MUNICIPALIDAD
OSORNO

OSORNO, 30 DIC 2024

MAT.: APRUEBASE "POLITICA GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION" DEL DEPARTAMENTO DE SALUD MUNICIPAL.

DECRETO N° 17.819 **/ VISTOS:**

El Departamento de Salud de la Ilustre Municipalidad de Osorno atendiendo a la relevancia que implica alcanzar niveles adecuados de integridad, confidencialidad y disponibilidad de la información, considera necesaria la creación de la **Política Gestión de Incidentes de Seguridad de la Información** basado en las normas oficiales chilena Nch-ISO 27001/2013, con la finalidad de establecer lineamientos y criterios para dotar al personal del Departamento de Salud de conocimientos, competencias y conciencia necesarios para cumplir sus roles como guardianes de los datos sensibles y activos de información.

.

CONSIDERANDO:

Lo dispuesto en la Ley N° 19.378 que establece Estatuto de Atención Primaria de Salud Municipal;

Lo dispuesto en la Ley N° 18.575 Orgánica Constitucional sobre Bases Generales de la Administración del Estado;

La Ley 18.883 Estatuto Administrativo para Funcionarios Municipales;

La Ley 19.880 que establece las Bases de los Procedimientos Administrativos que Rigen;

Los actos de los Órganos del Estado, en especial su art. 52, que establece que los actos administrativos no tendrán efectos retroactivos, salvo cuando produzcan efectos favorables para los interesados y no lesionen derechos de terceros; y

Las facultades que me confiere la Ley 18.695 Orgánica Constitucional de Municipalidad

Que, en Decreto N° 9336 de fecha 12 de agosto 2019 se constituye "**Comité de Seguridad de la Información (CSI)**" y Decreto N° 10093 de 30 agosto 2019 que nombra "**Política General de la Información del Departamento de Salud de la Ilustre Municipalidad de Osorno**".

I. MUNICIPALIDAD OSORNO DIRECCIÓN JURÍDICA

D E C R E T O:

APRUEBASE "POLITICA GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION", que como anexo en texto íntegro se incorpora al presente Decreto.

ANOTESE, COMUNIQUESE, CUMPLASE Y ARCHIVESE

I. MUNICIPALIDAD OSORNO SECRETARIA MUNICIPAL

ALCALDIA MUNICIPAL OSORNO

YAMIL UARAC ROJAS
SECRETARIO MUNICIPAL

JAIME BERTIN VALENZUELA
ALCALDE MUNICIPALIDAD OSORNO

JBV/YUR/MMM/LVM
DISTRIBUCIÓN:

- Administrador Municipal I. Municipalidad de Osorno.
- Encargado Seguridad de la Información DESMO.

I 1883865

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

DEPARTAMENTO DE SALUD

Elaborado por:	Aprobado por:
Luis Sergio Vidal Montiel Encargado de la Seguridad de la Información	Muriel Muñoz Moreno Jefe Departamento de Salud
MUNICIPALIDAD OSORNO UNIDAD TIC DEPARTAMENTO DE SALUD	I. MUNICIPALIDAD OSORNO JEFE DEPARTAMENTO DE SALUD DEPARTAMENTO DE SALUD

Contenido

I.- INTRODUCCION 3
II.- OBJETIVO GENERAL 3
III.- ALCANCE O ÁMBITO DE APLICACIÓN INTERNO 3
IV. DEFINICIONES 4
V. RECURSOS DE SEGURIDAD 5
1. Identificación de amenazas 5
2.- Flujo del proceso del incidente 5
VI.- ROLES y RESPONSABILIDADES 6
VII.- POLITICA. 7
1. Responsabilidades y procedimientos. 7
2.- Notificación de los eventos de seguridad de la información. 8
3.- Notificación de puntos débiles de la seguridad. 8
4.- Evaluación y decisión sobre los eventos de seguridad de la información. 8
5.- Respuesta a incidentes de seguridad de la información. 9
6.- Aprendizaje de los incidentes de seguridad de la información. 10
7.- Recopilación de evidencias 10
VIII. INCUMPLIMIENTO 11
IX. REVISIONES 11
X. MECANISMOS DE DIFUSION DE LA POLÍTICA 11
XI. CONTROL DE CAMBIOS. 11
ANEXO A 12

I.- INTRODUCCION

En administración, se define Gestión como el área de una organización que busca utilizar y aprovechar los recursos disponibles de la manera más eficiente posible. Esto, con el fin de mantener una producción fluida, mejorar los procedimientos y conducir la información de una forma adecuada y oportuna.

Entre las funciones más relevantes que tiene la gestión, está la planificación y organización del flujo de trabajo, así como del factor humano que se encarga de ejecutar las tareas requeridas. En seguridad de la información, la gestión se encarga de velar, supervisar y controlar los incidentes de seguridad de la información.

Se denomina incidente de seguridad de la información al evento no deseado que atenta contra la Confidencialidad, Integridad o Disponibilidad de la Información del Departamento de Salud Municipal.

Los eventos pueden manifestarse de varias maneras: infracción de la política de seguridad, medidas de seguridad inadecuadas o incompletas, la falta de concientización frente a un riesgo de seguridad de la información, desconocimiento de los procedimientos para mitigar los peligros de vulnerabilidades de la información, desconocimiento de las categorías documentales, entre otros.

Mitigar los incidentes de seguridad de la información es la identificación de las posibles amenazas que puede afectar los activos del Departamento de Salud, generar acciones correctivas y preventivas en vías de mejoras, manteniendo un registro actualizado de incidentes, del análisis y de las acciones realizadas.

La respuesta de solución no es solo individual, es un evento grupal, donde participa toda la organización. La pérdida o mal uso de un activo de información genera grietas que deben cerrarse en harás del resguardo y cuidado de la información.

II.- OBJETIVO GENERAL

Gestionar los incidentes de seguridad de la información frente a diversas amenazas internas o externas, con el fin de disminuir y minimizar el impacto frente a los activos de información del Departamento de Salud.

III.- ALCANCE O ÁMBITO DE APLICACIÓN INTERNO

La presente política es aplicable al Departamento de Salud Municipal y todas sus áreas en donde el Sistema de Gestión de Seguridad de la Información (SGSI) genera control a través de su Política General de Seguridad de la Información; es decir, sus procesos, funcionarios (planta, contrata, honorario, reemplazo o suplencia) y terceros con ocasión de un contrato, acuerdo u otra negociación.

Esta política contempla el siguiente control definido en la norma NCh-ISO 27001:2013

Anexo	Controles
A.16	**Gestión de incidentes de seguridad de la información**
A16.1	Gestión de incidentes de seguridad de la información y mejoras
A16.1.1	Responsabilidades y procedimientos
A16.1.2	Notificación de los eventos de seguridad de la información
A16.1.3	Notificación de puntos débiles de la seguridad
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información
A16.1.5	Respuesta a incidentes de seguridad de la información
A16.1.6	Aprendizaje de los incidentes de seguridad de la información
A16.1.7	Recopilación de evidencias

IV. DEFINICIONES

- **Activos de Información**: Corresponde a todos aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información de valor para la institución.
- **Amenaza**: Es un evento con el potencial de afectar negativamente la Confidencialidad, Integridad y/o disponibilidad de los Activos de Información de una organización.
- **Criticidad**: Medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.
- **Debilidad**: Cualquier evento o circunstancia que pudiera dar origen a un incidente de seguridad, a causa de la existencia de un riesgo no detectado o por la ineficacia o ausencia de control de seguridad de la información.
- **Evento de Seguridad:** Cualquier ocurrencia identificada en un sistema de información, servicio o estado de la red que indica una posible infracción en la seguridad de la información, en la política o fallo en los controles.
- **Evaluación de riesgos:** Es el proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.
- **Incidente de Seguridad:** Cuando el evento se puede clasificar como no deseado o inesperado dentro de los eventos de seguridad de la información y además tienen una probabilidad significativa de comprometer las operaciones comerciales y suponen una seria amenaza para la seguridad de la información.
    - **Ejemplos de incidentes de seguridad de la información**:
        - Pérdida de servicio, de equipos o de instalaciones;
        - Mal funcionamiento o sobrecargas del sistema;
        - Errores humanos;
        - No cumplimiento con políticas o procedimientos;
        - Violaciones de las disposiciones de seguridad física;
        - Mal funcionamiento de software o hardware;
        - Violaciones de acceso.
    - **Los incidentes obedecen a la siguiente clasificación**:

- Denegación de servicios computacionales.
- Código malicioso.
- Accesos no autorizados.
- Mal uso de recursos.
- Aplicativos de negocios. Violación de normativa de seguridad, código de ética y reglamento interno.

- **Impacto**: Resultado de un incidente de seguridad de la información.
- **ISO**: Organización Internacional de Normalización, con sede en Ginebra (Suiza).
- **ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO.
- **Riesgo**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **Vulnerabilidad**: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo de información.

V. RECURSOS DE SEGURIDAD

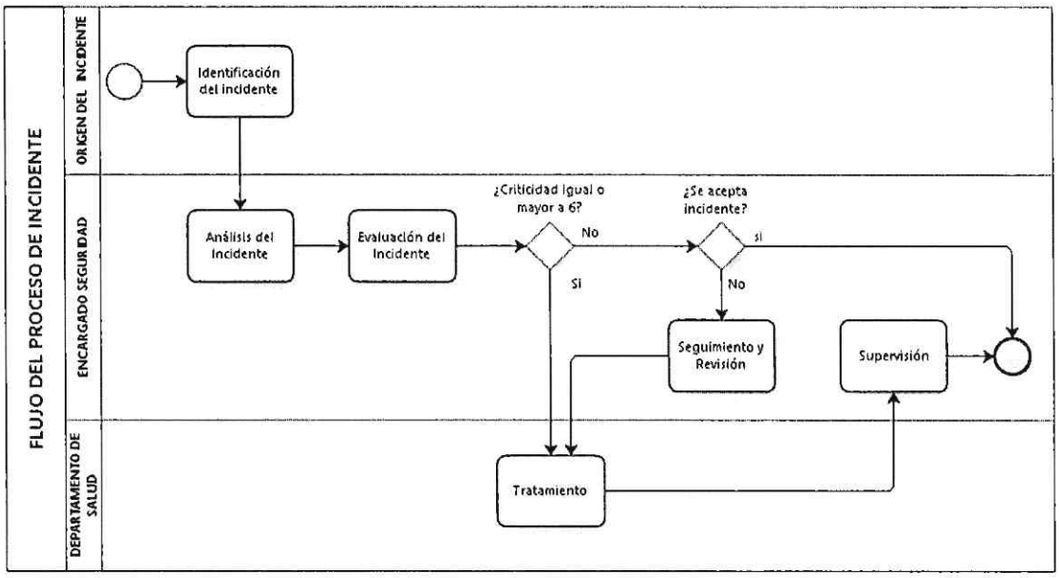
1. Identificación de amenazas

La identificación de las amenazas que potencialmente podrían afectar a la institución se las describe como fenómenos, sustancias, actividad humana o condición peligrosa que pueden ocasionar impactos de seguridad de la información. Es un factor ajeno y fuera de control, representado por un fenómeno físico que está latente, y que puede ocurrir y producir un desastre de información al manifestarse. A continuación, la amenazas que podría sufrir los activos de información:

ACTIVO	AMENZA
Entorno	Desastres naturales, Incendio
Equipamiento	Desastres naturales, Incendios, Fallas de hardware, Fallas de servicio Hurto.
Sistema de información	Hurto de código fuente, Accesos no autorizados, Falla de hardware Código malicioso.
Información	Hurto, Alteración, Divulgación no autorizada, Destrucción.
Recursos humanos	Desastres naturales, Incendios, Enfermedades, Huelgas, Ingeniería social

2.- Flujo del proceso del incidente

Para la gestión de la amenaza, se presenta un Flujo del Proceso que proporciona los pasos según la severidad de las consecuencias de los niveles de riesgo, que para esta metodología es la combinación de Urgencia / Impacto y su determinado color:



- **Origen del Incidente:** Se entiende como Origen, al punto inicial donde es descubierto el incidente, siendo cualquier área donde el Sistema de Gestión de Seguridad de la Información (SGSI) genera control a través de su Política General de Seguridad de la Información; es decir, sus procesos, funcionarios (planta, contrata, honorario, reemplazo o suplencia) y terceros con ocasión de un contrato, acuerdo u otra negociación.
- **Encargado de Seguridad**: Al identificar el incidente a través de sus vías de comunicación, deberá analizar y evaluar el grado de criticidad según el Mapa de Calor de Identificación de Incidente (VII Política, punto N° 4). Dependiendo de los niveles observados, se procederá a su tratamiento directo o indirecto. Si el nivel es alto, se iniciará su tratamiento de forma inmediata para anular o eliminar el incidente dejando al encargado de seguridad la supervisión. Si el incidente es de criticidad mediana, se procederá al seguimiento y revisión de incidente para gestionar su tratamiento. Si el incidente no presenta un riesgo severo para la organización se podría eventualmente aceptar.
- **Departamento de Salud**: Será el jefe del Departamento de salud quién designará el tratamiento y los responsables para gestionar el incidente según el nivel de criticidad.

VI.- ROLES y RESPONSABILIDADES

Encargado de la Seguridad de la Información:

1. Velar por el cumplimiento de los procesos descritos en la presente política y su difusión.
2. Informar al Departamento de Salud las vulnerabilidades realizadas por accesos no autorizados.
3. Debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

4. Debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al comité se Seguridad de la Información aquellos considerados pertinentes.

Comité de Seguridad:

1. Debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estima conveniente.

Funcionarios

1. Mencionar y dar a conocer cualquier evento sospechoso que pudiera desencadenar un incidente de Seguridad de la Información.

Unidad Tic

1. Dar solución a los incidentes de Seguridad TI detectados y normalizar la entrega de los servicios.
2. Registrar, clasificar y escalar los eventos de seguridad reportados.

Director(es), Jefes, Encargados de Unidad, Referente Técnico

1. Velar por el correcto cumplimiento de esta política.
2. Mencionar y dar a conocer cualquier evento sospechoso que pudiera desencadenar un incidente de Seguridad de la Información.

VII.- POLITICA.

1.- Responsabilidades y procedimientos.

1.1.- Responsabilidades

El Encargado de Seguridad de la información gestionará los incidentes, quién identificará o confirmará la amenaza, categorizará el incidente y le brindará los niveles de prioridad según su criticidad para realizar las tareas o procesos necesarios para gestionar el o los incidentes de forma oportuna.

Es responsabilidad de cada funcionario(a), proveedor de servicio o terceros con ocasión de un contrato, acuerdo u otra negociación, dar a conocer incidentes de información producidos o en vías de ser producidos producto de su labor o servicio que preste durante la vigencia del contrato o servicio.

1.2.- Procedimientos

Los procedimientos de incidentes son abordados a través del Formulario de Incidente de seguridad de la información y la comunicación con el punto de contacto (Anexo A).

2.- Notificación de los eventos de seguridad de la información.

Reportar de forma inmediata al Punto de Contacto a través de los canales de comunicación y administración formales de los eventos, incidentes o debilidades en cuanto a la seguridad de la información que identifiquen o se presenten.

Canales de comunicación:

a) Formulario de Incidentes de seguridad de la información (ANEXO A)
b) De forma telefónica: 64 2 208688 Anexo 8688
c) Correo electrónico: seguridad.informacion@salud.imo.cl
d) De forma presencial a Encargado de Seguridad, Matta # 455 Piso 2, Unidad TIC.

Algunas de las situaciones que se deberían considerar para el reporte de incidentes de seguridad incluyen:

a) Controles de seguridad ineficaces.
b) Vulnerabilidad en la integridad, la confidencialidad o disponibilidad de la información.
c) Incumplimientos en las Políticas de seguridad.
d) Incumplimiento en las disposiciones de seguridad física.
e) Cambios no controlados a los sistemas de información.
f) Fallas en el software y/o hardware.
g) Violaciones de accesos tanto físicos como a los sistemas de información.
h) Ataques de código malicioso.

Detectado un evento o incidente de seguridad, el Encargado de Seguridad de la información del Departamento de Salud deberá ser informado tan pronto como sea posible. Este supervisará las acciones necesarias para la resolución del incidente. Asimismo, mantendrá al resto del Comité de Seguridad de la Información al tanto del desarrollo de las actividades.

3.- Notificación de puntos débiles de la seguridad.

Se reportará e informará sobre cualquier debilidad sospechosa en la seguridad de la información de los sistemas o servicios tanto a los funcionarios como a los proveedores de servicio o terceros con ocasión de un contrato, acuerdo u otra negociación que utilizan los sistemas y servicios de información. Este proceso de información debe ser recíproco entre los usuarios y el Departamento de salud.

4.- Evaluación y decisión sobre los eventos de seguridad de la información.

El Punto de Contacto deberá evaluar el evento de seguridad de la información utilizando la escala de clasificación de eventos e incidentes de seguridad de la información y decidir si el evento se debería clasificar como un incidente de seguridad de la información. El análisis y evaluación del incidente pueden ayudar a identificar el tiempo de solución.

El nivel de prioridad para dar respuesta de solución se basará esencialmente en dos parámetros:

- **1) Impacto**: Determinará la importancia del incidente dependiendo de cómo éste afecta los procesos de la institución y/o el número de usuarios afectados:
  - **Bajo (1)**: No interrumpe los procesos generales de la institución y afecta solo a 1 usuario.
  - **Medio (2)**: Interrumpe momentáneamente los procesos de la institución y afecta a más de un usuario, pero a menos de cinco.
  - **Alto (3)**: Interrumpe seriamente los procesos de la institución y afecta a más de 5 funcionarios.

- **2) Urgencia**: Dependerá del tiempo máximo de espera que pueda aceptar el usuario para la resolución del incidente. A la aceptación de más tiempo de espera, significará que el incidente es menos urgente:
  - **Bajo (1):** El incidente de seguridad puede atenderse en un periodo mayor a 48 horas
  - **Medio (2):** El incidente de seguridad debe atenderse en un periodo máximo de 24 horas
  - **Alto (3):** El incidente de seguridad debe atenderse en un periodo máximo de 8 horas

  De la combinación de IMPACTO/URGENCIA se determina la Criticidad del incidente según gráfico de Mapa de Calor.

  - Nivel Crítico (6 a 9)
  - Nivel Grave (3 a 4)
  - Nivel Leve (1 a 2)

MAPA DE CALOR
IDENTIFICACION CRITICIDAD PARA LA ORGANIZACIÓN

		URGENCIA		
		Baja	Media	Alta
IMPACTO		1	2	3
Alta	3	3	6	9
Media	2	2	4	6
Baja	1	1	2	3

Criticidad:	
Aceptable	La incidencia tiene un efecto mínimo
Mediano	La incidencia tiene un efecto considerable
Alto	La incidencia tiene un efecto severo

5.- Respuesta a incidentes de seguridad de la información.

El Punto de Contacto y otras áreas pertinentes del Departamento de Salud deben responder ante los incidentes de Seguridad de la Información.

La respuesta debería incluir lo siguiente:

a) Recopilar la evidencia lo más pronto posible después de la ocurrencia.
b) Escalamiento, según sea necesario.
c) Asegurarse de que todas las actividades de respuesta se registren correctamente para el posterior análisis.
d) Comunicación de la existencia del incidente de seguridad de la información o cualquier detalle pertinente a otras personas u organizaciones internas o externas.
e) Manejar las debilidades de la seguridad de la información que causan o contribuyen al incidente.
f) Una vez que se ha manejado el incidente correctamente, se debería cerrar y registrar formalmente.
g) Se debe realizar un análisis post-incidente, según sea necesario, para identificar el origen del incidente.

6.- Aprendizaje de los incidentes de seguridad de la información.

Se debe utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.

La evaluación de los incidentes de seguridad de la información puede indicar la necesidad de contar con controles mejorados o adicionales para limitar la frecuencia, el daño y el costo de las ocurrencias futuras o bien se deben considerar en el proceso de revisión de las políticas de seguridad.

7.- Recopilación de evidencias

Se deben definir y aplicar procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir para propósitos de acciones legales y disciplinarias.

Cuando se siga el proceso disciplinario interno, la evidencia debe ser clara y suficiente para comprobar las acciones, para ello se deberá:

- Registrar información que rodea a la evidencia.
- Tomar fotografías del entorno de la evidencia (si aplica).
- Registrar la evidencia.
- Rotular todos los medios que serán tomados como evidencia.
- Almacenar toda la evidencia en forma segura.
- Generar copias de seguridad de la evidencia original.

Cuando la acción involucre la ley, ya sea penal o civil, la evidencia presentada debe ser conformada y aterrizada según las leyes correspondientes y ante la autoridad correspondiente y se deberá velar por la calidad e integridad de ésta.

Cualquier incumplimiento de políticas o procedimientos asociados a las materias enumeradas a continuación, podrían generar un incidente de seguridad que amerite una investigación y su correspondiente sanción disciplinaria o legal, según corresponda a la naturaleza y gravedad del incidente.

- Fuga o uso indebido de información.
- Violaciones de accesos tanto físicos como a los sistemas de información.
- Cambios no autorizados a la infraestructura tecnológica de la institución.
- Pérdida o robo de equipos y medios móviles.

- Vulneraciones a los controles de uso de recursos de internet.
- Vulneración a los controles de uso de equipos personales e instalación o uso ilegal de software.
- Uso indebido del correo electrónico institucional.
- Incumplimiento de políticas de cuentas de usuarios y contraseña.

VIII. INCUMPLIMIENTO

El incumplimiento de esta política de seguridad y privacidad de la información traerá consigo las consecuencias que apliquen a la normativa de la institución, incluyendo lo establecido en las normas que competen al Departamento de Salud en cuanto a seguridad y privacidad de la información se refiere.

IX. REVISIONES

Con el fin de asegurar su vigencia, actualización y mejora continua, la presente Política será revisada, al menos, una vez por año por parte del Comité de Seguridad de la Información, proponiendo al Departamento de Salud, las mejoras a implementar.

X. MECANISMOS DE DIFUSION DE LA POLÍTICA

La presente política, una vez aprobada, estará publicada en la página Web del Departamento de Salud (https://www.municipalidadosorno.cl/salud.php), en la intranet institucional (http://intranetosorno.cl), la página oficial del Departamento de Salud Municipal (www.desmo.cl) y será difundida para conocimiento y consulta de los funcionarios y terceros que prestan servicios, a través de difusión internas.

XI. CONTROL DE CAMBIOS.

Versión	Fecha	Principales Modificaciones (pagina /sección)	Motivo del cambio	Elaborado por	Aprobado por
V.1.0	18.12.2024	Creación del documento	-	Encargado CSI	• Presidente CSI • ESI

ANEXO A

FORMULARIO DE INCIDENTE

Fecha de notificación	____/____/	**Hora de notificación**	____:____

DATOS DE LA PERSONA QUE NOTIFICA			
Apellido y Nombres:			
Cesfam:		**Unidad**	
Correo electrónico:		**Tipo Contrato**	
Teléfono:	**Anexo:**	**Teléfono Particular**	

INFORMACIÓN SOBRE INCIDENTE			
Fecha en que observó incidente:	__/__/	**Hora en que observó incidente**	____:____
Marque con una "X" todas las opciones que considere aplicables			
	Uso indebido de información crítica		Modificación no autoriza de información sensible
	Uso prohibido de un recurso informático		Divulgación no autorizada de información personal
	Eliminación insegura de información		Intrusión física
	Modificación o eliminación no autorizada		Destrucción no autorizada de información
	Anomalía o vulnerabilidad técnica de software		Robo o pérdida de información
	Amenaza o acoso por medio electrónico		Interrupción prolongada en un sistema o servicio de red
	Ataque o infección por código malicioso (virus, gusanos, troyanos, malware, etc)		Modificación, instalación o eliminación no autorizada de software
	Robo o pérdida de recurso informático del Cesfam		Acceso o intento de acceso no autorizado a un sistema informático
	Otros no contemplados		Extracción de documentos sin autorización

INFORMACION SOBRE EL INCIDENTE
Describa el incidente:

INFORMACION SOBRE EL RECURSO AFECTADO					
¿El incidente aún está en proceso?		SI		NO	
¿Existe copia de respaldo de los datos o software afectado?		SI		NO	
¿El recurso afectado tiene conexión con la red del Departamento de Salud?		SI		NO	
¿El recurso afectado tiene conexión a Internet?		SI		NO	

_____

FIRMA

N° Incidente _____/

(uso exclusivo encargado seguridad)