Subsecretaría de Agricultura

PROCEDIMIENTO PARA GESTIÓN DE INCIDENTES

Código:	TI-PRO-04
Versión:	4.0
Fecha de la versión:	20-12-2017
Creado por:	Daniel Coronado Rojo
Aprobado por:	Jorge Vega Saavedra
Nivel de confidencialidad:	Uso Interno

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
12-07-2013	1.0	Cristobal Nef	Redacción del Documento.
30-12-2013	2.0	Cristobal Nef	Edición de los campos.
27-10-2015	3.0	Daniel Coronado	Modificación de controles de referencia a la norma ISO 27001:2013. Se agregaron puntos y se modificó ubicación y campos del registro de incidentes.
20-12-2017	4.0	Daniel Coronado	Se revisa y modifica los campos según la vigencia del contenido, de acuerdo a lo existente en la subsecretaría. Se actualizan los datos referentes a la legislación vigente y los requisitos contractuales. Se agregan los campos de "Ámbito de ejecución, y alcance" (pág. 4), "control legal y normativo" (pág. 4), "Documentos de referencia" (pág. 5), y "Definición respecto a las materias específicas abordadas" (pág. 6).

Enfoque de género

El uso de un lenguaje que no discrimine ni marque diferencias entre hombres y mujeres ha sido una preocupación en la elaboración de este documento. Sin embargo, y con el fin de evitar la sobrecarga gráfica que supondría el utilizar en español o/a para marcar la existencia de ambos sexos, se ha optado por utilizar el masculino genérico, en el entendido de que todas las menciones en tal género representen siempre a todos/as.

Confidencialidad

Tabla de contenido

Clasificación del Documento

Nivel de Confidencialidad: Uso Interno.
Nota de Confidencialidad: Documento disponible sólo a funcionarios de la Subsecretaría de Agricultura y personal externo autorizado.

1. Objetivo

El objetivo del presente documento es asegurar que la ocurrencia de incidentes y debilidades detectados en los sistemas de seguridad de la información, que relacionados entre ellos, generen acciones preventivas oportunas, así como las necesarias de carácter correctivo, además, establecer un método y enfoque consistente y eficaz en la gestión de los incidentes de seguridad de la información, y finalmente definir el alcance, marco de referencia y responsabilidades, respecto de la notificación de los registros y la gestión de los incidentes de la seguridad de la información, que afectan la disponibilidad, integridad y confidencialidad de los activos de información.

2. Ámbito de ejecución, y alcance

El procedimiento "TI-PRO-04 Procedimiento para gestión de incidentes", se aplica a todos quienes cumplen funciones en la Subsecretaría, ya sea en sus instalaciones o fuera de ellas, tanto a funcionarios, así como también, a personas naturales y jurídicas externas, públicas o privadas que presten servicios en la Subsecretaría o para este y que tengan participación en las actividades descritas en este documento.

El ámbito de ejecución de este procedimiento, son todos los activos de información de la Subsecretaría y aquellos bajo su responsabilidad que estén contemplados en el documento. Su cobertura se extiende a la información impresa y también a aquella almacenada electrónicamente, y transmitida por cualquier soporte o medio. Se debe precisar que el alcance aplica para los siguientes procesos de provisión de productos estratégicos de la Subsecretaría de Agricultura: Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.

3. Control legal y normativo

- D.S. N°14/2014. MODIFICA DECRETO Nº 181, DE 2002, QUE APRUEBA REGLAMENTO DE LA LEY 19.799 SOBRE DOCUMENTOS ELECTRÓNICOS, FIRMA ELECTRÓNICA Y LA CERTIFICACIÓN DE DICHA FIRMA, Y DEROGA LOS DECRETOS QUE INDICA,
- D.S. N°83/2004. Norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos,
- D.S. N°93/2006. Norma técnica busca minimizar reducción de correos electrónicos masivos en el estado y sus funcionarios,
- D.S. N°1/2015. APRUEBA NORMA TÉCNICA SOBRE SISTEMAS Y SITIOS WEB DE LOS ÓRGANOS DE LA ADMINISTRACIÓN DEL ESTADO,
- Ley N°17.336/2004. Ley sobre propiedad intelectual,
- Ley N°19.223/1993. Ley sobre figuras penales relativas a la informática,
- Ley N°19.628/1999. Ley sobre protección de la vida privada,
- Ley N°19.799/2002. Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma,
- Ley N°19.927/2004. Ley modifica códigos penales en materia de delitos sobre pornografía infantil,
- Ley N°19.880/2003. Ley sobre procedimientos administrativos que rigen los actos de los órganos del Estado,
- Ley N°20.285/2008. Ley sobre acceso a la información pública,
- Ley N° 19.496. Ley de Protección del Consumidor, N° 19.496, Artículo 28B,

- PNCS. Política Nacional de Ciberseguridad,
- UMyGD. Otras normas Unidad de Modernización y Gobierno Digital y
- Internet Segura – MINEDUC. Internet Segura.

4. Documentos de referencia.

- TI-SSI-01 Política General de Seguridad de la Información.
- Norma NCH ISO 27002:2013.
- TI-PRO-09 Procedimientos para el monitoreo de sistemas y activos TI.

5. Definiciones

A continuación, una definición de un término clave utilizado en este documento:

Activo de Información: Los activos de información son todos los elementos para la producción, el procesamiento, la emisión, el almacenaje, la comunicación, la visualización, los encargados y la recuperación de la información que tiene un elevado valor para la organización. Pueden clasificarse en personas, sistemas y datos.

Incidente: Un incidente es aquello que sucede en el curso de un asunto y que tiene la fuerza, por las implicancias que conlleva, de cambiar por completo su curso y por su puesto obstaculizar que la situación se desarrolle normalmente como se venía haciendo.

Propietario de la información: Es quien genera, mantiene y utiliza la información, siendo responsable de ella y de los procesos que se llevan a cabo en su procesamiento, a través de diversos medios, sean éstos manuales, mecánicos o electrónicos.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información; también puede involucrar otras propiedades como autenticidad, responsabilidad, no-repudio y confiabilidad.

Mesa de Ayuda: 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 (TI).

6. Roles y responsabilidades

Para cumplir con los objetivos de la presente política, se establecen los siguientes roles y responsabilidades:

Encargado de Seguridad de la Información: Funcionario a cargo del desarrollo e implementación de la Política del Sistema de Seguridad para el Servicio, así como también, de velar por la correcta aplicación tanto de esta política, como a su vez, de los instrumentos de apoyo utilizado para ello (Políticas y Procedimientos).

Comité de Seguridad de la Información: Es responsable por la existencia y cumplimiento de las medidas de seguridad de la información acorde con las necesidades de la Subsecretaría, los recursos disponibles y la normativa vigente.

Jefe Departamento TI: Responsable de definir los dominios de seguridad, implementar medidas de control para las excepciones de acceso directo desde dominios externos hacia servicios de producción entre otros accesos perimetrales de la red, gestionar y controlar el sistema de gestión de seguridad sobre la protección de los activos de información del servicio, conforme a la normativa vigente y los objetivos estratégicos institucionales.

Jefe Departamento Administración: Responsable de definir e implementar las medidas de control de acceso a las instalaciones de la institución, gestionar y controlar que todas las instalaciones del edificio a nivel central, como las oficinas regionales (Seremias) funcionen en condiciones adecuadas.

Mesa de Ayuda (personal): El personal o recurso humano encargado de Mesa de Ayuda son responsables de proporcionar respuestas y soluciones a los usuarios con problemas relacionado al uso de estaciones de trabajo y/o portátiles, periféricos, servicio de internet y de software.

Funcionario de la Subsecretaría de Agricultura: Responsable de cumplir con lo establecido en este documento y aplicarlo en su entorno laboral. Tiene la obligación de alertar de manera oportuna y adecuada, a través de canales y procedimientos formalmente establecidos, cualquier situación que pueda poner en riesgo la seguridad de la información.

7. Definición respecto a las materias específicas abordadas

El presente procedimiento aborda los siguientes controles de seguridad de la información:

Código control	Nombre control NCH ISO 27001:2013	Definición	Procesos estratégicos vinculados
A.7.2.3	Proceso disciplinario	Debe existir un proceso disciplinario formal y sabido por los empleados para tomar acciones en contra de los empleados que han cometido una infracción a la seguridad de la información	Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.
A.16.1.1	Responsabilidades y procedimientos	Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de la seguridad de la información.	Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.
A.16.1.2	Informe de eventos	Se deben informar, lo antes	Informe de Factibilidad

	en la seguridad de la información	posible, los eventos de seguridad de la información mediante canales de gestión apropiados.	para la Construcción, Red Agroclimática Nacional y Transferencias.
A.16.1.3	Reporte de las debilidades en la seguridad	Se debe requerir a todos los empleados y contratistas que usen los sistemas y servicios de información de la organización, que observen e informen cualquier debilidad (observada o que se sospeche) en la seguridad de la información de los sistemas o los servicios.	Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Los eventos de seguridad de la información se deben evaluar y decidir si van a ser clasificados como incidentes de seguridad de la información.	Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.
A.16.1.5	Respuesta ante incidentes de seguridad de la información	Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados.	Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Se debe utilizar conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.	Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.
A.16.1.7	Recolección de evidencia	La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información que pueda servir de evidencia.	Informe de Factibilidad para la Construcción, Red Agroclimática Nacional y Transferencias.

8. Modo de Operación: Gestión de Incidentes (control de referencia A.16.1.1)

La Gestión de Incidentes es fundamental para el Sistema de Seguridad, ya que permitirá tomar acciones correctivas y preventivas para mitigar riesgos que afecten a los activos de información.

8.1. Tipos de Incidentes.

Un Incidente de Seguridad de la Información es cualquier imprevisto que ponga en riesgo la confidencialidad, disponibilidad e integridad de cualquier activo de Información de la Subsecretaría de

Agricultura.

8.1.1. *Incidentes T.I.*

Son Incidentes donde se ven involucrados activos del tipo tecnológico, tales como Computadores, Documentos Digitales, Software, enlace de comunicaciones, infraestructura de datos, etc.

Se cuenta con cinco fuentes de información:

- Mesa de ayuda: Los incidentes que debe reportar la mesa de ayuda (soporte computacional) son problemas de conexión a internet, fallas de periféricos de las estaciones de trabajos, fallas de hardware de los computadores, problemas de acceso a las carpetas compartidas, virus en los computadores, pérdida de confianza en Active Directory y problemas de uso de los activos TI designado a los funcionarios.
- Administrador de servidores: Los incidentes que debe reportar el funcionario a cargo de la administración de servidores son la caída de los servidores, ataques informáticos a las páginas ministeriales, acceso no autorizados a plataformas internas.
- Herramientas de monitoreo: En complementación al punto anterior, las herramientas Zabbix y Nagios monitorean y reportan caída de servidores, sitios web y cámaras IP de vigilancia, por medio de un e-mail.
- Enlace de datos regional: La empresa a cargo de proveer los enlaces, debe reportar cuando uno de estos presenta una intermitencia significativa (más de media hora).
- Red conectividad del estado (RCE): El ministerio de interior, a cargo de la RCE, que provee de internet a la subsecretaría, debe reportar cada vez que el servicio presente problemas o intermitencia de larga duración.

El tratamiento de estos incidentes es responsabilidad del Departamento T.I.

8.1.2. *Incidentes Administrativos*

Son aquellos imprevistos en los que se vea involucrado la administración general de las dependencias físicas de la Subsecretaría, como cortes de luz, inundaciones, robos de activos, acceso en general.

El tratamiento de estos incidentes es responsabilidad del Departamento de Administración.

8.2. Debilidades

Una debilidad u vulnerabilidad, es un factor que podría provocar un posible incidente de seguridad, y para el cual se deben tomar medidas preventivas, con objetivo de evitar que se produzca el incidente.

8.3. Reporte de incidentes y debilidades (control de referencia A.16.1.3)

8.3.1. *Incidentes (control de referencia A.16.1.2).*

Los incidentes que tienen relación con los activos TI usados por parte de los funcionarios, deben ser reportados a **Mesa de Ayuda**, por medio del anexo asignado y/o por medio del correo electrónico.

En caso de estar fuera del alcance de Mesa de Ayuda, cada funcionario, proveedor o tercero que esté en contacto con activos de información de la Subsecretaría de Agricultura, debe reportar algún incidente según corresponda:

1. Toda la información y los eventos relacionados con activos tecnológicos deben ser reportados al **Oficial de Incidentes T.I.** quien realizará el registro correspondiente.
2. Todos los demás eventos (incluidos los activos no TI) deben ser reportados al **Oficial de Incidentes Administrativo** y será este quien realizará el registro.

El Mecanismo de contacto es a través del Anexo (en horario laboral) y el teléfono Celular (en horario extra laboral). Además, se pueden reportar mediante correo electrónico (*detallados en la sección "Responsables"*).

8.3.2. *Debilidades u vulnerabilidades.*

Las debilidades pueden desencadenar en incidentes futuros, por lo que el reporte de estas, tiene la misma importancia que un evento.

Cada funcionario, proveedor o tercero que se encuentre en presencia de una debilidad (futuro incidente) debe reportarlo al **Oficial de Incidentes T.I o al Oficial de Incidentes Administrativo** según corresponda. Para esto debe utilizar el mismo mecanismo de contacto que un incidente.

8.4. Evaluación y decisión sobre los eventos de seguridad de la información (control de referencia A.16.1.4)

Cuando se reporta una incidencia u debilidad, los responsables de gestionar los eventos, deben evaluar el grado de criticidad del evento detectado u reportado, para determinar si realmente afecta a la integridad de los Activos de Información de la subsecretaria, además cuantificar el daño que podría provocar en el funcionamiento de los procesos. La Criticidad del incidente se determina bajo dos parámetros los cuales son la clase de activos y nivel de daño.

8.4.1. *Clase de Activos*

Los Activos se clasifican en 3 Clases:

Clase C: Activos utilizado gran parte por los funcionarios de la subsecretaría, como el caso computadores, telefonía móvil e IP, softwares ofimáticos, impresoras y documentos en papel u similares que no son esenciales en la integridad y disponibilidad de los procesos de provisión.

Clase B: Equipamiento de mediana importancia, vale decir, cuya interrupción no agrava el funcionamiento de los procesos en la subsecretaria, como el sistema de reloj control, servidor call manager, cámaras de vigilancia IP y documentos u carpetas con información medianamente importantes.

Clase A: Activos de altísima importancia, cuya interrupción puede perjudicar gravemente el correcto funcionamiento de los procesos de la subsecretaria como son los Servidores Críticos, Softwares esenciales como PYR y Unibox, el hardware del Data Center, Informes o carpetas con información restringida de altísima importancia.

8.4.2. *Nivel de daño.*

El nivel de daño se clasifica en 3 niveles:

Bajo: Imprevisto u fallas de bajo impacto como son periféricos desconectados u defectuosos, problemas de funcionamiento a nivel de software con una resolución no dificultosa, entre otros.

Medio: Daño con un impacto de mediana consideración como son: daños a ciertas piezas de hardware (que pueden ser reemplazables), interrupciones del servicio de telefonía IP, Internet u suministro eléctrico, ataques informáticos del tipo DDOS, y daños a documentos en papel o carpetas de importancia, pero no comprometiendo completamente la integridad de este.

Alto: Imprevisto grave con un daño irreparable o cuya recuperación es muy difícil como son hurtos de equipos u robo de activos de información, daños por desastres naturales, subidas u baja de voltajes y los sabotajes.

8.4.3. *Tabla Matriz de Criticidad*

Para facilitar la decisión en la gestión de los incidentes, se usa un sistema de puntaje que variará según la naturaleza del activo y el grado de daño del incidente detectado, lo cual permitirá determinar el grado de priorización en el tratamiento de las incidencias.

8.4.3.1. Criterios en la determinación del puntaje en la Clase de Activos: *La cantidad de puntaje se determina según la importancia de la clase de activos, en el funcionamiento de los servicios de la subsecretaría. Siendo el valor 3 el máximo.*

Clase de Activos	Puntaje
Clase C	1
Clase B	2
Clase A	3

8.4.3.2. Criterios en la determinación del puntaje en el nivel de daño: *La cantidad de puntaje se determina según el tipo de daño, siendo el valor 3 el máximo.*

Nivel de Daño	Puntaje
Bajo	1
Medio	2
Alto	3

8.4.3.3. Criterios en la determinación del puntaje en el grado de criticidad: *Se calcula multiplicando el puntaje de la clase del activo, por el grado de daño. El nivel de criticidad se divide y determina en 3 grupos según el puntaje:*

Puntaje	Grado de Criticidad	Color de Celda
De 1 a 3	Baja	Verde
De 4 a 6	Leve	Amarrillo
De 7 a 9	Grave	Rojo

8.4.3.4. Matriz de grado de criticidad

Clase de Activos /Nivel de Daño	Bajo	Medio	Alto
Clase C	1	2	3
Clase B	2	4	6
Clase A	3	6	9

Por lo visionado en la matriz, un incidente que afecte a un activo de clase A con un nivel de daño alto, tiene más prioridad que un incidente en un activo clase B y C (cualquiera sea su daño).

8.5. Proceso de tratamiento para Incidentes de seguridad.

La persona que recibió la información sobre un incidente establece el origen y, si es necesario, sugiere medidas preventivas y correctivas.

El tratamiento del incidente involucra una solución del incidente, un análisis de causa para determinar la razón y una acción correctiva para evitar la recurrencia.

8.6. Respuesta ante incidente de Seguridad de la Información (control de referencia A.16.1.5)

La respuesta ante incidentes de seguridad de la información, va depender según la clase de activos TI que se vea afectados, además del nivel de daño.

De afectar a los Activos de Clase C y cuyo nivel de daños sean de nivel bajo y medio, los técnicos responsables del soporte de Mesa de Ayuda (en el caso de activos TI) y el Jefe Departamento de Administración (en caso de un activo no TI), deberán registrar todos los datos del incidente. El proceso de registro variará de la siguiente forma:

- En el caso de los activos TI, el personal de Mesa de Ayuda ingresa los datos del Incidente (nombre funcionario, tipo de activo involucrado, descripción del problema y medidas tomadas para su resolución), en el Dashboard de Mesa de Ayuda. Cada incidente tiene su respectivo Ticket con su propio ID (para más detalles revisar la TI-PRO-09 Procedimientos para el monitoreo de sistemas y activos TI).

- En el caso de los activos no TI, el Jefe Departamento de Administración o quien lo subrogue, lo registra en la planilla de incidentes, cuyos campos se detallará en el aparto de "registro de control de este procedimiento".

En caso que el nivel de daño del activo de clase C sea alto, y además que el incidente afecte a los activos de Clase B y A, el personal responsable de gestionar este tipo de incidentes, deben tomar en cuenta los siguientes puntos:

- Recopilar la evidencia lo más pronto posible, después de la ocurrencia del incidente.
- De ser un incidente que comprometa acciones legales, debe realizarse un análisis forense de la seguridad de la información.
- Si la incidencia es grave y sobrepasa el alcance de los Departamentos de TI y de Administración, debe ser escalado a los proveedores (dependiendo del SLA) u otros organismos según sea el caso.
- Registrar y Documentar las resoluciones de los incidentes, para realizar futuros análisis.
- Si el incidente involucra directamente a funcionarios de la subsecretaría y/o proveedores u organismo externos, deben ser notificados (e-mail, teléfono...).
- Identificar y registrar en el Registro de Incidentes, debilidades que causen o contribuyan al evento ocurrido en aquellos activos de Clase B y A.
- Una vez que el incidente se haya resuelto, debe ser documentado, y si además los activos involucrados son de Clase B y A, deben ser registrado y llenado todos los campos presentes en el **Registro de Incidentes**.

8.7. Aprendizaje a partir de los incidentes (control de referencia A.16.1.6)

El Encargado de Seguridad de la Información debe analizar cada tipo de incidente registrado en el "Registro de Incidentes", y si fuera necesario, debe sugerir medidas preventivas o correctivas, con objetivo de evitar que estos se repitan y causen mayor impacto en la institución.

8.8. Medidas disciplinarias; recolección de evidencia (controles de referencia A.7.2.3 y A.16.1.7)

El Encargado de Seguridad de la Información debe activar el proceso disciplinario por cada violación a las reglas de seguridad.

Si un incidente requiere de evidencia para poder cursar acciones legales, el Encargado de Seguridad de la Información es el responsable de recolectarla para su uso formal.

8.9. Responsables.

Los respectivos Oficiales de Incidentes, son los encargados de informar y dar apoyo al **Encargado de Seguridad de la Información**, en la corrección o prevención de un Incidente o Debilidad respectivamente.

El Oficial de Incidentes T.I. es el Jefe Departamento T.I. y el Oficial de Incidentes Administrativos es el Jefe Departamento Administración.

9. Registro de control de este procedimiento

Nombre del registro	*Ubicación de archivo*	*Persona responsable del archivo*	*Controles para la protección*	*Tiempo de retención*
Captura de pantalla del sistema de gestión de tickets	Adjunto como evidencia en este documento	-Jefe Departamento TI	No aplica	Válido según la vigencia de este documento.
Registro de Incidentes	Cuenta Informática, repositorio OneDrive.	-Oficial de Incidentes T.I. -Oficial de Incidentes Administrativos. -Encargado de Seguridad de la Información.	Solamente las tres personas responsables del activo pueden editar el registro.	Indefinido

Solamente el Encargado de Seguridad de la Información puede permitir el acceso a los registros a otros empleados. El registro de Incidentes y Debilidades se realizará en la Planilla **"Registro de Incidentes"** la cual tiene los siguientes campos:

- **Fecha:** Fecha en la cual se produjo el Incidente o el reporte de debilidad.
- **Categoría:** Indica si es un Incidente o una Debilidad.
- **Input:** Indica si proviene de la Mesa de Ayuda, del Administrador de Servidores, del proveedor de enlace de datos o de Administración.
- **Clase de activo:** A cuál de las 3 clases pertenece el activo afectado.
- **Nivel daño** (Aplica para los Incidentes)**:** Grado de avería o deterioro del activo.
- **Grado de Criticidad** (Aplica para los Incidentes)**:** Nivel de criticidad del incidente.
- **Descripción:** Reseña del Incidente o Debilidad.
- **Nombre - Entidad:** Persona o entidad que reportó el incidente/debilidad.
- **Tratamiento:** Forma en la cual se solucionó dicho incidente/debilidad.
- **Análisis de causa:** Observaciones sobre el por qué ocurrió dicho evento.
- **Acciones Correctivas** (Aplica para los Incidentes)**:** Indicar lo que se realizó para evitar nuevamente el Incidente

- **Tratada:** Si la debilidad o incidente fue resuelto o se está a la espera o no hay aparente solución.

10. Difusión

El "TI-PRO-04 Procedimientos para la gestión de incidentes" deberá ser difundida -según lo expresado en la Política General de Seguridad de la Información- por medio de la intranet institucional, o por vía circular o por decreto, y/o vía correo electrónico según sea pertinente, asegurándose una completa cobertura.

11. Validez y gestión de documentos

Este documento es válido desde el 20-12-2017

El propietario de este documento es el Jefe Departamento TI, quien deberá verificar la vigencia del contenido, por lo menos una vez al año. Si el documento necesita ser modificado y/o debe realizarse alguna actualización, tendrá que ser notificado al resto de los miembros del Comité de Seguridad de la Información.

La periodicidad de evaluación del documento debe hacerse al menos una vez cada un año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de debilidades o incidentes que no fueron reportados a las personas autorizadas.
- Cantidad de incidentes que no fueron tratados de la forma más adecuada.
- Cantidad de incidentes que no fueron anotados en el Registro de incidentes.
- Cantidad de incidentes para los cuales la evidencia para acciones legales fue inadecuada.
- Cantidad de violaciones a las reglas de seguridad en las que no se activó un proceso disciplinario.

Creado por:

Ingeniero Proyectos TI
Daniel Coronado Rojo

Validado por:

SUBSECRETARIA DE AGRICULTURA
JEFE DEPTO TECNOLOGIAS DE LA INFORMACIÓN

Jefe Departamento TI
Rafael Reyes Cuevas

Jefe Departamento de Administración
Claudio Yañez Gajardo

Aprobado por:

SUBSECRETARIA DE AGRICULTURA
JEFE DIVISION ADMINISTRATIVA

Encargado de Seguridad de la Información
Jefe División Administrativa
Jorge Vega Saavedra