Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

1. OBJETVO

Establecer las actividades para la respuesta y gestión efectiva de eventos, incidentes y debilidades de seguridad de la información que puedan presentarse en la Agencia de Desarrollo Rural (ADR), protegiendo los activos de seguridad de la información y minimizando los posibles impactos que puedan afectar la operación de la entidad.

2. ALCANCE

Aplica a los eventos o situaciones que puedan clasificarse como evento de seguridad, debilidad o incidente de seguridad de la información que afecten o puedan poner en riesgo la seguridad de la información y por lo tanto la continuidad de las operaciones de la ADR.

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 500 de marzo 10 de 2021 Ministerio de Tecnologías de la Información y Comunicaciones (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 seguridad de la Información:** se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.
- **Confidencialidad:** Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Cambio**: Cualquier adición, reemplazo, modificación o eliminación que afecte la infraestructura tecnológica productiva de la entidad.
- **Debilidad:** Vulnerabilidad de un activo o control que puede ser explotada por una o más amenazas.
- **Disponibilidad**: Es uno de los pilares de la seguridad de la información y este indica que la información pueda estar accesible y utilizable cuando lo requiera un usuario autorizado.
- **Evento de Seguridad de la Información**: Acontecimiento identificado en el estado de un sistema, servicio o red que indica un posible incumplimiento o falla en las políticas o controles de seguridad de la información o de una situación desconocida que puede ser relevante para la seguridad. (En este punto si bien existe una situación, la misma no ha afectado la integridad, disponibilidad o confidencialidad).
- **Incidente de Seguridad de la Información:** Uno o una serie de eventos de seguridad de la información inesperados o no deseados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (Se ha impactado por lo menos uno de los pilares de seguridad de la información, disponibilidad, confidencialidad o integridad).
- **Integridad**: Es uno de los pilares de la seguridad de la información y este conlleva el mantenimiento de la exactitud, completitud y confiabilidad de la información.
- **Requerimiento**: Este proceso se refiere a todas las solicitudes que generan los usuarios y que no están asociadas a un incidente en un servicio.

COPIA CONTROLADA

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

5.1. ROLES Y RESPONSABILIDADES EN EL PROCEDIMIENTOS DE EVENTOS, INCIDENTES Y DEBILIDADES DE SEGURIDAD DE LA INFORMACIÓN.

Los roles encargados de llevar a cabo una adecuada gestión de incidentes, eventos y debilidades de seguridad de la información son:

Este documento es fiel copia del original que reposa en el sistema de información de la Agencia de Desarrollo Rural. Su impresión se considera copia no controlada.

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

- Funcionarios de la Oficina de Tecnología de la Información
- Gestor de incidentes de seguridad de la información
- Oficial de Seguridad de la información.
- Gestor de Riesgos de Seguridad de la Información

Las responsabilidades se encuentran detalladas en las actividades de este procedimiento.

5.2. COMUNICACIÓN Y DOCUMENTACIÓN INICIAL DE LA SITUACIÓN

Cuando cualquier funcionario, contratista o terceras partes identifiquen un incidente, evento o debilidad de seguridad de la información, es imperativo notificarlo de manera inmediata al Grupo TIC utilizando uno de los siguientes medios de comunicación disponibles:

- Plataforma de Mesa de Ayuda.
- Teléfono (601) 7482227 extensión 5900.
- Correo electrónico dirigido a cualquier miembro de la Oficina de Tecnología de la Información.
- En persona, mediante una visita a las oficinas de la Oficina de Tecnología de la Información.

Adicionalmente, en aquellos casos donde sea pertinente, la Oficina de Tecnología de la Información notificara al funcionario que potencialmente esté involucrado en el evento o incidente de seguridad de la información. Dicha notificación se llevará a cabo a través de correo electrónico o mediante la herramienta de Mesa de Ayuda.

COPIA CONTROLADA

El funcionario de la Oficina de Tecnología de la Información que identifique o que reciba el reporte del incidente, evento o debilidad por un medio diferente a la mesa de ayuda, será el responsable de generar el respectivo caso o incidente en la plataforma de Mesa de Ayuda con el fin de iniciar la gestión pertinente y mantener un registro completo de las situaciones reportadas.

Para los eventos y debilidades reportadas se deberá generar un caso de requerimiento de soporte categorizado como evento o debilidad, el mismo será asignado al Oficial de Seguridad. Para los incidentes de seguridad de la información que sean remitidos por los usuarios, por medio de la mesa de ayuda como un caso de soporte. El funcionario que sea designado para resolver la situación generara el respectivo incidente en la mesa ayuda para continuar con la gestión de este.

5.3. CLASIFICACIÓN DE EVENTOS, DEBILIDADES O INCIDENTES

Sera responsabilidad del responsable asignado de resolver la situación, verificar que la misma se encuentre bien clasificada. De no estar correctamente clasificada, deberá solicitar al Administrador de Mesa Ayuda, la reclasificación de esta y reasignación según sea el caso.

5.3.1. Clasificación de criticidad de eventos de seguridad

Si la situación presentada se considera un evento de seguridad de la información, las acciones a realizar se determinarán de acuerdo con las siguientes escalas:

- **Evento de criticidad Baja:** Posibles anomalías o situaciones detectadas por los sistemas de información y/o personas que puedan ser relevantes para la seguridad de la información. Con el fin de evitar que el evento vuelva a ocurrir se deberá implementar controles y verificar si se encuentra en planes de concientización o si se requiere una comunicación específica para la situación.

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

- **Eventos de Criticidad Media:** Son eventos que no comprometen la operación normal de los activos de información, procesos o servicios, es decir, que pueden ser controlados en forma paralela a la operación por parte del ingeniero especialista.

- **Evento de criticidad Alta:** Implica el daño de un activo y el posible incumplimiento de una política de seguridad pero que no presenta resultados negativos en cuanto a la afectación de los pilares de seguridad de la información. Con el fin de evitar que el evento vuelva a ocurrir se deberá realizar una solicitud de acción de mejora.

5.3.2. Debilidades de seguridad de la información

Si la situación presentada se considera una debilidad de seguridad de la información se procederá a remitir la situación presentada al responsable de la gestión de riesgos de seguridad de la información. Quien evaluara que este identificada como unas vulnerabilidades o para que sea incluido en la matriz de riesgos de seguridad digital del proceso y formular el plan de tratamiento correspondiente.

5.3.3. Clasificación de criticidad de incidentes de seguridad

Si la situación presentada se considera un incidente de seguridad de la información deberá indicarse su impacto de acuerdo con los siguientes niveles de criticidad:

COPIA CONTROLADA

Tabla 1. Clasificación de criticidad de incidentes de seguridad de la información

NIVEL	DESCRIPCIÓN
Extenso	Situación de seguridad que implican un paro total o suspensión de las operaciones del negocio por un tiempo prolongado
Significativo	Situación de seguridad que comprometen la operación normal de algunos procesos del negocio, pero que pueden ser controlados en forma paralela al desarrollo de las demás actividades del negocio
Moderado	Situación que comprometen la integridad, confidencialidad o disponibilidad de las operaciones del negocio de forma muy leve, y que por lo tanto no requieren una acción inmediata
Menor	Situación que comprometen la integridad, confidencialidad y/o disponibilidad a un grupo localizado de usuarios o que causan un impacto muy limitado de las operaciones del negocio, y que por lo tanto no requieren una acción inmediata
Soporte	Eventos que no comprometen las operaciones del negocio y que afectan a solo un usuario y que por lo tanto pueden tramitarse como un REQUERIMIENTO o SOLICITUD DE CASO DE SOPORTE.

Fuente: Elaboración propia

Así mismo, si el incidente es de impacto EXTENSO y afecta todos los servicios establecidos por el proceso de Gestión de Tecnologías de la Información y las Comunicaciones en forma crítica; la Alta Dirección, el Jefe de Tecnología de la Información o el Gestor de Continuidad de Negocio, podrán activar el Plan de Recuperación Tecnológica (DRP) que haya definido la entidad.

En caso de que la situación reportada sea un incidente repetitivo, el Oficial de Seguridad de la información,

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

deberá escalar el caso al Gestor de problemas, quien con el colaborador encargado de la infraestructura o sistema de información afectado deberá realizar las actividades necesarias para establecer la causa raíz del incidente.

Las situaciones que serán catalogadas como incidente, serán las que se encuentren en el nivel Extenso, Significativo, Moderado y menor. Las demás situaciones serán catalogadas como casos de soporte de usuario y deberán ser cargadas como un caso o requerimiento en la mesa de ayuda.

Los incidentes se deberán cargar por la opción de Incidente de la Mesa de Ayuda para que sean asignadas de forma automática al Gestor de Incidentes, quien procederá con la verificación y clasificación del incidente según sea el caso.

5.4. ASIGNACIÓN DEL INCIDENTE

Una vez se realice la clasificación del Incidente, el Gestor de Incidentes, procederá a realizar la asignación de este a los colaboradores de la Oficina de Tecnología de la Información, quienes serán los encargados de documentar las acciones de corrección, acompañar en el proceso de análisis de causas, establecimiento y ejecución de plan de mejora, y lecciones aprendidas.

COPIA CONTROLADA

5.5. GESTIÓN DEL INCIDENTE

Revisar si la situación se ha presentado previamente consultando la Base de Datos de Conocimiento y ejecutar las tareas allí indicadas.

Si es una situación nueva, se deberá realizar un análisis inicial de la situación e iniciar con la implementación de las siguientes acciones:

5.5.1. Acciones de contención

Las acciones de contención de un incidente de seguridad son pasos críticos que se deben tomar para minimizar el daño e impactos. Cuando se encuentra en proceso un incidente el colaborador designado para apoyar la solución del incidente, se podrá apoyar en el Grupo de Seguridad de la Información y los demás colaboradores del proceso de la Oficina de tecnología de la Información según sus roles para la ejecución de las actividades requeridas.

Si bien las actividades de contención dependen del tipo de incidente presentado. Se debe tener en cuenta los siguientes aspectos según aplique:

a. **Identificación y Aislamiento:** En esta etapa, se detecta el incidente y se toman medidas inmediatas para detener su propagación y limitar su alcance. Esto implica aislar la amenaza, desconectar sistemas comprometidos o segmentar la red para evitar que el incidente se propague.
Nota: Para la contención si se requiere realizar algún cambio en la infraestructura o configuración, se podrá acudir a los cambios de emergencia conforme a lo establece el Procedimiento Gestión de Cambios de Seguridad de la Información.

b. **Contención de la actividad maliciosa:** Si el incidente está relacionado con una actividad maliciosa, se busca contener y detener lo antes posible. Esto puede implicar bloquear direcciones IP, deshabilitar cuentas comprometidas o eliminar malware.

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

Nota: Todas las acciones que se ejecuten para la contención, desde el ticket del escalamiento y las diversas configuraciones que se realicen, deberán tenerse en cuenta para ser documentadas posteriores a la contención del incidente.

c. **Preservación de la evidencia:** Durante la contención, también se debe tener cuidado de preservar la evidencia relacionada con el incidente. Esto es fundamental para investigaciones futuras y posibles acciones legales.

Nota: Con el objetivo de preservar la evidencia, se debe hacer un registro constantemente el detalle de las acciones realizadas para contención y corrección sin omitir las diferentes actividades ejecutadas, desde acciones de cambios en el hardware, escalamiento a proveedores hasta la configuración de los sistemas.

5.5.2. Acciones de corrección

Corresponde a las medidas que una organización debe tomar después de la contención del incidente de seguridad, para solucionar los problemas y prevenir futuros incidentes similares.

a. **Restauración de la funcionalidad:** Una vez que el incidente está bajo control y aislado, se procede a trabajar en la restauración de la funcionalidad normal del sistema o servicio afectado. Esto puede implicar la restauración desde copias de seguridad limpias.
b. **Implementación de medidas de seguridad adicionales:** Se identifican las vulnerabilidades que permitieron el incidente y se toman medidas para parchear o corregir esas vulnerabilidades. Además, se implementan mejoras en la seguridad para prevenir futuros incidentes similares.

COPIA CONTROLADA

5.5.3. Plan de acción de mejora

Una vez se han recuperado los servicios y el mismo se encuentra estable, se iniciará las actividades de documentación. Estas iniciaran con la respuesta y ejecución de las siguientes preguntas y acciones, que deberán ser respondidas por el colaborador que se haya designado para apoyar la solución del incidente:

1. ¿Por qué sucedió o a que se atribuye el problema?
2. Documente y enumere el paso a paso que se ejecutó para la contención y corrección de la situación, desde el escalamiento a proveedores (Evidencia imágenes, pantallazos, números de Ticket) y las acciones o cambios ejecutados tanto en hardware como en software.
3. ¿Se cuenta con controles para detectar o identificar este tipo de situaciones?
4. Alternativas para prevenir que se vuelva a presentar el incidente
5. Duración de la afectación de los servicios en horario hábil (Fecha y hora de inicio y finalización)

Con la información proporcionada, se establecerá una base para que el colaborador designado, con el respaldo del Gestor de Incidentes, realice un análisis de la causa raíz y proceda a definir un plan de acción, así como a llevar a cabo las actividades necesarias para prevenir o mitigar el riesgo de que el incidente vuelva a ocurrir en la infraestructura tecnológica.

Para el análisis de causas, se podrá utilizar técnicas o herramientas como lluvia de ideas, los 5 porqués o espina de pescado. Así mismo, se podrán utilizar las herramientas que se establezcan en el Sistema Integrado de Gestión de la ADR, para la gestión de acciones correctivas o de mejora.

- Si el incidente es reiterativo o no tiene una causa o solución conocida se escala a un problema y deberá ser gestionado en el procedimiento de **PR-GTI-017 GESTIÓN DE PROBLEMAS DE**

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

SEGURIDAD DE LA INFORMACIÓN.

- Si la solución del incidente es realizar o ejecutar un cambio, se debe actuar de acuerdo con lo establecido en el procedimiento **PR-GTI-002 GESTIÓN DEL CAMBIO DE SEGURIDAD DE LA INFORMACIÓN**.

- Si se exceden las capacidades técnicas del funcionario asignado puede contarse con recursos adicionales como proveedores, fabricantes o autoridades pertinentes para la contención de este.

Una vez gestionado el incidente, debe procederse a una fase de monitoreo para verificar el comportamiento de este durante un periodo de tiempo específico.

5.5.4. Monitoreo del incidente

Una vez ejecutadas las acciones necesarias para contener y erradicar el incidente, se deberá iniciar con el Monitoreo de este, para verificar que la situación ha sido controlada adecuadamente, el monitoreo del incidente se deberá realizar por al menos tres (3) semanas, para poder proceder a su cierre.

Si el incidente se presenta nuevamente se deberá volver a gestionar el mismo hasta encontrar nuevas soluciones y la verdadera causa raíz.

COPIA CONTROLADA

5.5.5. Cierre del incidente

Una vez se establece la solución del incidente, se debe realizar al cambio de estado de este, indicando la finalización de las actividades y la afectividad de estas, posteriormente se ejecutará el costeo del incidente si el mismo tiene un nivel mayor a moderado o según sea solicitado por el Jefe de la Oficina de tecnología.

5.5.6. Costear el incidente

Una vez se lleve a cabo el proceso de cierre del incidente se deberá costear el mismo. Para ejecutar el coste se deberá emplear el formato para **F-GTI-004 COSTEO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.**

El informe de costos de incidentes debe ser retroalimentación a la alta dirección, por parte del jefe de tecnología de la información en la revisión por la dirección que se realice anualmente al Subsistema de Gestión de Seguridad y Privacidad de la Información.

5.6. APOYO DE TERCEROS EN LA GESTIÓN DE INCIDENTES

Cuando el incidente desborde las capacidades de atención del profesional asignado por parte de la Oficina de Tecnología de la Información y las comunicaciones TIC, el mismo podrá apoyarse en los proveedores o terceras partes, como entidades de gobierno.

Para establecer los posibles contactos, podrá acudir al formato F-GTI-005 Contactos con Autoridades y Grupos de Interés del Sistema de Gestión de Seguridad De La Información. Donde se encuentran documentados las autoridades y proveedores que actualmente tiene contratados la ADR, para el soporte y mantenimiento de su plataforma tecnológica.

Las acciones, solicitudes o escalamiento que se realice a terceros, deberán ser contemplado en la gestión y seguimiento del incidente, por lo cual deberá ser documentados como parte de las acciones de corrección con su

Este documento es fiel copia del original que reposa en el sistema de información de la Agencia de Desarrollo Rural. Su impresión se considera copia no controlada.

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

respectiva evidencia.

5.6.1. CONSERVACIÓN DE EVIDENCIA DE INCIDENTES DE SEGURIDAD

Si bien la conservación de evidencia en casos de incidentes de seguridad es de relevancia crítica para facilitar una investigación adecuada, es necesario que este proceso se realice de manera que se priorice la operación continua de la entidad. La preservación y custodia de evidencia debe llevarse a cabo con la debida consideración, de modo que se minimicen las posibles interrupciones, permitiendo así que la organización pueda mantener sus operaciones en curso, al tiempo que garantiza la integridad de la información necesaria para una investigación efectiva.

Así mismo, en la ejecución de actividades de contención o corrección del incidente no se pedirá que se documente inmediatamente la gestión continua de las actividades. Sin embargo, es responsabilidad del colaborador asignado para la gestión del incidente, llevar una bitácora o un desglose de las diferentes acciones que se vayan ejecutando para posteriormente documentarlas de forma detallada.

5.6.2. LECCIONES APRENDIDAS

El Gestor de Incidentes según el tipo de incidente, determinara si el mismo requiere la generación de lecciones aprendidas, en cuyo caso como mínimo se deberán incluir los siguientes aspectos:

- **Descripción del incidente:** Detalles de lo que sucedió para que el incidente se hiciera evidente.
- **Causa Raíz:** Identificación de la causa principal que provocó el incidente.
- **Acciones de solución:** Explicación de las medidas tomadas para restaurar el servicio o resolver el incidente.
- **Lecciones aprendidas:** Recomendaciones sobre las acciones a seguir para prevenir la recurrencia del incidente o minimizar su impacto.

COPIA CONTROLADA

Si el incidente puede ser utilizado a modo de concientización, se comunicará a todos los funcionarios del Ministerio de Transporte, con el fin de evitar su recurrencia.

5.6.3. CONTACTOS CON AUTORIDADES Y GRUPOS DE INTERÉS

Con el propósito de permitir que la entidad lleve a cabo una gestión eficiente de situaciones o eventos que puedan surgir, así como de las distintas instancias de la política de seguridad y su relación directa con grupos de interés y autoridades, ya sea para la gestión o reporte de incidentes, la mejora continua, la retroalimentación y la adquisición de conocimiento por parte de la ADR en relación a las mejores prácticas en seguridad de la información, así como para recibir alertas tempranas relacionadas con ataques y vulnerabilidades, junto con su posible mitigación o solución, además de obtener acceso a asesoramiento en materia de seguridad de la información.

Se establece la necesidad de identificar y documentar las autoridades y grupos de interés, los cuales deben ser registrados en el **F-GTI-005 CONTACTO CON AUTORIDADES Y GRUPOS DE INTERÉS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**. Conforme a lo anterior es responsabilidad del Grupo de Seguridad de la Información de la Entidad, documentar los aspectos relacionados con autoridades. Y el demás personal de la Oficina de Tecnología de la Información, debe documentar y mantener actualizado el listado de contactos con proveedores o terceras partes con los que el proceso de Gestión de Tecnología de la Información y las Comunicaciones tenga contratos, acuerdos o convenios vigentes.

Así mismo dentro de este formato y con base a la normatividad vigente, se deberá establecer y documentar

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

5. CONDICIONES GENERALES PARA EL DESARROLLO DEL PROCEDIMIENTO

que tipos de incidentes deberán ser reportados o escalados a las autoridades correspondientes.

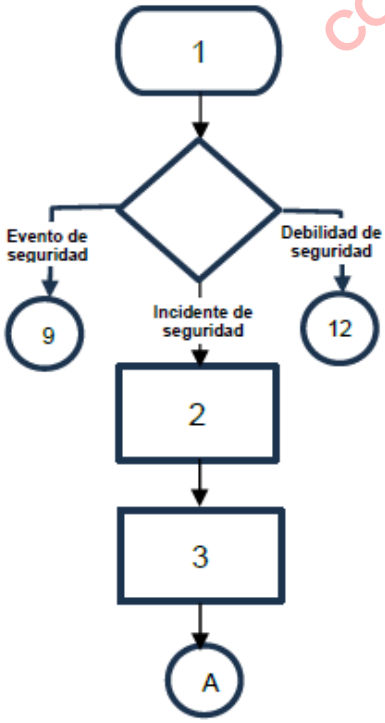
5.6.4. VERIFICACIÓN

El Oficial de Seguridad podrá solicitar en cualquier momento, la generación de un reporte de los incidentes de seguridad ocurridos y el estado actual de los mismos. Así mismo, podrá revisar la concordancia de la información reportada por los diferentes colaboradores en el formato de Autoridades y Grupos de Interés del Sistema de Gestión de Seguridad De La Información, con el fin de verificar la adecuada gestión de estos y generar el informe correspondiente.

6. DESARROLLO

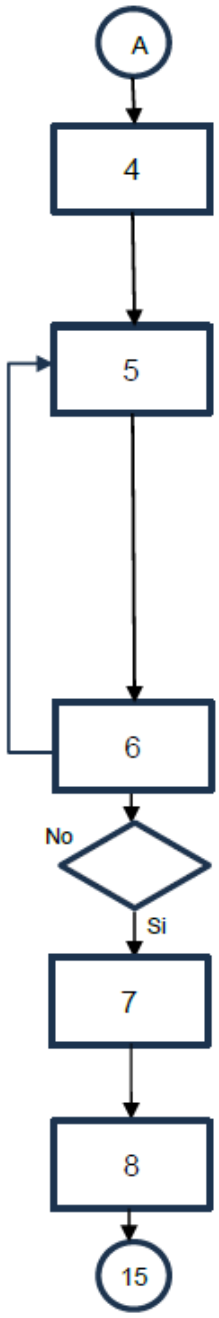
SIMBOLO							
SIGNIFICADO	Terminador (Inicio o Fin de un proceso)	Etapa de proceso	Decisión (si o no)	Conector (Conector con otros procesos)	Línea de flujo (Dirección y sentido del plujo del proceso)	Documento	Símbolo de comentario o nota

COPIA CONTROLADA

DIAGRAMA DE FLUJO	No.	ACTIVIDAD	RESPONSABLE	REGISTRO
	1	Reportar la situación considerada como evento, incidente o debilidad de seguridad de la información. por medio de los medios definidos en el número 5.1. COMUNICACIÓN Y DOCUMENTACIÓN INICIAL DE LA SITUACIÓN, y verificación por parte del funcionario de tecnología para realizar clasificación.	Usuarios ADR	Ticket de mesa de ayuda Correo electrónico Incidente de mesa de ayuda
		¿El evento se clasifica como? **Incidente de seguridad:** Continuar a la actividad 2 **Evento de seguridad:** ir a la actividad 9 **Debilidad de seguridad:** ir a la actividad 12	Funcionario de la Oficina de Tecnología de la Información	
	2	Crear un incidente en la mesa de ayuda y se asigna de forma automática al Gestor de Incidentes de seguridad de la información.	Funcionario de la Oficina de Tecnología de la Información	Incidente mesa de ayuda
	3	Asignar el incidente en la plataforma de mesa de ayuda al funcionario que tenga la pertinencia para la documentación, gestión y respuesta. Así mismo notificara al Oficial de Seguridad de la información	Gestor de incidentes de seguridad de la información.	Incidente mesa de ayuda

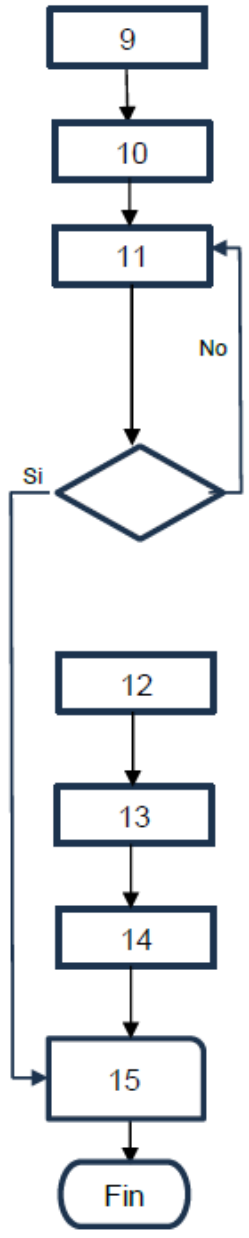
Este documento es fiel copia del original que reposa en el sistema de información de la Agencia de Desarrollo Rural. Su impresión se considera copia no controlada.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

DIAGRAMA DE FLUJO	No.	ACTIVIDAD	RESPONSABLE	REGISTRO
	4	Ejecutar acciones de erradicación, corrección y/o contención según corresponda. En este punto se apoyará en los proveedores o personal del Grupo TIC o entidades de gobierno para reporte del incidente y solicitud de apoyo. Así mismo según los impactos asociados podrá acudir a la ejecución de cambios de urgencia según lo establezca el **PROCEDIMIENTO GESTIÓN DE CAMBIOS DE SEGURIDAD DE LA INFORMACIÓN.**	Funcionario asignado de la Oficina de Tecnología de la Información	Incidente mesa de ayuda Documentado con acciones
	5	Realizar diligenciamiento de formato de gestión de incidentes de seguridad de la información e iniciar el proceso de documentación e identificación de causa raíz, y establecer el plan de mejoramiento para evitar que el incidente de se vuelva a presentar. **NOTA:** Esta actividad deberá ser ejecutada una vez se contenga el incidente, el funcionario de la Oficina de Tecnología responsable de la gestión del incidente, en apoyo con el Gestor de incidentes y Oficial de Seguridad de la Información.	Funcionario asignado de la Oficina de Tecnología de la Información Gestor de incidentes Oficial de Seguridad de la información.	Análisis de causas y plan de mejoramiento
	6	Realizar monitoreo del incidente, una vez se haya ejecutado las actividades del plan de mejora, el funcionario de la Oficina de Tecnología asignado para la gestión del incidente debe por un tiempo determinado no mayor a 30 días, verificar que se haya solucionado el incidente por completo.	Funcionario asignado de la Oficina de Tecnología de la Información.	Incidente mesa de ayuda
		¿Incidente solucionado? **Si,** continuar actividad 7 **No,** Volver a la actividad 5	Gestor de incidentes Oficial de Seguridad de la información.	
	7	Realizar costeo del incidente, para calcular los impactos económicos de la situación presentada, para este costeo emplear el **FORMATO COSTEO DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.**	- Funcionario asignado de la Oficina de Tecnología de la Información para la gestión del incidente. - Gestor de incidentes	Formato costeo de incidentes de seguridad de la información
	8	Documentar las lecciones aprendidas del incidente, y notificar a las autoridades o entidades necesarias según el tipo de incidente, de conformidad al Formato Contactos con Autoridades y Grupos de Interés del Sistema de Gestión de Seguridad De La Información, e ir a la actividad 15.	- Funcionario asignado de la Oficina de Tecnología de la Información para la gestión del incidente. - Gestor de incidentes	Incidente mesa de ayuda

COPIA CONTROLADA

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

DIAGRAMA DE FLUJO	No.	ACTIVIDAD	RESPONSABLE	REGISTRO
	9	Verificar si el evento se reportó por la mesa de ayuda o de lo contrario generar un caso en la mesa de ayuda como categoría Evento de Seguridad de la Información. Para que la plataforma de Mesa de Ayuda lo asigne automáticamente al Oficia de Seguridad.	Funcionario de la Oficina de Tecnología de la Información que reciba el reporte de evento, incidente o debilidad.	Ticket de mesa de ayuda
	10	Clasificar el evento entre, Alto, Medio y Bajo y asignar al colaborador de la Oficina de Tecnología que apoyara en la gestión del evento.	Gestor de Incidentes	Ticket de mesa de ayuda
	11	Ejecutar acciones establecidas para la mitigación y establecer acciones para prevenir la materialización de un posible incidente y comunicar al Oficial de Seguridad la ejecución una vez se hayan ejecutado las actividades para verificar la efectividad de estas.	- Funcionario asignado de la Oficina de Tecnología de la Información para la gestión del evento.	Ticket de mesa de ayuda
		¿Las acciones y controles para prevenir la materialización fueron adecuadas? **Si**, continuar actividad 15. **No**, volver actividad 11.	Gestor de incidentes Oficial de Seguridad de la información.	
	12	Verifica si la debilidad se reportó por medio de la mesa de ayuda o de lo contrario generar un caso en la mesa de ayuda como categoría debilidad de Seguridad de la Información. Para que la plataforma de Mesa de Ayuda lo asigne automáticamente al Gestor de Riesgos de Seguridad de la Información.	Funcionario de la Oficina de Tecnología de la Información que reciba el reporte de evento, incidente o debilidad.	Ticket de mesa de ayuda
	13	Verificar si la debilidad se encuentra identificada en la matriz de riesgos de seguridad digital del proceso, si no adicionar la debilidad como una vulnerabilidad.	Gestor de Riesgos de Seguridad de la Información de la Oficina de Tecnología.	Ticket de mesa de ayuda
	14	Definir controles y plan de tratamiento para mitigar posibles riesgos de seguridad de la información, e informar a los responsables del tratamiento.	Gestor de Riesgos de Seguridad de la Información de la Oficina de Tecnología.	Ticket de mesa de ayuda
	15	Documentar los resultados en el caso o incidente cargado en la mesa de ayuda y notificar a los usuarios que realizaron los respectivos reportes conforme a lo establecido en el **PROCEDIMIENTO DE GESTIÓN DE REQUERIMIENTOS Y SOLICITUDES TIC.** **FIN DEL PROCEDIMIENTO.**	- Funcionario asignado de la Oficina de Tecnología de la Información para la gestión del evento, incidente o debilidad. - Gestor de Incidentes	Ticket de mesa de ayuda Incidente de mesa de ayuda

COPIA CONTROLADA

7. DOCUMENTOS ASOCIADOS

- Formato Costeo de Incidentes de Seguridad de la Información
- Procedimiento Gestión de Cambios de Seguridad de la Información.

Clasificación de la Información: Publica ☒ Reservada ☐ Clasificada ☐

7. DOCUMENTOS ASOCIADOS

- Procedimiento Gestión de requerimientos y solicitudes TIC.
- Formato Contactos con Autoridades y Grupos de Interés del Sistema de Gestión de Seguridad De La Información
- Formato Gestión de incidentes de seguridad de la información.

8. CONTROL DE CAMBIOS

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	29/04/2024	Creación 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

COPIA CONTROLADA