| | PROCEDIMIENTO | Versión 1 |
|---|---|---|
| | GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN | PR-GST-06 |
| | | FECHA EDICIÓN 20-11-2020 |

## 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 aporten en la generación de 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 recuperación del servicio comprometido (si aplica), posteriormente la contención y erradicación del incidente; y finaliza con el cierre del incidente a través de la mesa de servicio.

## 3. BASE LEGAL

- Ley 527 de 1999
- Ley 594 de 2000
- Ley 599 del 2000
- Ley 679 de 2001
- Ley 1266 de 2008
- Ley 1273 de 2009
- Ley 1341 de 2009
- Ley 1712 de 2014
- Ley 1581 de 2012
- Decreto 886 de 2014
- Decreto 1377 de 2013
- Decreto 1078 de 2015
- Decreto 1499 de 2017
- ISO/IEC 27001 versión 2013
- ISO/IEC 27042 versión 2014
- ISO/IEC 27037 versión 2012
- Manual para Procedimientos de Cadena de Custodia
- Documento Conpes 3995

## 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 esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la Entidad.

| REVISÓ | APROBÓ |
|---|---|
| John Patiño<br>**Nombre: John Edilson Patiño Tenorio**<br>Cargo: Coordinador Grupo de Gestión de Gobernabilidad de la Información y Gestión del Conocimiento<br>Fecha: 20-11-2020 | **Nombre: Alfonso Javier Celedón Simón**<br>Cargo: Jefe Oficina de Tecnologías de la Información y las Comunicaciones<br>Fecha: 20-11-2020 |

**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 Ministerio de Agricultura y Desarrollo Rural. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado.

**4.4.** **Confidencialidad:** Propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000:2018].

**4.5.** **Contención**: Acciones necesarias para garantizar el control del incidente mientras se realiza un análisis más detallado y se definen las acciones necesarias para remediar el incidente.

**4.6.** **Disponibilidad:** Propiedad de ser accesible y utilizable a la demanda por una entidad autorizada. [ISO/IEC 27000:2018].

**4.7.** **Evento**: Aparición o cambio de un conjunto particular de circunstancias. [ISO/IEC 27000: 2018]

**4.8.** **Eventos en seguridad de la información:** Ocurrencia identificada de un sistema, servicio o estado de la red que indica una posible violación de la política de seguridad de la información o el fracaso de los controles, o una situación previamente desconocida que puede ser la pertinente a seguridad. [ISO/IEC 27000: 2018].

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

**4.10.** **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**.**

**4.11.** **Gestión de Incidentes de Seguridad de la Información**: Procesos para detectar, informar, evaluar, responder, tratar, y aprender de los incidentes de seguridad de la información. [ISO/IEC 27000: 2018].

**4.12.** **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.

**4.13.** **Incidente en seguridad de la información:** Un evento o una serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad

significativa de comprometer las operaciones de la organización y amenaza la seguridad de la información. [ISO/IEC 27000: 2018].

**4.14.** **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.

**4.15.** **Investigación forense de seguridad de la información**: Aplicación de técnicas de investigación y análisis para recolectar, registrar y analizar información de incidentes de seguridad de la información [ISO/IEC 27035:2012]

**4.16.** **Integridad:** Propiedad de exactitud y completitud. [ISO/IEC 27000:2018].

**4.17.** **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.

**4.18.** **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.

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

**4.20.** **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.

**4.21.** **Vulnerabilidad:** Preservación de la confidencialidad, integridad y disponibilidad de la información. [ISO/IEC 27000:2018].

## 5. CONDICIONES GENERALES

### 5.1. PREVENCIÓN

La gestión de incidentes tiene como objetivo principal la atención, tratamiento y respuesta eficaz a cualquier evento o incidente que afecte la disponibilidad de los servicios tecnológicos requeridos en el Ministerio. En este proceso de prevención de incidentes se incluye las actividades de tipo proactivo, que permitan a la Entidad estar preparada para responder y enfrentar incidentes de seguridad. Entre las actividades principales para prevenir incidentes de seguridad se encuentran las capacitaciones a los servidores públicos y contratistas de la Entidad, la identificación de riesgos y la aplicación de controles de seguridad de la información en la organización.
Para una eficaz prevención o preparación ante los eventos e incidentes de seguridad de la información se requiere el compromiso de la alta dirección, las partes interesadas y la ejecución

de actividades por parte de los servidores públicos y contratistas responsables de los activos de información.

A continuación, se describen las actividades que la entidad realiza de manera preventiva:

a) Aplicación de planes de sensibilización y entrenamiento a los servidores públicos y contratistas en los relacionado con la seguridad de la información.
b) Análisis periódico de gestión de riesgos en seguridad de la información o cuando se presente cambios significativos en el Ministerio a nivel organizacional de procesos o en la tecnología.
c) Auditorías periódicas a la seguridad de la información.
d) Gestión de parches o actualizaciones de software de manera automática o manual.
e) Implementación de controles de red eficaces de conformidad con las políticas específicas de seguridad de la información.
f) Controles para la prevención de código malicioso con herramientas centralizadas especializadas.
g) Aplicación de acciones para el aseguramiento de los equipos de cómputo, activos críticos, de conformidad con las políticas específicas de seguridad de seguridad de la información.

### 5.2. 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 de la información que puedan afectar la integridad, confidencialidad y disponibilidad de los activos de información. Este equipo, con el apoyo de la Oficina TIC, generará planes de contención, erradicación y recuperación de los servicios y sistemas afectados, para prever y apoyar la continuidad de 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.

### 5.3. 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 de la información 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. La finalidad de este registro es establecer la ocurrencia o no del incidente y/o evento de seguridad de la información.

Cuando la mesa de servicio asigne el evento o incidente al Oficial de Seguridad de la Información, él deberá suministrar la información adicional relacionada con la cronología del evento o 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:

Incidentes: cuando se presenta una situación de seguridad de la información a través de la cual se explotan vulnerabilidades de los activos de información materializando riesgos asociados a estos, comprometiendo la confidencialidad, integridad o disponibilidad de estos. La atención de los incidentes de seguridad de la información debe ser atendidos de manera inmediata.

Evento: son aquellas situaciones que habiendo ocurrido no generaron un impacto real sobre un activo de información, pero sí merecen atención oportuna.

Ejemplos de eventos de seguridad: control de seguridad inefectivo, cambios no controlados, errores en software o hardware, incumplimientos a políticas o procedimientos, infracciones a la seguridad física, errores humanos, entre otros.

Ejemplos de incidentes de seguridad de la información: cambios no autorizados, incumplimiento reiterativo a las políticas o procedimientos, código malicioso, denegación de servicio, destrucción o modificación de datos, revelación de información, intrusión, uso inaceptable de activos, violación de acceso, violación a la ley de protección de datos, entre otros.
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.

## 5.4. RECOLECCIÓN, ASEGURAMIENTO Y ANÁLISIS DE EVIDENCIAS DIGITALES

Estas actividades comprenden el hallazgo, recaudo, aseguramiento, transporte, custodia y análisis de las evidencias de un incidente y/o evento de seguridad de la información.

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 y/o incidente de seguridad de la información.

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 evento y/o incidente de seguridad de la información reportado 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

### 5.5. CONTENCIÓN, ERRADICACIÓN Y RECUPERACIÓN

Una vez se ha establecido si se trata de un evento o un 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:

**5.5.1. Contención:** son las acciones para evitar la propagación del evento o repetición del incidente de seguridad de la información reportado o 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 y a la estrategia para contenerlo.

A continuación, se exponen algunos ejemplos de estrategias de tratamiento:

**Tabla 1 -** Estrategia de Contención

| EVENTO Y/O INCIDENTE DE SEGURIDAD | ESTRATEGIA |
|---|---|
| **Accesos no Autorizados** | Bloqueos de cuenta<br>Apagado de la máquina<br>Bloqueo de puertos |
| **Códigos Maliciosos** | Desconexión de la red del equipo afectado<br>Bloqueo de Puertos<br>Actualización de herramientas de detección y bloqueo de software malicioso |
| **Reconocimiento** | Nuevas reglas de filtrado<br>Bloqueo de Puertos |
| **Corrupción** | Retiro de funcionario<br>Bloqueo de Cuentas |

**5.5.2. Erradicación y Recuperación:** una vez realizada la contención, se debe dar continuidad a la erradicación, 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 TI de MinAgricultura. Adicionalmente, para el caso de los incidentes de seguridad de la información 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 2 -** Estrategia de recuperación de incidentes de seguridad

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

## 5.6. COMUNICACIÓN

Cuando se presente un incidente de seguridad de la información, a través del Comité de Seguridad, o el que haga sus veces, 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.

El Ministerio de Agricultura y Desarrollo Rural determina y reconoce como instancias de la política de seguridad digital a:

- El Comité de Seguridad Digital.
- El Centro Cibernético Policial (CCP).
- Las Unidades cibernéticas de las Fuerzas Militares.

Ante un incidente de seguridad de la información, y previa verificación y aprobación Comité de Seguridad o el que haga sus veces, se debe reportar en primera instancia a las siguientes partes interesadas:

- Proceso de control interno a la gestión, gestión del talento humano y/o gestión para la contratación (cuando se logré comprobar la participación de un funcionario de la Entidad en la materialización del incidente presentado)
- ponal.csirt@policia.gov.co (Centro de respuesta a incidentes de seguridad informática de la Policía Nacional)
- incidentesseginf@mintic.gov.co (equipo de coordinación de incidentes de seguridad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones)
- csirtgob@mintic.gov.co (CSIRT de Gobierno Digital)

- Comando Conjunto Cibernético de las Fuerzas Militares (CCOCI)

Aquellos incidentes de seguridad de la información que estén relacionados con afectación de datos personales en la organización requieren una comunicación detallada mediante la construcción de informes internos que deben ser reportados a la Superintendencia de Industria y Comercio (contactenos@sic.gov.co) y los titulares afectados en el incidente mencionando. Debe contener como mínimo la siguiente información:

- Descripción del incidente
- Hora y fecha de inicio del incidente y de finalización
- Cantidad de titulares afectados en el incidente
- Posibles consecuencias al titular
- Tipo de información comprometida en el incidente
- Medidas tomadas por parte de la organización para mitigar cualquier impacto

### 5.7. 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 y reporte cuando este es evidenciado a través de las diferentes alertas y/o medios de comunicación que posea el Ministerio el potencial evento y/o incidente de seguridad de la información de seguridad.<br><br>Nota.<br>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<br>Llamada telefónica<br>Chat |

| Nº | ACTIVIDAD | RESPONSABLE | DOCUMENTO |
|---|---|---|---|
| **2** | Registre la situación de seguridad de la información en la herramienta de gestión, documentando los datos solicitados en el mismo, tales como: línea cronológica, activo de información involucrado o afectado, identificación de las fuentes de información, entre otros. | Mesa de Servicio | Registro en la herramienta de gestión |
| **3** | Clasificar la situación de seguridad de la información (evento o incidente) si se trata de un incidente se debe registrar el impacto sobre los activos de información. Todo ello se debe documentar en el registro de la herramienta de gestión<br><br>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.* ©<br><br>Si se clasifica como un 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 |
| **4** | Realizar 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.<br><br>Nota.<br>Dentro de la planeación para la atención del incidente de seguridad, se debe tener en cuenta los tiempos, así como aquellas necesidades de recursos logísticos, humanos, áreas interesadas, entre otros aspectos. | ERISI<br>Oficial de Seguridad de la Información | Plan de Acción |
| **5** | Recolectar las evidencias de los activos de MinAgricultura que con ocasión del incidente de seguridad se ven afectados. | ERISI | Informes de Recolección de Evidencias |

| Nº | ACTIVIDAD | RESPONSABLE | DOCUMENTO |
|---|---|---|---|
| | 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. © | Oficial de Seguridad de la Información | Formato cadena de custodia F01-PR-GST-06<br><br>Evidencias |
| **6** | Realizar una contención del incidente evitando cualquier tipo de propagación que pueda seguir afectando los activos de información del MinAgricultura. © | ERISI<br>Oficial de Seguridad de la Información<br>Oficina de TIC | Informe de Contención del incidente de seguridad de la Información en la herramienta de gestión |
| **7** | Eliminar cualquier causa raíz que pudiera existir con ocasión de la incidencia presentada. Elaborar un plan de remediación, con la finalidad de poder cerrar las vulnerabilidades detectadas. | Grupo ERISI<br>Oficial de Seguridad de la Información<br>Oficina de TIC | Informe de Erradicación y Remediación<br>en la herramienta de gestión |
| **8** | Evaluar 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 de Seguridad o el que haga sus veces<br>Oficina Jurídica<br><br>Oficina de Comunicaciones | Acta del Comité.<br>Informe de Contención del incidente de seguridad de la Información en la herramienta de gestión<br><br>Evidencias Digitales |
| **9** | Realizar un registro detallado de toda gestión de incidentes de seguridad, con el fin de poder desarrollar acciones correctivas para posteriores eventos o incidentes.<br><br>Nota: Las acciones correctivas se adelantan aplicando el “Procedimiento acciones preventivas, correctivas y de mejora (PR-SIG-06).” | ERISI<br>Oficial de Seguridad de la Información | Registro herramienta de gestión<br><br>Formato solicitud de acciones preventivas, correctivas o de mejora (F01-PR-SIG-06)<br><br>Informe de recolección de Evidencias,<br>Informe de Contención del incidente,<br>Informe de Erradicación y remediación, en la herramienta de gestión. |

| Nº | ACTIVIDAD | RESPONSABLE | DOCUMENTO |
|---|---|---|---|
| **10** | Notificar al que reportó la situación de seguridad y cerrar el evento o incidente de Seguridad de la Información actualizando en la mesa de ayuda el estado del incidente. | ERISI<br>Oficial de Seguridad de la Información<br>Mesa de Ayuda | Registro en la herramienta de gestión |

## 7. DOCUMENTOS DE REFERENCIA

Políticas de Seguridad y Privacidad de la Información
Información registrada en la herramienta de gestión del SGSI
Formato de Cadena de Custodia F01-GST-PR-06

## 8. HISTORIAL DE CAMBIOS

| Fecha | Versión | Descripción |
|---|---|---|
| 25-11-2016 | 1 | Primera versión del documento |
| 20-11-2020 | 2 | Actualización del documento, de conformidad con los lineamientos de la materia |