f.). *Tipos de seguridad informática*. España. Recuperado de https://www.viewnext.com/tipos-de-seguridad-informatica/.