Clasificación de la Información: Publica ☐ Reservada ☐ Clasificada ☒

1. OBJETIVO

Establecer y estandarizar las actividades para identificar, prevenir y tratar las vulnerabilidades técnicas a los que están expuestos los componentes de la infraestructura tecnológica o activos de información de la Agencia de Desarrollo Rural.

2. ALCANCE

Todos los componentes de infraestructura tecnológica o activos de información de la Agencia de Desarrollo Rural.

3. MARCO NORMATIVO APLICABLE

- Decreto 767 de 2022 - 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
- Resolución número 500 de marzo 10 de 2021 Ministerio de Tecnologías de la Información y Comunicaciones de Colombia (MINTIC) Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

4. DEFINICIONES

- **Activo de Información:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la entidad.
- **Amenaza:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la entidad.
- **Infraestructura Tecnológica:** Plataformas de cómputo utilizadas para proporcionar servicios de conexión a usuarios internos y externos y proveedores en un ambiente digital (servidores, computadores de escritorio, computadores portátiles, dispositivos de Internet, etc.). Servicios de telecomunicaciones que proporcionan conectividad de datos, voz y video. Servicios de administración de datos que almacenan y administran datos corporativos y proporcionan la capacidad de analizar los datos.
- **Ingeniería Social:** Técnicas especializada o empírica del uso de acciones estudiadas o habilidades sociales (tales como: la influencia, la persuasión y la sugestión), que buscan directa o indirectamente que un usuario revele información sensible o adopte conductas riesgosas sin estar consciente de los riesgos que esto implica.
- **Prueba de vulnerabilidades:** Práctica de identificar brechas de seguridad en los activos de información y obtener información confidencial haciendo uso de la manipulación de usuarios legítimos.
- **Remediación:** Corrección de las debilidades o vulnerabilidades en un sistema, aplicación, red o infraestructura tecnológica
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

5.1. ROLES Y RESPONSABILIDADES EN EL PRESENTE DOCUMENTO

Los roles encargados de llevar a cabo una adecuada gestión de vulnerabilidades son:

- **Oficial De Seguridad De La Información:** Ejecutar pruebas internas de vulnerabilidad o estructurar el proceso para que un tercero las ejecute a conformidad con las necesidades de la Agencia de Desarrollo Rural, así mismo, comunicar las vulnerabilidades a los responsables para ejecutar las actividades de remediación en las aplicaciones o servicios que tengan dichas debilidades.
- **Tercero/Proveedor:** Ejecutar las pruebas de vulnerabilidad contratadas por la agencia de acuerdo con las necesidades y el alcance establecido en el contrato.
- **Gestores de Aplicaciones:** Realizar desarrollos o ajustes en las aplicaciones de la Agencia de Desarrollo

Clasificación de la Información: Publica ☐ Reservada ☐ Clasificada ☒

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

Rural para mitigar las vulnerabilidades identificadas.

- **Gestor de Infraestructura:** Realizar ajustes en los servidores o equipos de cómputo de forma masiva con el objetivo de mitigar las posibles vulnerabilidades identificadas.
- **Gestor de Redes:** Realizar ajustes en los equipos de comunicaciones con el objetivo de mitigar las posibles vulnerabilidades identificadas.
- **Gestor de Bases De Datos:** Realizar configuraciones, actualizaciones y/o ajustes en los equipos de comunicaciones con el objetivo de mitigar las posibles vulnerabilidades identificadas.
- **Administrador de seguridad:** Realizar configuraciones, actualizaciones y/o ajustes en los equipos de seguridad perimetral con el objetivo de mitigar las posibles vulnerabilidades identificadas.

5.2. LINEAMIENTOS GENERALES

Para la identificación de vulnerabilidades técnicas de los activos de información de la entidad, es responsabilidad exclusiva de la Oficina de Tecnologías de la información, la cual, para la identificación realizara las siguientes acciones:

- Los responsables de la administración de cada plataforma verificaran de manera periódica la información publicada por parte del fabricantes o foros de seguridad en relación con nuevas vulnerabilidades identificadas o tiempo de salida de soporte que puedan afectar los sistemas de información de la Entidad.

- Se deberá realizar como mínimo una (1) prueba de vulnerabilidad al año, dichas pruebas deberán ser realizadas por un ente independiente, con el fin de garantizar la objetividad del desarrollo de estas, en caso contrario, el responsable de seguridad de la información podrá efectuarlas.

- Los desarrollos o servicios que sean contratados por la Agencia de Desarrollo Rural, y que tengan una exposición pública en Internet, deberán incluir y aprobar un proceso de análisis de vulnerabilidades y ethical hacking que debe ser asumido por el proveedor contratado. Sin lo anterior no se deberá permitir la liberación del sistema de información en un entorno productivo.

La ejecución de planes preventivos o correctivos que requieran ser aplicados en la infraestructura tecnológica, derivados de la identificación de vulnerabilidades técnicas, son responsabilidad de los colaboradores que administren dicha infraestructura tecnológica. Lo anterior, aplicando los lineamientos del PROCEDIMIENTO GESTIÓN DE CAMBIOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

No está permitido el uso de herramientas de escaneo o explotación de vulnerabilidades dentro de la entidad, ni la ejecución de ningún tipo de análisis o prueba por parte de entidades externas o usuarios de la entidad sin previa autorización de la Alta Dirección, Jefe de la Oficina de Tecnología de la Información o del Responsable de Seguridad de la Información, de evidenciarse lo anterior, se deberá aplicar el PROCEDIMIENTO GESTIÓN DE EVENTOS, INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

5.3. PLANIFICACIÓN Y APROBACIÓN DEL PLAN DE PRUEBAS DE VULNERABILIDADES

Las pruebas de vulnerabilidad para la infraestructura tecnológica siempre deben tener como fin el detectar y mitigar las vulnerabilidades que estén presentes en la infraestructura tecnológica.

De conformidad a lo anterior, Las pruebas de vulnerabilidad independiente de que sean contratadas o realizadas por la entidad, el responsable de seguridad de la información deberá definir un programa de evaluación de vulnerabilidades que debe ser ejecutado para la infraestructura tecnológica y sistemas de información seleccionados. Este plan debe contar con los siguientes elementos:

Clasificación de la Información: Publica ☐ Reservada ☐ Clasificada ☒

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

- Dispositivos que van a ser cubiertos dentro de las pruebas.
- Alcance de las pruebas sistemas de información y equipos en la red de datos
- Tipo de pruebas a realizar (Externas, Internas, con o sin conocimiento del dispositivo).
- Nivel de explotación de vulnerabilidades (Detección, explotación intrusiva, negación de servicio, entre otros).
- Implicaciones y consideraciones a tener en cuenta antes, durante y después de las pruebas realizadas a los dispositivos.

El programa de evaluación de vulnerabilidades propuesto por el Oficial de Seguridad de la Información será revisado y aprobado por el Jefe de la Oficina de Tecnologías de la Información.

5.4. SELECCIÓN DE PROVEEDOR PARA LA EJECUCIÓN DE LAS PRUEBAS

Las pruebas de vulnerabilidad pueden ser realizadas directamente por el oficial de seguridad de la información o un proveedor externo seleccionado por la entidad. Sin embargo, no se debe repetir el ejecutor de las pruebas, en periodos consecutivos, es decir, el mismo proveedor no deberá realizar dos pruebas de vulnerabilidad seguidas, a menos que el proceso de contratación por temas de la selección así lo determine.

5.5. EJECUCIÓN DE PRUEBAS DE VULNERABILIDAD

El ejecutor de las pruebas debe realizar un plan para el cumplimiento del programa de evaluación de vulnerabilidades, donde se establezca un cronograma detallado de fechas y horario de las actividades. Así mismo, debe entregar informe de pruebas de vulnerabilidad, recomendaciones y pruebas finales de verificación.

De evidenciarse alguna vulnerabilidad critica en la ejecución de la prueba, se debe reportar inmediatamente al Jefe de la Oficina de Tecnología o al Oficial de Seguridad de la Información para tomar acción inmediata sobre la misma.

Una vez finalizada la etapa de pruebas, el ejecutor debe consolidar la información recopilada y generar un informe técnico que debe ser entregado al jefe de la Oficina Tecnología de la Información y un informe con un resumen gerencial para ser presentado a la Alta Dirección.

El informe técnico presentado debe contemplar los siguientes aspectos:

- Dispositivos cubiertos en las pruebas.
- Evidencia recopilada.
- Vulnerabilidades identificadas e impacto estimado.
- Recomendaciones para cierre de vulnerabilidades.

Si el proceso de análisis de vulnerabilidades es realizado por la Entidad, quedará bajo responsabilidad de la Oficina Tecnología de la Información la generación de los planes de acción para la implementación de las recomendaciones realizadas. En caso contrario de ser contratado, se realizará proceso de remediación, conforme a lo establecido en el anexo técnico.

El informe deberá ser remitido al responsable de la gestión de riesgos para alimentar las debilidades o vulnerabilidades detectadas en incluirlas como riesgos de seguridad digital en la Matriz de Riesgos y con lo anterior documentar el plan de tratamiento.

NOTA: EL informe de vulnerabilidades se deberá tratar como información RESERVADA, únicamente estará

Clasificación de la Información: Publica ☐ Reservada ☐ Clasificada ☒

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

bajo custodia del responsable de Seguridad de la Información y el jefe de la Oficina Tecnología información.

5.6. REMEDIACIÓN DE VULNERABILIDADES

Toda identificación de vulnerabilidades deberá ser remediada o se le deben implementar medidas compensatorias. El responsable del activo de información que presente vulnerabilidades será encargado de desplegar, coordinar o ejecutar las acciones, recomendaciones que se requieran, y deberá retroalimentar el avance.

En dado caso que para la implementación de acciones compensatorias o de remediación se requiera hacer un cambio en la infraestructura, se deberá proceder conforme al PROCEDIMIENTO GESTIÓN DE CAMBIOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

5.7. SISTEMAS DE INFORMACIÓN PUBLICADOS EXTERNAMENTE

Todos los sistemas de información que sean modificados o adquiridos y que estén publicados externamente, se les deberá realizar un análisis de vulnerabilidades antes de su paso a producción, la anterior actividad podrá ser realizada por un proveedor contratado o el responsable de seguridad de la información.

El responsable de la gestión de infraestructura deberá validar que antes de la liberación y publicación del servicio externamente, que se hayan realizado las pruebas de vulnerabilidades y remediado las mismas.

5.8. REVISIONES PERIÓDICAS DE ALERTAS DE SEGURIDAD

El personal del Grupo de Seguridad de la Información de la Oficina de Tecnología de la Información realizará verificación de alertas de seguridad emitidas por organizaciones y foros de seguridad de la información de orden nacional e internacional con el fin de verificar vulnerabilidades y eventos de seguridad que se hayan presentado o que sean susceptibles de ocurrencia.

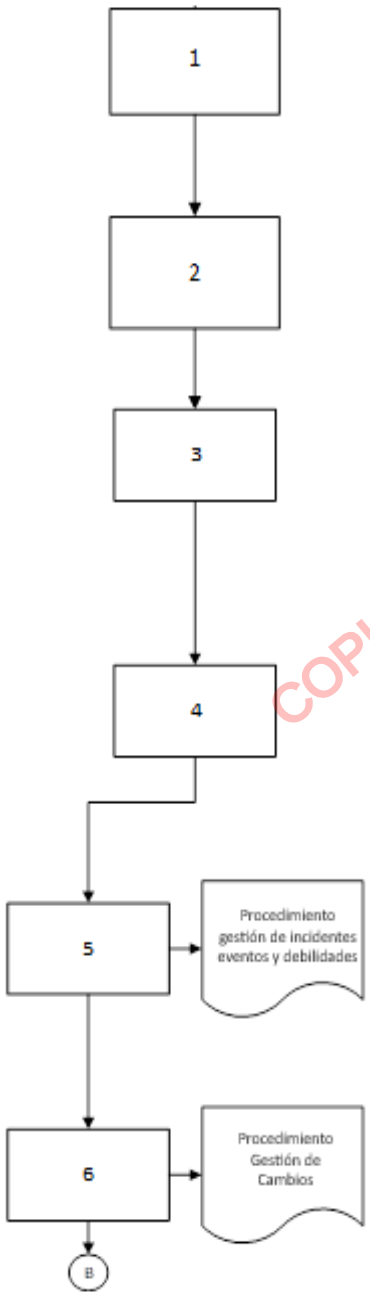
En caso de encontrar información crítica respecto a amenazas o vulnerabilidades que puedan afectar la infraestructura tecnológica, se debe generar una comunicación al Jefe de la Oficina Tecnología de la Información y comunicar la debilidad conforme al PROCEDIMIENTO GESTIÓN DE EVENTOS, INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN, con el fin de que se tomen inmediatamente las acciones preventivas necesarias para evitar algún impacto a las infraestructura tecnológica de la Entidad.

En caso de materializarse una vulnerabilidad se deben seguir los lineamientos establecidos en el PROCEDIMIENTO GESTIÓN DE EVENTOS, INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN.

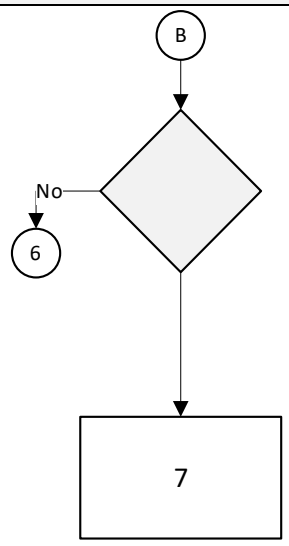
6. DESARROLLO

SIMBOLO							
SIGNIFICADO	Terminador (Inicio o Fin de un proceso)	Actividad	Decisión (si o no)	Conector de página	Conector (Conector con otros procesos)	Línea de flujo (Dirección y sentido del plujo del proceso)	Documento

Clasificación de la Información: Publica ☐ Reservada ☐ Clasificada ☒

DIAGRAMA DE FLUJO	No.	ACTIVIDAD	RESPONSABLE	REGISTRO
	1	Definir el alcance de las pruebas para los sistemas de información que sean objeto de los análisis de vulnerabilidades, para diseñar los planes.	Oficial de Seguridad de la Información (OTI)	Documento programa de evaluación de vulnerabilidades
	2	Ejecutar las pruebas definidas en los planes. NOTA: Si en el proceso de ejecución se identifica una vulnerabilidad critica o de alto impacto, se deberá comunicar inmediatamente para la remediación y no se debe esperar hasta el final para notificar.	Oficial de Seguridad de la Información (OTI) Proveedor/Tercero (Entidad Contratada)	Informe de ejecución de análisis de vulnerabilidades
	3	Consolidar la evidencia obtenida y generar los informes técnicos y gerenciales de las pruebas de vulnerabilidad.	Oficial de Seguridad de la Información (OTI) Proveedor/Tercero (Entidad Contratada)	Informe de ejecución de análisis de vulnerabilidades
	4	Presentar a la Alta Dirección un informe gerencial que muestre el resultado del Ethical Hacking y las vulnerabilidades más críticas para la entidad, de allí se informará a la alta dirección que se iniciará la ejecución de actividades para remediación o mitigación de las vulnerabilidades encontradas. En el mismo se deberán presentar las vulnerabilidades que no pueden ser solucionadas por que se requiere recursos financieros o de personal. Lo anterior con el objetivo que la alta dirección evalué la asignación de recursos o la aceptación del riesgo.	Jefe OTI (OTI) Oficial de Seguridad de la Información (OTI) Alta Dirección	Acta de comité de gestión y desempeño institucional
	5	Documentar la generalidad de las vulnerabilidades encontradas conforme lo indica el PROCEDIMIENTO GESTIÓN DE EVENTOS, INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN	Gestor de riesgos del SGSI (OTI)	Matriz gestión de riesgos de seguridad digital
	6	Ejecutar los planes de acción para mitigar las vulnerabilidades, empleando el respectivo PROCEDIMIENTO GESTIÓN DE CAMBIOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Gestores de Aplicaciones (OTI) Todos los Responsables de Componentes (OTI)	Solicitudes de cambio

Clasificación de la Información: Publica ☐ Reservada ☐ Clasificada ☒

DIAGRAMA DE FLUJO	No.	ACTIVIDAD	RESPONSABLE	REGISTRO
		¿Fueron cerradas adecuadamente las vulnerabilidades? SI - Fueron cerradas, ejecutar la actividad 7 NO - Ejecutar la actividad 6 y realizar nuevas actividades de remediación	Oficial de Seguridad de la Información (OTI) Proveedor/Tercero (Entidad Contratada)	
	7	Generar el informe donde se indique formalmente el cierre de las vulnerabilidades con base a las acciones ejecutadas por la Oficina de Tecnologías de la Información. **FIN DEL PROCEDIMIENTO**	Oficial de Seguridad de la Información (OTI) Proveedor/Tercero (Entidad Contratada)	Informe de remediación de vulnerabilidades técnicas.

7. DOCUMENTOS ASOCIADOS

- POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
- PROCEDIMIENTO GESTIÓN DE CAMBIOS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN
- PROCEDIMIENTO GESTIÓN DE EVENTOS, INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1.0	23/05/2014	Primera versión del documento

ELABORÓ	REVISÓ	APROBÓ
Nombre: Hugo Alejandro Casallas Larrotta **Cargo:** Contratista **Dependencia:** Oficina de Tecnologías de la información	**Nombre:** Oscar Luis Felipe Pedraza Quintero **Cargo:** Contratista **Dependencia:** Oficina de Tecnologías de la información **Nombre:** Walter Silva Combita **Cargo:** Contratista **Dependencia:** Oficina de Planeación	**Nombre:** Olga Lucia Morales Nova **Cargo:** Jefe Oficina de Tecnología de la Información **Dependencia:** Oficina de Tecnología de la Información