Anexo 3
Resolución MinTIC 1519 del 2020
Estándares de publicación y divulgación información

El presente anexo contiene las condiciones mínimas técnicas y de seguridad digital aplicables a los sujetos obligados en sus sitios web:

Anexo 1			Cumple	Observación
3.2 CONDICIONES DE SEGURIDAD DIGITAL	A	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) recomendado por la Dirección de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.	SI	La Agencia tiene implementado el Modelo de Seguridad y Privacidad de la Información.
	B	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.	SI	La Agencia cuenta con un procedimiento para la gestión de incidentes de seguridad, en el cual se establece la comunicación con el ColCERT en caso de materialización de incidentes críticos y altos.
	1	Implementar controles de seguridad durante todo el ciclo de vida del desarrollo de software	SI	La Agencia implementa controles de seguridad en todas las fases del ciclo de vida del desarrollo de software, con el fin de mitigar riesgos desde el diseño hasta la operación de los sistemas.
	2	Implementar o exigir controles de seguridad relacionados con el control de la autenticación, definición de roles y privilegios y separación de funciones	SI	La Agencia implementa y exige controles de seguridad que incluyen mecanismos de autenticación, definición de roles y privilegios, así como la separación de funciones, con el fin de garantizar el acceso adecuado y minimizar los riesgos asociados al uso indebido de los sistemas

	3	Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).	SI	La Agencia exige al proveedor de hosting el cumplimiento de medidas de seguridad robustas, incluyendo políticas actualizadas y un nivel de madurez en seguridad alineado con las mejores prácticas del sector.
	4	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	SI	La Agencia aplica mecanismos de hardening en sus sistemas, eliminando configuraciones y credenciales por defecto, deshabilitando métodos HTTP inseguros como PUT, DELETE y TRACE, y restringiendo la administración remota para reducir la superficie de exposición
	5	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; y (v) la verificación y comprobación del token de CSRF (cuando aplique).	SI	La Agencia realiza pruebas de vulnerabilidades que permiten identificar fallos relacionados con la integridad del código, como entradas no validadas, cookies sin atributos de seguridad, cabeceras HTTP mal configuradas, carga de archivos sin restricciones adecuadas y ausencia de tokens CSRF. Estas pruebas permiten detectar y corregir riesgos como inyecciones, XSS y otras amenazas que comprometen la seguridad de las aplicaciones
	6	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	SI	La Agencia cuenta con un sistema de monitoreo de seguridad a través de su infraestructura de SIEM y el apoyo del SOC, lo cual permite ejecutar acciones como: escaneo de archivos potencialmente maliciosos, identificación de vulnerabilidades, análisis de patrones de comportamiento para detectar actividades sospechosas, verificación contra listas negras y monitoreo del tráfico en tiempo real para la detección de posibles ataques de denegación de servicios (DoS o DDoS)
	7	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	SI	Cuando aplica, la Agencia exige la implementación de mecanismos de autenticación en los sitios web, que incluyan la creación de contraseñas fuertes y su renovación periódica, asegurando en todo momento la accesibilidad para personas con discapacidad.
	8	Mantener actualizado el software, frameworks y plugins de los sitios web.	SI	La Agencia mantiene actualizados el software, los frameworks y los plugins utilizados en los sitios web, cuando aplica, con el fin de

				corregir vulnerabilidades, mejorar el rendimiento y garantizar la seguridad y estabilidad de las plataformas digitales
	9	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.	PARCIALMENTE	El portal de la entidad no cuenta actualmente con mecanismos CAPTCHA u otras medidas visibles para la limitación de intentos de acceso. No obstante, se revisará la pertinencia de su implementación cuando aplique, en función del tipo de servicios ofrecidos y el nivel de exposición del portal.
	10	Ocultar y restringir páginas de acceso administrativo	SI	La Agencia oculta y restringe, las páginas de acceso administrativo mediante controles de autenticación, segmentación de red y otras medidas de seguridad, con el fin de prevenir accesos no autorizados y proteger los entornos críticos.
	11	Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.	SI	La Agencia restringe, cuando aplica, la escritura de archivos desde la web mediante la asignación de permisos de solo lectura, con el fin de minimizar el riesgo de modificaciones no autorizadas y proteger la integridad de la información y de los entornos web.
	12	Crear copias de respaldo.	SI	La Agencia crea y mantiene copias de respaldo de la información y los servicios críticos, como parte de su estrategia de continuidad del negocio y recuperación ante incidentes
	13	Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.	SI	La Agencia almacena, cuando aplica, trazas o logs de auditoría que registran eventos de seguridad, accesos (logins) y otras actividades relevantes, con el fin de garantizar la trazabilidad.
	14	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.	PARCIALMENTE	La Agencia garantiza, conexiones seguras en sus portales mediante el uso de certificados digitales y protocolos SSL/TLS (HTTPS), con el fin de proteger la integridad y confidencialidad de la información, y reforzar la confianza de los usuarios. Adicionalmente, se emplea cifrado en la estructura de las peticiones para prevenir la manipulación de parámetros en entornos transaccionales. No se incluye cabeceras de seguridad como CSP o X-Frame-Options.
	15	Implementar mensajes genéricos de error, que no revelen información acerca de la tecnología usada, excepciones o parámetros que dispararon el error específico, los cuales deberán ser comprensibles por parte de las personas, incluyendo la accesibilidad para las personas con discapacidad	PARCIALMENTE	La Agencia implementa, cuando aplica, mensajes de error genéricos que no revelan detalles sobre la tecnología utilizada, excepciones internas o parámetros específicos que hayan generado el error.

	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.	SI	La Agencia protege, las aplicaciones evitando que su funcionamiento interno pueda ser expuesto o analizado por terceros no autorizados. Para ello, se utilizan mecanismos que dificultan la manipulación o comprensión del código, reduciendo así el riesgo de usos indebidos.
	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	SI	Se establecen restricciones sobre el formato y tamaño de los archivos que pueden ser cargados, con el fin de prevenir riesgos de seguridad
	18	Sanitización de caracteres especiales (secuencia de Escape de variables en el código de Programación)	SI	La Agencia aplica, cuando corresponde, procesos de limpieza y control sobre los caracteres especiales utilizados en el código, con el fin de evitar que puedan ser interpretados de forma maliciosa o generar comportamientos no deseados en las aplicaciones.
	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).	SI	La Agencia realiza análisis de vulnerabilidades en sus aplicaciones considerando las recomendaciones establecidas por la guía de desarrollo seguro de aplicaciones y servicios web seguros de OWASP. Estas prácticas permiten identificar y mitigar riesgos comunes de seguridad, alineándose con los estándares internacionales del desarrollo seguro
	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	SI	La Agencia implementa medidas de protección en sus servidores para evitar accesos no autorizados y prevenir ataques que puedan afectar el funcionamiento o la seguridad de los sistemas, como la alteración de información o la sobrecarga de los servicios
	21	Incorporar validación de formularios tanto del lado del cliente como del lado del servidor	SI	La Agencia incorpora, cuando aplica, validaciones en los formularios tanto en el navegador del usuario como en los servidores, con el fin de asegurar que la información ingresada sea correcta y proteger los sistemas ante posibles usos indebidos
	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.	SI	La Agencia cuenta con un sistema de monitoreo de seguridad a través de su infraestructura de SIEM y el apoyo del SOC, lo cual permite ejecutar acciones como: escaneo de archivos potencialmente maliciosos, identificación de vulnerabilidades, análisis de patrones de comportamiento para detectar actividades sospechosas, verificación contra listas negras y monitoreo del tráfico en tiempo real para la detección de posibles ataques de denegación de servicios (DoS o DDoS)

	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.	SI	La Agencia cuenta con planes de contingencia, recuperación ante desastres (DRP) y continuidad del negocio (BCP) debidamente aprobados.
	24	Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados	SI	La Agencia restringe, la escritura de archivos en el servidor web mediante la asignación de permisos adecuados según los roles y privilegios definidos, con el fin de prevenir modificaciones no autorizadas y proteger la integridad de la información.
	25	Implementar sistemas antivirus en el servidor web, para garantizar medidas contra infecciones de malware a los archivos del mismo.	SI	La Agencia cuenta con soluciones de seguridad tipo endpoint implementadas en sus servidores web, que permiten detectar y prevenir infecciones por malware, garantizando así la protección de los archivos y la integridad de los servicios publicados.
	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.	SI	La Agencia controla, cuando aplica, el escalamiento de privilegios en los sistemas operativos, servidores web y bases de datos que conforman la infraestructura del portal, mediante la asignación adecuada de roles, la aplicación del principio de mínimos privilegios y el monitoreo de actividades sospechosas, con el fin de prevenir accesos indebidos o elevación no autorizada de permisos
	27	Realizar análisis estático del código con el objetivo de identificar vulnerabilidades que se encuentra en la programación de las aplicaciones	PARCIALMENTE	Aunque la Agencia realiza pruebas de vulnerabilidades como parte de su estrategia de seguridad, el análisis estático del código fuente se lleva a cabo de manera parcial.
	28	Cumplir con la estandarización de código fuente para portales web, siguiendo las buenas prácticas del W3C (World Web Wide Consortium), de forma que permita la correcta visualización de la información a los usuarios.	PARCIALMENTE	La Agencia cumple parcialmente con la estandarización del código fuente en su portal web, conforme a las buenas prácticas definidas por el World Wide Web Consortium (W3C). Aunque la información es accesible y funcional para la mayoría de los usuarios, se evidencian aspectos que requieren mejoras técnicas para alcanzar una conformidad completa. Entre estos se destacan observaciones relacionadas con la validación del código, el uso adecuado de elementos semánticos y el cumplimiento de lineamientos de accesibilidad. Asimismo, se detectan advertencias menores en la validación HTML/CSS que podrían afectar la visualización en ciertos navegadores o dispositivos.
	29	Adoptar validadores HTML y CCS para la continua revisión del sitio web y su mejora continua, a través de las buenas prácticas del W3C (World Web Wide Consortium).	PARCIALMENTE	La Agencia cumple parcialmente con la estandarización del código fuente en su portal web, conforme a las buenas prácticas definidas por el World Wide Web Consortium (W3C). Aunque la información es accesible y funcional para la mayoría de los

				usuarios, se evidencian aspectos que requieren mejoras técnicas para alcanzar una conformidad completa. Entre estos se destacan observaciones relacionadas con la validación del código, el uso adecuado de elementos semánticos y el cumplimiento de lineamientos de accesibilidad. Asimismo, se detectan advertencias menores en la validación HTML/CSS que podrían afectar la visualización en ciertos navegadores o dispositivos.
	30	Cumplir con los estándares definidos para la integración al Portal Único del Estado Colombiano GOV.CO, incluyendo la validación de la codificación, en caso de que les aplique.	SI	La Agencia cumple a los estándares definidos para la integración al Portal Único del Estado Colombiano – GOV.CO. Se han implementado adecuadamente los lineamientos de codificación, estructura, navegación e interoperabilidad establecidos, garantizando la alineación con los requerimientos del ecosistema GOV.CO y facilitando el acceso unificado a los servicios e información institucional.
	31	Incluir lenguaje común de intercambio para la generación y divulgación de la información y datos estructurados y no estructurados dispuestos en medios electrónicos, como los sitios web de los sujetos obligados y el Portal Único del Estado Colombiano GOV.CO, en caso de que les aplique	SI	La Agencia cumple a los estándares definidos para la integración al Portal Único del Estado Colombiano – GOV.CO. Se han implementado adecuadamente los lineamientos de codificación, estructura, navegación e interoperabilidad establecidos, garantizando la alineación con los requerimientos del ecosistema GOV.CO y facilitando el acceso unificado a los servicios e información institucional.
	32	Implementar un sistema de control de versiones (Git), que permitan planear y controlar la vida de la aplicación, y en una fase a mediano plazo poder implementar un sistema de integración, cambio y despliegue continuo.	SI	La Agencia cuenta con un sistema para llevar el control de las versiones del portal web, lo que permite organizar y dar seguimiento a los cambios que se realizan en su desarrollo.

La presente se expide al 24 de julio de 2025.

SINDY VANESSA RIVERA SANCHEZ
JEFE OFICINA ASESORA DE SISTEMAS Y TECNOLOGÍAS DE INFORMACIÓN