




## MUNICIPIO DEL DISTRITO METROPOLITANO DE QUITO




**INFORME DE LA DIRECCIÓN METROPOLITANA DE INFORMÁTICA  
AL  
PLENO DEL CONCEJO METROPOLITANO DE QUITO**

**2022-ABR**

	<b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b>  <b>(2022-ABR) – Información sensible</b>	<b>Versión: 01</b> <b>MDMQ-AG-2021-</b> <b>INSTRUCTIVO Nro.001-</b> <b>F.004</b>  <b>Informe N°</b> <b>DMI-INF001-CMQ</b>
---	---	---

## CONTENIDO

1	Glosario.....	3
2	Antecedentes .....	4
3	Necesidad de tratar la información con carácter de acceso restringido .....	4
4	Objetivo.....	4
5	Marco Legal .....	4
6	Desarrollo.....	5
6.1	Hechos sucedidos .....	5
6.2	Acciones técnicas emprendidas (detección, análisis y contención) (semana 1).....	6
6.2.1	Día 2022-ABR-16 al 2022-ABR-17 .....	6
6.2.2	Día 2022-ABR-18 al 2022-ABR-22 .....	7
6.3	Acción Judicial (2022-ABR-18) .....	8
6.4	Acciones de Notificación.....	9
6.5	Acciones planificadas .....	10
6.5.1	Estrategia Operativa .....	10
6.5.2	Estrategia de fortalecimiento de la Seguridad de la Infraestructura Tecnológica del GAD-DMQ.....	11
7	Resultados obtenidos.....	12
8	Conclusiones y recomendaciones .....	13
8.1	Conclusiones.....	13
8.2	Recomendaciones.....	14
9	Firmas de responsabilidad .....	14
10	Anexos.....	16

	<p align="center"><b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b></p> <p align="center">(2022-ABR) – Información sensible</p>	<p align="center">Versión: 01 MDMQ-AG-2021- INSTRUCTIVO Nro.001- F.004</p> <p align="center">Informe N° DMI-INF001-CMQ</p>
---	---	--

## 1 Glosario

### ◆ Software libre:

- “«Software libre» es el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que **los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software**. Es decir, el «software libre» es una cuestión de libertad, no de precio. Para entender el concepto, piense en «libre» como en «libre expresión», no como en «barra libre». En inglés, a veces en lugar de «free software» decimos «libre software», empleando ese adjetivo francés o español, derivado de «libertad», para mostrar que no queremos decir que el software es gratuito.” (GNU)

### ◆ Malware:

- “Malware es un término genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, spyware, adware, software de miedo, etc. Puede tomar la forma de código ejecutable, scripts, contenido activo y otro software.” (Oracle)

### ◆ Máquina virtual:

- “Las máquinas virtuales son ordenadores de software que proporcionan la misma funcionalidad que los ordenadores físicos. Como ocurre con los ordenadores físicos, ejecutan aplicaciones y un sistema operativo. Sin embargo, las máquinas virtuales son archivos informáticos que se ejecutan en un ordenador físico y se comportan como un ordenador físico. En otras palabras, las máquinas virtuales se comportan como sistemas informáticos independientes.” (VMWARE)

### ◆ Ciberataque:


- “Son intentos no deseados de robar, exponer, alterar, deshabilitar o destruir información mediante el acceso no autorizado a los sistemas informáticos.” (IBM)

### ◆ Ransomware:

- “Este tipo específico de software malicioso se usa para extorsionar. Cuando un dispositivo logra ser atacado con éxito, el malware **bloquea la pantalla o cifra la información almacenada en el disco** y se solicita un rescate a la víctima con los detalles para efectuar el pago. (ESET)”

### ◆ Como ataque un Ransomware:

- De manera general intentan cifrar toda la información a su alcance, de manera de evitar que el usuario acceda al sistema operativo. (ESET)
- Estos ataques generalmente son estudiados con varios meses atrás, hasta conocer el diseño de la infraestructura tecnológica, ubicando activos estratégicos para el ataque.

	<p align="center"><b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b></p> <p align="center">(2022-ABR) – Información sensible</p>	<p align="center">Versión: 01 MDMQ-AG-2021- INSTRUCTIVO Nro.001- F.004</p> <p align="center">Informe N° DMI-INF001-CMQ</p>
---	---	--

## 2 Antecedentes

La infraestructura tecnológica de la Dirección Metropolitana de Informática del GAD DMQ, fue objeto de un ciberataque, cuyas consecuencias se materializaron en el transcurso de la mañana del 16 de abril del 2022.

El origen fue un malware <sup>1</sup>(software hostil intrusivo, virus informático) de tipo Ransomware<sup>2</sup>, de los más sofisticados que esta industria ha producido.

La consecuencia del ciberataque fue la afectación de los servicios automatizados con los cuales el GAD DMQ atiende a la ciudadanía, servidores y funcionarios municipales, ocasionado por el comprometimiento de la infraestructura tecnológica.

## 3 Necesidad de tratar la información con carácter de acceso restringido

La información respecto del incidente informado, debido a la sensibilidad intrínseca por tratarse de estrategias para la defensa de la infraestructura tecnológica de la institución, debería ser tratada como información sensible y de acceso restringido.

Esto debido a que su divulgación en la situación actual, podría ser utilizada por los atacantes para una acción que comprometa negativamente las operaciones de la infraestructura tecnológica.

## 4 Objetivo

Informar al Concejo Metropolitano de Quito, en la sesión ordinaria No. 216 a llevarse a cabo el martes 26 de abril de 2022, a partir de las 09h00, en el numeral VI de su orden del día, respecto al ataque cibernético a la infraestructura tecnológica de la Dirección Metropolitana de Informática del GAD DMQ y las acciones emprendidas desde el momento de la detección.


## 5 Marco Legal

- ◆ Constitución de la República del Ecuador en sus artículos: Art. 83, Art. 195, Art. 233, Art. 226.

---

<sup>1</sup> **Malware** es un **término** genérico utilizado para describir una variedad de software hostil o intrusivo: virus informáticos, gusanos, caballos de Troya, software de rescate, **spyware**, adware, software de miedo, etc

<sup>2</sup> Ransomware de tipo blackcat: ALPHV (BlackCat) es un sofisticado programa de tipo ransomware escrito en el lenguaje de programación Rust. Este programa se utiliza en operaciones de Ransomware-as-a-Service (RaaS).


	<b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b>  <b>(2022-ABR) – Información sensible</b>	<b>Versión: 01</b> <b>MDMQ-AG-2021- INSTRUCTIVO Nro.001-F.004</b>  <b>Informe N°</b> <b>DMI-INF001-CMQ</b>
---	---	--

- ◆ Código Orgánico de la Función Judicial en su Art. 282.
- ◆ Código Orgánico Integral Penal (COIP) en sus artículos: Art. 17, Art. 277, Art. 232, Art. 421.
- ◆ Ley Orgánica de Protección de Datos Personales en su Art. 43.
- ◆ Código Municipal para el Distrito Metropolitano de Quito, reformas hasta el 01-sep.-2021. libro I.3: De La Participación Ciudadana, capítulo V, VI, y VII; libro III.2: De La Conectividad, Capítulo IV; en Art. 349, Art. 359 y Art. 1156.
- ◆ Código de las Normas de Control Interno, Contraloría General Del Estado, del 14-dic.-2009 modificado el 16-dic.-2014, Núm. 410.
- ◆ Políticas de Tecnología de la Información del GAD del DMQ, 2018, Art. Políticas de Tecnología - 2018 Art. 10.

## 6 Desarrollo

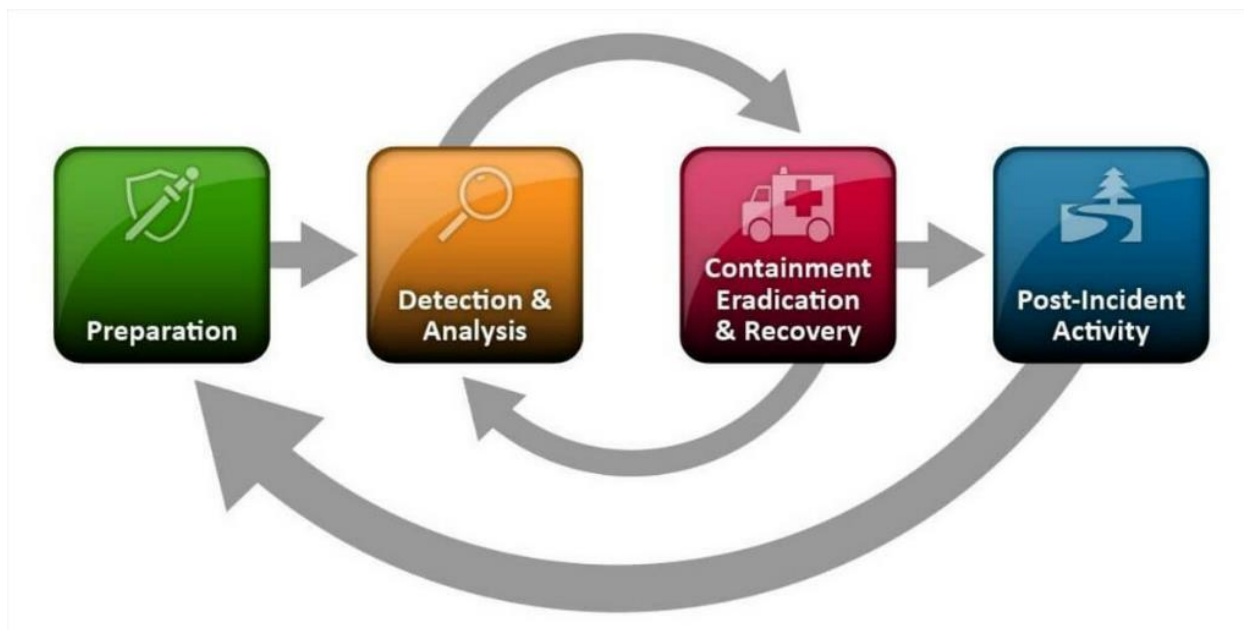
### 6.1 Hechos sucedidos

- ◆ En la madrugada del sábado 16-ABR-2022 se evidenciaron las consecuencias de un agresivo ciberataque dirigido hacia la infraestructura tecnológica del GAD DMQ, orientado encriptar recursos informáticos estratégicos, con el fin de dejar sin operación a los servicios automatizados que presta el Municipio de Quito.
- ◆ La dispersión del ataque pudo ser detectada y contenida el día sábado, de lo que se puede encontrar en el reporte de herramientas y gracias a las tareas programadas para fortalecer la seguridad, que desarrollaba el equipo técnico de la DMI.
- ◆ Foco del ataque:
  - Consola del administrador de la virtualización, dejando inutilizado el acceso al visor de las máquinas virtuales.
  - Consola de control de los respaldos, encriptándola y dejando sin acceso a los respaldos (aunque los respaldos existen y no se ha determinado que estén afectados).
- ◆ El municipio cuenta con los respaldos completos de la información para poder volver a las operaciones normales.
- ◆ En las tareas de verificación de los respaldos que realiza el personal técnico, se ratificando que la integridad de la información no se ve comprometida.
- ◆ En las tareas de limpieza de virus, de los equipos de usuario final que se procede a conectar a los segmentos de red, se identifica aún la presencia del “adversario”.

	<b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b>  (2022-ABR) – Información sensible	Versión: 01 MDMQ-AG-2021- INSTRUCTIVO Nro.001- F.004  Informe N° DMI-INF001-CMQ
---	--	---

## 6.2 Acciones técnicas emprendidas (detección, análisis y contención) (semana 1)

Para el tratamiento de este incidente de ciber seguridad, se ha tomado varios criterios de la NIST<sup>3</sup> cuyo marco general es el siguiente:




### 6.2.1 Día 2022-ABR-16 al 2022-ABR-17

Las acciones técnicas emprendidas desde el momento de la detección del ataque se encuentran descritas en el **“Informe técnico de evento de ataque ransomware a la infraestructura tecnológica del GAD-DMQ”**, de fecha 2022-ABR-17 (**Anexo 1**), que en su parte fundamental se dedicaron a la detección y análisis del ataque.

Las principales tareas realizadas fueron:

- a. Verificación de funcionamiento en el firewall. Los parámetros se encontraron normales.
- b. Se verificó accesos a servicio internos. No existía respuesta.
- c. Se aisló los segmentos de red para evitar la propagación.
- d. Se procede a bajar el servicio de VPN.
- e. Se procede a desactivar el servicio de internet a nivel general del Municipio.
- f. Levantamiento del Inventario de activos informáticos comprometidos: carpetas compartidas, bases de datos, máquinas virtuales (con bases de datos y aplicativos), equipos de usuario final de la administración del Data Center.
- g. Plan de acción para contención de la propagación del malware.
- h. Plan de acción para la recuperación de operaciones.

<sup>3</sup> National Institute of Standards and Technology (NIST):

	<p align="center"><b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b></p> <p align="center"><b>(2022-ABR) – Información sensible</b></p>	<p align="center">Versión: 01 MDMQ-AG-2021- INSTRUCTIVO Nro.001- F.004</p> <p align="center">Informe N° DMI-INF001-CMQ</p>
---	--	--

- i. Se tomó contacto con el Sr. Procurador del GAD DMQ, para realizar la denuncia a Fiscalía. Pendiente entregar el informe técnico de la DMI (entregado el domingo 17 de abril).
- j. Se coordinó acciones con entidades relacionadas que consumen servicios del GAD DMQ: AMT, Registro de la Propiedad, AMC y Secretaría de la Movilidad. Estas acciones están encaminadas a operar bajo esta modalidad de contingencia.

Una vez contenido el ataque, mediante correo electrónico de fecha 2022-ABR-17, la Dirección Metropolitana de Informática, notifica el ciberataque a la infraestructura tecnológica; a las autoridades: Sr. Alcalde, Srtas., Sras. y Sres. Concejales, Sr. Procurador, Sr. Administrador General.

Se dispone por parte de las autoridades, publicar en redes sociales el incidente ocurrido para conocimiento de la ciudadanía.

### 6.2.2 Día 2022-ABR-18 al 2022-ABR-22

El 18 de abril del 2022, acorde al Informe de actividades desarrolladas (DMICBR-01) **(Anexo 2)**, en las conclusiones y recomendaciones se describe lo siguiente:

*“(..) evidencia aún la presencia del malware atacante en máquinas de varias dependencias del GAD –DMQ, las cuales se procedió a aislarlas y planificar su formateo y reinstalación previo a su conexión a los segmentos de red*

*Continuar con la verificación del estado de respaldos de información, para catalogar fechas de último backup de todos los aplicativos, bases de datos y máquinas virtuales.*

*Los servicios y aplicaciones core de las instituciones deben ser priorizados para su puesta en producción, permitiendo la revisión tanto técnica como funcional que permitan minimizar la posibilidad de que el malware persista dentro de la infraestructura tecnológica y se vuelva a activar (...)*”

El 19 de abril del 2022, acorde al Informe de actividades desarrolladas (DMICBR-02) **(Anexo 3)**, en las conclusiones y recomendaciones se describe lo siguiente:

*“(...) Se evidencia aún la presencia del malware atacante en carpetas compartidas en el repositorio central ISILON del centro de Datos GAD-, las cuales se procedió a aislarlas reinstalación previa a su conexión a los segmentos de red.*

*Continuar con la verificación del estado de respaldos de información, para catalogar fechas de último backup de todos los aplicativos, bases de datos y máquinas virtuales.*


*Se están realizando pruebas internas tanto técnica como funcional que permitan minimizar la posibilidad de que el malware persista dentro de la infraestructura tecnológica de los sistemas. SITRA, PORTAL quito.gob.ec, MAILING (...)*”

El 20 de abril del 2022, acorde al Informe de actividades desarrolladas (DMICBR-03) **(Anexo 4)**, en las conclusiones y recomendaciones se describe lo siguiente:

*“(...) Se evidencia aún la presencia del malware atacante en máquinas ubicadas en localidades externas al Municipio de Quito a servidores en el centro de datos del GAD – DMQ –DMI.*

*Continuar con la verificación del estado de respaldos de información, para catalogar fechas de último backup de todos los aplicativos, bases de datos y máquinas virtuales.*

*Se están realizando pruebas internas tanto técnica como funcional que permitan minimizar la posibilidad de que el malware persista dentro de la infraestructura tecnológica de los sistemas de las aplicaciones y sistemas que se han puesto en producción.*

 <p>Por un <b>Quito</b> Digno</p>	<p><b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b></p> <p>(2022-ABR) – Información sensible</p>	<p>Versión: 01 MDMQ-AG-2021- INSTRUCTIVO Nro.001- F.004</p> <p>Informe N° DMI-INF001-CMQ</p>
--	---	--

- No se recomienda aún permitir que las aplicaciones estén expuestas a internet.**
- En necesario continuar con el monitoreo del tráfico interno de acceso a las aplicaciones y servicios que se han puesto en operación. (...)* **[énfasis señalado]**

El 21 de abril del 2022, acorde al Informe de actividades desarrolladas (DMICBR-04) **(Anexo 5)**, en las conclusiones y recomendaciones se describe lo siguiente:

*"(...) Se evidencia aún la presencia del malware atacante en máquinas ubicadas en localidades externas al Municipio de Quito a servidores en el centro de datos del GAD – DMQ – DMI.*

- Continuar con la verificación del estado de respaldos de información, para catalogar fechas de último backup de todos los aplicativos, bases de datos y máquinas virtuales.*
- No se recomienda aun permitir que las aplicaciones estén expuestas a internet.**
- Es necesario continuar con el monitoreo del tráfico interno de acceso a las aplicaciones y servicios que se han puesto en operación. (...)* **[énfasis señalado]**

El 22 de abril del 2022, acorde al Informe de actividades desarrolladas (DMICBR-05) **(Anexo 6)**, en las conclusiones y recomendaciones se describe lo siguiente:

*"(...) Se evidencia aún la presencia del malware atacante en máquinas ubicadas en localidades externas al Centro de Datos del Municipio de Quito.*

- No se recomienda aun permitir que las aplicaciones estén expuestas a internet. [énfasis señalado]**
- En necesario continuar con el monitoreo del tráfico interno de acceso a las aplicaciones y servicios que se han puesto en operación. (...)* **[énfasis señalado]**


### 6.3 Acción Judicial (2022-ABR-18)

Con fecha 18 de abril la Mgs. Carolina Pantoja Freire, en calidad de Subprocuradora Metropolitana, representante legal y judicial del Gobierno Autónomo Descentralizado del Distrito Metropolitano de Quito de conformidad con las Resoluciones Nro. AQ 012-2021 y AQ 011-2022 del Alcalde Metropolitano, de 11 de octubre de 2021 y 16 de marzo de 2022, respectivamente, y el Oficio Nro. 00015/SV de fecha 16 de marzo de 2022, comparece y presenta la DENUNCIA signada con el No.170101822043050 ante la FISCALÍA GENERAL DEL ESTADO, señalando casilla judicial 934 del Palacio de Justicia de la ciudad de Quito, y en el casillero electrónico 00717010006, así como en los correos electrónicos: [zaida.almeida@quito.gob.ec](mailto:zaida.almeida@quito.gob.ec) y [patrocinio.mdmq@quito.gob.ec](mailto:patrocinio.mdmq@quito.gob.ec).

La denuncia No.170101822043050 **(Anexo 7)**, por presunto delito de **ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS** tipificado y sancionado en el artículo 232 del Código Orgánico Integral Penal solicita a la FISCALÍA GENERAL DEL ESTADO disponer el inicio de la investigación previa, conforme lo establecido en el artículo 580 del Código Orgánico Integral Penal y se realice la práctica de las diligencias señaladas en el punto **6. SOLICITUD DE DILIGENCIAS**.

En la denuncia presentada se anexan algunos documentos, entre esos: *"Informe técnico de evento de ataque ransomware a la infraestructura tecnológica del GAD-DMQ"*, de fecha 2022-ABR-17. (Anexo 1)



	<b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b>  <b>(2022-ABR) – Información sensible</b>	<b>Versión: 01</b> <b>MDMQ-AG-2021-</b> <b>INSTRUCTIVO Nro.001-</b> <b>F.004</b>  <b>Informe N°</b> <b>DMI-INF001-CMQ</b>
---	---	---

#### 6.4 Acciones de Notificación

Mediante correo electrónico de fecha 2022-ABR-17, la Dirección Metropolitana de Informática, notifica el ciberataque a la infraestructura tecnológica y se remite el “**Informe técnico de evento de ataque ransomware a la infraestructura tecnológica del GAD-DMQ**” a las autoridades, señor Alcalde y Concejales Municipales. **(Anexo 8)**.


Mediante Oficio Nro. GADDMQ-DMI-2022-0002-O-CNTG-I de 20 de abril de 2022 **(Anexo 9)**, la Dirección Metropolitana de Informática, presentó a la Asesoría del Despacho de la Procuraduría Metropolitana del GAD del DMQ, conforme lo dispone la Ley Orgánica de Protección de Datos Personales, la Denuncia No. 170101822043050 por ataque a la integridad de sistemas informáticos.

Mediante Oficio GADDMQ-DMI-2022-00629-O de 20 de abril de 2022 **(Anexo 10)** la Dirección Metropolitana de Informática, informa a las autoridades, señor Alcalde y Concejales Municipales, el avance de las tareas de contención del Ciberataque direccionado contra el GAD DMQ, así como también de las actividades llevadas a cabo para la recuperación de operaciones automatizadas del Municipio, adjuntando archivo denominado “**dmi, 04-20, Informe incidente de Seguridades, 2022-ABR-20.pdf**”

Mediante Oficio Nro. GADDMQ-DMI-2022-00637-0 de 21 de abril de 2022 **(Anexo 11)**, la Dirección Metropolitana de Informática, dando cumplimiento a la Ley Orgánica de Protección de Datos Personales, en su artículo 43, notifica la vulneración de la seguridad de datos personales a la Autoridad de Protección de Datos Personales y la Agencia de Regulación y Control de las Telecomunicaciones.

Mediante Oficio GADDMQ-DMI-2022-00638-O de 21 de abril de 2022 **(Anexo 12)** la Dirección Metropolitana de Informática, informa a las autoridades, señor Alcalde y Concejales Municipales, el avance de las tareas de contención del Ciberataque direccionado contra el GAD DMQ, así como también de las actividades llevadas a cabo para la recuperación de operaciones automatizadas del Municipio, adjuntando archivo denominado “**dmi, 04-21, Informe incidente de Seguridades, 2022-ABR-21.pdf**”

Mediante Oficio GADDMQ-DMI-2022-00644-O de 22 de abril de 2022 **(Anexo 13)** la Dirección Metropolitana de Informática, informa a las autoridades, señor Alcalde y Concejales Municipales, el avance de las tareas de contención del Ciberataque direccionado contra el GAD DMQ, así como también de las actividades llevadas a cabo para la recuperación de operaciones automatizadas del Municipio, adjuntando archivo denominado “**dmi, 04-22, Informe incidente de Seguridades, 2022-ABR-22.pdf**”

 <p>Por un <b>Quito</b> Digno</p>	<b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b>  <b>(2022-ABR) – Información sensible</b>	<b>Versión: 01</b> <b>MDMQ-AG-2021-</b> <b>INSTRUCTIVO Nro.001-</b> <b>F.004</b>  <b>Informe N°</b> <b>DMI-INF001-CMQ</b>
--	---	---

## 6.5 Acciones planificadas

### 6.5.1 Estrategia Operativa

1. Plan progresivo y priorizado de restauración de servicios, primera fase en la intranet.
2. Paulatinamente los servicios se van liberando para acceso desde internet. **(Anexo 14)**

#### PLAN PROGRESIVO Y PRIORIZADO DE RESTAURACIÓN DE SERVICIOS

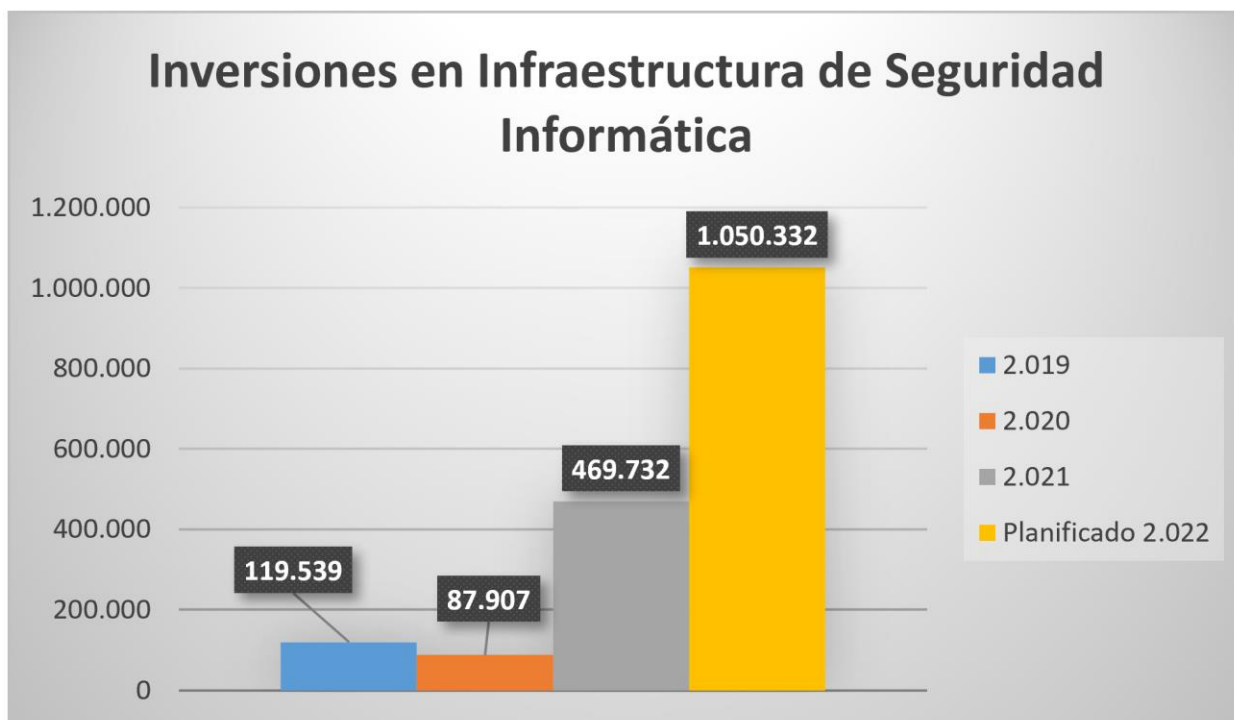
AGRUPACIÓN	SISTEMA	DESCRIPCIÓN	PLANIFICACIÓN		
			SEMANA 1	SEMANA 2	SEMANA 3
FINANCIERO	SAO	Sistema de Administración de Órdenes de Pago	▶		
	TELLER	Sistema de Recaudación Municipal	▶		
	Consulta de Obligaciones	Sistema para consultas de obligaciones	▶		
	Conexión con IFIs	Servicio web de interconexión	▶		
	Cuadros Bancarios	Cuadros bancarios			
	Botón de pagos	Botón de pagos			
	Patentes	Administración de Patentes - Intranet			
	Certificados digitales	Certificados digitales			
	SIPARI	Sistema de Planificación y Administración de Recursos Institucionales	▶		
RECURSOS HUMANOS	SIGEN	Sistema de Generación de Nomina y ejecución	▶		
	ICAM	Plataforma virtual de capacitación			
	ZKS	Sistema registro de huellas			
DOCUMENTAL	Sistema de Control de Asistencias de RR.HH.	Control de asistencia			
	SITRA	Sistema de Tramite	▶		
CATASTROS	SIREC-Q	Sistema de Registro Catastral de Quito para año actual	▶		
	Personas	Sistema para administración de personas	▶		
	Seguridades	Administración de usuarios			
	IRM	Informe de Regulación Metropolitana	▶		
	Cedula Catastral	Cedula Catastral			
	SIREC-Q - Integración RP (Consolas)	Integración entre SIREC-Q y Registro de la Propiedad			
SIN CLASIFICACIÓN	Mi ciudad	Sistema mi ciudad - Administración de Proyectos			
	Replica SRI	Servicio para replicar información del SRI			
	Sitio Web quito.gob.ec	Portal de acceso interno			
	Vehículos	Sistema para gestión de vehículos			
	Intranet	Portal Interno del Distrito Metropolitano de Quito (INTRANET)			
	SKELTA	Servicios expuestos para implementación con BPM			
	STL	Sistema de tramites en línea			
	Portal Administrativo Municipal - PAM	Portal administrativo municipal			
TRIBUTARIO	Core tributario Fase II (Transferencia de dominio)	Transferencia de dominio			
	CERVUS	Aplicativo Web de Gestión de los Impuestos Prediales (Exoneraciones, Cálculo, y Determinaciones)			
	LUAE	Licencia única de actividades económicas			
	PUCA	Permiso único de Comerciante Autónomo (PUCA)			


3. Integración de personal especializado.

Fortalecimiento de perfiles profesionales que permitan gestionar la seguridad informática con estrategias especializadas, de la mano con la conformación de la Secretaria de Gestión de TICS para reforzar la estabilidad del ecosistema de infraestructura tecnológica, acompañado por capacitaciones, desarrollo personal, evaluación del desempeño, sueldo, turnos rotativos, horarios, entre otros.

6.5.2 Estrategia de fortalecimiento de la Seguridad de la Infraestructura Tecnológica del GAD-DMQ

- ◆ Ejecución de los proyectos planificados que prevén un sistema de control con mayores capas de contención contra amenazas.
- ◆ Fortalecimiento de la infraestructura actual, a través de la continuación del plan de hardening (endurecimiento/fortalecimiento de seguridades en infraestructura existente: servidores, planificado desde 2021-NOV y en ejecución) y de las políticas de acceso a la red, que prevea mayores controles, hasta tener menores indicios de la presencia del “adversario” en la red.
- ◆ A continuación, se presenta la inversión en infraestructura de seguridades que ha tenido el GAD-DMQ. (Anexo 15)



	<b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b>  <b>(2022-ABR) – Información sensible</b>	<b>Versión: 01</b> <b>MDMQ-AG-2021- INSTRUCTIVO Nro.001-F.004</b>  <b>Informe N°</b> <b>DMI-INF001-CMQ</b>
---	---	--

## 7 Resultados obtenidos

1. Contención del ciberataque, sin neutralización total.
2. Habilitación de Servicios Internos (en intranet, para acceso de funcionario y servidores municipales).


### RESTAURACIÓN DE SERVICIOS DE COMUNICACIÓN

SERVICIOS DE COMUNICACIÓN	HABILITADO LUNES -MARTES
Navegación a Internet	✔
Correo Electrónico modalidad 365 (nube)	✔
Correo Electrónico Exchange (servidor data center)	✔

3. Habilitación de Aplicativos. **(Anexo 16)**

### RESULTADOS DE RESTAURACIÓN DE SERVICIOS (Semana 1: 18 al 22 -ABR.-2022)


AGRUPACIÓN	SISTEMA	DESCRIPCIÓN	EJECUTADO SEMANA 1
FINANCIERO	SAO	Sistema de Administración de Órdenes de Pago	✔
	TELLER	Sistema de Recaudación Municipal	✔
	Consulta de Obligaciones	Sistema para consultas de obligaciones	✔
	Conexión con IFIs	Servicio web de interconexión	✔
	SIPARI	Sistema de Planificación y Administración de Recursos Institucionales	✔
RECURSOS HUMANOS	SIGEN	Sistema de Generación de Nomina y ejecución	✔
DOCUMENTAL	SITRA	Sistema de Trámite	✔
CATASTROS	SIREC-Q	Sistema de Registro Catastral de Quito para año actual	✔
	Personas	Sistema para administración de personas	✔
	IRM	Informe de Regulación Metropolitana	✔

	<p align="center"><b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b></p> <p align="center">(2022-ABR) – Información sensible</p>	<p align="center">Versión: 01 MDMQ-AG-2021- INSTRUCTIVO Nro.001- F.004</p> <p align="center">Informe N° DMI-INF001-CMQ</p>
---	---	--

## 8 Conclusiones y recomendaciones

### 8.1 Conclusiones

- ◆ El ciberataque a la infraestructura tecnológica de la Dirección Metropolitana de Informática del GAD DMQ, realizado el 16 de abril de 2022, afectó a una de las plataformas tecnológicas virtualizadas, con las cuales presta los servicios a la ciudadanía y a los funcionarios y servidores municipales en todas sus dependencias.
- ◆ El ciberataque comprometió y dejó sin operación la computadora y máquinas virtuales que administran la plataforma de virtualización, y la computadora y máquina virtual que administra la plataforma del sistema de respaldos de información.
- ◆ El equipo técnico de la DMI ha realizado el aislamiento de las máquinas físicas y virtuales que fueron comprometidas, conteniendo la acción de los componentes de software que utiliza el atacante para su diseminación y contaminación.
- ◆ El equipo técnico de la DMI, con el apoyo de sus socios tecnológicos, ha contenido el ciberataque y ha restituido el control y la administración de toda la plataforma tecnológica, a nivel de usuario y a nivel de las plataformas tecnológicas en el centro de Datos de la DMI.
- ◆ El equipo técnico de la DMI ha contenido los efectos de este primer ataque, preservado la integridad de toda la información. Y cuenta con todos los respaldos de la información de los sistemas de información que prestan servicio a la ciudadanía.
- ◆ El equipo técnico de la DMI, con el apoyo de sus socios tecnológicos ha implementado nuevas herramientas de monitoreo y seguridad para elevar el nivel de protección de todas las plataformas tecnológicas del GAD DMQ.
- ◆ Los sistemas de monitoreo de acceso a las plataformas tecnológicas de GAD-DMQ, detecta tráfico de red que evidencia aún la presencia del malware atacante en máquinas ubicadas en localidades externas al Centro de Datos del Municipio de Quito.
- ◆ En seguimiento del protocolo adecuado para el tratamiento de este tipo de incidentes, el equipo técnico de la DMI está progresivamente restituyendo los servicios tecnológicos para los usuarios internos del municipio que permitan la atención a la ciudadanía en los balcones de servicio.


	<b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b>  <b>(2022-ABR) – Información sensible</b>	<b>Versión: 01</b> <b>MDMQ-AG-2021-</b> <b>INSTRUCTIVO Nro.001-</b> <b>F.004</b>  <b>Informe N°</b> <b>DMI-INF001-CMQ</b>
---	---	---

## 8.2 Recomendaciones


- ◆ Es necesario continuar con el monitoreo del tráfico interno de acceso a las aplicaciones y servicios que se han puesto en operación.
- ◆ Posterior a la operación de los sistemas, es conveniente restaurar paulatinamente la exposición de las mismas en el internet, en seguimiento de los procedimientos del protocolo que tratan este tipo de incidentes.
- ◆ Dotar de nueva infraestructura de seguridad informática.
- ◆ Agilizar procesos de contratación.
- ◆ Integrar personal especializado en ciberataques.

## 9 Firmas de responsabilidad

NOMBRE	FECHA	FIRMA
APROBADO POR: <b>franz v. enríquez pozo</b>  DIRECTOR METROPOLITANO DE INFORMÁTICA	2022-ABR	
ELABORADO Y REVISADO POR: ING. LUIS GUSTAVO CASTILLO PAREDES JEFE DE UNIDAD DE SERVICIOS DE PRODUCCIÓN	2022-ABR	
ELABORADO Y REVISADO POR: ING. DAVID ANTONIO MERA LARREA JEFE DE UNIDAD REDES Y SEGURIDADES	2022-ABR	

	<b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b>  <b>(2022-ABR) – Información sensible</b>	<b>Versión: 01</b> <b>MDMQ-AG-2021-</b> <b>INSTRUCTIVO Nro.001-</b> <b>F.004</b>  <b>Informe N°</b> <b>DMI-INF001-CMQ</b>
---	---	---

<b>NOMBRE</b>	<b>FECHA</b>	<b>FIRMA</b>
ELABORADO Y REVISADO POR: MGS. FAUSTO EMILIO NARANJO CALDERÓN JEFE DE INGENIERÍA DE SOLUCIONES	2022-ABR	
ELABORADO Y REVISADO POR: ING. MIRTHA PATRICIA PALACIOS LÓPEZ JEFE DE CENTRO DE ATENCIÓN TECNOLÓGICA	2022-ABR	
ELABORADO Y REVISADO POR: ING. BORIS ANDREY ENRÍQUEZ MEDINA JEFE DE PROYECTOS	2022-ABR	

	<p align="center"><b>Informe de ataque cibernético dirigido hacia la plataforma tecnológica GAD DMQ</b></p> <p align="center"><b>(2022-ABR) – Información sensible</b></p>	<p align="center">Versión: 01 MDMQ-AG-2021- INSTRUCTIVO Nro.001- F.004</p> <p align="center">Informe N° DMI-INF001-CMQ</p>
---	--	--

## 10 Anexos

- ◆ Anexo 1: "Informe técnico de evento de ataque ransomware a la infraestructura tecnológica del GAD-DMQ"
- ◆ Anexo 2: Informe de actividades desarrolladas (DMICBR-01) 2020-ABR-18
- ◆ Anexo 3: Informe de actividades desarrolladas (DMICBR-02) 2020-ABR-19
- ◆ Anexo 4: Informe de actividades desarrolladas (DMICBR-03) 2020-ABR-20
- ◆ Anexo 5: Informe de actividades desarrolladas (DMICBR-04) 2020-ABR-21
- ◆ Anexo 6: Informe de actividades desarrolladas (DMICBR-05) 2020-ABR-22
- ◆ Anexo 7: Denuncia No.170101822043050 ante la Fiscalía General del Estado
- ◆ Anexo 8: Correo electrónico de fecha 2022-ABR-17
- ◆ Anexo 9: Oficio Nro. GADDMQ-DMI-2022-0002-O-CNTG-I, 2020-ABR-20
- ◆ Anexo 10: Oficio Nro. GADDMQ-DMI-2022-00629-O, 2020-ABR-20
- ◆ Anexo 11: Oficio Nro. GADDMQ-DMI-2022-00637-O, 2020-ABR-21
- ◆ Anexo 12: Oficio Nro. GADDMQ-DMI-2022-00638-O, 2020-ABR-21
- ◆ Anexo 13: Oficio Nro. GADDMQ-DMI-2022-00644-O, 2020-ABR-23
- ◆ Anexo 14: Plan progresivo y priorizado de restauración de servicios
- ◆ Anexo 15: Certificado POA
- ◆ Anexo 16: Resultados de restauración de servicios (semana 1) 2022-ABR-18 al 22