ACTA DE LA SESIÓN Nro. 055 - ORDINARIA
DE LA COMISIÓN DE CONECTIVIDAD

VIERNES, 22 DE ABRIL DE 2022

En el Distrito Metropolitano de Quito, siendo las 10h07, de 22 de abril de 2022, conforme la convocatoria de 19 de abril de 2022, se lleva a cabo mediante plataforma virtual "Teams", la Sesión Nro. 55 - Ordinaria de la Comisión de Conectividad, presidida por el concejal Juan Carlos Fiallo.

Por disposición del señor presidente de la Comisión, se procede a constatar el quórum legal y reglamentario, para la instalación de la sesión virtual, mismo que se encuentra conformado por las siguientes concejalas y concejales: Luz Elena Coloma y Juan Carlos Fiallo.

REGISTRO DE ASISTENCIA – INICIO SESIÓN		
INTEGRANTE COMISIÓN	**PRESENTE**	**AUSENTE**
Juan Carlos Fiallo	1	
Paulina Izurieta Molina		1
Luz Elena Coloma	1	
TOTAL	2	1

Además, se encuentran presentes los siguientes funcionarios: Santiago David Ochoa Beltrán de la Secretaría de Desarrollo Productivo y Competitividad; Franz Enríquez Pozo, Director Metropolitano de Informática; Nadia Raquel Ruiz Maldonado, Secretaria General de Planificación; Helen Cristina Fabara Villacis de la Secretaría General de Planificación; Erick Mozo y Luis Gustavo Castillo Paredes, funcionarios de la Dirección Metropolitana de Informática; Ángelo Marino Rodríguez Cóndor de la Secretaría General de Coordinación Territorial y Participación Ciudadana; María Isabel Cepeda Zambrano de la Procuraduría Metropolitana; Gladys Marili Hernández Villalba y Hugo Tarapues del despacho del concejal Juan Carlos Fiallo; Álvaro Andrés Orbea Cevallos y Nelly Annai Gómez Velásquez, asesores del despacho de la concejala Luz Elena Coloma; Said Flores, técnico de la Secretaría General del Concejo Metropolitano.

La abogada Hillary Herrera, delegada de la Secretaría General del Concejo Metropolitano de Quito a la Comisión de Conectividad, por disposición del señor presidente procede a dar lectura del orden del día:

1.- Aprobación del acta de la sesión Nro. 054 – Extraordinaria del 08 de abril de 2022.
2.- Conocimiento y resolución sobre el proyecto de Ordenanza propuesto por el Alcalde Metropolitano de Quito, relacionado con la *"REFORMATORIA A LA ORDENANZA METROPOLITANA 001-2019, QUE CONTIENE EL CÓDIGO MUNICIPAL PARA EL DISTRITO METROPOLITANO DE QUITO LIBRO III.2 CAPÍTULO IV DEL SISTEMA DE GOBIERNO ELECTRÓNICO DEL DISTRITO METROPOLITANO DE QUITO".*
3.- Informe de los hechos ocurridos con el sistema informático del Distrito Metropolitano de Quito del 16 al 18 de abril del 2022, a cargo de la Dirección Metropolitana de Informática.
4.- Varios.

Se pone en consideración el orden del día y se toma votación, registrando los siguientes resultados:

REGISTRO DE VOTACIÓN					
INTEGRANTES COMISIÓN	**A FAVOR**	**EN CONTRA**	**ABSTENCIÓN**	**EN BLANCO**	**AUSENTE**
Juan Carlos Fiallo	1				
Paulina Izurieta Molina					1
Luz Elena Coloma	1				
TOTAL	2	0	0	0	1

Con dos votos a favor, queda aprobado el orden del día planteado.

DESARROLLO DE LA SESIÓN

Primer punto: Aprobación del acta de la sesión Nro. 054 – Extraordinaria del 08 de abril de 2022.

- Sesión Nro. 054 – Extraordinaria del 08 de abril de 2022;
Sin existir observaciones y por disposición del presidente de la Comisión de Conectividad, concejal Juan Carlos Fiallo, se procede a tomar votación del acta No. 054 – Extraordinaria del 08 de abril de 2022, registrando los siguientes resultados:

REGISTRO DE VOTACIÓN					
INTEGRANTES COMISIÓN	A FAVOR	EN CONTRA	ABSTENCIÓN	EN BLANCO	AUSENTE
Juan Carlos Fiallo	1				
Paulina Izurieta Molina					1
Luz Elena Coloma	1				
TOTAL	2	0	0	0	1

Con dos votos a favor, la Comisión de Conectividad aprueba el acta No. 054 – Extraordinaria del 08 de abril de 2022.

Segundo punto: Conocimiento y resolución sobre el proyecto de Ordenanza propuesto por el Alcalde Metropolitano de Quito, relacionado con la *"REFORMATORIA A LA ORDENANZA METROPOLITANA 001-2019, QUE CONTIENE EL CÓDIGO MUNICIPAL PARA EL DISTRITO METROPOLITANO DE QUITO LIBRO III.2 CAPÍTULO IV DEL SISTEMA DE GOBIERNO ELECTRÓNICO DEL DISTRITO METROPOLITANO DE QUITO".*

El concejal Juan Carlos Fiallo, Indica que existen dos proyectos de Ordenanza que tratan el mismo tema (conformación del Gobierno Electrónico) y que los mismos ya han sido calificados por la Secretaria General del Concejo. Adicionalmente informa que se han realizado mesas de trabajo, para poder unificar estos dos proyectos en uno solo.

Siendo las 10h15 ingresa a la sesión la concejala Paulina Izurieta Molina.

Erik Mozo, funcionario de la Dirección Metropolitana de Informática, informa sobre los avances, en base al proyecto de Ordenanza en referencia e indica que uno de los acuerdos a los que se llegó, es que el Concejo deberá aprobar un Plan de digitalización, mismo que se evaluará permanentemente.

Álvaro Andrés Orbea Cevallos, asesor del despacho de la concejala Luz Elena Coloma, señala que la creación de este Plan va a servir para saber cómo se está avanzando en el Municipio como Gobierno Electrónico, por lo que solicita al presidente de la Comisión su apoyo para la construcción de un artículo, para saber qué es lo que debería contener el Plan, para que exista una mayor claridad del mismo.

El concejal Juan Carlos Fiallo, manifiesta que este Plan debe contener lineamientos, indicadores, metas; y, sobretodo que el objetivo general sea la solución de un problema, el mismo que deberá ser claro, preciso y sin inconsistencias.

Nadia Raquel Ruiz Maldonado, Secretaria General de Planificación, señala que en la Administración General existe un comité de tecnologías de la información que tiene varias funciones, pero su rol es definir, conducir y evaluar políticas internas, todo lo contrario, a lo que se plantea en este Gobierno Electrónico el mismo que está dirigido para toda la ciudadanía.

Erik Mozo, funcionario de la Dirección Metropolitana de Informática, señalo tres cosas indispensables que debería contener este Plan, que es: un diagnostico actual de la digitalización y los procesos de conectividad de las entidades Municipales; de cuáles son las políticas que se tienen planteadas, para alcázar los objetivos en materia de digitalización; y, finalmente la definición de metas y plazos para la aplicación de este Plan.

La concejala Luz Elena Coloma, sugirió que se termine la redacción del nuevo texto de Ordenanza y se soliciten los informes necesarios para poder seguir avanzando.

El concejal Juan Carlos Fiallo, eleva a **moción:** que el Proyecto de *"ORDENANZA SUSTITUTIVA DEL CAPÍTULO IV, LIBRO III.2, DEL SISTEMA DE GOBIERNO ELECTRÓNICO DEL DISTRITO METROPOLITANO DE QUITO"* de iniciativa del Concejal Metropolitano, Magíster Juan Carlos Fiallo Cobos; y, el proyecto de *"ORDENANZA REFORMATORIA A LA ORDENANZA METROPOLITANA 001-2019, QUE CONTIENE EL CÓDIGO MUNICIPAL PARA EL DISTRITO METROPOLITANO DE QUITO LIBRO III.2 CAPÍTULO IV DEL SISTEMA DE GOBIERNO ELECTRÓNICO DEL DISTRITO METROPOLITANO DE QUITO"* de iniciativa del Señor Alcalde Metropolitano, Doctor Santiago Guarderas Izquierdo, sean trabajados de manera conjunta para que, en una próxima sesión se presente a la Comisión de Conectividad, un solo proyecto de Ordenanza unificado.

REGISTRO DE VOTACIÓN					
INTEGRANTES COMISIÓN	**A FAVOR**	**EN CONTRA**	**ABSTENCIÓN**	**EN BLANCO**	**AUSENTE**
Juan Carlos Fiallo	1				
Paulina Izurieta Molina	1				

Luz Elena Coloma	1				
TOTAL	3	0	0	0	0

Con tres votos a favor, la Comisión de Conectividad; **resolvió:** que el Proyecto de *"ORDENANZA SUSTITUTIVA DEL CAPÍTULO IV, LIBRO III.2, DEL SISTEMA DE GOBIERNO ELECTRÓNICO DEL DISTRITO METROPOLITANO DE QUITO"* de iniciativa del Concejal Metropolitano, Magíster Juan Carlos Fiallo Cobos; y, el proyecto de *"ORDENANZA REFORMATORIA A LA ORDENANZA METROPOLITANA 001-2019, QUE CONTIENE EL CÓDIGO MUNICIPAL PARA EL DISTRITO METROPOLITANO DE QUITO LIBRO III.2 CAPÍTULO IV DEL SISTEMA DE GOBIERNO ELECTRÓNICO DEL DISTRITO METROPOLITANO DE QUITO"* de iniciativa del Señor Alcalde Metropolitano, Doctor Santiago Guarderas Izquierdo, sean trabajados de manera conjunta para que, en una próxima sesión se presente a la Comisión de Conectividad, un solo proyecto de Ordenanza unificado.

Tercer punto: Informe de los hechos ocurridos con el sistema informático del Distrito Metropolitano de Quito del 16 al 18 de abril del 2022, a cargo de la Dirección Metropolitana de Informática.

Franz V. Enríquez Pozo, Director Metropolitano de Informática, explica sobre el ciberataque dirigido al Distrito Metropolitano de Quito, los hechos sucedido, la naturaleza del ciberataque, el esquema de protección del GAD-DMQ y la evolución de la afectación,

(Se adjunta como anexo 1, la presentación de la Dirección Metropolitano de Informática)

Luis Gustavo Castillo Paredes, funcionario de la Dirección Metropolitana de Informática, da a conocer que tanto el software libre como el propietario, son atacados por igual con herramientas muy sofisticadas.

Los concejales miembros de la Comisión, realizan sus observaciones e inquietudes respecto al ciberataque dirigido al Municipio del Distrito Metropolitano de Quito. Preguntan si existen respaldos?, cuál fue el procedimiento que se siguió?, cuál es la seguridad con la que cuenta el MDMQ en base a lo sucedido?, se está realizando la auditoria correspondiente?; y , si existe la opción de cambiarse a un software libre.

Franz V. Enríquez Pozo, director Metropolitano de Informática; manifiesta que se tendría que analizar la implementación de un software libre en el Municipio del Distrito Metropolitano de Quito y que sería una opción.

El concejal Juan Carlos Fiallo, solicita a la Dirección Metropolitana de Informática, remita a la Comisión de Conectividad, un informe pormenorizado, sobre lo expuesto, respecto los artículos del COOTAD y la implantación del software libre en base a la factibilidad tanto técnica como económica.

Cuarto punto: Varios.

Los miembros de la Comisión manifiestan que no tienen ningún tema adicional por tratar.

Siendo las 12h19, habiendo agotado el orden del día, el señor presidente de la Comisión, concejal Juan Carlos Fiallo, declara clausurada la sesión.

REGISTRO ASISTENCIA – FINALIZACIÓN SESIÓN		
INTEGRANTES COMISIÓN	**PRESENTE**	**AUSENTE**
Juan Carlos Fiallo	1	
Paulina Izurieta Molina	1	
Luz Elena Coloma	1	
TOTAL	3	0

Para constancia de lo actuado, firman el señor presidente de la Comisión de Conectividad y el señor Secretario General del Concejo Metropolitano de Quito.

Firmado electrónicamente por:
JUAN CARLOS FERNANDO FIALLO COBOS

PABLO ANTONIO SANTILLAN PAREDES
Firmado digitalmente por PABLO ANTONIO SANTILLAN PAREDES
Fecha: 2022.07.13 15:28:54 -05'00'

Mgs. Juan Carlos Fiallo Cobos
PRESIDENTE DE LA COMISIÓN DE CONECTIVIDAD

Abg. Pablo Santillán Paredes
SECRETARIO GENERAL DEL CONCEJO METROPOLITANO DE QUITO

REGISTRO ASISTENCIA – RESUMEN DE SESIÓN		
INTEGRANTES COMISIÓN	**PRESENTE**	**AUSENTE**

Juan Carlos Fiallo	1	
Paulina Izurieta Molina	1	
Luz Elena Coloma	1	
TOTAL	3	0

Acción:	**Responsable:**	**Unidad:**	**Fecha:**	**Sumilla:**
Elaborado por:	Hillary Herrera	SCCN	2022-04-29	
Revisado por:	Samuel Byun	PSGC (S)	2022-04-29	

ANEXO 1

Ciberataque dirigido al GAD-DMQ

DMI

2022-ABR-22

Ciberataque dirigido al GAD DMQ

Agenda:

1. Hechos sucedidos
   a) Hora inicio y estrategia del ataque
   b) Comprometimiento información, segmentos de red, aplicativos
2. Naturaleza del ciberataque
   a) Origen
   b) Tecnología
   c) Alcance
   d) Contexto de los ciberataques
3. Seguridad informática en el GAD-DMQ
   1. Ecosistema
   2. Nuevo diseño
4. Evolución del Ciberataque y siguientes pasos:

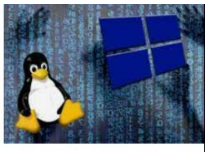
Hechos sucedidos (1/2)

- En la madrugada del día 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.
- 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).
- 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.

Hechos sucedidos (2/2)

- El municipio cuenta con los respaldos de la información para poder volver a las operaciones normales.
- En las tareas de verificación de los respaldos, hasta el momento no se evidencia pérdidas de la misma.
- 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”, a (19 de abril del 2022).

Naturaleza del Ciberataque



- El “adversario” es clasificado por las herramientas de identificación del malware como un ciberataque de tipo ransonware.
- “Since its first emergence in November 2021, the Cybereason Nocturnus team has been tracking the BlackCat Ransomware (aka ALPHV), which has been called “2021’s most sophisticated ransomware”. ”

  https://www.cybereason.com/blog/cybereason-vs.-blackcat-ransomware

- “La nueva operación de ransomware ALPHV, también conocida como BlackCat, se lanzó el mes pasado y puede ser el ransomware más sofisticado del año, con un conjunto de funciones altamente personalizables que permite ataques en una amplia gama de entornos corporativos”. https://diarioinforme.com/alphv-blackcat-el-ransomware-mas-sofisticado-de-este-ano/

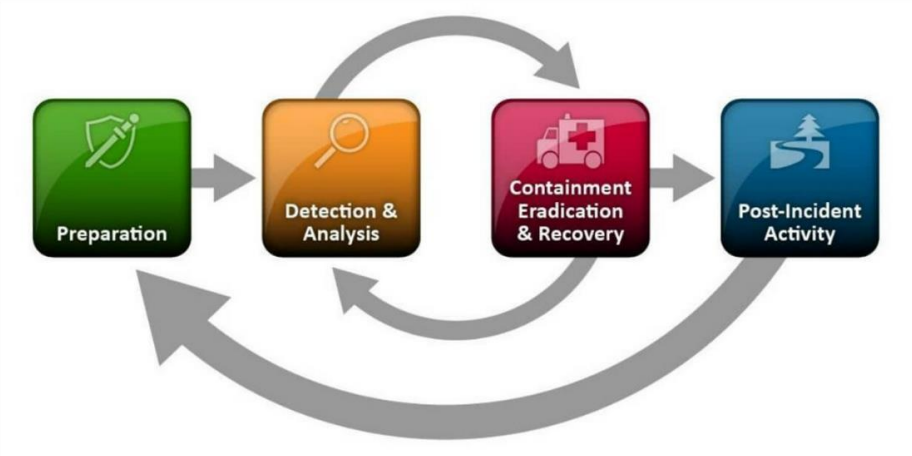
Naturaleza del Ciberataque

- Uno de los elementos únicos del ransomware BlackCat es que está escrito en Rust , que no es un lenguaje de codificación común para malware y ransomware. *“Rust es un lenguaje de programación multiparadigma y de propósito general diseñado para el rendimiento y la seguridad. ”*
- “Debido al énfasis de Rust en el rendimiento, el proceso de cifrado es muy rápido y, además, Rust es multiplataforma, lo que facilita la creación de variantes tanto para Windows como para Linux. ”
- “El ransomware BlackCat tiene variantes de Windows y Linux.”
  - https://www-cybereason-com.translate.goog/blog/cybereason-vs.-blackcat-ransomware?_x_tr_sl=en&_x_tr_tl=es&_x_tr_hl=es&_x_tr_pto=wapp

Contexto de ataques

- En el año 2021, la Fiscalía del Ecuador recibió 7.000 denuncias sobre ciberdelitos (los que son reportados, se estima un número mayor de los sucedidos).
- Los centros de monitoreo de virus/malware detectan diariamente 10.000 variaciones de infecciones del tipo ransomware.
- El 99% de la información que captura el malware de rescate (ransomeware) no puede ser decodificada.
- Ataque Costa Rica (IMN -> prueba para ataque masivo a todos los sitios del estado)
- Ataque al Senado de Argentina
- El regreso a operaciones automatizadas, en las instituciones que han sido víctimas de estos delitos, ha sido de varias semanas y en algunos casos meses.

Respuesta a incidentes de seguridad (NIST)



Seguridad informática en el GAD-DMQ

Situación encontrada 2021-OCT:

- Herramientas de seguridad: firewall, prevención de intrusos, antivirus, firewall aplicaciones

Corto plazo (6 meses: NOV-ABR):

- Actualización de herramientas para la seguridad informática. Renovación de suscripciones.
- Hardening de la infraestructura (servidores y demás elementos para robustecer la seguridad).
- Medidas de control más robusto para acceso a recursos informáticos.
- Diseño de un esquema de seguridad más robusto (con otras capas de seguridad).

Mediano Plazo:

- Visión de sistemas de control de amenazas soportados por firewalls especializados (de aplicaciones, bases de datos) así como también de monitoreo por servicios internacionales de control de amenazas (SOC).
- En el mes de mayo está planificado publicar los procesos de adquisición de los elementos necesarios para robustecer la seguridad de la infraestructura tecnológica.
- Fortalecimiento de perfiles profesionales que permitan gestionar la seguridad con estrategias especializadas, de la mano con la conformación de la Secretaría de Gestión de TICS

Evolución de la afectación

- Los primeros días posteriores al Ciberataque, el equipo técnico se dedicó a la detección extensiva de agentes y malware en general, remanente en la infraestructura central.
- El día martes de la presente semana los usuarios ya contaron con Correo electrónico, navegación por internet y validación del Sistema SIREC-Q (que gestionar los procesos de Catastros).
- El día miércoles ya se contó ya con el Sistema documental en línea, para uso interno de los funcionarios, con limitaciones en consultas de anexos en documentos históricos, y total funcionalidad en trámites nuevos.
- En la primera semana posterior al incidente se tiene restaurado varios sistemas de información con los que se atiende los servicios a la ciudadanía.

Evolución de la afectación – habilitación de servicios y sistemas

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)	✔

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 Tramite	✔
CATASTROS	SIREC-Q	Sistema de Registro Catastral de Quito para año actual	✔
	Personas	Sistema para administración de personas	✔
	IRM	Informe de Regulación Metropolitana	✔

Siguientes pasos

- Fortalecimiento de la infraestructura de seguridades, que con aliados tecnológicos se ha podido realizarla en el corto plazo y ejecución de las inversions planificadas para el mediano plazo (2022-2023).
- Levantamiento de los sistemas que permite prestar los servicios ciudadanos.
- Fortalecimiento de perfiles informáticos que permitan la gestión de la seguridad.