FECHA DE EMISIÓN DEL INFORME O SEGUIMIENTO	**Día:**	20	**Mes:**	02	**Año:**	2025

1. No. DE INFORME O SEGUIMIENTO:	**5**
2. NOMBRE DEL INFORME O SEGUIMIENTO:	INFORME DE GESTION AL ACCESO A LA INFORMACIÓN PÚBLICA, ACCESIBILIDAD WEB, SEGURIDAD DIGITAL, Y DATOS ABIERTOS – RESOLUCIÓN 1519 DE 2020 MINTIC Y FURAG
3. INTRODUCCIÓN:	Este informe propone evaluar los lineamientos que deben atender los sujetos obligados para cumplir con la Resolución N°1519 de 24 de agosto de 2020 "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos" Se establecen los criterios para la estandarización de contenidos e información, accesibilidad web, seguridad digital, datos abiertos y formulario electrónico para Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD). - Directrices de accesibilidad web - Estándares de publicación y divulgación de contenidos e información. - Condiciones mínimas técnicas y de seguridad digital. - Condiciones mínimas de publicación de datos abiertos.
4. OBJETIVO:	Hacer seguimiento al cumplimiento de los lineamientos indicados en la Resolución 1519 de 2020 de MinTic en la Superintendencia de Sociedades.
5. ALCANCE:	Verificar el cumplimiento de los lineamientos establecidos por MinTIC, conforme a la Resolución 1519 de 2020: Accesibilidad Web establecidas en el Anexo 1, Estándares de publicación y divulgación de contenidos e información establecidos en el Anexo 2, Condiciones mínimas técnicas y de seguridad digital establecidos en el Anexo 3, y Condiciones mínimas de publicación de datos abiertos

	establecidos en el Anexo 4 de la Resolución 1519 de 2020, emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic), tomando como fuente la herramienta Matriz ITA (Índice de Transparencia y Acceso a la Información) y el Certificado de Confiabilidad de Accesibilidad Web de la Entidad. Efectuar el seguimiento al cumplimiento de las políticas de implementación de los criterios de accesibilidad web en las páginas de la sección de servicios al ciudadano del sitio web, que establece pautas para garantizar la accesibilidad a personas con diversas discapacidades.
6. NORMATIVIDAD:	- NTC 5854 (accesibilidad a Páginas Web) - Ley 1712 de 20214 (Transparencia y Acceso a la Información Pública) - Decreto 1078 de 2015 (Decreto Único Reglamentario del Sector de Tecnología de la Información y las comunicaciones). - Resolución 1519 de 2020 de Min TIC "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos" (Anexos 1, 2, 3 y 4) - Guía GCOM-G-001 Guía Publicación Internet Intranet - Directiva No. 006 de la Procuraduría General de la Nación "Modificación del Plazo para el diligenciamiento de la información en el índice de Transparencia y acceso a la información pública (ITA), de conformidad con el artículo 23 de la Ley 1712 de 2014" - Decreto 1862 de 2015, por el cual se corrige un yerro en la Ley 1712 de 2014". - Artículo 16 del Decreto 2106 de 2019, "Gestión documental electrónica y preservación de la información…"

7. DESARROLLO DEL INFORME O SEGUIMIENTO

En cumplimiento de la resolución 1519 de 2020, "Por la cual se definen los estándares y directrices para la publicación de la información señalada en la Ley 1712 de 2014, estableciendo los criterios para la estandarización de contenidos e información, accesibilidad web, seguridad digital, datos

7. DESARROLLO DEL INFORME O SEGUIMIENTO

abiertos y el formulario electrónico para Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD), y se definen los requisitos relativos al acceso a la información pública, accesibilidad web, seguridad digital y datos abiertos", y en coherencia con lo dispuesto en el Decreto 1078 de 2015, se busca desarrollar e impulsar el Gobierno Digital en las entidades públicas para generar mayor valor a través de lo digital, definiendo condiciones, criterios y lineamientos para las publicaciones disponibles en los portales o sitios web principales de las entidades.

Directrices de accesibilidad web
La entidad deberá cumplir con los estándares AA de la Guía de Accesibilidad de Contenidos Web (WCAG) en su versión 2.1, conforme al Anexo 1 de la resolución 1519 de 2020, aplicable en todos los procesos de actualización, estructuración, reestructuración, diseño y rediseño de sus portales web y sedes electrónicas, así como de los contenidos existentes en los mismos.

Estándares de publicación y divulgación de contenidos e información.
Deberá cumplirse con los estándares de publicación y divulgación de contenidos e información aplicables a sus sitios web y sede electrónica, establecidos en el Anexo 2 de la resolución 1519 de 2020.

Información digital archivada.
Se debe garantizar y facilitar a los solicitantes el acceso a toda la información previamente divulgada, de conformidad con el Decreto 1862 de 2015 y el artículo 16 del Decreto 2106 de 2019. Los sujetos obligados deben garantizar condiciones de conservación y/o archivo para la consulta posterior de la documentación digital disponible en sus sitios web, conforme a las Tablas de Retención Documental aprobadas de acuerdo con los lineamientos del Archivo General de la Nación.

Condiciones mínimas técnicas y de seguridad digital.
Las entidades deberán observar las condiciones mínimas técnicas y de seguridad digital definidas en el Anexo 3 de la resolución 1519 de 2020.

Condiciones mínimas de publicación de datos abiertos.
Se deberán publicar datos abiertos y agruparlos en el Portal Datos Abiertos del Estado colombiano - datos.gov.co conforme a las directrices del Anexo 4 (Requisitos mínimos de datos abiertos) de la resolución 1519 de 2020.

En cumplimiento de la resolución 1519 de 2020 y en coherencia con lo dispuesto en el Decreto 1078 de 2015, se busca desarrollar e impulsar el Gobierno Digital en las entidades públicas para generar un mayor valor a través de lo digital, definiendo condiciones, criterios y lineamientos para las publicaciones disponibles en los portales o sitios web principales de las entidades.

Anexo 1: Directrices de accesibilidad web
El Anexo 1 define los estándares de accesibilidad para garantizar el acceso autónomo e independiente de las personas con discapacidad, especialmente aquellas con discapacidad sensorial e intelectual, a los sitios web y contenidos gestionados por los sujetos obligados.

7. DESARROLLO DEL INFORME O SEGUIMIENTO

A partir del 1 de enero de 2022, los sujetos obligados deberán cumplir como mínimo con los estándares AA de la Guía de Accesibilidad de Contenidos Web (WCAG) en su versión 2.1, la cual ofrece directrices sobre cómo hacer que el contenido sea accesible para la mayoría de los usuarios, independientemente de sus condiciones personales, tecnológicas o del entorno en que se encuentren.

Los principios que orientan la accesibilidad web son los siguientes:

- Perceptible: La información y los componentes de la interfaz deben ser presentados de forma que los usuarios puedan percibirlos, incluyendo alternativas de texto, subtítulos y uso adecuado del color, entre otros.
- Operable: Los componentes de la interfaz y la navegación deben ser accesibles y operables por los usuarios, incluyendo accesibilidad mediante teclado, órdenes por voz y pantallas táctiles.
- Comprensible: Los textos deben ser legibles y claros, utilizando un lenguaje sencillo y facilitando la previsibilidad en el funcionamiento de la interfaz.
- Robusto: El contenido web debe ser interpretable por una amplia gama de usuarios y tecnologías de asistencia, incluyendo herramientas de accesibilidad.

Anexo 2: Estándares de publicación y divulgación de información
Este anexo proporciona las directrices para cumplir con los estándares de publicación y divulgación de información en los sitios web y sedes electrónicas, garantizando el acceso autónomo e independiente de las personas con discapacidad sensorial e intelectual.

Aplica a los medios electrónicos, sitios web y sedes electrónicas, y contiene los estándares de publicación y divulgación de información para cumplimiento de los sujetos obligados, en desarrollo de lo dispuesto en la Ley 1712 del 2014, parágrafo 3 del artículo 9, define que los sujetos obligados deben observar lo establecido por la estrategia de gobierno en línea en cuanto a la publicación y divulgación de la información; y en el Decreto 1081 del 2015, artículo 2.1.1.2.1.1, define que el MinTIC "expedirá los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley 1712 del 2014, con el objeto de que sean dispuestos en forma estandarizada".

Anexo 3: Condiciones mínimas técnicas y de seguridad digital
Las entidades deberán adoptar medidas para garantizar la seguridad digital y mitigar los riesgos de incidentes cibernéticos o filtración de datos personales. Algunas de las medidas incluyen:

1. Adoptar autónomamente políticas para implementar un sistema de gestión de seguridad digital y de seguridad de la información, conforme con las buenas prácticas internacionales. Entre otros podrán implementar los estándares de la familia ISO 27000 y/o los recomendados por el Instituto Nacional de Tecnología y Estándares (NIST, por sus siglas en inglés). Para cumplimiento de lo anterior se requiere la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI)

7. DESARROLLO DEL INFORME O SEGUIMIENTO

recomendado por la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

2. Las entidades públicas del orden nacional y territorial, en caso de incidentes cibernéticos graves o muy graves, conforme con los criterios de su sistema de gestión de seguridad digital y seguridad de la información, deberán reportarlos por tardar dentro de las 24 horas siguientes a su detención al CSIRT-Gobierno. Para el resto de los sujetos obligados, deberán reportar al ColCERT del Ministerio de Defensa Nacional. 1. Implementar controles de seguridad durante todo el ciclo de vida del desarrollo de software.

3. Implementar o exigir controles de seguridad relacionados con el control de la autenticación, definición de roles y privilegios y separación de funciones

4. Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).

5. Aplicar mecanismos de hardening para eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos HTTP peligrosos como put, delete, trace y restringir en lo posible la administración remota.

6. Proteger la integridad del código, mediante: (i) la validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get), Cookies (habilitar atributos de seguridad como Secure y HttpOnly), y, cabeceras HTTP; (ii) la sanitización de los parámetros de entrada: es decir, que cuando se reciba la información de dichas variables

Adicional a lo anterior y de manera específica, los sujetos obligados deberán implementar los siguientes controles en el desarrollo de sitios web y aplicaciones:

7. Ejecutar monitoreos de seguridad sobre las páginas web que contemple, entre otras, las siguientes acciones: escaneo de archivos infectados, escaneo de vulnerabilidades, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios.

8. Exigir mecanismos de autenticación dentro de los sitios web a través de la creación de contraseñas fuertes y solicitar renovaciones periódicas de las mismas garantizando la accesibilidad de persona con discapacidad.

9. Mantener actualizado el software, frameworks y plugins de los sitios web.

10. Restringir el uso de login contra ataques de fuerza bruta, implementando, entre otros: mecanismos de captcha accesibles o auto detectable, y/o limitar la tasa de intentos de login.

7. DESARROLLO DEL INFORME O SEGUIMIENTO

11. Ocultar y restringir páginas de acceso administrativo.

12. Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.

13. Crear copias de respaldo.

14. Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.

15. Garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales, para evitar la manipulación de parámetros en las peticiones. (adicional al cifrado SSL), También deben habilitar las cabeceras de seguridad, entre otras las siguientes: Content-Security-Policy (CSP), X-Content-Type-Options, X-Frame-Options, X-XSS-Protection, Strict-Transport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, Feature-Policy.

16. Proteger el binario de la aplicación, a través de métodos de ofuscación que impidan realizar procedimientos de ingeniería inversa (reversing) para analizar la lógica de la aplicación.

17. Sanitización de parámetros de entrada mediante la eliminación de etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un «script», además de la restricción de formatos y tamaños para subida de archivos.

18. Sanitización de caracteres especiales (secuencia de Escape de variables en el código de Programación)

19. Revisar las recomendaciones de seguridad en la guía de desarrollo seguro de aplicaciones y Servicios Web Seguros de la Open Web Application Security Project (OWASP).

20. Implementar en los servidores los controles necesarios (hardware o software) de protección de acceso y de ataques como Cross-site scripting, SQL injection o Denial-of-service, entre otros.

21. Incorporar validación de formularios tanto del lado del cliente como del lado del servidor.

22. Implementar monitoreos de seguridad sobre la plataforma tecnológica que hace parte del sitio web (escaneo de vulnerabilidades, escaneo de archivos infectados, análisis de patrones para detectar acciones sospechosas, verificación contra listas negras, monitoreo del tráfico para detectar ataques de denegación de servicios) y realizar las acciones de mitigación correspondientes.

23. Establecer los planes de contingencia, DRP y BCP, que permita garantizar la continuidad de la sede electrónica o del sitio web 7/24 los 365 días del año.

7. DESARROLLO DEL INFORME O SEGUIMIENTO

24. Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.

25. Implementar sistemas antivirus en el servidor web, para garantizar medidas contra infecciones de malware a los archivos del mismo.

26. Controlar el escalamiento de privilegios en los Sistemas Operativos, servidor web y Bases de datos que hacen parte de la infraestructura del portal web.

Anexo 4: Requisitos mínimos de datos abiertos
Los sujetos obligados deben disponer de una sección de datos abiertos, conforme a los lineamientos de la Guía Nacional de Datos Abiertos y la Guía de Estándares de Calidad e Interoperabilidad de Datos Abiertos.www.datos.gov.co.

Este portal especializado permite a los usuarios acceder a los datos abiertos del Gobierno colombiano con el fin de investigar, desarrollar aplicaciones, crear visualizaciones e historias que puedan ser utilizados, así como conocer las visualizaciones e investigaciones creadas a partir de dichos datos abiertos.

A continuación, se establecen los siguientes requerimientos:

1. Los sujetos obligados de niveles nacional, territorial y órganos autónomos, deben disponer de una sección de datos abiertos, incluyendo la información disponible, de acuerdo con los lineamientos de la Guía Nacional de Datos Abiertos en Colombia y la Guía de Estándares de Calidad e Interoperabilidad de Datos Abiertos, o la que haga sus veces.

2. Los sujetos obligados que cuenten con portal propio de datos abiertos deben federar o vincular la información con el Portal de Datos Abiertos www.datos.gov.co o el que haga sus veces.

3. Los datos publicados en línea por parte de los sujetos obligados de niveles nacional, territorial y órganos autónomos, deben vincularse y automatizarse para su apertura en el Portal de Datos Abiertos www.datos.gov.co o el que haga sus veces.

4. La Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones creará y publicará la Hoja de Ruta de Datos Abiertos Estratégicos para el Estado Colombiano, mediante la cual, se catalogarán los datos abiertos y sus respectivos metadatos que se consideren críticos, estratégicos o muy importantes para asegurar su permanente disponibilidad pública y actualización, por parte de los sujetos obligados de niveles nacional, territorial y órganos autónomos, en el Portal de Datos Abiertos www.datos.gov.co, o el que haga sus veces.

5. Los sujetos obligados de niveles nacional, territorial y órganos autónomos deben crear el registro de activos de información y demás instrumentos que aplique, conforme lo dispone el artículo

7. DESARROLLO DEL INFORME O SEGUIMIENTO

2.1.1.2.1.4 del Decreto 1081 del 2015, en la herramienta disponible en el Portal de Datos Abiertos datos.gov.co, o el que haga sus veces.

Para el análisis y verificación de los anexos, se desarrolló un Excel con los 4 anexos, el cual se adjunta al presente informe.

ANEXO 1

Accesibilidad Web de la Supersociedades - En cumplimiento de la Ley 1712 de 2014 y la Resolución 1519 de 2020 - MinTIC

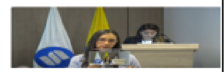
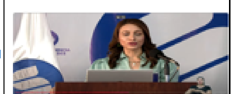
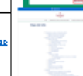
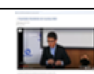
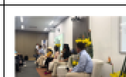
Ítem	Requisito	Cumple Si	Cumple No	Cumple N/A		Observaciones OCI / Conclusión	Recomendaciones	Evidencias	IMAGEN
	Criterios Generales de Accesibilidad Web para contenidos audiovisuales web								
1	Subtítulos o Closed Caption. A partir del 1 de enero del 2022, todos los sujetos obligados deberán incluir en el 100% de los contenidos audiovisuales (videos) nuevos la opción de subtítulos incorporados o texto escondido (closed caption) auto activable por los usuarios. Esta disposición no aplica para transmisiones en vivo y en directo.	Si				Se observa que la Entidad, ha cumplido con la aplicación de la Ley 1712 de 2014 y la Resolución 1519 de 2020	NA	https://www.youtube.com/watch?v=uSB4JiTYv6u8t=4545s	
2	Lengua de Señas Colombiana para casos específicos: A partir del 1 de enero del 2022, las entidades del Gobierno Nacional, deberán presentar sus contenidos audiovisuales con Lengua de Señas Colombiana, para los siguientes cuatro casos: alocuciones presidenciales, información sobre emergencias y desastres, información sobre seguridad ciudadana, rendición de cuentas anual de los entes centrales de cada sector del Gobierno Nacional. Esta disposición aplica para las tipologías de videos, referidas anteriormente, distribuidas en vivo y en directo, en diferido o grabados.	Si				Se observa que la Entidad, ha cumplido con la implementación del lenguaje de señas.	NA	https://www.youtube.com/watch?v=KTXHS2MP5Yr8t=4995s	
	Mapa del sitio								
3	Disponer un enlace en el pie de página del sitio web (footer) para acceder al mapa o índice del sitio, con actualización permanente, en el que se facilite la búsqueda y accesibilidad a los contenidos o temáticas incluidos en el sitio web.	Si				Se observa que la Entidad, dispone de un enlace de pie de página del sitio web.	NA	https://www.supersociedades.gov.co/	
4	Disponer de un mapa del sitio en formato XML para que sea visible a los motores de búsqueda, de forma que se facilite la accesibilidad a los usuarios.	Si				Se realiza la busqueda por el navegador del Mapa de sitio de la Supersociedades y se ubica	NA	https://www.supersociedades.gov.co/mapa_del_sitio	
	Criterios de Cumplimiento de Accesibilidad								
5	CC1 Alternativa texto para elementos no textuales: Elementos estáticos como fotografías, imágenes, diagramas, mapas y similares, como también, los sonidos cortos de alerta, vibraciones u otros que constituyen elementos no textuales, deben indispensablemente llevar un texto alternativo que cumpla con el mismo propósito que este elemento tiene para quienes lo pueden ver, escuchar o sentir.	Si				Se observa el texto alterno, al colocar el mouse sobre la imagen	Se recomienda colocar siempre los textos alternos a todas las imagenes	https://www.supersociedades.gov.co/[illegible]/proyecto-centro-estudios-societarios	
6	CC2 Complemento para videos multimedia: Se debe sincronizar la multimedia o lo audiovisual en el momento y tiempo preciso, incorporando subtitulación o lengua de señas, inclusive se puede establecer la opción de audio descripción.	Si				Los videos como rendición de cuentas, cuentan con subtitulación y lenguaje de señas.	NA	https://www.supersociedades.gov.co/videos/-/asset_publisher/cesk/content/transmisi%25C3%25B3n-rendici%25C3%25B3n-de-cuentas-2022	
7	CC3 Guía para solo video o solo audio: Los elementos de información que fueron solo video o solo audio deberán llevar, como alternativa, el texto del guion que los originó. Con ello podrá ser entendible la información por parte de muchos usuarios que no acceden al sonido o video.	Si				Los videos se trasmiten por Youtube, lo que permite ver el video y/o escuchar el audio.	NA	https://www.youtube.com/watch?v=FAUjmuTuPL8	
8	CC4 Textos e imágenes ampliables y en tamaños adecuados: Los textos e imágenes deben ser conformados de manera que puedan ser visualizados sin mayor esfuerzo, lo anterior no implica hacer los contenidos grandes, solo se requiere ser visibles a cualquier usuario. Un ejemplo de lo anterior, es disponer fuentes de texto de tamaño 12, dado que son adecuados para lectura en pantallas de computador de escritorio. Debe verificarse que los distintos contenidos puedan aumentarse de tamaño hasta un 200% mediante el navegador u otra herramienta, sin que ellos se deformen o monten, ni generen	Si				Se observa que la Entidad, ha cumplido con la aplicación de la Ley 1712 de 2014 y la Resolución 1519 de 2020	NA	https://www.supersociedades.gov.co/documents/20122/725888/07-Libro-Pronunciamientos-Administrativos-VII.pdf/4e8c7890-f855-437b-0ea3-136e6e734eda?t=1709602980295	
9	CC5 Contraste de color suficiente en textos e imágenes: El contraste de color, de forma general, debe estar dado por colores de textos e imágenes cuyos fondos sean oscuros si los colores originales son claros, o viceversa.	Si				Se observa que la Entidad, ha cumplido con la aplicación de la Ley 1712 de 2014 y la Resolución 1519 de 2020	NA	https://www.supersociedades.gov.co/documents/20122/1229118/ActividadMultinivel.pdf/5c3c8ca1-e234-00f1-1df3-9224151ea972?t=1654534029636	
10	CC6 Imágenes alternas al texto cuando sea posible: la información debe entregarse mediante texto y acompañarse con la imagen que grafique lo descrito en el texto.	Si				Se observa que la Entidad, ha cumplido con la aplicación de la Ley 1712 de 2014 y la Resolución 1519 de 2020	NA	https://www.youtube.com/watch?v=Qa0xl3jLrxc	

Imagen 1. Correspondiente a la pestaña 1 Accesibilidad del Excel Matriz_verificacion_anexos_resolucion1519-2020-SuperSoc

7. DESARROLLO DEL INFORME O SEGUIMIENTO

ANEXO 2

Superintendencia de Sociedades (en cumplimiento de la Ley 1712 de 2014 y la Resolución 1519 de 2020 - MinTIC)

Anexo No 2. Estándares de publicación y divulgación de contenidos e información.

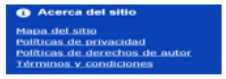
Ítem	Requisito	¿Cumple con la totalidad? Sí	No	NA	OBSERVACIONES A LA OCI - RECOMENDACIONES PARA ASEGURAR LA IMPLEMENTACIÓN DEL LINEAMIENTO (publicatoria a 31 de diciembre de 2021)	CONCLUSIÓN	RECOMENDACIÓN	ENLACE DE PUBLICACIÓN DE EVIDENCIAS	IMAGEN
1	2.1 Incluir un tap bar ubicado en la parte superior, que redireccione al Portal Única del Estado Colombiano GOV.CO	Si			Se encuentra publicado en la página el portal único del estado Colombiano.	Se observa que la Entidad, ha cumplido con incluir el portal único del estado Colombiano GOV.CO.	NA	https://www.supersociedades.gov.co/	
2	2.2 Footer a pie de página ubicado en la parte inferior del portal bajo el diseño de GOV.CO que contenga: *Imagen del Portal Única del Estado Colombiano y el logo de la marca país CO - Colombia *Nombre de la entidad, como mínimo una dirección incluyendo el departamento (si aplica) y municipio o distrito. *Vínculo a redes sociales, para ser redireccionado en las botones respectivas. La autoridad deberá, en virtud del artículo 16 del Decreto 2106 de 2019, y del capítulo V del Decreto Nacional 1080 de 2014, y demás normas expedidas por el Archivo General de la Nación relacionadas, disponer de la necesaria para que la emisión, recepción y gestión de comunicaciones oficiales, a través de las diversas canales electrónicas, se cuente un adecuado tratamiento archivístico y sean debidamente alineada con la gestión documental electrónica y de archivo digital. *Datos de contacto, incluyendo: teléfono conmutador, línea gratuita o línea de	Si			Se encuentra publicado en la página la imagen del portal único del Estado Colombiano.	Se observa que la Entidad, ha cumplido con la implementación del portal único Colombiano y el logo de la marca país.	NA	https://www.supersociedades.gov.co/	
3	2.3 publicar en el pie de página o Footer los documentos aprobados que hagan referencia a Términos y Condiciones, Política de Privacidad y Tratamiento de Datos Personales, Política de Derechos de Autor y Automatización de una Sobre los Contenidos y otros que correspondan de acuerdo con la normatividad vigente.	Si			Se evidencia el cumplimiento del numeral, el cual se encuentra en la página principal	Se está dando cumplimiento al numeral	NA	https://www.supersociedades.gov.co/	
	2.4 Habilitar como mínimo tres (3) menús destacados en el encabezado del sitio web y en la parte inferior de la barra superior Tap bar - incluyendo Transparencia y Acceso a la Información Pública, Atención y Servicios a la Ciudadanía y Participa	Si			En la página se encuentra publicado los menús destacados en el sitio web.	Se está dando cumplimiento al numeral	NA	https://www.supersociedades.gov.co/	
	* Toda documentos información, deberán ser publicados en forma cronológica del más reciente al más antiguo.	Si			Se observa que en la página de la Entidad, se encuentra publicada información de forma cronológica.	Se observa que la Entidad, ha cumplido con la información de forma cronologica, desde el más reciente al mas antiguo.	NA	https://www.supersociedades.gov.co/	
	*Los contenidos información dispuesta para los usuarios deberán ser accesibles conforme con el Anexo 1 de la presente Resolución, y utilizar un lenguaje claro.	Si			En la página se encuentra publicada la información accesible a los usuarios.	Se observa que la Entidad, ha cumplido con la información accesible para los usuarios, con lenguaje claro.	NA	https://www.supersociedades.gov.co/	
	* Se debe contar con un buscador en el que la ciudadanía pueda encontrar información, datos contenidos. Se requiere disponer de búsqueda a partir del texto del contenido, tipología, temas, subtemas, palabras claves, entre otros.	Si			Se observa la publicación del buscador en que la ciudadanía pueda encontrar información.	Se observa que la Entidad, ha cumplido con la implementación de un buscador en el que la ciudadanía pueda encontrar información, datos o contenido.	NA	https://www.supersociedades.gov.co/	

Imagen 2. Correspondiente a la pestaña 2 y 3, Anexo 2 Estándares de publicación y divulgación información del Excel Matriz_verificacion_anexos_resolucion1519-2020-SuperSoc

7. DESARROLLO DEL INFORME O SEGUIMIENTO

ANEXO 3

f vmdkctnfsbdcv tcfgxv

Anexo No. 3 de la Resolución 1519 de 2020 Condiciones Mínimas Técnicas y de Seguridad Digital

Ítem	Requisito	¿Se ejecutaron actividades			Observaciones OCI	CONCLUSIONES	RECOMENDACIONES	Evidencias
		Si	No	N/A				
	Condiciones de Seguridad Digital							
1	Adoptar autónomamente políticas para implementar un sistema de gestión de seguridad digital y de seguridad de la información, conforme con las buenas prácticas internacionales. Entre otros se podrán implementar los estándares de la familia ISO 27000 y/o los recomendados por el Instituto Nacional de Tecnología y Estándares (NIST, por sus siglas en inglés).	x			En resumen, la OCI realiza un análisis estructurado que incluye la revisión de las políticas, procedimientos, auditorías y controles que demuestran el cumplimiento de la ISO 27001 en la gestión de seguridad de la información. Este análisis asegura que la entidad no solo cumpla con la certificación, sino también con las normativas nacionales como la Ley 1712 y la Resolución 1519.	El análisis estructurado de la OCI garantiza que la entidad cumpla tanto con la ISO 27001 como con las normativas nacionales, asegurando una gestión adecuada de la seguridad de la información.	Mantener una revisión continua de políticas y procedimientos para asegurar el cumplimiento constante de las normativas y la mejora continua en la gestión de seguridad de la información.	La entidad esta certificada en ISO 27001
2	¿Se presentaron incidentes cibernéticos graves o muy graves, conforme con los criterios de su sistema de gestión de seguridad digital y seguridad de la información? De ser afirmativa la respuesta por favor indicar si fueron reportados dentro de las 24 horas siguientes a su detención a las instancia pertinentes.	x			cs az yxqgTVC BYNMGHNMIJ	La ausencia de incidentes es positiva, pero es crucial evaluar la capacidad de respuesta ante incidentes futuros para asegurar la continuidad del cumplimiento de normas y regulaciones.	Desarrollar y probar planes de contingencia y respuesta ante incidentes para garantizar una reacción efectiva ante posibles eventos que puedan comprometer el cumplimiento normativo.	No se han presentado en el año Incidentes con esa categoria
3	Implementar controles de seguridad durante todo el ciclo de vida del desarrollo de software	x			Estas acciones técnicas no solo son esenciales para la seguridad y eficiencia de los sistemas que gestionan la información pública, sino que también cumplen con los principios de acceso seguro, disponibilidad y protección de la información establecidos por la Ley 1712 y la Resolución 1519.	Las acciones técnicas son fundamentales para garantizar la seguridad y eficiencia de los sistemas, asegurando el cumplimiento de los principios de acceso seguro y protección de la información establecidos por la Ley 1712 y la Resolución 1519.	Fortalecer las medidas de seguridad y disponibilidad de los sistemas, manteniendo el cumplimiento de la normativa vigente y mejorando la protección de la información pública.	Se realiza análisis de código estadico, análisis de librería, implantación de oauth 2.0 y análisis de vulnerabilidades e implementación de métricas en el IIS
4	Implementar o exigir controles de seguridad relacionados con el control de la autenticación, definición de roles y privilegios y separación de funciones	x			El Directorio Activo (AD) de la entidad centraliza la gestión de usuarios, roles y permisos, garantizando que los funcionarios tengan acceso adecuado a las aplicaciones necesarias, en este caso el VPN, el sistema Kactus. El proceso para la asignación de permisos y creación de usuarios.	El Directorio Activo centraliza eficazmente la gestión de usuarios, roles y permisos, asegurando que los funcionarios tengan acceso adecuado a las aplicaciones críticas como el VPN y el sistema Kactus.	Optimizar el proceso de asignación de permisos y creación de usuarios, asegurando que se cumplan los principios de mínimo privilegio y revisando periódicamente los accesos para mantener la seguridad.	Permisos configurados en el LDAP,conexión por VPN y deteccion por Microsoft Entra ID 
5	Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).			X	Cuando la entidad maneja su infraestructura web de manera on-premise, sin un proveedor de hosting externo, es crucial que implemente medidas de seguridad robustas y optimice el nivel de madurez en seguridad para proteger los datos e información pública. Esto garantiza el cumplimiento de normativas como la Ley 1712 y la Resolución 1519, y refuerza la confianza de los ciudadanos en el acceso seguro a la información pública, evitando riesgos cibernéticos y asegurando la integridad de los datos gestionados internamente.	La gestión de infraestructura web on-premise requiere medidas de seguridad robustas para proteger los datos públicos, garantizar el cumplimiento de normativas y mantener la confianza ciudadana en el acceso a la información.	Implementar controles de seguridad avanzados y evaluar regularmente el nivel de madurez en seguridad para asegurar la protección de la información y minimizar los riesgos cibernéticos.	La entidad no tiene contratado servicio de hosting, ya que el portal web funciona on premise. 
6	Aplicar mecanismos de hardening para eliminar configuraciones y credenciales por defecto, además de deshabilitar métodos HTTP peligrosos como put, delete, trace y restringir en lo posible la administración remota.		x		Se verifico que al utilizar Swagger para documentar y consumir la API de un calendario de eventos no solo mejora la claridad y accesibilidad de la documentación, sino que también potencia la eficiencia del desarrollo y la integración. La capacidad de interactuar con la API de manera visual facilita la identificación de problemas y la implementación de mejoras.	El uso de Swagger para documentar y consumir la API del calendario de eventos mejora la claridad de la documentación y facilita el desarrollo, la integración y la identificación de problemas de manera visual.	Continuar utilizando Swagger para mantener una documentación accesible y actualizada, y fomentar su uso para optimizar la eficiencia en el desarrollo e integración de futuras APIs.	– 02_SwaggerCalendarioEventos.PNG
7	Proteger la integridad del código, mediante: (i) la validación exhaustiva de: inputs, variables post y get (no enviar parámetros sensibles a través del método get), Cookies (habilitar atributos de seguridad como Secure y HttpOnly), y, cabeceras HTTP. (ii) la sanitización de los parámetros de entrada: es decir, que cuando se reciba la información de dichas variables se eliminen etiquetas, saltos de línea, espacios en blanco y otros caracteres especiales que comúnmente conforman un script, además de la restricción de formatos y tamaños de subidas de archivos. (iii) la sanitización y escape de variables en el código. (iv)verificación estándar de las Políticas de Origen de las cabeceras	x			Se pudo establecer que la prohibición del Uso de Código Fuente: Según las políticas del contrato, no está permitido el uso ni la distribución del código fuente del sistema. Para asegurar que no se está accediendo o utilizando de manera indebida, se implementan las siguientes medidas: Auditorías de Seguridad, Control de Accesos y Monitoreo de Actividades	La prohibición del uso y distribución del código fuente, respaldada por políticas contractuales, se refuerza con medidas de seguridad como auditorías, control de accesos y monitoreo, lo que garantiza la protección y el cumplimiento de las normativas.	Implementar auditorías regulares y mejorar los controles de acceso y monitoreo para asegurar que el código fuente no sea utilizado de manera indebida y se mantenga la integridad del sistema.	03-04_IntegridadCodigo 03-07_Sanitizacion 03_ResticcionFormatos_tamañoArchivos
8	*Ejecutar monitoreos de seguridad sobre las páginas web que contemple, entre otras, las siguientes acciones:	x			El **WAF** (Web Application Firewall) de la entidad está diseñado para proteger las aplicaciones web de ataques comunes, como inyecciones SQL, scripting entre sitios (XSS), y denegación de servicio (DoS), mediante el filtrado y monitoreo del tráfico HTTP/HTTPS. Esto añade una capa crítica de seguridad, bloqueando amenazas antes de que lleguen a las aplicaciones internas.	El WAF de la entidad proporciona una protección eficaz contra ataques comunes en aplicaciones web, como inyecciones SQL, XSS y DoS, al filtrar y monitorear el tráfico HTTP/HTTPS, fortaleciendo la seguridad de las aplicaciones internas.	Mantener el WAF actualizado con las últimas reglas de seguridad y realizar auditorías periódicas para garantizar su efectividad en la detección y bloqueo de amenazas emergentes.	Por el WAF de la Entidad y estamos con CSIRT Gobierno
	*Escaneo de archivos infectados	x			Esta técnica es esencial en la ciberseguridad para prevenir ataques mediante la contención de potenciales amenazas antes de que afecten al sistema real.	La contención de amenazas es una técnica clave en ciberseguridad, ya que permite mitigar riesgos antes de que impacten negativamente en el sistema real.	Implementar medidas de contención de amenazas en tiempo real y realizar pruebas periódicas para garantizar que los sistemas estén protegidos contra posibles ataques cibernéticos.	 sanbox
	*Escaneo de vulnerabilidades	x			Se pudo verificar que los análisis han proporcionado un diagnóstico detallado de las vulnerabilidades, lo que permite a la entidad tomar las **medidas correctivas** necesarias para mitigar cualquier riesgo identificado y mejorando la seguridad de la infraestructura tecnológica.	El análisis detallado de vulnerabilidades ha permitido identificar riesgos y tomar medidas correctivas para mejorar la seguridad de la infraestructura tecnológica de la entidad.	Realizar análisis de vulnerabilidades de forma regular y aplicar medidas correctivas de manera oportuna para mantener una infraestructura tecnológica segura y resistente a posibles amenazas.	Se han ejecutado pruebas de vulnerabilidad en varios sitios pertenecientes al dominio de la entidad, con el fin de identificar posibles riesgos de seguridad y garantizar la integridad de nuestros sistemas. Estos análisis permitirán tomar las medidas correctivas necesarias para mitigar cualquier vulnerabilidad detectada. 
	*Análisis de patrones para detectar acciones sospechosas *Verificación contra listas negras	x			La Entidad cuenta con el **WAF** que protege las aplicaciones web que bloquean las solicitudes sospechosas basadas en patrones de ataque conocidos, mientras que el **firewall** asegura que solo el tráfico legítimo pueda llegar a los sistemas internos, al integrar los dominios maliciosos, esta refuerza su capacidad de prevención ante amenazas	El uso del WAF y firewall refuerza la seguridad de la entidad al bloquear solicitudes sospechosas y garantizar que solo el tráfico legítimo acceda a los sistemas internos, y mejorando la capacidad de prevención ante amenazas.	Mantener actualizados los patrones de ataque del WAF y revisar periódicamente las configuraciones del firewall para asegurar una protección continua y optimizada contra amenazas cibernéticas.	Por el WAF y el FW de la entidad incorporando las IP'S y Dominios en lista negras 

Imagen 3. Correspondiente a la pestaña 4, Anexo 3 Estándares de publicación y divulgación información del Excel Matriz_verificacion_anexos_resolucion1519-2020-SuperSoc

7. DESARROLLO DEL INFORME O SEGUIMIENTO

ANEXO 4

Superintendencia de Sociedades (en cumplimiento de la Ley 1712 de 2014 y la Resolución 1519 de 2020 - MinTIC)

Anexo No. 4 de la Resolución 1519 de 2020 Requisitos Mínimos de Datos Abiertos

Ítem	Requisito	¿Cumple en su totalidad? Si	No	N/A	Observaciones OCI	CONCLUSIONES	RECOMENDACIONES	Evidencia
Portal de Datos Abiertos								
1	1. Los sujetos obligados de niveles nacional, territorial y órganos autónomos, deben disponer de una sección de datos abiertos, incluyendo la información disponible, de acuerdo con los lineamientos de la Guía Nacional de Datos Abiertos en Colombia y la Guía de Estándares de Calidad e Interoperabilidad de Datos Abiertos, o la que haga sus veces.	X			Estas guías fueron desarrolladas con el objetivo de promover la transparencia, el acceso a la información pública y la reutilización de los datos por parte de la ciudadanía y otras entidades.	Estas guías refuerzan la transparencia y la confianza ciudadana, facilitando el acceso a la información pública y fomentando el uso de datos abiertos para la innovación y participación.	Asegurar la calidad y actualización de los datos publicados, promover la interoperabilidad entre plataformas y capacitar al personal para mejorar la gestión de la información pública.	https://www.datos.gov.co/browse?Informaci%C3%B3n-de-la-Entidad_Nombre-de-la-Entidad=Superintendencia+de+Sociedades&page=1
2	2. Los sujetos obligados que cuenten con portal propio de datos abiertos deben federar o vincular la información con el Portal de Datos Abiertos www.datos.gov.co o el que haga sus veces.	X			Esta practica está alineada con lo exigido por la Ley de Transparencia y Acceso a la Información Pública y las directrices de la Guía Nacional de Datos Abiertos. La publicación de estos datos en formatos abiertos permite a la ciudadanía acceder, reutilizar y redistribuir la información, promoviendo así la transparencia y el control social sobre las actividades de la Superintendencia de Sociedades. Ampliar la variedad de datos publicados y facilitar su comprensión para mejorar el acceso y la utilidad de la información para el público.	La publicaciones de datos en formatos abiertgos fortalece la transparencia y permite a la ciudadanía participar activamnte en el control de las actividades de la Supoerintendencia de Sociedades.	Ampliar la variedad de datos publicados y facilitar su comprensión para mejorar el acceso y la utilidad de la información para el público.	En la sección de Transparencia y acceso a la información del portal de la superintendencia de sociedades numeral 7 se encuentra el apartado de datos abiertos donde se vinculan los set de datos obligatorios por norma. al portal de datos abiertos. Registro de Activos de Información - Decreto 103 de 2015, art. 37 Esquema de Publicación de Información - Decreto 103 de 2015, art. 41 Índice de Información Clasificada y Reservada - Decreto 103 de 2015, art. 39 https://www.datos.gov.co/browse?Informaci%C3%B3n-de-la-Entidad_Nombre-de-la-Entidad=Superintendencia+de+Sociedades&page=1
3	3. Los datos publicados en línea por parte de los sujetos obligados de niveles nacional, territorial y órganos autónomos, deben vincularse y automatizarse para su apertura en el Portal de Datos Abiertos www.datos.gov.co o el que haga sus veces.	X			Este enfoque escalonado asegura que la información sea publicada de manera estratégica, permitiendo que se prioricen aquellos conjuntos de datos que aporten un valor significativo al acceso a la información pública, mientras se evalúa y mejora la calidad y automatización de otros data sets a lo largo del tiempo.	El enfoque escalonado permite priorizar la publicación de datos de alto valor, optimizando el acceso a informaión relevante mientras mejora la calidad.	Mantener un proceso continuo de evaluación y ajuste para garantizar que los datos prioritarios se publiquen de forma estratégica y se optimicen progresivamente.	Los data sets principales se encuentran automatizados y se encuentran publicados unos conjuntos de datos que en los seguimientos y plan de trabajo del Plan Nacional de Infraestructura de Datos se entrará a evaluar su publicación para estudiar la pertinencia de una futura automatización. https://www.datos.gov.co/browse?Informaci%C3%B3n-de-la-Entidad_Nombre-de-la-Entidad=Superintendencia+de+Sociedades&page=1
4	4. Los sujetos obligados de niveles nacional, territorial y órganos autónomos deben crear el registro de activos de información y demás instrumentos que aplique, conforme lo dispone el artículo 2.1.1.2.1.4 del Decreto 1081 del 2015, en la herramienta disponible en el Portal de Datos Abiertos datos.gov.co, o el que haga sus veces.	X			La Oficina Asesora de Planeación (OAP) es la encargada de la actualización de esta información, lo que asegura que los datos estén actualizados y cumplan con los requisitos de calidad establecidos. Dado que es necesario que estos conjuntos de datos sean compartidos en el formato estándar exigido por Datos Abiertos, la solicitud a la OAP para que facilite los datos en el formato correspondiente es adecuada y oportuna. Esto permite cargarlos correctamente en la plataforma de datos abiertos, asegurando el cumplimiento de los lineamientos de interoperabilidad, accesibilidad y reutilización de la información, en beneficio de todos los usuarios interesados.	La actgualización de datos por la OAP, asegura cumplimiento de calidad y permite que la información se publique en formatos estandarizados, facilitando el acceso para todos los usuarios.	Establecer un proceso regular de revisión y solicitud de formatos adecuados para que la OAP mantenga la calidad y disponibilidad de los datos en la plataforma de datos abiertos.	La información se encuentra publicada en el portal de datos abiertos, federada al portal de la Superintendencia de Sociedades mediante vínculos. La actualización de esta información está a cargo de la Oficina Asesora de Planeación. Solicitamos a la OAP que comparta este conjunto de datos en el formato establecido por Datos Abiertos, y así poder cargarlo como corresponde. https://www.datos.gov.co/Econom%C3%ADa-y-Finanzas/Registro-de-Activos-de-Informaci%C3%B3n/reym-ypum
Estándares de Publicación de Datos Abiertos								
5	1. Los sujetos obligados que cuenten con portales propios de datos abiertos, deberán federarlos al Portal de Datos Abiertos www.datos.gov.co o el que haga sus veces, de forma que éste último sea punto de acceso a los datos abiertos.	X			Esto implica que los conjuntos de datos vinculados desde portales institucionales, como el de la Superintendencia de Sociedades, deben estar correctamente accesibles desde datos.gov.co, de manera que los usuarios puedan acceder a toda la información pública desde un único punto centralizado. Este enfoque facilita el uso de los datos y asegura su correcta difusión. www.datos.gov.co o el que haga sus veces, de forma que éste último sea punto de acceso a los datos abiertos	Centralizar los datos en datos.gov.co mejora el acceso y difusión de la información pública, facilitando que los usuarios encuentren toda la información en un solo portal.	Asegurar que todos los datos institucionales estén correctamente enlazados y actualizados en datos.gov.co para garantizar un acceso unificado y eficaz para los usuarios.	https://www.datos.gov.co/browse?Informaci%C3%B3n-de-la-Entidad_Nombre-de-la-Entidad=Superintendencia+de+Sociedades&page=1 www.datos.gov.co o el que haga sus veces, de forma que éste último sea punto de acceso a los datos abiertos.
6	2. El registro de activos de información y el análisis de criticidad de la información, debe cargarse a través de la herramienta disponible en el Portal de Datos Abiertos, datos.gov.co, o el que haga sus veces.	X			Una vez verificada la información, se puedo establecer que los lineamientos establecidos por Datos Abiertos, solicitados formalmente a la OAP que facilitan los conjuntos de datos en el formato adecuado conforme a las directrices del portal de datos abiertos. Esto permite cargar la información correctamente y asegurar que esté disponible en los formatos establecidos para su consulta.	El cumplimiento de los lineamientos de Datos Abiertos garantiza que los datos se publiquen en formatos adecuados, facilitando su acceso y consulta en el portal de datos abiertos.	Mantener una verificación continua de los formatos y lineamientos para asegurar la correcta publicación y accesibilidad de los datos proporcionados por la OAP.	La información se encuentra publicada en el portal de datos abiertos, federada al portal de la Superintendencia de Sociedades mediante vínculos. La actualización de esta información está a cargo de la Oficina Asesora de Planeación. Solicitamos a la OAP que comparta este conjunto de datos en el formato establecido por Datos Abiertos, y así poder cargarlo como corresponde. https://www.datos.gov.co/Econom%C3%ADa-y-Finanzas/Registro-de-Activos-de-Informaci%C3%B3n/reym-ypum
7	3. Aprobar y publicar la licencia de datos abiertos, mediante la cual se determina el alcance, uso y aprovechamiento que los particulares o terceros interesados puedan efectuar sobre los mismos. En todo caso, se sugiere que la licencia reconozca la producción o generación de los datos por parte de la entidad pública, señalando que ésta no será responsable por la utilización, tratamiento, transformación de los datos, ni tampoco, sobre cualquier tipo de responsabilidad legal o económica sobre el uso directo o indirecto que se realice.	X			Se pudo verificar que los usuarios deben proporcionar una atribución adecuada, reconocer la autoría de la entidad pública que publicó el conjunto de datos, y no imponer restricciones adicionales que limiten estos derechos. Esta práctica promueve la transparencia, el acceso libre y el aprovechamiento de la información pública, asegurando que los datos abiertos sean un recurso accesible y reutilizable para todos.	La atribución adecuada de la autoría fomenta la transparencia y garantiza que los datos abiertos sean un recurso accesible y reutilizable sin restricciones adicionales	Difundir pautas claras sobre atribución para asegurar que los usuarios respeten la autoría y aprovechen los datos públicos de manera responsable y libre.	Las publicaciones en el portal de datos abierto están resguardadas bajo el licenciamiento Creative Commond V4 https://creativecommons.org/licenses/by-sa/4.0/legalcode

Imagen 4. Correspondiente a la pestaña 5, Anexo 4 datos abiertos del Excel Matriz_verificacion_anexos_resolucion1519-2020-SuperSoc

Dado al alcance del seguimiento a cada uno de los numerales de los anexos, se adjunta el siguiente Excel, al presente informe: Matriz_verificacion_anexos_resolucion1519-2020-SuperSoc.

8. RECOMENDACIONES

En el archivo Excel "Matriz_verificacion_anexos_resolucion1519-2020-SuperSoc", se encuentran algunas observaciones/conclusiones y recomendaciones sobre los numerales evaluados de los Anexos 1, 2, 3 y 4.

Para continuar con el cumplimiento y mejora del Anexo 1 (Accesibilidad), se recomienda:

- Incluir siempre textos alternativos para todas las imágenes y documentos publicados en la página web.
- Actualizar las migas de pan en sitios y micrositios.
- Mantener actualizado el buscador de la página web para garantizar la eficiencia en las búsquedas.

En relación con el Anexo 2 (Requisitos de Identidad Visual y Estándares de Publicación), se recomienda:

- Continuar cumpliendo con la normativa vigente sobre publicaciones.
- Actualizar los logos, además de los procesos y procedimientos de la entidad.
- Mantener actualizados los directorios en caso de cambios.
- Mantener actualizado y publicado el directorio de servidores públicos.

Para el Anexo 3 (Seguridad Digital), se recomienda:

- Realizar una revisión continua de las políticas y procedimientos para asegurar el cumplimiento de la normativa y mejorar la gestión de la seguridad.
- Desarrollar y probar planes de contingencia y respuesta ante incidentes para garantizar una reacción efectiva ante posibles eventos que comprometan el cumplimiento normativo.
- Fortalecer la seguridad y disponibilidad de los sistemas, asegurando el cumplimiento de la normativa vigente y mejorando la protección de la información pública.
- Optimizar el proceso de asignación de permisos y creación de usuarios, garantizando el cumplimiento del principio de mínimo privilegio y realizando revisiones periódicas para mantener la seguridad.
- Implementar controles de seguridad avanzados y evaluar regularmente el nivel de madurez en seguridad para proteger la información y minimizar riesgos cibernéticos.
- Continuar utilizando herramientas como Swagger para mantener una documentación accesible y actualizada, así como realizar auditorías periódicas y mejorar los controles de acceso y monitoreo.
- Mantener el firewall WAF actualizado con las últimas reglas de seguridad, realizar auditorías periódicas para garantizar su efectividad, y aplicar medidas de contención de amenazas en tiempo real para proteger los sistemas contra ataques cibernéticos.
- Realizar regularmente el análisis de vulnerabilidades y la aplicación de medidas correctivas oportunas, ayudará a mantener una infraestructura tecnológica segura.
- Implementar soluciones específicas para la mitigación de ataques DDoS, como servicios de protección en la nube.

8. RECOMENDACIONES

- Asegurar que, el archivo README esté actualizado con los cambios en el calendario y que el archivo Excel incluya todos los eventos relevantes.
- Mantener un sistema de autenticación robusto, realizar auditorías regulares de acceso, y proporcionar capacitación periódica al personal sobre políticas de seguridad, son medidas clave.
- Mantener copias de seguridad actualizadas y realizar pruebas periódicas de recuperación para garantizar su efectividad.
- Mantener las configuraciones de firewall actualizadas, realizar análisis regulares para detectar y neutralizar posibles amenazas y establecer procedimientos claros para la actualización controlada de aplicaciones.
- Contribuir a mejorar la seguridad y la experiencia del usuario, mediante la implementación de procesos automáticos de sanitización de datos y el seguimiento de las recomendaciones de seguridad en el desarrollo de aplicaciones y servicios web.

En cuanto al Anexo 4 (Datos Abiertos), se recomienda:

- Asegurar la calidad y actualización de los datos publicados, promover la interoperabilidad entre plataformas y capacitar al personal para mejorar la gestión de la información pública.
- Ampliar la variedad de datos publicados y facilitar su comprensión para mejorar el acceso y la utilidad de la información para el público.
- Mantener un proceso continuo de evaluación y ajuste para garantizar la publicación estratégica de los datos prioritarios, así como establecer un proceso regular de revisión y solicitud de formatos adecuados para que la OAP mantenga la calidad y disponibilidad de los datos en la plataforma de datos abiertos.
- Asegurar que, todos los datos institucionales estén correctamente enlazados y actualizados en datos.gov.co, garantizando un acceso unificado y eficaz para los usuarios.
- Realizar una verificación continua de los formatos y lineamientos para asegurar la correcta publicación y accesibilidad de los datos, y difundir pautas claras sobre atribución para asegurar el uso responsable de los datos públicos.
- Actualizar regularmente el plan de apertura para incluir nuevos conjuntos de datos y documentar claramente los procedimientos de carga para facilitar su seguimiento y mejora continua.

Se sugiere aplicar estas recomendaciones para continuar cumpliendo con los lineamientos establecidos en la Resolución 1519 de 2020 de Min TIC.

9. CONCLUSIONES

Es pertinente realizar los ajustes necesarios en el sitio web de manera oportuna, tomando como referencia las observaciones y oportunidades de mejora registradas en el presente informe, las cuales están alineadas con los estándares de Accesibilidad, Publicación y Divulgación de Información, Seguridad Digital Web y Requisitos Mínimos de Datos Abiertos del MinTIC.

Se cumple con los 36 numerales del Anexo 1, correspondientes a Accesibilidad.

Se cumple con los 50 numerales del Anexo 2, correspondientes a Requisitos de Identidad Visual y Estándares de Publicación.

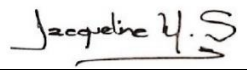
De los 38 numerales del Anexo 3, correspondiente a Seguridad Digital, el numeral 5 y el numeral 22 no aplican, los numerales 6 y 12 no se están cumpliendo en la Entidad y los restantes 34 numerales se están cumpliendo adecuadamente.

Se cumple con los 8 numerales del Anexo 4, correspondientes a Datos Abiertos.

Como conclusión, se puede evidenciar que la Superintendencia de Sociedades está cumpliendo con la aplicación de las recomendaciones y lineamientos de los Anexos 1, 2, 3 y 4 de la Resolución 1519 de 2020 de Min TIC.

Para constancia se firma en Bogotá D.C., a los 20 días del mes de febrero del año 2025

10. RESPONSABLE DEL INFORME O SEGUIMIENTO

Nombre Completo	Responsabilidad	Firma
Jacqueline Murillo Sanchez	Jefe de Oficina de Control Interno	
Diana Paola Aguasaco Munevar	Auditora