MUNICIPALIDAD DE
TEMUCO

DECRETO Nº 4912

TEMUCO, 21 NOV 2025

V I S T O S:

1.- El Reglamento Interno N° 006 de fecha 20.12.2023, sobre estructuras, funciones y coordinación del Municipio de Temuco y sus modificaciones posteriores.

2.- La Ley 18.883, Estatuto Administrativo para Funcionarios Municipales.

3.- Las facultades contenidas en la Ley 18.695, Orgánica Constitucional de Municipalidades.

CONSIDERANDO:

1.- Que el Municipio de Temuco, está preocupado de mejorar su gestión interna, como así también aquella que permita mejorar la calidad de los servicios que se entregan a la comunidad.

2.- Que existe la necesidad de sistematizar, contextualizar y formalizar el Proceso de "Gestión de Incidentes de Ciberseguridad", de la Municipalidad de Temuco, para contribuir al mejoramiento de los procesos internos institucionales.

3189009

MUNICIPALIDAD DE
TEMUCO

D E C R E T O:

1.- Apruébese el Manual de Proceso que a continuación se indica:

NOMBRE DEL MANUAL	GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD
OBJETIVO DEL MANUAL	Sistematizar y estandarizar conforme a la nueva legislación vigente, el proceso de Gestión de Incidentes de Ciberseguridad.
AMBITO DE ACCIÓN	Mejora continua de los procesos internos del Municipio

2.- El presente manual reemplaza en su totalidad al aprobado por decreto N°4361 de fecha 23.11.2022.

3.- Se hace presente que el referido manual, debidamente refrendado por el Sr. Secretario Municipal, se entiende formando parte integrante del presente decreto, el cual está compuesto de 17 hojas.

ANÓTESE, COMUNÍQUESE Y ARCHÍVESE.

JUAN ARANEDA NAVARRO
SECRETARIO MUNICIPAL

ROBERTO NEIRA ABURTO
ALCALDE

JOS/est

Distribución

- Todas las unidades municipales

TEMUCO
MUNICIPIO CIUDADANO

MANUAL DE PROCESOS

"Gestión de Incidentes de Ciberseguridad"

Elaboró	Revisó	Aprobó
Jefferson Poblete Depto de Tecnologías	Oriana Castro Dubrent Encargada Depto. Calidad	Exel Silva Troppa Jefe Depto de Tecnologías

MUNICIPALIDAD DE TEMUCO
DEPTO. TECNOLOGÍA

I. ANTECEDENTES

La gestión de incidentes de seguridad de la información contempla actividades claves, tales como: el monitoreo, detección, registro y reporte a áreas pertinentes de un incidente de seguridad de la información, su análisis, su declaración como incidente y descarte; su pronta solución, su escalamiento a autoridades internas como externas, su respuesta y seguimiento.

I.1. DEFINICIONES

- **Ciberseguridad**
  - Preservación de la confidencialidad e integridad de la información y de la disponibilidad y resiliencia de las redes y sistemas informáticos, con el objetivo de proteger a las personas, la sociedad, las organizaciones o las naciones de incidentes de ciberseguridad.
- **Ciberataque:**
  - Intento de destruir, exponer, alterar, deshabilitar, o exfiltrar u obtener acceso o hacer uso no autorizado de un activo informático.
- **Vulnerabilidad:**
  - Debilidad de un activo o control que puede ser explotado por una o más amenazas informáticas.
- **Autenticación:**
  - Propiedad de la información que da cuenta de su origen legítimo.
- **Confidencialidad:**
  - Propiedad que consiste en que la información no es accedida o entregada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:**
  - Propiedad que consiste en que la información está disponible y es utilizable cuando es requerida por un individuo, entidad o proceso autorizado.
- **Integridad**:
  - Propiedad que consiste en que la información no ha sido modificada o destruida sin autorización.

- **Resiliencia o Continuidad Operacional:**
  - Capacidad de las redes y sistemas informáticos para seguir operando luego de un incidente de ciberseguridad, aunque sea en un estado degradado, debilitado o segmentado, y la capacidad de las redes y sistemas informáticos para recuperar sus funciones después de un incidente de ciberseguridad.
- **Seguridad de la información:**
  - Actúa en un ámbito mucho más amplio que la ciberseguridad, ya que busca proteger la información en todas sus formas (digital, física, verbal). Abarca políticas, procedimientos, controles físicos (como cerraduras), humanos (capacitación) y tecnológicos.
- **Activo informático:**
  - Toda información almacenada en una red y sistema informático que tenga valor para una persona u organización.
- **Red y sistema informático**:
  - Conjunto de dispositivos, cables, enlaces, enrutadores u otros equipos de comunicaciones o sistemas que almacenen, procesen o transmitan datos digitales.
- **Prestadores de servicios:**
  - Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de este.
- **ANCI:**
  - Es una autoridad nacional que se encarga de la ciberseguridad y de proteger las infraestructuras críticas del país. Este organismo tiene la responsabilidad de desarrollar, coordinar e implementar políticas y estrategias de ciberseguridad para salvaguardar tanto a entidades públicas como privadas.
- **Equipo de Respuesta a Incidentes de Seguridad Informática o CSIRT:**
  - Centros multidisciplinarios que tienen por objeto prevenir, detectar, gestionar y responder a incidentes de ciberseguridad o ciberataques, en forma rápida y efectiva, y que actúan conforme

a procedimientos y políticas predefinidas, ayudando a mitigar sus efectos.

- **Evento de Ciberseguridad:**
  - Cualquier evento que notifique el SOC y que debe ser clasificado, priorizado e investigado de acuerdo con su criticidad.
- **Falso Positivo Ciberseguridad:**
  - Un falso positivo se refiere a una situación en la cual una herramienta de seguridad o un sistema de detección indica incorrectamente la presencia de una amenaza que, en realidad, no existe.
- **Incidente de Ciberseguridad:**
  - Todo evento que perjudique o comprometa la confidencialidad o integridad de la información, la disponibilidad o resiliencia de las redes y sistemas informáticos, o la autenticación de los procesos ejecutados o implementados en las redes y sistemas informáticos.
  - En algunas plataformas estos incidentes son clasificados con prioridad “baja,” “Media,” Alta” y “Critica”.
  - La ley de ciberseguridad define que los Incidentes con efecto significativo deben ser reportados a la ANCI, estos incidentes son aquellos que comprometan:
    - La disponibilidad, confidencialidad o integridad de sistemas o datos.
    - La autenticación o continuidad operacional.
    - La seguridad de personas o servicios esenciales.
- **Ticket y Requerimiento**:
  - Se solicita un Ticket al correo de soporte técnico para solucionar o analizar un problema. Requerimiento es la solicitud para realizar alguna configuración o cambio en las plataformas.
- **Centro de Operaciones de Seguridad (SOC):**
  - Es una unidad centralizada que se encarga de monitorear, detectar, prevenir y responder a incidentes de seguridad informática en tiempo real. El cual tiene diferentes niveles de soporte de acuerdo con la criticidad.

II. FUNCIONES DE LA UNIDAD

Las funciones de la Unidad son resguardo de la información Municipal, tales como bases de datos, correos electrónicos documentos digitales, almacenados en servidores y pc.

De acuerdo con el Reglamento Interno N° 006 de fecha 20.12.2023, sobre estructuras, funciones y coordinación del Municipio de Temuco.

- Custodiar y preservar la información informática, tanto de las Bases de Datos de servidores, como computadores, asignados; unidades o funcionarios municipales, como también de la inversión en materia de sistemas, que estén asignados a su unidad.
- Supervisar el funcionamiento de los equipos y los mantenimientos preventivos y correctivos.
- mantener y administrar las redes, sistemas y equipos computacionales del sistema.
- Velar por la integridad de la información almacenada tanto en las bases de datos de servidores, como de computadores, a asignados a unidades o funcionarios municipales, además de elaborar, ejecutar y cumplir con los planes de contingencia necesarios en caso de pérdida de dicha información.

III. OBJETIVO DEL MANUAL.

Definir un marco de trabajo para enfrentar los incidentes de ciberseguridad.

- Resguardar los activos de la información, mediante controles de seguridad aplicables a partir del análisis, evaluación y tratamiento de los riesgos que afecten su confidencialidad, integridad y disponibilidad.
- Asegurar la continuidad operacional a través de acciones tendientes a gestionar los incidentes y a resolver contingencias que se detecten.

IV. OBJETIVO DEL PROCESO.

Definir un procedimiento, para gestionar los incidentes de ciberseguridad manteniendo la continuidad operativa del municipio y dando cumplimiento a la Ley de Ciberseguridad.

La gestión de continuidad de las operaciones considerara aspectos claves, tales como: la definición de una estructura organizacional adecuada para resolver acciones en cada plan; la determinación de escenarios posibles; un análisis de riesgos y consecuencias asociadas a dichos escenarios; las estrategias de continuidad de los procesos; el desarrollo de procedimientos alternativos de operación, si corresponde; los componentes informáticos y no informáticos de apoyo y las acciones de recuperación ante contingencias.

V. ALCANCE DEL MANUAL

El presente Manual es aplicable a funcionarios de planta, contrata y honorarios que formen parte de la Municipalidad de Temuco, así como también a asesores, consultores, practicantes y personas naturales o jurídicas que presten servicios para la Municipalidad.

Funcionarios de los Diferentes Departamentos de Tecnologías o Informática, incluidos Municipalidad, Educación, Salud y Cementerio.
Adicionalmente, empresas que dan servicio a la municipalidad, por ejemplo, Opciones, SMC, etc.

VI. CONTROL DEL MANUAL

El resguardo, control y correcta implementación del siguiente manual de procesos estará bajo la responsabilidad del Jefe del Departamento de Tecnologías.

VII. REFERENCIA NORMATIVA

- Ley 21.180 Ley de Transformación Digital del Estado.
- Ley 21.459 Establece normas sobre delitos informáticos, deroga la ley n° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest.
- Ley 21.663 Ley Marco de Ciberseguridad
- Ley 20.285 sobre acceso a la información pública.

VIII. DOCUMENTACIÓN

- Informe incidente de ciberseguridad (anexo)
- Reglamento Interno N° 006 de fecha 20.12.2023, sobre estructuras, funciones y coordinación del Municipio de Temuco
- Decreto 295 Aprueba Reglamento De Reporte De Incidentes De Ciberseguridad De La Ley N° 21.663
- La Resolución Exenta N° 7/2025 de la Agencia Nacional de Ciberseguridad aprueba la taxonomía de incidentes de ciberseguridad, clasificándolos en diversas categorías según su naturaleza y efecto
- 42_DPM_2025 del 23/04/2025 Designa como encargado de Ciberseguridad de la Municipalidad de Temuco a Don Patricio Turra.

IX. PRODUCTOS

Reportes sobre incidentes de ciberseguridad con efecto significativo, acorde con el Decreto Supremo N° 295/2024 según lo exigido por la Ley 21.663 – Ley Marco de Ciberseguridad y la Resolución Exenta N° 7/2025 de la ANCI que define la taxonomía de incidentes de ciberseguridad. La información contenida en estos reportes se considera reservada, conforme a la Ley 20.285 sobre acceso a la información pública.

La ley establece los siguientes plazos de notificación en la Plataforma oficial de la Agencia Nacional de Ciberseguridad (ANCI) https://portal.anci.gob.cl:

- Alerta temprana: Dentro de 3 horas.
- Segundo reporte: Dentro de 72 horas.

- Informe final: Dentro de 15 días corridos desde la alerta.

X. USUARIOS

Funcionarios de los Diferentes Departamentos de Tecnologías o Informática, incluidos Municipalidad, Educación, Salud y Cementerio.

XI. PROVEEDORES

Los proveedores con los cuales se deberá interactuar son los siguientes:

- **Soporte Técnico Computadores:** OPCIONES Es la empresa que arrienda los computadores, a su vez, se encargan del soporte técnico de estos equipos. En el caso de computadores Municipales, el soporte técnico esta a cargo del Depto de Tecnologías.

- **SOC:** GTD / SECURESOFT Es el proveedor de Internet y servicios de Ciberseguridad, además es el administrador del FIREWALL, SIEM, XSOAR, XDR, CLOUDFLARE, PAGINA WEB, SERVICIOS AZURE, SERVIDOR VIRTUAL (Iaas), ACTIVE DIRECTORY.S

- **Gestor de Ciberseguridad:** NIS es la empresa que presta servicios de asesorías.

XII. DESCRPCIÓN DEL PROCESO

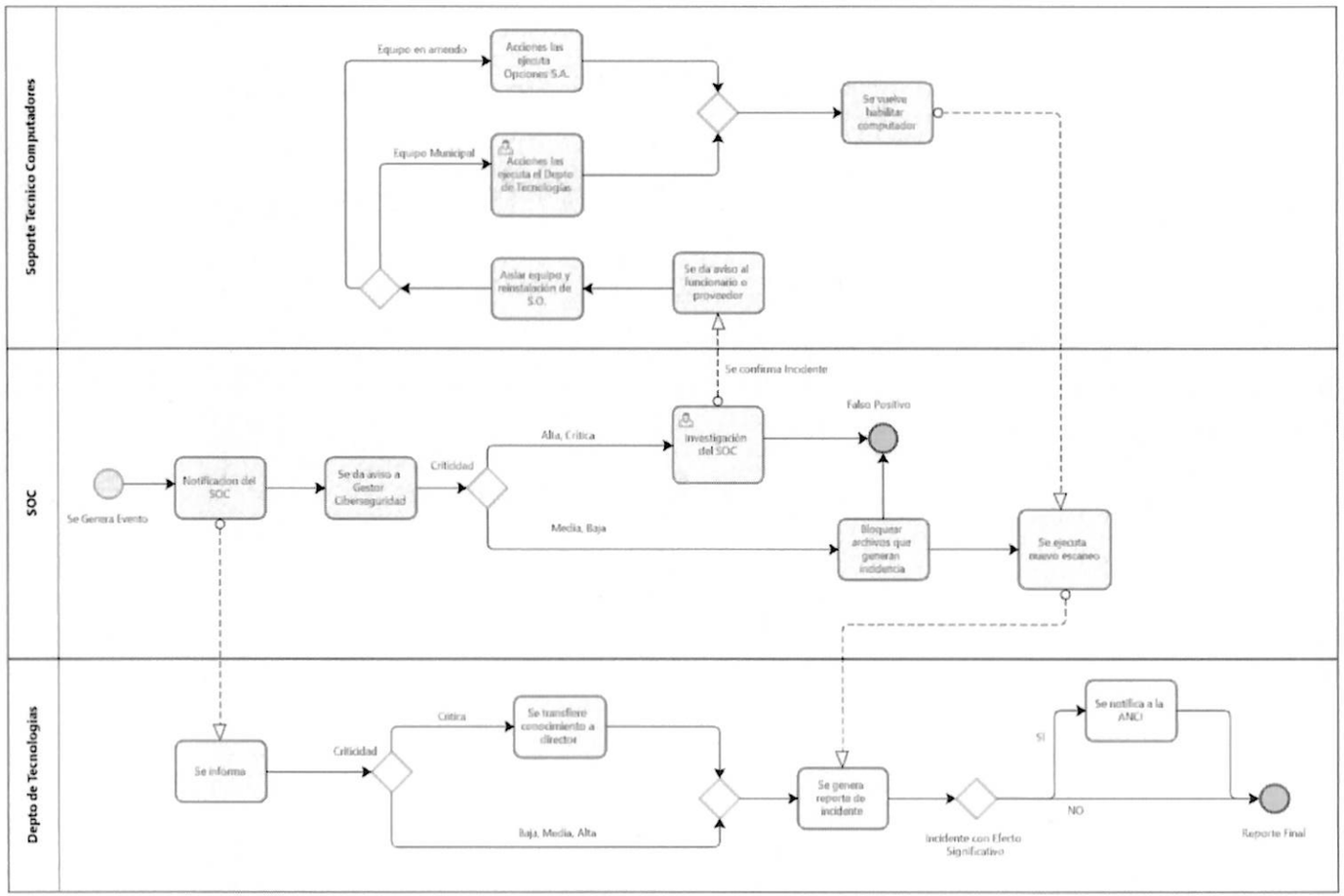
RESPONSABLE	N°	ACTIVIDAD	DOCUMENTO (email)
SOC (GTD).	1	El SOC se encarga de registrar los eventos de ciberseguridad en el sistema de tickets y notificarlos a la Municipalidad	**Depto de Tecnologías** Jefferson.poblete@temuco.cl Ignacio.diaz@temuco.cl Cristiang@temuco.cl Exel.silva@temuco.cl omorales@temuco.cl juan.obreque@temuco.cl Luis.campos@temuco.cl awitzel@temuco.cl
Depto de Tecnologías. **Gestor Ciberseguridad (NIS).**	2	Se deberá evaluar en conjunto con el gestor de ciberseguridad, si Existe amenaza o no, y si esta representa un incidente con efecto significativo. - **Existe amenaza:** Se avalúan las acciones de contención, mitigación y posterior remediación. - **No existe amenaza:** Se marca como falso positivo y se omite.	**Gestor Ciberseguridad (NIS)** **alertasmunitemuco@nis.cl**
Gestor Ciberseguridad (NIS).	3	Al concluir que existe una amenaza, el Gestor de Ciberseguridad deberá clasificar y asignar la criticidad de este incidente, de acuerdo con la severidad se tomaran las siguientes acciones: - **Severidad Alta y Critica:** Se aísla el equipo de la red	**Levantar requerimiento al SOC para investigar incidente:** Operaciones.SOC@grupogtd.com **Gestor Ciberseguridad (NIS)** **alertasmunitemuco@nis.cl**

		para evitar su propagación y se procede con la reinstalación o restauración del sistema operativo, posteriormente se investiga cuando, donde y como se generó el incidente de ciberseguridad. - **Severidad media**: Se escanea el equipo desde la plataforma de ciberseguridad, bloqueando los archivos que generan alertas de incidencias, se avaluara posteriormente si es pertinente reinstalación del sistema operativo. **Severidad baja:** Se escanea el equipo desde la plataforma de ciberseguridad, bloqueando los archivos que generan alertas de incidencias.	
Gestor Ciberseguridad (NIS).	4	Al concluir que existe una amenaza, el Gestor de Ciberseguridad deberá clasificar y asignar la criticidad de este incidente, de acuerdo con la severidad se tomaran las siguientes acciones: - **Severidad Alta y Critica:** Se aísla el equipo de la red para evitar su propagación. Se notifica al SOC para	**Gestor Ciberseguridad (NIS)** **alertasmunitemuco@nis.cl** **SOC (GTD)** Operaciones.SOC@grupogtd.com

		que realice una investigación del incidente, como, cuando y donde se generó el incidente. - **Severidad media**: Se escanea el equipo desde la plataforma de ciberseguridad, bloqueando los archivos que generan alertas de incidencias, se avaluara posteriormente si es pertinente reinstalación del sistema operativo. - **Severidad baja:** Se escanea el equipo desde la plataforma de ciberseguridad, bloqueando los archivos que generan alertas de incidencias.	
Depto de Tecnologías.	5	Una vez clasificado y priorizado se notifica al funcionario afectado, explicando las acciones que se ejecutaran para contener, remediar e investigar el incidente.	Correo electrónico a funcionario afectado.
Soporte Técnico Computadores (OPCIONES y Depto de Tecnologías)	6	En el caso de un incidente de Severidad ALTA y CRITICA asociado a un computador: • Computador Municipal: Se le reinstala el sistema operativo, acciones a cargo del Depto de Tecnologías. • Computador en Arriendo: Se le reinstala el sistema	**Soporte Técnico Computadores Municipales:** Richard.oviedo@temuco.cl pedro.parada@temuco.cl **Soporte Técnico Computadores en Arriendo:** soporte@opciones.cl

		operativo, acciones a cargo del proveedor OPCIONES.	
Depto de Tecnologías.	7	En caso de que haya sido un incidente de carácter crítico, se deberá hacer una transferencia de conocimiento al Director. • Si es un incidente con efecto significativo, se debe reportar a la ANCI de acuerdo con la ley de ciberseguridad.	**Informe Incidente de ciberseguridad. anexo N° 1** **Director:** jorge.quezada@temuco.cl **Notificar a la ANCI:** https://portal.anci.gob.cl

XIII. DIAGRAMA.



XIV.- ANEXOS Y FORMULARIOS

ANEXO N° 1

INFORME INCIDENTE DE CIBERSEGURIDAD *N°____*

ID	01
Nombre	Grandoreiro
Clase de alerta	Malware Bancario
Nivel de riesgo	Critico
Incidente con efecto significativo	NO
Fecha	13/09/2022

RESUMEN

Imagen N°1: Logs generados en Firewall Perimetral

Fuente: Elaboración Propia.

Estos logs se generaron en el Firewall Perimetral Palo Alto, por donde pasa todo el tráfico de red de la Municipalidad de Temuco.

"Grandoreiro es el nombre de un software malicioso, un troyano bancario escrito en el lenguaje de programación Delphi. Está dirigido a usuarios de Brasil, México, España y Perú. Los ciberdelincuentes intentan infectar los ordenadores con este tipo de software para generar ingresos mediante el uso indebido de la información robada por programas como Grandoreiro.

Estos troyanos roban información relacionada con las operaciones bancarias, por lo que las víctimas se exponen al riesgo de sufrir pérdidas monetarias." (pcrisk.es, 2022)

ACCIONES.

- **Acciones Contención:**

1.- Aislar el computador en la plataforma CORTEX XDR.

2.- Aislar el computador de la red (desconectar o bloquear del switch, AP o Firewall).

3.- Realizar escaneo masivo en todos los computadores en búsqueda de propagación

4.- Verificar e Identificar IP Externa maliciosa en el Firewall.

5.- En caso de que el malware llegara a través de phishing (Correo Electrónico), se deben borrar masivamente estos correos.

- **Acciones de Remediación:**

1.- Reinstalar Sistema Operativo del Computador.

2.- Bloquear IP externa maliciosa en Firewall.

3.- Bloquear IP externa maliciosa en plataforma de Correos.

Una vez verificado todo lo anterior, tanto la contención como la remediación, se puede habilitar nuevamente el computador en la plataforma CORTEX XDR.

* Fueron un total de 8 equipos donde se ejecutó el mismo procedimiento, hasta que se dejaron de generar los logs.

RECOMENDACIONES

- Generar una campaña de capacitación entre los funcionarios para evitar el phishing.
- Investigar los dominios maliciosos conocidos y proceder a bloquearlos desde la consola de correos.
- Lograr la implementación de CORTEX XDR en la totalidad de los equipos, para aislar el equipo inmediatamente al generar una alerta critica.
- Evitar que los usuarios tengan permisos de administradores en los computadores, principio de privilegios mínimos.

REFERENCIAS

1. Base de conocimiento de Mitre ATT&CK: Grandoreiro, Software S0531 | MITRE ATT&CK®
2. Attack Navigator de ATT&CK: ATT&CK® Navigator (mitre-attack.github.io)