República de Chile
Provincia de Linares
Dirección de Adquisiciones
Departamento de Informática

DECRETO EXENTO Nº: 2979 /

PARRAL, 30 junio 2022

VISTOS:

1.- Las Facultades que me confiere la Ley N° 18.695/88, Ley Orgánica Constitucional de Municipalidades y sus posteriores modificaciones.
2.- La Sentencia definitiva de fecha 10 de junio del 2021 dictada por el Tribunal Electoral Regional del Maule.
3.- Acta de Proclamación de fecha 16 de junio del 2021 del Tribunal Electoral Regional del Maule.
4.- Juramento prestado en Sesión de instalación del Honorable Concejo Comunal de Parral celebrada el 28 de junio del 2021.
5.- Declaración de Asunción de funciones efectuada por el Decreto Afecto N° 1.282 del 29 de junio del 2021."
6.- El reglamento interno sobre el uso de Tecnologías de la Información de la Ilustre Municipalidad de Parral año 2011.
7.- El Decreto Exento N° 4569 de fecha 30 de Septiembre de 2011, que aprueba el Reglamento Interno sobre el Uso de Tecnologías de la Información de la Ilustre Municipalidad de Parral año 2021.-

DECRETO:

1.- **ESTABLECESE**, el procedimiento de supervisión y revisión de equipos en caso de detección de incidentes a la seguridad de la información.

PROCEDIMIENTO DE SUPERVISIÓN Y REVISIÓN DE EQUIPOS EN CASO DE DETECCIÓN DE INCIDENTES

Los incidentes a la seguridad de la información son un riesgo constante como Municipalidad, la conservación de los datos manteniendo su integridad y operatividad son el propósito del desarrollo del procedimiento de supervisión y revisión de equipos Municipales en caso de detección de incidentes.

DEFINICIONES

- **Amenaza:** Probabilidad de ocurrencia, durante un periodo especifico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos de riesgo.
- **Contingencia:** Evento o suceso que ocurre, en la mayoría de los casos, de forma inesperada y que causa alteraciones en los patrones normales de funcionamiento.
- **Elementos en riesgo:** Se refiere a la población, las construcciones, la infraestructura, las edificaciones de las actividades económicas y otros espacios donde estas se desarrollan, los servicios públicos y el medio ambiente natural que son susceptibles de daños como consecuencia de la ocurrencia de un fenómeno natural o producido por el hombre (artificial).

- **Vulnerabilidad:** La vulnerabilidad se refiere al grado de perdidas relacionadas con un elemento de riesgo, que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud.
- **Riesgo:** Se refiere a la cuantificación de los posibles daños ocasionados a los elementos de riesgo como consecuencia de un fenómeno natural o artificial en términos de vidas perdidas, personas heridas, daños materiales y ambientes e interrupciones de la actividad económica.
- **Gravedad:** Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, critica, catastrófica y se definen según el factor de evaluación (victimas, pérdidas económicas, suspensión de operación, daño ambiental).
- **Seguridad:** Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencional, puedan ser modificados, destruidos o divulgados.
- **Datos:** Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.
- **Incidente:** Es una violación con éxito de las medidas de seguridad, como el robo de información, borrado de archivos con datos valioso, robo de equipos, PC, entre otros.
- **Activo:** Son todo aquellos recursos o componentes, tanto tangibles como lógicos que constituyen infraestructura, patrimonio, conocimiento y reputación en el mercado.

OBJETIVO

El objetivo es establecer un procedimiento de acción ante la detección de incidentes que afecten el normal funcionamiento de los procesos y la operatividad, definiendo los pasos a seguir para cuidar y proteger los activos de la información.

IDENTIFICACIÓN DE UN INCIDENTE

Para identificar un incidente de seguridad, determinar su alcance y los sistemas afectados por el mismo, se deben desarrollar mecanismos de análisis como la revisión de logs detectados por el firewall, registros y fuentes de información para detectar anomalías.

Los incidentes más comunes se definen como:

- **Comportamiento inusual de cuentas:** Cualquier anomalía en el comportamiento de una cuenta de usuario puede indicar que alguien la esta utilizando para ingresar a una red privada.
- **Acceso a servidores y datos:** Consiste en los usuarios no autorizados que intentan acceder a servidores o datos, solicitando acceso a información que no esta relacionada a la ejecución de sus funciones laborales. Considera inicios de sesión en momentos anormales desde ubicaciones inusuales o desde múltiples ubicaciones en periodos de tiempo breves.
- **Anomalías tráfico de red**: Trafico de entrada y salida de la red como carga de archivos grandes a aplicaciones de nube personales, descarga de archivos a dispositivos de almacenamiento externo, envió masivo de mensajes de correo electrónico con archivos adjuntos fuera de la Municipalidad, entre otros.
- **Trafico hacia o desde lugares desconocidos:** Para la Municipalidad cualquier trafico enviado a otros países puede indicar una actividad maliciosa. Los administradores deben investigar cualquier tráfico a redes desconocidas asegurando la legitimidad.

- **Consumo excesivo:** Un aumento en el rendimiento de la memoria del servidor o los discos duros puede significar que un atacante los esté accediendo ilegalmente.
- **Cambios de configuración:** Los cambios que no se han aprobado, como la reconfiguración de servicios, la instalación de programas de inicio o los cambios en el firewall son una señal de posible actividad maliciosa. Lo mismo ocurre con las tareas programadas que se han agregado.
- **Archivos ocultos:** Estos pueden considerarse sospechosos debido al nombre de archivo, tamaño, ubicaciones, que indican que los datos o registros pueden haberse filtrado.
- **Cambios sin notificaciones:** Estos incluyen bloqueos de cuentas de usuario, cambios de contraseña o cambios repentinos en los sectores de trabajo.
- **Comportamiento anormal de navegación:** Esto podría ser redirecciones inesperadas, cambios en la configuración del navegador o ventanas emergentes repetidas.
- **Entradas de registro sospechosas:** Esto sucede principalmente cuando el malware infecto los sistemas de Windows. Es una de las principales formas en que el malware garantiza que permanece en el sistema infectado.

PROCEDIMIENTO DE ACCIÓN

Posterior a la identificación de un incidente, se debe determinar el alcance y los sistemas afectados o potencialmente dañados, con el propósito de tomar acciones para solucionar el incidente manteniendo la seguridad de la información, su integridad y operatividad.

1. Determinar el tipo de incidente
    a. Interno o Externo: determinar si el incidente es originado por motivos internos o factores externos que atentan contra la seguridad de la información.
    b. Origen del incidente: Verificar los puntos de origen del incidente, rastrear el punto de inicio del peligro.
2. Identificar logs entregados por el firewall
    a. Verificar direcciones de la red: Verificar los accesos a la red Municipal y los elementos de la red a la computadora.
    b. Identificar logs: Verificar el registro del firewall para detectar incidentes, riegos o peligros.
3. Revisar información proporcionada por la red
    a. Determinar uso red: Verificar que la utilización de la red este en normalidad, sin incidentes o alteraciones a la operatividad.
    b. Revisar sobreconsumos: Verificar que no existan sobreconsumos que estén generando riesgos, incidentes o afecten la operatividad Municipal.
4. Revisar el equipo que origina el incidente
    a. Localizar direcciones IP: Ante la detección de un incidente rastreado mediante el firewall, se determinan las direcciones IP que están generando alteraciones al funcionamiento y se localiza su ubicación física.
    b. Asistir a revisión y supervisión en terreno: Determinado la localización y las direcciones IP se procede a revisar el equipo que esta generando los incidentes a la seguridad.
5. Tomar medidas de control
    a. Estudiar el origen del incidente: Estudiar el motivo por el que se produce el incidente, verificar contenido malicioso o malware.
    b. Eliminar origen de malware: Ante la detección de malware se procede a la eliminación de todos los archivos contaminados, se analiza el equipo mediante el antivirus y se verifica la correcta funcionabilidad.

   c. Escalar los daños y su distribución: Se estudia la magnitud de los daños, los riesgos y peligros generados, la ramificación para tener un control del incidente.
6. Verificar la operatividad
   a. Revisión de operatividad de los sistemas: Una vez tomada las medidas de control se procede a revisar la operatividad de los sistemas y la vuelta a la normalidad.
   b. Comprobar solución del incidente: Verificación de la solución al incidente, normalidad en el funcionamiento y operatividad.
7. Tomar medidas de prevención
   a. Aplicar medidas de prevención: Estudiar los motivos que origino el incidente, desarrollar medidas de prevención y aplicarlas.
   b. Capacitar a funcionarios sobre incidente: Informar a los funcionarios Municipales sobre los incidentes informáticos, las causas y los problemas que conlleva. Capacitar sobre las medidas de prevención.
8. Notificar y reportar incidente
   a. Informe de incidente: Generar un reporte que identifique el incidente, especifique las causas, origen, medidas de control y estrategias aplicadas para mantener la funcionabilidad y operatividad de los sistemas.
   b. Notificar a funcionarios estado actual: Informar a los funcionarios sobre el incidente ocurrido y sobre la vuelta a la normalidad de las funciones.

REVISIÓN DE EQUIPOS

Para la revisión de equipos se establece un protocolo a fin de establecer el paso a paso que se debe realizar al momento de la revisión del equipo en caso de detección de un incidente a la seguridad de la información.

1. Notificar a la Jefatura o Directivo

El procedimiento es informar a la Jefatura o Directivo mediante correo electrónico sobre el incidente a la seguridad de la información, los datos obtenidos del estudio y explicar el plan de acción a realizar, las medidas que se tomaran y la revisión de equipos a realizar en caso de ser necesario.

2. Participantes del proceso

En el proceso de revisión del equipo deberá estar presente el usuario responsable del equipo o la jefatura o el/la directivo, mas el personal del departamento de informática a cargo de realizar la revisión del equipo.

3. Ejecución de la revisión

La ejecución de la revisión del equipo la realizara funcionarios del departamento de informática y el procedimiento se distribuye en los siguientes pasos:

   a. Verificación de la dirección IP
   b. Revisión de los softwares instalados
   c. Revisión del historial web
   d. Revisión del historial de descargas
   e. Revisión de descargas
   f. Revisión de papelera

4. Documentación de procedimiento

República de Chile
Provincia de Linares
Dirección de Adquisiciones
Departamento de Informática

Se realiza un informe sobre el procedimiento de revisión del equipo, se tomarán capturas de pantalla o se grabara en caso de ser necesario. El informe debe contener el nombre del usuario responsable del equipo, departamento o dirección a la que pertenece, fecha, horario y una captura de pantalla por cada punto del procedimiento junto con una descripción detallada de los resultados.

Este informe debe estar firmado por la Jefatura o Directivo y el funcionario del departamento de informática a cargo de realizar la revisión del equipo.

ANOTESE, REFRENDESE, COMUNIQUESE Y CUMPLASE.

ALEJANDRA ROMAN CLAVIJO
SECRETARÍA MUNICIPAL

PAULA RETAMAL URRUTIA
ALCALDESA DE PARRAL

PRU/RRV/EGP/JAH

DISTRIBUCIÓN

1.- Oficina de Partes
2.- Dirección Control
3.- Departamento de Informática
4.- COPIA DIGITAL (todos@parral.cl)