De conformidad con lo dispuesto en los Decretos 2482 de 2012, 1499 de 2017, de creación y actualización del Modelo Integrado de Planeación y Gestión, Políticas de Gobierno Digital y Seguridad Digital, la ITRC cumple con los criterios definidos en el Anexo 3 de la Resolución 1519 de 2020.

N°	REQUERIMIENTO	DESCRIPCIÓN DEL CUMPLIMIENTO
1	Implementar controles de seguridad durante todo el ciclo de vida del desarrollo de software.	El portal ya se encuentra en producción. No se tiene programado ningún desarrollo adicional por el momento para el mejoramiento de alguna funcionalidad, sin embargo, en caso de requerirse algún tipo de ajustes, se cuenta con un sandbox. El procedimiento incluye que una vez superadas todas las pruebas, se pasa a producción. En caso de que algo salga mal, se realiza el procedimiento de Rollback.
2	Implementar o exigir controles de seguridad relacionados con el control de la autenticación, definición de roles y privilegios y separación de funciones.	Como rol único y principal, se tiene una cuenta de administrador sobre el CMS del portal. Desde esta cuenta se carga todo el contenido de interés del público a nivel interno (Intranet) y externo (página web)
3	Exigir medidas de seguridad al proveedor del hosting (políticas de seguridad robustas y un nivel de madurez en seguridad optimizado).	No se tiene hosting, se cuenta con servidores propios, alineados con las políticas de seguridad de la Información en la entidad.
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.	Se eliminaron usuarios alternos al principal, se aseguró el CMS dando los permisos correspondientes para usuario público y administrador en caso de requerir subir información. Se cuenta con las actualizaciones de plugins y core.
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 6 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).	El CMS cuenta con la seguridad correspondiente para el envío seguro de la información y se asegura que el perfil público esté limitado.

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.	El monitoreo y protección se realiza a través de FortiWeb, FortiSandbox y FortiGate. (Escaneo de vulnerabilidades no se realiza)
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.	Se tiene solo el usuario necesario para la administración del CMS, y se cambia de contraseña cada 3 meses por seguridad, aplicando las recomendaciones para contraseñas seguras.
8	Mantener actualizado el software, frameworks y plugins de los sitios web.	Se encuentra actualizado
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.	Se tiene control de login a 5 intentos.
10	Ocultar y restringir páginas de acceso administrativo.	Las páginas de interés interno o del personal administrativo se tiene asegurado.
11	Restringir la escritura de archivos desde la web a través de la asignación de permisos de solo lectura.	Los permisos asignados a las carpetas del CMS en el servidor web, son las recomendadas de acuerdo con el fabricante.
12	Crear copias de respaldo.	Se cuenta con copias de respaldo.
13	Almacenar trazas o logs de auditoría de los eventos de seguridad, logins, entre otros.	Se aseguran los logs desde la parte administrativa únicamente y de acuerdo con el rol asignado para la administración de esto archivos.
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[1]Transport-Security (HSTS), Public-Key-Pins (HPKP) Referrer-Policy, Feature[1]Policy.	Se encuentra Implementado en la Agencia ITRC.

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.	Se encuentra Implementado en la Agencia ITRC.
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.	Se tiene asegurado el servidor web desde el código e infraestructura
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.	Se encuentra Implementado en la Agencia ITRC.
18	Sanitización de caracteres especiales (secuencia de Escape de variables en el código de Programación) 7.	Se encuentra Implementado en la Agencia ITRC.
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).	No se cuenta con desarrollo de software
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.	Se encuentra Implementado en la Agencia ITRC.
21	Incorporar validación de formularios tanto del lado del cliente como del lado del servidor.	Se encuentra Implementado en la Agencia ITRC.
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.	El monitoreo y protección se realiza a través de Fortiweb, forti sandbox y fortigate. (Escaneo de vulnerabilidades no se realiza)
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.	DRP se puede dar por cumplidlo, pero BCP no hay continuidad como tal en el momento.
24	Restringir la escritura de archivos en el servidor web a través de la asignación de permisos de roles y los privilegios asociados.	Se encuentra Implementado en la Agencia ITRC.

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.	Se encuentra Implementado en la Agencia ITRC.

Firmado digitalmente por MILTHON CESAR LONDOÑO JURADO
Fecha: 2023.08.29 17:03:57 '-05'00

_____

MILTHON CESAR LONDOÑO JURADO
JEFE OFICINA ASESORA DE TECNOLOGÍAS DE LA INFORMACIÓN