MINAGRICULTURA	PROCEDIMIENTO	Versión 1
	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	PR-GST-06
		FECHA EDICIÓN 25-11-2016

1. OBJETIVO

Administrar eficaz y oportunamente todos aquellos incidentes y/o eventos de seguridad de la información que atenten contra las características de confidencialidad, integridad y disponibilidad de los activos de información del Ministerio de Agricultura y Desarrollo Rural, mediante acciones correctivas pertinentes que generen una base de datos de conocimiento y acciones proactivas al interior de la Entidad.

2. ALCANCE

Inicia con la detección, registro y clasificación del incidente y/o evento de seguridad de la información; luego se realiza su correspondiente análisis e investigación; continúa con la contención y erradicación del mismo, a través de un plan de recuperación; y finaliza con el cierre del incidente a través de la mesa de servicio.

3. BASE LEGAL

- Ley 527 de 1999
- Ley 599 del 2000
- Ley 1266 de 2008
- Ley 1273 de 2009
- Ley 1712 de 2014
- Ley 1581 de 2012
- Decreto 886 de 2014
- Decreto 1377 de 2013
- ISO/IEC 27001 versión 2013
- ISO/IEC 27042 versión 2014
- ISO/IEC 27037 versión 2012
- Manual para Procedimientos de Cadena de Custodia

4. DEFINICIONES

4.1. **Activo:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas, etc.) que tenga valor para la Entidad.

4.2. **Cadena de Custodia:** es un procedimiento documentado y controlado que se le aplica a toda evidencia física o elemento material probatorio desde su recolección hasta su disposición final, en donde se puede observar su descripción e identificación, una línea de tiempo, y las personas que han participado en su custodia.

4.3. **Clasificación de la Información:** es el ejercicio por medio del cual se determinan la(s)

categorías asignadas a cada tipo de información en MinAgricultura. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado.

4.4. **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.

4.5. **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada.

4.6. **Evento de Seguridad:** ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

4.7. **ERISI:** Equipo de respuesta a Incidentes de Seguridad de la Información.

4.8. **Estampa de Tiempo:** certificar mediante una secuencia de caracteres que un conjunto de datos ha existido y no ha sido modificado en un espacio de tiempo determinado. La secuencia de caracteres está relacionada con la fecha y el momento en que ocurre dicho evento y específicamente cuando fue creado en un sistema de cómputo.

4.9. ***Hardening***: (ingles: endurecimiento) es el proceso de asegurar un sistema informático mediante la reducción de vulnerabilidades en el mismo, esto se logra eliminando software, servicios, usuarios, innecesarios en el sistema, así como cerrando puertas de acceso que tampoco estén en uso.

4.10. **Incidente de Seguridad:** evento único o serie de eventos de seguridad de la información inesperada o no deseada que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

4.11. **Informática Forense:** es la aplicación de técnicas científicas y analíticas especializadas a infraestructura de TIC que permiten identificar, preservar, analizar, custodiar y presentar datos – *Evidencia Digital* – de tal manera que sean válidos dentro de un proceso legal y/o administrativo preservando su valor probatorio.

4.12. **Integridad:** propiedad de la información relativa a su exactitud y completitud.

4.13. **Imagen Forense:** copia binaria de la información que se encuentra en un medio de almacenamiento, la cual es trasladada a otro, sin que se cambien ninguna de sus características y/o atributos.

4.14. **Lugar de la Escena:** lugar de ocurrencia de un incidente y/o evento de seguridad. Entiéndase en la investigación como cualquier lugar mueble o inmueble donde se presuma la comisión de un hecho en contra de la norma y el sitio en donde se sospeche la presencia de elementos materia de prueba y evidencia física relacionados con la misma.

4.15. Seguridad de la Información: preservación de la confidencialidad, integridad y disponibilidad de la información.

4.16. Técnicas *HASHING* o *CHECKSUMS*: son funciones matemáticas y algorítmicas que tiene como propósito principal detectar cambios en una secuencia de datos para proteger la integridad de estos, verificando que no haya discrepancias entre los valores obtenidos al hacer una comprobación inicial y otra final tras el tratamiento realizado.

4.17. Vulnerabilidad: debilidad de un activo o control que pueda ser explotado por una o más amenazas.

5. CONDICIONES GENERALES

5.1. EQUIPO DE RESPUESTA A INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN (ERISI)

El Oficial de Seguridad de la Información del Ministerio de Agricultura y Desarrollo Rural (MinAgricultura en adelante) debe activar al ERISI cuando se presente incidentes y/o eventos de seguridad que puedan afectar la integridad, confidencialidad y disponibilidad de los activos de información. Este equipo con el apoyo de la Oficina de las TIC, generará planes de contención, erradicación y recuperación de los servicios y sistemas afectados, para prever y apoyar la continuidad de los servicios en MinAgricultura.

El ERISI podrá estar conformado según la naturaleza del incidente por:

- Especialistas en plataforma tecnológica
- Especialista de base de datos
- Especialista sistemas operacionales
- Especialista telecomunicaciones y redes
- Oficial de Seguridad de la Información
- Líderes funcionales de los Sistemas de Información

De ser necesario y de acuerdo con la naturaleza del incidente a tratar se pueden vincular a otros profesionales como abogados o técnicos en otras disciplinas relacionadas con el incidente.

5.2. DETECCIÓN Y ANÁLISIS DEL INCIDENTE O EVENTO DE SEGURIDAD

Los incidentes y/o eventos de seguridad de la información pueden ser identificados y/o detectados a través de todas o algunas de las siguientes fuentes de información:

- Alertas de las plataformas de TIC
- Fallas de sistemas informáticos
- Reportes de usuario
- Registros de las herramientas administrativas

- Consolas de antivirus
- Comunicaciones anónimas
- Redes sociales
- Mesa de Servicio
- Ciudadanía
- Reportes de grupos especializados

Todo evento y/o incidente de seguridad debe ser registrado por la mesa de servicio a través de la herramienta de gestión donde se documentan los datos de la fuente de información, con su respectiva valoración de credibilidad, así como una ponderación de la información suministrada. La finalidad de este registro es establecer la ocurrencia o no del incidente y/o evento de seguridad.

Cuando la mesa de servicio asigne el incidente al oficial de seguridad de la información, él debe registrar la información adicional relacionada con la cronología del incidente de seguridad, el activo de información afectado, estableciendo su nivel de criticidad de acuerdo con la matriz de activos de información, así como otros datos que permitan evaluar plenamente la incidencia.

Los niveles de clasificación de los incidentes y/o eventos de seguridad son:

Tabla 1 – Prioridad de los incidentes y/o eventos de Seguridad

NIVEL	VALOR DEL ACTIVO	TIEMPO DE ATENCION
MUY ALTO	81-100	1 HORA
ALTO	61-80	6 HORAS
MEDIO	41-60	12 HORAS
BAJO	21-40	2 DIAS
MUY BAJO	1-20	1 SEMANA

NOTA: Para establecer la prioridad del incidente y/o evento de seguridad de la información, es necesario remitirse a inventario de activos de información del Ministerio de Agricultura y Desarrollo rural, en su columna *DISPONIBILIDAD*, aquí se establece la criticidad, el cual esta evaluado frente a la operación y al cumplimiento de la misión y objetivos estratégicos del MinAgricultura.

El Grupo ERISI deberá realizar un análisis pormenorizado del incidente y/o evento de seguridad, y a partir de ello, desarrollara un plan de acción en el cual quedarán plasmadas las actividades que se ejecutarán frente a la recolección de las evidencias, la contención y erradicación del incidente, así como la recuperación del activo de información en caso de que se haya afectado la continuidad del negocio.

5.3. RECOLECCIÓN, ASEGURAMIENTO Y ANÁLISIS DE EVIDENCIAS DIGITALES

Estas actividades comprenden el hallazgo, recaudo, aseguramiento, transporte, custodia y análisis de las evidencias digitales que con ocasión de un incidente y/o evento de seguridad de la información que se haya recogido por parte del Grupo ERISI en el lugar de la escena.

Las evidencias que podrían encontrarse y recaudarse con ocasión del incidente de seguridad de la información son entre otras:

- Log Servidores
- Log de aplicaciones
- Log de Sistemas operacionales
- Log de Herramientas de Seguridad
- Computadores de Escritorio
- Computadores Portátiles
- *Smartphone*
- *Tablet*
- Buzones de correo electrónico
- Archivos almacenados en sistemas informáticos
- Registro de cámaras de seguridad
- Testimonios
- En general cualquier evidencia que pueda dar indicios sobre la ocurrencia del evento de seguridad

El recaudo de la evidencia debe documentarse en el lugar en donde se encuentren –*lugar de la escena*–, mediante los diferentes medios de fijación (descriptivos y fotográficos y/o video gráficos).

El aseguramiento de la evidencia digital se hace mediante técnicas propias de la informática forense, es decir, se identifica inicialmente la información contenida en los medios de almacenamiento recaudados, mediante técnicas criptográficas denominadas *HASHING* o *CHECKSUMS*; así mismo, se extraen copias idénticas de los datos a través de la extracción de imágenes forenses físicas o lógicas y, de ser posible, se extrae una estampa de tiempo –*Time Stamping*–; finalmente, se realiza el diligenciamiento de la Cadena de Custodia **F01-PR-GST-06**, cumpliendo de esta manera con los preceptos básicos frente al aseguramiento de pruebas digitales y/o computacionales.

Las evidencias recaudadas serán analizadas en detalle con la finalidad de encontrar información pertinente para la investigación, logrando así determinar y comprobar la ocurrencia de los hechos frente al incidente de seguridad denunciado y, de ser posible, identificar a los responsables.

Para la realización de las actividades de recaudo y análisis de evidencias computacionales se pueden usar según su disponibilidad, los siguientes elementos:

- Portátiles Forenses
- Laboratorios Fijos de Análisis Forense
- *Software* de adquisición de imágenes Forenses
- *Software* de Recolección de Evidencias
- Kit de Respuesta a Incidentes
- *Software* de Análisis forense
- Medios de almacenamiento

5.4. CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Una vez se ha establecido el impacto del incidente de seguridad de la información, es necesario y pertinente que se ejecuten las actividades de contención, erradicación y recuperación, tal y como se describen a continuación:

5.4.1. Contención: son las acciones tendientes a evitar la propagación del incidente de seguridad de la información detectado, previniendo daños sobre los activos de información del Ministerio de Agricultura y Desarrollo Rural, así como sobre su infraestructura de TIC.

Este grupo de acciones deben enfocarse en la detección del incidente y a la estrategia para contenerlo. A continuación, se exponen algunos ejemplos de estrategias de tratamiento:

Tabla 2 - Estrategia de Contención de Incidentes de Seguridad

INCIDENTE DE SEGURIDAD	ESTRATEGIA
Accesos no Autorizados	Bloqueos de cuenta Apagado de la máquina Bloqueo de puertos
Códigos Maliciosos	Desconexión de la red del equipo afectado Bloqueo de Puertos Actualización de herramientas de detección y bloqueo de software malicioso
Reconocimiento	Nuevas reglas de filtrado Bloqueo de Puertos
Corrupción	Retiro de funcionario Bloqueo de Cuentas

5.4.2. Erradicación y Recuperación: una vez se contiene el incidente de seguridad de la información, este debe erradicarse, es decir, eliminar cualquier tipo de rastro que pudiera existir con ocasión de comportamiento inusual en los activos de información y/o en la infraestructura de TIC de MinAgricultura. Adicionalmente, debe existir una restauración inmediata de la arquitectura y/o servicios de TIC que devuelvan de manera oportuna y

eficaz no solo las funcionalidades al sistema, sino que permitan realizar seguidamente las actividades de endurecimiento –*Hardening*–, todo esto con el propósito de cerrar las vulnerabilidades detectadas.

A continuación, se exponen algunas estrategias de recuperación:

Tabla 3 - Estrategia de Contención de Incidentes de Seguridad

INCIDENTE DE SEGURIDAD	ESTRATEGIA
Denegación de Servicios	Restitución del servicio caído Restauración de *Backups*
Códigos Maliciosos	Corrección de Efectos Restauración de *Backups* Actualización de Antivirus
Vandalismo	Nuevas reglas de filtrado Bloqueo de Puertos
Corrupción	Recuperación del Sitio *Web* Restauración de *Backups*
Intrusión	Restauración de equipos y servicios Recuperación de los Datos Restauración de *Backups*

5.5. COMUNICACIÓN

A través del Comité Institucional de Desarrollo Administrativo se tomarán las decisiones que sean necesarias y pertinentes para las comunicaciones internas y externas que se deban emitir con motivo del incidente de seguridad de la información. Así mismo, el comité determinará la necesidad de coordinar todas aquellas denuncias que deban ser instauradas ante los entes de control y vigilancia, aportando para ello las evidencias recaudadas, así como aquellos informes desarrollados con ocasión de la administración del incidente.

5.6. BASE DE DATOS DE CONOCIMIENTO

En la Gestión de Incidentes de Seguridad de la Información, uno de los aspectos más importantes es la mejora continua, ello implica retroalimentar los temas de seguridad al interior del Ministerio de Agricultura y Desarrollo Rural, y, por ende, mantener siempre un registro de lecciones aprendidas. Este registro, debe estar debidamente documentado, puesto que, con ello, se pueden conocer los pormenores frente a la gestión de incidentes de seguridad, las acciones ejecutadas, los recursos asignados, los resultados, las dificultades, información que permite actuar frente a situaciones similares en caso de presentarse.

6. DESARROLLO

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
1	Detecte el incidente y/o evento potencial de seguridad cuando este es evidenciado a través de las diferentes alertas y/o medios de comunicación que posea el Ministerio. Nota. Algunos ejemplos de alertas y/o medios son: alertas de las plataformas de TIC, caídas del sistema, reportes de usuario, registros de las herramientas administrativas, consolas de antivirus, comunicaciones anónimas, redes sociales, Mesa de servicio, ciudadanía, entre otros.	Funcionarios, contratistas, mesa de servicio, administradores de infraestructura y ciudadanía	Correo electrónico Llamada telefónica
2	Registre el incidente y/o evento de seguridad de la información en la herramienta de gestión, documentando los datos solicitados en el mismo, tales como: línea cronológica del incidente, activo de información involucrado, identificación de las fuentes de información, entre otros.	Mesa de Servicio	Registro en la herramienta de gestión
3	Clasifique el incidente de seguridad conforme la tabla No. 1 del numeral 5.2. ponderando el impacto que puede causar al Ministerio de Agricultura y Desarrollo Rural y los tiempos de respuesta. Todo ello se debe documentar en el registro de la herramienta de gestión Si se clasifica como un incidente de seguridad de la información, este deberá ser remitido al Oficial de Seguridad de la Información del Ministerio de Agricultura y Desarrollo Rural, quien activará al ERISI. *Ir al paso 4.* © Si no se clasifica como un incidente o evento de seguridad de la información, este deberá ser finalizado. *Ir al paso 10.*	Mesa de Servicio/ Oficial de Seguridad de la Información	Registro la herramienta de gestión

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
4	Realice un plan de acción que le permita definir las actividades que se deben ejecutar con ocasión de la administración del Incidente de Seguridad. Para ello, determine los lugares a intervenir frente al recaudo de las evidencias, las acciones de contención, erradicación y recuperación, frente a los servicios y/o plataformas afectadas por la incidencia. Nota. Dentro de la planeación para la atención del incidente y/o evento de seguridad, se debe tener en cuenta los tiempos, así como aquellas necesidades de recursos logísticos, humanos, áreas interesadas, entre otros aspectos.	ERISI Oficial de Seguridad de la Información	Plan de Acción
5	Recolecte las evidencias en las áreas u oficinas de MinAgricultura que con ocasión del incidente y/o evento de seguridad estén afectadas. Para ello, se aplicarán los lineamientos propios de Cadena de Custodia e Informática Forense, preservando, ante todo, el valor probatorio de las pruebas que se recolecten. ©	ERISI Oficial de Seguridad de la Información	Informes de Recolección de Evidencias Formato cadena de custodia F01-PR-GST-06 Evidencias
6	Realice una contención del incidente con apoyo de la Oficina de las TIC evitando cualquier tipo de propagación que pueda seguir afectando los activos de información del MinAgricultura. ©	ERISI Oficial de Seguridad de la Información Oficina de TIC	Informe de Contención del incidente de seguridad de la Información en la herramienta de gestión
7	Elimine la cualquier causa raíz del evento que pudiera existir con ocasión de la incidencia presentada con apoyo de la Oficina de las TIC, y elabore un plan de remediación, con la finalidad de poder cerrar las vulnerabilidades detectadas.	Grupo ERISI Oficial de Seguridad de la Información Oficina de TIC	Informe de Erradicación y Remediación en la herramienta de gestión
8	Evalúe la necesidad de notificar y denunciar a los entes de control según sea el caso, las disposiciones establecidas frente a la ocurrencia de los incidentes de seguridad y su impacto dentro de MinAgricultura.	Comité Institucional de Desarrollo Administrativo Oficina Jurídica	Acta del Comité Institucional de Desarrollo Administrativo. Informe de Contención del incidente de

Nº	ACTIVIDAD	RESPONSABLE	DOCUMENTO
		Oficina de Comunicaciones	seguridad de la Información en la herramienta de gestión Evidencias Digitales
9	Realice un registro detallado de toda gestión de incidentes de seguridad, con el fin de poder desarrollar acciones correctivas para posteriores eventos o incidentes. Nota: Las acciones correctivas se adelantan aplicando el procedimiento "Procedimiento acciones preventivas, correctivas y de mejora (PR-SIG-06)."	ERISI Oficial de Seguridad de la Información	Registro herramienta de gestión Formato solicitud de acciones preventivas, correctivas o de mejora (F01-PR-SIG-06) Informe de recolección de Evidencias, Informe de Contención del incidente, Informe de Erradicación y remediación, en la herramienta de gestión.
10	Cierre el incidente de Seguridad de la Información actualizando en la mesa de ayuda el estado del incidente.	ERISI Oficial de Seguridad de la Información Mesa de Ayuda	Registro en la herramienta de gestión

7. DOCUMENTOS DE REFERENCIA

Políticas de Seguridad y Privacidad de la Información
Formato Inventario de Activos de Información F01-PR-GST-10
Formato de Cadena de Custodia F01-GST-PR-06

8. HISTORIAL DE CAMBIOS

Fecha	Versión	Descripción
25-11-2016	1	Primera versión del documento