1. OBJETIVO

Entregar los lineamientos necesarios con el fin de detectar, reportar, evaluar y dar respuesta a los eventos o incidentes de seguridad y privacidad de la información que se presenten en la plataforma tecnológica e identificar las lecciones aprendidas con el fin salvaguardar la confidencialidad, integridad y disponibilidad de los activos.

2. ALCANCE

Inicia desde el reporte o caso de un evento o incidente que comprometa la confidencialidad, integridad y disponibilidad de la información de la ADR hasta el cierre de este. Su nivel de aplicación es en todas las dependencias de la ADR, incluidas las UTT.

3. BASE LEGAL

Decreto 1008 del 14 de junio de 2018 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.

4. DEFINICIONES

Analista del Operador de Mesa de Servicio: Recibe la información de los Colaboradores de la ADR, registra los casos en la herramienta de Mesa de Servicio y es el primer contacto para la Gestión de los Incidentes de Seguridad de la Información.
Aprovechamiento de vulnerabilidades Informáticas: Aprovechamiento de vulnerabilidades de los sistemas de información, tales como configuraciones, protocolos y programas, para obtener información sobre la ADR.
Antivirus: Programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema.
Base de Conocimiento: Es un tipo de base de datos para la gestión del conocimiento. Provee los medios para la recolección, organización y recuperación computarizada de conocimiento.
Botnet: Grupo de computadores reclutados en redes, controlados centralmente por el autor del Bonet, se forman deliberadamente para infectar masivamente los computadores en redes, crear denegación de servicios, envió de spam, etc.
Código malicioso: Es un término que hace referencia a cualquier conjunto de códigos, especialmente sentencias de programación, que tiene un fin malicioso
Escalamiento: Cuando un recurso que recibe una solicitud que no puede solucionar por si solo y requiere la ayuda de una persona o grupo con mayor conocimiento del tema específico.
Escaneo de redes: Uso de software para escaneo de redes y así adquirir información acerca de las configuraciones de red, puertos, servicios y vulnerabilidades existentes.
Evento de seguridad de la información: Presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.
Evento de seguridad de la información: Un evento de seguridad de la información es la presencia identificada de un estado que indica un incumplimiento posible de la política de seguridad de la información, una falla de los controles de seguridad, o una situación desconocida que puede ser pertinente para la seguridad de la información.
Gestor de Incidentes: Es el rol responsable de identificar, priorizar y analizar la información referente al incidente y toma la decisión de coordinar un equipo de respuesta. Realiza el seguimiento de las acciones emprendidas para la contención y/o erradicación del incidente.
Gusano de red: Tipo de programa maliciosos que se disemina y replica automáticamente a través de las redes, aprovechando las vulnerabilidades de los sistemas de información en las redes.
Herramienta de Gestión de Servicios: Aplicación que ayudan a la gestión de TI de la ADR; para el caso de la ADR, es el software en donde se documentan los servicios de gestión tecnológica como Incidentes, Requerimientos, Problemas, Controles de Cambios, entre otros
Impacto: Es un efecto que ocurre a causa de la materialización de un riesgo y que va en detrimento de uno o más de los recursos importantes del negocio (Recursos: Financiero, Imagen, Ambiental, Humano, entre otros).
Incidente Crítico: Es un evento que representa una seria amenaza para la entidad, y afecta de forma inmediata a uno o más recursos muy importantes o pone en peligro información sensitiva o confidencial de la ADR, se considera crítica para la misión de la ADR
Incidente de seguridad de la información: Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de los activos de información. Los incidentes de seguridad de la información son hechos inevitables sobre cualquier ambiente de información, y estos pueden ser bastante notorios e involucrar un impacto fuerte sobre la información de la organización.
Malware: Programa de software que introducido en los equipos y sistemas de una organización los bloquea o controla, “secuestra” información, roba o elimina datos, causa pérdidas millonarias y conlleva graves riesgos legales y de reputación. Los virus y programas ocultos en páginas webs, en ficheros o en el software sin licencia amenazan seriamente el funcionamiento y la seguridad de las empresas.
Mesa de Servicios: Es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación
Phishing: Convencer a los usuarios para que divulguen información importante, tal como detalles de cuentas bancarias y usuarios y contraseñas, mediante el uso de correos electrónicos engañosos.
Ransomware: Es un programa de software malicioso que infecta tu computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema

Respuesta a incidente: Permite solucionar o dar respuesta aceptable para un Incidente de Seguridad de la Información, puede ser registrado en la Base de Conocimiento.
Spyware: Es un software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.
Virus informático: Conjunto de instrucciones o códigos informáticos que se inserta en los programas de computador, tiene la capacidad de auto replicarse y usualmente porta una carga útil que afecta el funcionamiento del computador, destruye datos, altera y pone en riesgo la información.

5. CONDICIONES ESPECIALES

Pasos para la efectividad de atención de un evento o incidente del seguridad y privacidad de la información

Recolectar Información Preliminar

Todos los eventos o incidentes del seguridad y privacidad de la información deben ser reportado a la Oficina de Tecnologías de la Información por medio de la mesa de servicio y/o llamando a la ext.5900 y diligenciado un caso en la herramienta www.soporte.adr.gov.co o en el correo electrónico mesadeservicio@adr.gov.co
Una vez se tenga el caso del evento o incidente de seguridad, se debe realizar la recolección de información preliminar con base en el caso la detección o reporte de una anomalía en los componentes o activos, con el fin de evidenciar si realmente es un evento o un incidente de seguridad de la información o solo se trata de una falsa alarma, por parte del Analista Ingeniero de soporte del operador de Mesa de Servicio diligenciado la encuesta descrita del formato “Reporte de Gestión de Incidente o Evento De Seguridad”, Ítem 1-2-3.
El Profesional de la Oficina de Tecnologías de la Información con el rol de Gestor de Incidentes de Seguridad de la Información debe diligenciar en el formato “Reporte de Gestión de Incidente o Evento De Seguridad”, en los siguientes ítems del formato:
Ítem 4. componentes/Activos Afectados (Si los hay, suministre la descripción del componente o activo afectado dentro del incidente o relacionado con él, incluidos serie, licencia y versión, en donde sea pertinente) seleccionando: información/Datos, Hardware, Software, Comunicaciones, Documentación, Procesos y describa en la casilla correspondiente.
Ítem 5: seguido de la recolección de la evidencia se debe enmarcar el evento o incidente de la seguridad de la información según los siguientes factores, clases (esta clasificación puede cambiar al final de la atención del incidente), en el formato.

Factor		Definición
Importancia del sistema de Información	Sistema de información especialmente importante Sistema de información importante	Esta clase se entrega de acuerdo a la dependencia del(os) proceso(s) afectado por el sistema de información
	Sistema de información comunes	
Perdida del negocio	Perdida del negocio especialmente grave	Parálisis grande de la institución. hasta el punto de parar la operación del(os) proceso(s) afectado(s) y/o daño muy grave en la confidencialidad, integridad y disponibilidad de datos clave del negocio
	Perdida del negocio grave	Interrupción de las operaciones de la institución durante un tiempo prolongado o la Parálisis local del proceso afectado. hasta el punto de influir gravemente en la operación del proceso y/o causar daño grave en la confidencialidad, integridad y disponibilidad de datos clave del negocio
	Perdida del negocio considerable	Interrupción de las operaciones de la institución hasta el punto de influir considerablemente en la operación del proceso afectados y/o causar daño considerable en la confidencialidad, integridad y disponibilidad de datos importantes del negocio
	Perdida menor del negocio	Interrupción de las operaciones de la institución por un tiempo corto, hasta el punto de influir de alguna manera en la operación del proceso afectados y/o causar impacto menor en la confidencialidad, integridad y disponibilidad de datos importantes del negocio
Impacto social	Impacto social especialmente importante	Efectos adversos que abarcan la mayoría de los departamentos y ciudades, que representan una gran amenaza para la seguridad nacional, causa alteraciones sociales y afecta seriamente el interés público.
	Impacto social importante	Efectos adversos que abarcan la mayoría de las ciudades o municipios, que representan una amenaza para la seguridad nacional, causa pánico social y afecta el interés público.

Evaluación

Ítem 6: Definir los aspectos, cual aplica y proceder a clasificar de acuerdo a estos factores se debe incluir el incidente en algún valor de las clases conforme a la tabla y de ahí definir el nivel de prioridad con el cual se deberá atender el evento o incidente de seguridad de la información, en el formato.

Clase	Prioridad (TRIAGE)	Descripción *(La clase se define de acuerdo a las tres conductas que más se asemejen de los factores)*
Muy grave (Clase 4)	**Emergencia: Impacto severo, Atención inmediata (1)**	*Actúan sobre Sistema de información especialmente importante, dan como resultados Perdida del negocio especialmente grave, y conducen a un Impacto social especialmente importante.*
Grave (Clase 3)	**Critica: Impacto medio, Atención inmediata (2),** (Si no hay uno prioridad (1), máximo tiempo antes de atención 30 minutos)	*Actúan sobre Sistema de información especialmente importante, o sistemas de información importantes, y dan como resultados Perdida graves para el negocio, o conducen a un Impacto social importante.*
Menos grave (Clase 2)	**Media: Impacto Bajo, Atención inmediata (3),** (Si no hay uno prioridad (1), (2) máximo tiempo antes de atención 60 minutos)	*Actúan sobre Sistema de información importante, o sistemas de información comunes, y dan como resultados Perdidos considerables para el negocio, o conducen a un impacto social considerable.*
Menor (Clase 4)	**Baja: Impacto Bajo, Atención inmediata (4),** (Si no hay uno prioridad (1), (2), (3) máximo tiempo antes de atención 90 minutos)	*Actúan sobre Sistema de información importante, o sistemas de información comunes, dan como resultados Perdida menores o ninguna pérdida para el negocio, conducen a impactos social menores o ningún impacto social y no se requieren acciones y no hay consecuencias.*
Falsa Alarma	**No Aplica**	*Diligenciar Formato de evento ITEM 1-2-3*

Ítem 7: categoría del incidente de seguridad de la información, ya teniendo definidos los factores, la clase y prioridad de atención del incidente de seguridad de la información, el Gestor de Incidentes de Seguridad de la Información, deberá categorizar el incidente en una y solo una de las categorías (En el caso que se evidencien una o más categorías se deberá marcar con una (x) la que origino la ocurrencia del incidente no las que derivaron de ella), definida la categoría el Gestor de Incidentes de Seguridad de la Información deberá definir la(s) amenaza(s) que se materializaron en el incidente, ellas deben encontrase dentro de la categoría escogida. Debe diligenciar en el formato “Reporte de Gestión de Incidente o Evento De Seguridad” (Indique con una x los tipos de amenazas involucradas)
Nota: En el caso que el incidente no se encuentre en alguna de las categorías definidas en el formato de atención a incidentes informáticos, al final de la tabla se encuentra la opción "otros", en el cual se deberá especificar la categoría y las amenazas que se derivan de esta.

Ítem 8: costo de recuperación del incidente en el ítem 6, si aplica poner el costo de recuperación por los diferentes aspectos y para por su clasificación del criterio que incumplen (Incumplimiento Legal, Sanciones, Costo Monetario, Pérdida de Imagen y Afectación a la Operación de la ADR) contabilizar el costo total teniendo en cuenta el valor de la hora del recurso humano, hardware, software para la recuperación del incidente y diligenciar en el formato

Respuesta del incidente de seguridad de la información

La etapa de respuesta tiene como objetivo solucionar el incidente, hacer que el impacto en la plataforma sea lo mínimo posible y tener el incidente bajo control, esto de acuerdo a lo definido en la etapa de evaluación diligenciando el Ítem 9 del formato “Reporte de Gestión de Incidente o Evento De Seguridad”, de igual forma se deberán verificar las siguientes acciones:

Verificar si es necesario activar los procedimientos de continuidad del negocio y comunicaciones al personal involucrado.
Identificar recursos internos e identificar recursos externos para responder ante el incidente
Realizar análisis forense de seguridad de la información en caso de que sea necesario y verificar los factores, clases, prioridad y categorización del incidente en el caso que sea necesario.
Escalar el incidente en caso de ser necesario para revisiones o decisiones posteriores
Uso de directrices para una documentación minuciosa de las acciones adelantadas.
Actualización de la base de datos de conocimiento, el Gestor de Incidentes de Seguridad de la Información deberá responderse las siguientes preguntas como mínimo: ¿En qué consiste el incidente?, ¿cómo fue causado y que o quien lo causo?, ¿que afecta o podría afectar?, ¿el impacto real o potencial?, ¿cómo se ha tratado hasta el momento?
Identificación de lecciones aprendidas

Ítem 9: diligenciar en su totalidad la solución del incidente teniendo en cuenta el formato “Reporte de Gestión de Incidente o Evento De Seguridad” en Acciones tomadas para solucionar el incidente, Acciones planificadas para solucionar el incidente, Acciones pendientes, Lecciones aprendidas

En esta fase es importante que se identifiquen las lecciones aprendidas, estas pueden arrojar lecciones como:

Necesidad de actualizaciones
Toma de conciencia sobre seguridad de la información
Implementación de controles
Inclusión de nuevos riesgos de seguridad
Cambios en los procedimientos y/o formatos de los procesos de TI
Entre otros

Por último, la lección aprendida debe llevar a identificar patrones, áreas cítricas, implementación de acciones preventivas para reducir la probabilidad de futuros incidentes, estas deben ser consignadas en el formato de atención a incidentes.

Documentación y cierre del Incidente

Después de que se tenga bajo control el incidente y se hallan identificado las lecciones aprendidas, el Gestor de Incidentes de Seguridad de la Información de incidentes de la información deberá verificar el diligenciamiento del formato "Reporte de Incidente de Seguridad de la Información" con todos los campos requeridos, la información referente al ítem 10 de conclusiones y reportar o notificar ala entidades de gobierno.
Firmar el reporte y archivar la carpeta asignada para tal fin y reportar para el cumplimiento de indicadores de la seguridad de la información.

6. DESARROLLO

N°	ACTIVIDAD	DESCRIPCIÓN	RESPONSABLE	REGISTRO
1	Recolectar Información Preliminar	DESCRIPCIÓN 1. Detectatando o recibeiendo a través de medios humanos (Administradores, usuario final, terceras partes, mesa de ayuda, CSIR, medios de comunicación, conversaciones directas, fuentes abiertas, etc.) o automáticos (periféricos de seguridad, auditorias, centro de operaciones de seguridad, correo electrónico, teléfono, etc.) una alarma de la ocurrencia de un evento incidente de seguridad de la información, la cual se debe categorizar de acuerdo la lista de posibles afectaciones. 2. Tener o abrir caso en herramienta de servicio de soporte Mesa de servicios www.soporte.adr.gov.co o al correo electrónico mesadeservicio@adr.gov.co 3. Realizando entrevista con la descripción del incidente o evento para diligenciar formato “Reporte de Gestión de Incidente o Evento De Seguridad” - ¿Que ocurrió? - ¿Como ocurrió? - ¿Por qué ocurrió? - ¿Daños iniciales sobre componentes o activos afectados- ¿Impactos adversos para el negocio? - ¿Cualquier vulnerabilidad identificada? 4. Realizando la recolección de información preliminar con base en la detección o reporte de una anomalía en los componentes o activos, con el fin de evidenciar si realmente es un evento o un incidente de seguridad de la información o solo se trata de una falsa alarma. 5. Diligenciando Ítem 1-2-3 y para incidente todo el formato “Reporte de Gestión de Incidente o Evento De Seguridad” Nota: solo diligenciar Ítem 1-2-3 si es un evento	Analista Ingeniero de soporte del operador de Mesa de Servicio	www.soporte.adr.gov.co mesadeservicio@adr.gov.co Reporte de Gestión de Incidente o Evento De Seguridad
		Enmarcando el evento o incidente de la seguridad de la información según los		

2	Clasificar el Incidente	factores Importancia del sistema de Información, Perdida del negocio e Impacto social, diligenciar ítem 5 del formato	Gestor de Incidentes de Seguridad de la Información	Reporte de Gestión de Incidente o Evento De Seguridad
3	Evaluar incidente	Define los aspectos, aplicabilidad y procede a clasificar de acuerdo a estos factores, se debe incluir el incidente en algún valor de las clases conforme el ítem 6 del formato.	Gestor de Incidentes de Seguridad de la Información	Reporte de Gestión de Incidente o Evento De Seguridad
4	Categorizar el incidente	1. categorizando el incidente en una y solo una de las categorías (En el caso que se evidencien una o más categorías se deberá marcar con una (x) la que origino la ocurrencia del incidente no las que derivaron de ella), definida la categoría el Gestor de Incidentes de Seguridad de la Información deberá definir la(s) amenaza(s) que se materializaron en el incidente, ellas deben encontrase dentro de la categoría escogida. Debe diligenciar el ítem 7 del formato. Nota: En el caso que el incidente no se encuentre en alguna de las categorías definidas en el formato de atención a incidentes informáticos, al final de la tabla se encuentra la opción "otros", en el cual se deberá especificar la categoría y las amenazas que se derivan de esta. 2. Contabilizando el costo de recuperación de incidente si aplica Debe diligenciar el ítem 8 del formato.	Gestor de Incidentes de Seguridad de la Información	Reporte de Gestión de Incidente o Evento De Seguridad
5	Responder el incidente de seguridad de la información	Solucionando el incidente, hacer que el impacto en la plataforma sea lo mínimo posible y tener el incidente bajo control, esto de acuerdo con lo definido en la etapa de evaluación, verificando acciones y diligenciando el Ítem 9 del formato Nota: en el caso de ser un evento reportado por una entidad externa o interno se toman las acciones recomendadas y se deja evidencia de las actividades realizadas con el fin de prevenir ese incidente en la entidad	Gestor de Incidentes de Seguridad de la Información	Reporte de Gestión de Incidente o Evento De Seguridad
		Diligenciando en su		

6	Identificar de lecciones aprendidas	totalidad el ítem 9, es importante que se identifiquen las lecciones aprendidas, estas pueden arrojar lecciones como: • Necesidad de actualizaciones • Toma de conciencia sobre seguridad de la información • Implementación de controles • Inclusión de nuevos riesgos de seguridad • Cambios en los procedimientos y/o formatos de los procesos de TI • Entre otros	Gestor de Incidentes de Seguridad de la Información	Reporte de Gestión de Incidente o Evento De Seguridad
7	Documentar y cerrar del Incidente	Teniendo bajo control el incidente y se hallan identificado las lecciones aprendidas, el Gestor de Incidentes de Seguridad de la Información de incidentes de la información deberá verificar el diligenciamiento del formato "Reporte de Incidente de Seguridad de la Información" con todos los campos requeridos, la información referente al ítem 10 de conclusiones y reportar o notificar a la entidades de gobierno. Firmar el reporte y archivar la carpeta asignada para tal fin y reportar para el cumplimiento de indicadores de la seguridad de la información Nota: en caso de que la investigación del incidente arroje una categoría diferente se deberá realizar el cambio y en las conclusiones formato explicar las razones de su cambio. Enviar el reporte a ente regulador colCERT y CSIRT	Profesional de la Oficina de Tecnologías de la Información con el rol de Gestor de Incidentes de Seguridad de la Información o Oficial de seguridad	Reporte de Gestión de Incidente o Evento De Seguridad
8	Entregar de documentación	Recibe la documentación del reporte de gestión de incidentes eventos de seguridad en la ADR, para realizar el informe de gestión del área, el cual se presentara al Comité Institucional de Gestión y Desempeño de la Agencia de Desarrollo Rural los resultado de Seguridad y privacidad de la información.	Jefe de la Oficina de Tecnologías de la Información	Reporte de Gestión de Incidente o Evento De Seguridad

7. DOCUMENTOS ASOCIADOS

FORMATO REPORTE DE GESTIÓN DE INCIDENTE O EVENTO DE SEGURIDAD
Guía Técnica Colombiana GTC-ISO/IEC 27035 "Tecnología de la Información. Técnicas de Seguridad y Gestión de Incidentes de Seguridad de la Información".

VERSIÓN	FECHA	RAZÓN DE LA ACTUALIZACIÓN
1	02/Oct/2017	Actualización de normatividad vigente

ELABORÓ	REVISÓ	APROBÓ
Nombre: CATALINA SANABRIA **Cargo:** 2.4. Oficina de Tecnologías de la Información **Fecha:** 05/Jun/2020	**Nombre:** Leonardo Alfonso Murillo Corrales **Cargo:** 2.4. Oficina de Tecnologías de la Información **Fecha:** 11/Jun/2020	**Nombre:** Victor Manuel Mondragon Maca **Cargo:** 2.4. Oficina de Tecnologías de la Información **Fecha:** 18/Jun/2020