MUNICIPALIDAD DE
TEMUCO

DECRETO Nº 4163 /

TEMUCO, 23 NOV. 2022

V I S T O S:

1.- El Reglamento Interno N° 004 de fecha 27.05.2021, 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 interno-institucionales.

D E C R E T O:

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

2595121

MUNICIPALIDAD DE
TEMUCO

NOMBRE DEL MANUAL	"GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD"
OBJETIVO DEL MANUAL	Definir un procedimiento para enfrentar los incidentes de ciberseguridad, que afectan a los equipos y dispositivos computacionales de la municipalidad.
AMBITO DE ACCION	aplicable a funcionarios municipales de planta, contrata y honorarios que formen parte de la Municipalidad de Temuco

2.- 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 14 hojas.

ANOTESE, COMUNIQUESE Y ARCHIVESE.

JUAN ARANEDA NAVARRO
SECRETARIO MUNICIPAL

ROBERTO NEIRA ABURTO
ALCALDE

MUNICIPALIDAD DE TEMUCO
DEPARTAMENTO DE CALIDAD Y
MEJORAMIENTO A LA GESTION

MARV / OCD / PTP
C.C. Oficina de Partes,
Depto. informática.
Depto. Acreditación, Capacitación y PMG

TEMUCO
MUNICIPIO CIUDADANO

MANUAL DE PROCESOS

"Gestión de incidentes de ciberseguridad"

Elaboró	Revisó	Aprobó
Patricio turra P. Ignacio Diaz Castillo.	Oriana Castro Dubrenil Encargada Depto. Calidad	

I. ANTECEDENTES

La gestión de incidentes de seguridad de la información contempla actividades claves, tales como: la 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

- **La Ciberseguridad**
  - Son las medidas para proteger los sistemas informáticos – incluyendo el hardware, el software y los datos– de ataques y riesgos cibernéticos
  - Es el conjunto de procedimientos y herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.
  - La ciberseguridad o seguridad informática es el conjunto de infraestructuras computacionales y softwares de protección de datos que defienden a un sistema informático de ataques piratas o de cualquier peligro transmitido a través de softwares maliciosos. Por tanto, queda definida como las prácticas de protección de la información computacional y del procesamiento de esta tienen la finalidad de evitar que personas no.
- **la seguridad informática**
  - se centra en prevenir y combatir ataques cibernéticos, robos de identidad y manipulación de datos confidenciales, fomentar un entorno seguro en la red y las aplicaciones, recuperar la información después de posibles ataques y educar a los usuarios para que estos sepan qué pueden y qué no pueden hacer. Autorizadas tengan acceso o puedan manipular los datos de una persona o corporación.
- **Datos informáticos:**
  - Toda representación de hechos, información o conceptos expresados en cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

- **Sistema informático:**
  - Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
- **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.
- **Ciber seguridad**
  - Proceso para la prevención de ataque a la integridad de un sistema informático.

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 al: Reglamento Interno N°04 de fecha 27 mayo 2021.Art. N° 98.

- 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 que atacan a los equipos computacionales de la municipalidad.

- 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 revertir y resolver contingencias que se detecten.

IV. OBJETIVO DEL PROCESO.

Definir un procedimiento, para gestionar los incidentes de ciberseguridad de manera eficiente y segura, manteniendo la continuidad operativa del municipio.

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.

Todos los funcionarios que trabajan con equipos computacionales, adicionalmente, empresas que dan servicio a la municipalidad, como, por ejemplo, Opciones S.A.

VI. CONTROL DEL MANUAL

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

VII. REFERENCIA NORMATIVA

- Ley 21.180 Ley de Transformación Digital del Estado.
- Ley 21459 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.
- Decretos N° 14, Ministerio de Economía, Fomento y Turismo 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).

VIII. DOCUMENTACIÓN

- Informe incidente de ciberseguridad (anexo)
- Normas de gestión de la seguridad de la información
  - ISO/IEC 27017 Controles de Seguridad para Servicios Cloud.
  - ISO/IEC 20000-1 Gestión de Servicios.
  - ISO 22301 Gestión de Continuidad de Negocio.

- Ley 21459 (20-jun-2022) M. de Justicia y Derechos Humanos | Ley Chile. Biblioteca del Congreso Nacional de Chile. La presente ley, actualiza la legislación chilena en materia de delitos informáticos, adecuándola a las exigencias del Convenio de Budapest, del cual Chile es parte.20 jun 2022.

IX. PRODUCTOS

Un reporte sobre el incidente, generado por la plataforma de ciberseguridad, además del reporte generado después de haber desarrollado las acciones de mitigación, dejándolo como referencia para futuros incidentes de similares características.

X. USUARIOS

Funcionarios(as) de todas las direcciones que trabajen con equipos computacionales.

XI. PROVEEDORES

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

- **Opciones S.A.:** Es la empresa que arrienda la mayoría de los equipos informáticos que están en la municipalidad, a su vez, se encargan del soporte técnico de estos equipos.

- **Telsur:** Es el proveedor de internet, además es el administrador del firewall, tanto locales como el perimetral, en estos firewalls se generan logs asociados a el tráfico de la red.

- **Lazos:** Es la empresa que administra el Active Directory de la municipalidad, con ellos se gestiona la creación de directivas para los equipos computacionales.

- **Vigencia de Contratos :** Los contratos con empresas por periodo de 36, meses, al cabo del cual se debe actualizar el presente manual.

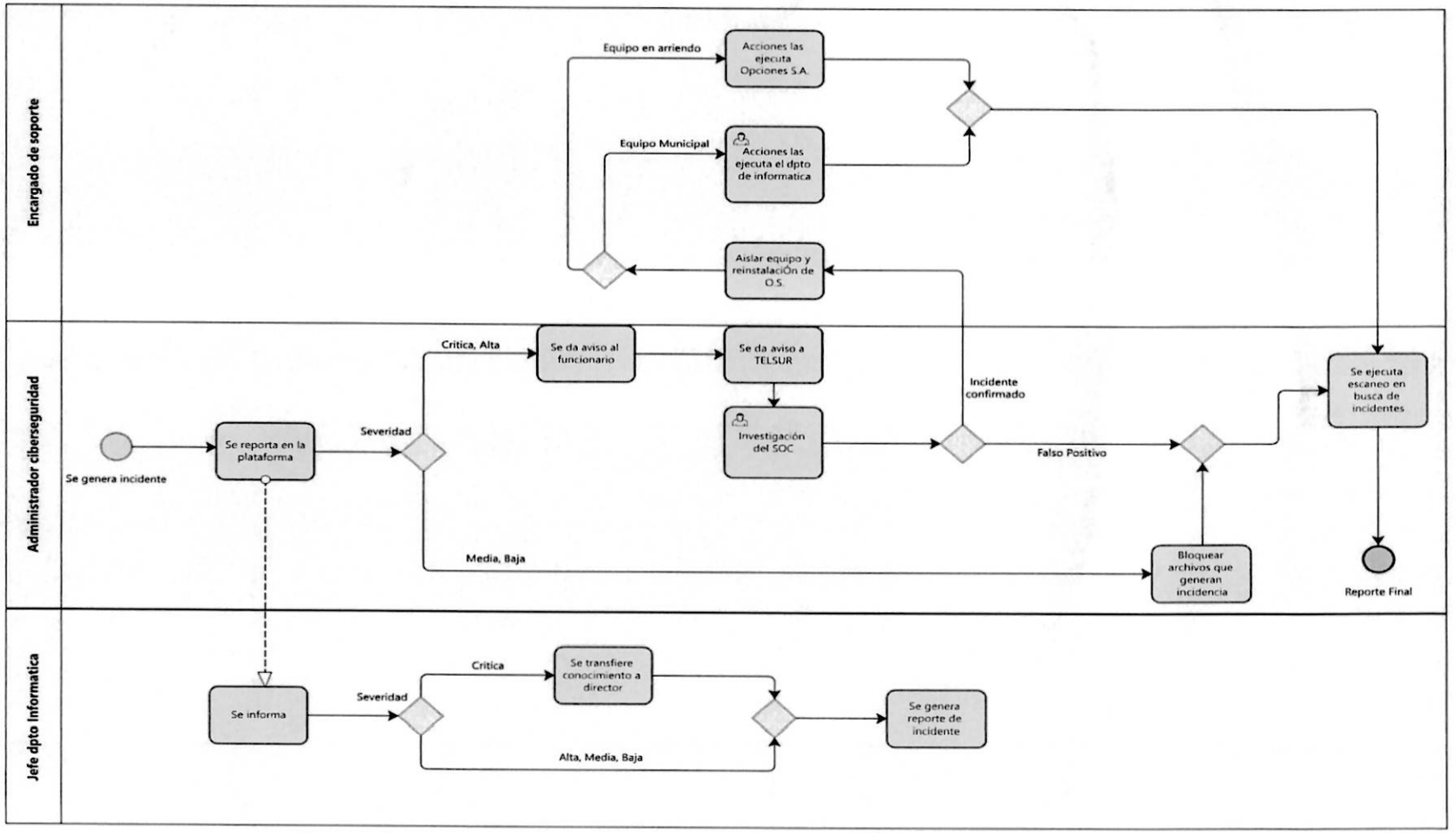
XII. DESCRPCIÓN DEL PROCESO

RESPONSABLE	N°	ACTIVIDAD	DOCUMENTO (email)
Administrador de plataforma de ciberseguridad	1	Al generarse un incidente de seguridad, el administrador de la plataforma debe dar aviso al jefe del departamento de informática.	pturra@temuco.cl
Jefe departamento de informática	2	Deberá evaluar, en conjunto con el administrador de la plataforma de ciberseguridad, si el incidente no corresponde a un falso positivo, y si realmente representa una amenaza para la integridad de los datos del equipo afectado. - **Existe amenaza:** Se avalúan las acciones de mitigación y posterior remediación. - **No existe amenaza:** Se marca como falso positivo y se omite.	**Correo a Administrador de plataforma de seguridad Jefferson.poblete@temuco.cl Ignacio.diaz@temuco.cl**
Administrador de plataforma de ciberseguridad	3	Al concluir que existe una amenaza, el administrador de la plataforma de ciberseguridad deberá asignar la severidad de este incidente, de acuerdo a la severidad se tomaran las acciones de mitigación. **Severidad critica:** Se aísla el equipo de la red para evitar su propagación y se procede con la reinstalación del sistema operativo, posteriormente se investiga cuando, donde y como se generó el incidente de ciberseguridad. Complementariamente a esto, se le dará aviso al ISP de la municipalidad, en estos momentos Telsur, ellos se encargarán de investigar a nivel de	Levantar requerimiento a través de CATE telsur_cat_empresas@grupogtd.com - Soporte técnico externo - soporte@opciones.cl - - servicio técnico interno - Richard.oviedo@temuco.cl

		firewall el comportamiento del incidente, reportando si es necesario acciones adicionales. **Severidad alta:** Se aísla el equipo de la red para evitar su propagación y se procede con la reinstalación 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.	
Funcionario encargado de servicio técnico en conjunto con el administrador de la plataforma de ciberseguridad	4	Una vez que se determina que el incidente representa una amenaza para la integridad de los datos, se comunica el procedimiento al funcionario afectado, explicando las acciones que se ejecutaran en su equipos si corresponde.	Correo electrónico
Funcionario encargado de servicio técnico	5	En caso de que el sistema operativo deba ser reinstalado, y el equipo es de propiedad de la municipalidad, el encargado de soporte será quien haga esta acción, en cambio, si el equipo pertenece a un arriendo, se deberá gestionar un ticket para que técnicos	soporte@opciones.cl Richard.oviedo@temuco.cl

		de la empresa Opciones S.A. acudan al lugar y tomen las acciones necesarias.	
Administrador de plataforma de ciberseguridad	6	Tendrá que hacer un escaneo del equipo luego de que se le reinstale el sistema operativo, generando un reporte de los resultados obtenidos, validando que el incidente de seguridad esté solucionado.	pturra@temuco.cl cristiang@temuco.cl Luis.campos@temuco.cl awitzel@temuco.cl
Jefe departamento de informática	7	En caso de que haya sido un incidente de carácter crítico, se deberá hacer una transferencia de conocimiento al director de la unidad, esta transferencia de conocimiento la hará el jefe del departamento de informática en colaboración con el administrador de la plataforma de ciberseguridad.	**Informe Incidente de ciberseguridad. anexo N° 1**

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
Fecha	13/09/2022

RESUMEN

	09/13 17:09:30	spyware	Grandoreiro Command and Control Traffic Detection	critical	LAN_MPLS	INTERNET	192.168.47.54		51.81.42.59
	09/13 17:09:20	spyware	Grandoreiro Command and Control Traffic Detection	critical	LAN_MPLS	INTERNET	192.168.47.54		51.81.187.70

Imagen N°1: Logs generados en Firewall Perimetral

Fuente: Elaboración Propia.

Estos logs se generaron en el firewall perimetral de PaloAlto, por donde pasa todo el tráfico de la MPLS 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.

- **Mitigación**

1.- Aislar el equipo a través de la herramienta "isolation", provista por CORTEX XDR.
2.- Aislar el equipo a nivel de capa 2 (desconectar físicamente del switch o router).
3.- Reinstalar sistema operativo.

- **Remediación**

1.- verificar tráfico del sitio en el cual se encuentra el equipo infectado, en búsqueda de su propagación.
2.- Bloquear tráfico hacia los servidores donde se comunicaba el malware.
3.- En caso de que el malware llegara a través de phishing (Correo Electronico), bloquear el dominio desde el cual se envió.

Una vez verificado todo lo anterior, tanto la mitigación como remediación, deshacer el "isolation" desde la plataforma CORTEX XDR y habilitar para seguir trabajando.

* 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 office 365.
- Lograr la implementación de CORTEX XDR en la totalidad de los equipos, para aislar el equipo inmediatamente al generar una alerta critica.

COMPLEMENTO

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)