

Memorando Nro. GADDMQ-SGDTIC-2024-00502-M

Quito, D.M., 07 de agosto de 2024

PARA: Sra. Maria Cristina Lopez Gomez de la Torre
Concejala Metropolitana
DESPACHO CONCEJAL LOPEZ GOMEZ DE LA TORRE MARIA
CRISTINA

ASUNTO: Solicitud de Información licencias

De mi consideración:

Con un cordial y atento saludo, en atención al memorando Nro. GADDMQ-DC-LGMC-2024-0321-M de 30 de julio de 2024, mediante el cual solicita a esta Secretaría, la siguiente información:

"(...)

1. *Informar sobre el periodo de vigencia y fecha de caducidad del contrato de las licencias de antivirus (endpoint) con las que cuenta el Municipio Metropolitano de Quito.*
2. *Informar cual es la plataforma de Anti-Spam con la que cuenta el Municipio Metropolitano de Quito y la vigencia de su licencia. En vista que a diario ingresan correos no deseados a los buzones enlazados al servidor Ms Exchange (on-premise).*
3. *Informar el plan de contingencias ante ciberataques.*

(...)"

Al respecto me permito informar lo siguiente:

Esta Secretaría de Gobierno Digital y Tecnologías de Información y Comunicaciones, gestiona la infraestructura tecnológica del GAD del DMQ, por lo que cuenta con una arquitectura de seguridad de TIC, que implementa un modelo de seguridad por profundidad, lo que significa que un usuario al acceder a un servicio informático pasa por varias capas compuestas por equipos tecnológicos especializados en análisis de seguridad informática; para fortalecer este modelo, se encuentra en ejecución un Contrato de servicios de seguridad informática, el cual tiene una vigencia hasta el mes de mayo de 2025. Con este servicio, se permite mejorar la visibilidad en aspectos de seguridad, mediante la correlación de eventos que se generan en las distintas capas de seguridad y monitoreo de tráfico de red.

Adicionalmente, esta Secretaría emitió el procedimiento para el control de virus para la atención de tickets generados por el Centro de Operaciones de Seguridad (SOC) del GAD del DMQ; el cual, tiene como objetivo establecer un mecanismo para que los funcionarios de la Unidad de Servicios Tecnológicos (UST) y técnicos desconcentrados del GAD del DMQ implementen soluciones efectivas para controlar virus y parásitos informáticos para las diferentes alertas de seguridad informática a nivel de endpoints, generadas por el SOC en el GAD del DMQ.

Acerca de la información solicitada en el número 1, referente a "Informar sobre el periodo de

Memorando Nro. GADDMQ-SGDTIC-2024-00502-M

Quito, D.M., 07 de agosto de 2024

vigencia y fecha de caducidad del contrato de las licencias de antivirus (endpoint) con las que cuenta el Municipio Metropolitano de Quito." es importante informar que la protección contra virus y amenazas de la seguridad de Windows se encuentra activada en todas las computadoras (endpoints) del GAD del DMQ; y, que con el objeto de reforzar la seguridad de TIC esta Secretaría se encuentra en proceso de adquisición de una solución tecnológica de mejores características técnicas en comparación con un antivirus de acuerdo a las tendencias de ciberseguridad de última generación. Cabe mencionar que este proceso de adquisición se encuentra por finalizar la etapa preparatoria.

Respecto al numeral 2 de su pedido, se informa que esta Secretaría una vez que generó las acciones correspondientes, conforme las disposiciones de la Ley Orgánica del Sistema Nacional de Contratación Pública y su Reglamento General de aplicación, ejecutó el procedimiento de contratación de Subasta Inversa Electrónica para la contratación de la plataforma de Anti-Spam, dicho proceso se encuentra en la etapa de adjudicación. Es importante mencionar que esta plataforma tendrá un periodo de 2 años de vigencia.

Por ultimo, dando atención a lo solicitado en el punto 3, respecto a *"Informar el plan de contingencias ante ciberataques"*, se informa que esta Secretaría tiene aprobado y emitido el Plan de Respuesta de Incidentes de Ciberseguridad, el mismo que cuenta con el apoyo de un proveedor externo, el cual se encuentra certificado como CERT (Computer Emergency Response Team); cabe mencionar que sus procesos también se encuentran certificados en la ISO 27001, esto permite que el GAD del DMQ cuente con una efectiva gestión de respuesta ante incidentes de ciberseguridad, dicho Plan contempla un flujo de trabajo para las siguientes fases: preparación, detección y análisis, contención y, actividades post incidente.

Es importante señalar que la información relacionada con la seguridad de TIC es de carácter confidencial; por lo cual, para mayor detalle, sugerimos respetuosamente una mesa de trabajo conjunta.

Con sentimientos de distinguida consideración.

Atentamente,

Documento firmado electrónicamente

Ing. Ligia Alexandra Álava Freire
SECRETARIA DE GOBIERNO DIGITAL Y TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES
SECRETARÍA DE GOBIERNO DIGITAL Y TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Memorando Nro. GADDMQ-SGDTIC-2024-00502-M

Quito, D.M., 07 de agosto de 2024

Referencias:

- GADDMQ-DC-LGMC-2024-0321-M

Copia:

Sra. Dra. Libia Fernanda Rivas Ordóñez
Secretaria General
SECRETARÍA GENERAL DEL CONCEJO METROPOLITANO DE QUITO

Sr. Jose Luis Baquero Subia
Funcionario Directivo 9
DESPACHO CONCEJAL LOPEZ GOMEZ DE LA TORRE MARIA CRISTINA

Sr. Mgs. Luis Alexander Vélez Bedoya
Jefe de la Unidad de Seguridad de TIC - FD7
SGDTIC-DMIST-UNIDAD DE SEGURIDAD DE TIC

Sr. Mgs. Andrés Aníbal Riofrio Córdova
Director Metropolitano de Infraestructura y Seguridad de TIC- Funcionario Directivo 5
SGDTIC-DIRECCIÓN METROPOLITANA DE INFRAESTRUCTURA Y SEGURIDAD DE TIC

Sra. Abg. Verónica Alexandra Pérez Sarmiento
Coordinador Legal- fd6
SGDTIC-COORDINACIÓN LEGAL

Sr. Ing. Juan Carlos Fiallos Quinteros
Coordinador Técnico FD6
SGDTIC-COORDINACIÓN TÉCNICA

Acción	Siglas Responsable	Siglas Unidad	Fecha	Sumilla
Elaborado por: Luis Alexander Vélez Bedoya	lv	SGDTIC-DMIST-US	2024-08-02	
Revisado por: Andrés Aníbal Riofrio Córdova	ar	SGDTIC-DMIST	2024-08-05	
Aprobado por: Ligia Alexandra Álava Freire	lá	SGDTIC	2024-08-07	

