Informe técnico

Tema: Sesión Nº 55 de la Comisión de Conectividad
Fecha: Miércoles 27 abril 2022

Sumario

Cuadro de registro de cambios

Fecha	Versión	Responsable	Cargo	Cambios	Firma
27 abril 2022	1.0	David Ochoa	SDPC Legal	Redacción	SOB

Cuadro de aprobación del documento

Fecha	Versión	Responsable	Cargo	Rol	Firma

Introducción

1. Con fecha 22 de abril de 2022, tuvo lugar la Sesión ordinaria N° 55 de la Comisión de Conectividad, del eje económico del Concejo Metropolitano, donde se abordó sobre dos puntos:
    a. Ordenanza reformatoria a los artículos del Código Municipal que regulan el Consejo de Gobierno Electrónico.
    b. Hechos ocurridos en el sistema informático municipal el 16 a 18 de abril
2. En cumplimiento de la delegación contenida en oficio GADDMQ-SDPC-2022-0310-O, participé en dicha sesión como delegado de esta Secretaría.
3. Este informe resume lo abordado en la sesión además de proporcionar información adicional que pueda servir a la Comisión para el análisis del evento informático iniciado el 16 de abril pasado.

Desarrollo del informe

La Comisión de Conectividad sigue el siguiente procedimiento de trabajo:

- Sesiona los viernes cada 15 días, tanto de manera presencial como virtual.
- Realiza mesas de trabajo para el desarrollo de tres proyectos de ordenanza:
    - Ordenanza para reformar los artículos 1152 a 1156 del Código Municipal, que regula las entidades encargadas del gobierno electrónico municipal.
    - Ordenanza sobre soterramiento de cables: En 2017, la Corte Constitucional declaró inconstitucional ciertas secciones de la Ordenanza Metropolitana 022 sobre instalación de redes (actualmente artículos 2032 a 2039 del Código Municipal), por lo que se requiere una ordenanza reformatoria para adecuar las normas al marco constitucional.
    - Ordenanza que trata sobre innovación: En 2012, el Concejo aprobó una Ordenanza 263 sobre el régimen de fomento a las innovaciones (tecnológicas o no), a la investigación científica y a saberes ancestrales y creaciones originales, contenido en los actuales artículos 1194 a 1204 del Código Municipal codificado.

La sesión del pasado 22 de abril abordó la primera de estas ordenanzas y el incidente informático iniciado el 16 de abril de 2022.

Proyecto de ordenanza sobre el Consejo de Gobierno Electrónico

Actualmente existen dos proyectos de ordenanza para reformar los artículos 1152 a 1156 del Código Municipal, que establecen un Consejo de Gobierno Electrónico y asignan atribuciones a varias entidades municipales. Esta sección del informe resume el estado actual de este proyecto de reforma.

Antecedente normativo

El 13 de octubre de 2005, el Concejo Metropolitano aprobó una Ordenanza 159 (R O 154 de 28 de noviembre de 2005) que regulaba el uso de las tecnologías de información y comunicación (TIC) en el Municipio.

Esta norma abarcaba:

1. Definiciones sobre TIC y la política municipal sobre ella.
2. Principios de actuación en relación a TIC: neutralidad tecnológica, equivalencia funcional, libre competencia, protección a la provacidad e intimidad, protección a la libertad de expresión, acceso a la información y libertad de contratación.
3. En 7 artículos regula el manejo de datos personales (sensibles) de la ciudadanía por parte del Municipio, incluyendo el deber de establecer medidas técnicas de protección de datos.
4. Se reconocen derechos a acceder a información y a solicitar rectificación de errores.
5. Se establecen políticas municipales elementales en materia de TIC.
6. Art. 20: *"Es obligación del Municipio estandarizar los procedimientos administrativos, de tal manera, que sus Dependencias, las Empresas Municipales y Corporación utilicen procedimientos iguales o similares"*.
7. Previo a implmenetar nuevos programas, se requería autorización de la Asesoría de Desarrollo Institucional y de la Direcciòn Metropolitana de Informática.
8. Art. 23: *"Las dependencias del Municipio, las Empresas Municipales y Corporaciones podrán desarrollar sus aplicaciones informáticas, previo el cumplimiento del procedimiento establecido en el presente documento, de tal forma que sean compatibles e interrelacionados con las demás aplicaciones existentes en el Municipio, para ello, la Dirección Metropolitana de Informática deberá certificar que las especificaciones d ella aplicación a desarrollarse cumplen con las características mencionadas"*.
9. Obligación de que el acceso a datos personales, se requiera autenticación con identidad y contraseña.
10. Obligación de uso de firmas electrónicas en la contratación pública.
11. Regulación de medios de pago electrónico.
12. Regulación del correo electrónico.
13. Sección IV sobre el uso de software de código abierto en el Municipio.
14. Asigna la responsabilidad de aplicación de esta ordenanza en la Administración General y su Dirección Metropolitana de Informática.

Normativa vigente

Apenas dos años más tarde, el 3 de agosto de 2007, se deroga dicha ordenanza mediante la Ordenanza Metropolitana 236, que actualmente forma parte del Código Municipal codificado, en sus artículos 1145 a 1193, donde se regula sobre:

1. Objetivo y ámbito territorial de aplicación.
2. Principios: simplificación administrativa, proporcionalidad, eficiencia, neutralidad tecnológica, accesibilidad, confidencialidad, seguridad y protección de datos, participación, autenticidad de la información, entre otros.
3. Derechos de la ciudadanía en relación a TIC (incluye confidencialidad de datos personales, entre otras).

4. Deberes de los ciudadanos en relación a TIC (buena fe, etc.).
5. La propiedad intelectual de todos los proyectos, planes y estrategias generados en el Municipio le pertenece al Municipio.
6. Obligaciones de la administración municipal en relación a TIC.
7. Instituye un Consejo de Gobierno Electrónico.
8. Denomina Nodos Zonales de Gobierno Electrónico a las unidades de TIC de cada entidad municipal.
9. Denomina Unidad Central de Gobierno Electrónico a la Dirección Metropolitana de Informática o a la entidad que haga sus veces.
10. Asigna atribuciones concretas en relación a TIC a la Secretaría de Comunicación.
11. Asigna atribuciones concretas a la Dirección Metropolitana de Informática.
12. Definición y uso de la telemática en procedimientos administrativos.
13. Obligación de difundir la información administrativa y la normativa municipal.
14. Procedimiento para volver electrónicos los trámites administrativos.
15. Emisión electrónica de certificados y documentos, para evitar uso de papel.
16. Sesiones del Concejo y sus comisiones puedne ser virtuales.
17. Archivo informático de solicitudes en una base de datos (actual SITRA).
18. Derecho a acceso a información: conforme LOTAIP (Ley Transparencia).
19. Áreas de acción: Teleeducación, Telemedicina, Teleseguridad, Teletransporte, Teleturismo, Telecomercialización, Teleambiente, Teletrabajo, Teleservicios, Acceso a internet, Redes móviles de telefonía celular.
20. Obligación municipal de establecer sistemas de tratamiento y disposición de desechos tecnológicos.
21. Plazo para diagnosticar el uso de TIC para definir políticas: 6 meses desde agosto 2007.
22. Los datos sobre TIC y políticas digitales serán reportados al Observatorio del Distrito.

Luego, en 2020, se aprobó la Ordenanza Metropolitana N.º 014 que incorporó seis artículos que regulan los puntos de internet municipal en espacios públicos.

Obstáculos identificados en la normativa vigente

El Consejo de Gobierno Electrónico no ha podido sesionar nunca debido a:

1. Sólo el Alcalde metropolitano está facultado a delegar la asistencia a este Consejo. El resto de integrantes no tiene esta facultad.
2. No se establece cuál secretaría representa a cada uno de los cuatro ejes de intervención municipal (El art. 67 del Código Municipal establece los ejes de: Gobernabilidad, Territorio, Social y Económico, pero cada eje representa el trabajo de varias Secretarías dentro de sí).
3. El Código Municipal exigía que asista un delegado del Consejo de Educación Superior, entidad ajena al Municipio (que jamás asistió).

4. El Consejo de Gobierno Electrónico tiene actualmente atribución para formular políticas sobre conectividad digital, pero no tiene capacidades para formular política pública.

La evidencia de que las normas de la Ordenanza Metropolitana 236 no fueron óptimas se encuentra en que el Consejo de Gobierno Electrónico nunca ha podido sesionar desde su creación en 2007, debido a:

- Falta de autorización expresa para delegar.
- Falta de certidumbre de cuáles Secretarías integran este Consejo.
- El Consejo de Educación Superior nunca nombró un delegado, debido principalmente a que dicha entidad, al pertenecer al nivel central de gobierno, no está obligada a nombrar delegado al Consejo, dado que dicha atribución no consta en la normativa nacional que rige al CES.

Por estos motivos, se han recibido dos proyectos de ordenanza reformatoria, los cuales han sido calificados y remitidos a la Comisión de Conectividad.

El jueves 21 de abril tuvo lugar una mesa de trabajo, con la participación de los delegados de los concejales que integran esta comisión (Juan Carlos Fiallo, Paulina Izurieta y Luz Elena Coloma), además de la Dirección Metropolitana de Informática (DMI) y demás entidades relacionadas.

Consensos para elaborar la ordenanza reformatoria

Producto de este trabajo, se presentó a la Comisión los siguientes consensos que guiarán la redacción del proyecto unificado de ordenanza reformatoria:

1. El Consejo de Gobierno Electrónico estará integrado por:
    1. Alcalde o su delegado.
    2. Presidente de la comisión de conectividad, o su delegado.
    3. El Administrador General, vía su Dirección de Servicios Ciudadanos.
    4. Secretaría General de Planificación o su delegado.
    5. Secretaría General de Coordinación Territorial o su delegado.
    6. Secretaría de Desarrollo Productivo y Competitividad o su delegado.
    7. Entidad o secretaría responsable de TIC, o su delegado.
2. La secretaría de este Consejo ya no estará a cargo de DMI sino de la Secretaría de Comunicación.
3. El Consejo tendrá solamente atribución de recibir la propuesta de política pública que elabore la entidad rectora de TIC que determine el Alcalde, en ejercicio de sus atribuciones de organizar administrativamente el gobierno autónomo descentralizado.
4. Ya no habrá delegado del Consejo de Educación Superior.

En la sesión de 22 de abril, la Comisión de Conectividad aprobó estos acuerdos y dispuso a los equipos de trabajo avanzar en una redacción unificada de ambos proyecto de ordenanza.

Asimismo, la Comisión resolvió unificar ambos proyectos en un solo trámite.

Siguientes actividades en relación a este proyecto

La siguiente mesa de trabajo sobre este tema será este viernes 29 de abril. Tras la presentación de un proyecto unificado, la comisión deberá elaborar y aprobar un informe de comisión para remitir este proyecto al Pleno del Concejo.

Informe DMI sobre suceso informático de 16 de abril

La Dirección Metropolitana de Informática presentó a la Comisión de Conectividad el siguiente informe sobre la caída de servicios informáticos en el Municipio desde el pasado sábado 16 de abril:

1. **Hechos sucedidos**
    1. Hora de inicio: En la madrugada del 16 abril 2022 se evidenciaron consecuencias de un ciberataque dirigido a la infraestructura tecnológica del Municipio, orientado a encriptar recursos inormáticos estratégicos para dejar sin operación los servicios automatizados del Municipio.
    2. Foco del ataque:
        1. Consola del administrador de la virtualización, dejando inutilizado el acceso al visor de las máquinas virtuales.
        2. 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).
    3. Funcionarios de la DMI pudieron detener la expansión del ataque al haberse encontrado trabajando el sábado 16 de abril 2022.
    4. En las tareas de limpieza del virus de los equipos de usuario final para conectarlas a los segmentos de red, se identifica aún la presencia del adversario hasta al menos 19 de abril 2022.
2. **Naturaleza del ataque**
    1. Origen: Ransomware (ataque para pedir un rescate o ransom).
    2. Tipología: Blackcat o ALPHV. Surgió desde noviembre 2021 y fue catalogado como el ransomware más sofisticado de acuerdo a la red “Cybereason Nocturnus team” debido a que tiene un conjunto de funciones altamente personalizables que permite ataques en una amplia gama de entornos corporativos.
    3. Características: Blackcat está escrito en Rust, un lenguaje de programación multi programa y de propósito general diseñado para el rendimiento. No es común que los ataques ransomware estén escritos en Rust.
    4. *“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”*
3. **Esquema de protección del GAD DMQ**
    1. El Municipio viene preparándose para potenciales ataques informáticos.
    2. A octubre 2021 el Municipio se encontraba con herramientas de seguridad y prevención de intrusos.
    3. En el corto plazo (desde noviembre 2021 a abril 2022), la DMI se ha preocupado por cumplir las siguientes actividades:

1. Actualización de herramientas para la seguridad informática.
2. Renovación de suscripciones de soporte y asistencia.
3. Hardening de la infraestructura (servidores y demás elementos para robustecer la seguridad).
4. Medidas de control más robusto para acceso a recursos informáticos.

4. En el mediano plazo, DMI plantea incorporar las siguientes medidas:
   1. Visión de sistemas de control de amenazas soportadas por firewalls encriptados (tanto de aplicaciones como de bases de datos), así como también de monitoreo mediante la suscripción a sistemas de monitoreo de amenazas (SOC).
   2. Para el mes de mayo 2022 está planificada la publicación de la contratación para adquirir elementos necesarios para robustecer la seguridad de loa infraestructura tecnológica.
   3. Fortalecimiento de perfiles profesionales en DMI y los nodos de gobierno electrónico en cada entidad municipal.

4. Contexto del ataque:

1. En el año 2021, la Fiscalía de Ecuador recibió 7.000 denuncias sobre ciberdelitos (se estima que existe sub registro por falta de denuncias).
2. Los centros de monitoreo de virus/malware detectan diariamente 10.000 variaciones de infecciones del tipo ransomware.
3. El 99% de la información que captura el malware para pedir rescate no puede ser decodificada (o des-encriptada).
4. Hay casos recientes. Por ejemplo, hace dos semanas, el Gobierno de Costa Rica vio atacado su instituto geográfico. Tras una insuficiente contención, el ataque se volvió masivo a todos los sitios del Estado.
5. Hubo, por ejemplo, un ataque reciente al senado argentino.

5. Evolución de la afectación

1. El ataque fue contenido en las primeras horas de detectado, lo que previno que pueda encriptar más información.
2. Hay determinadas bases de datos que están actualmente encriptadas por el agente externo. No se ha recibido amenaza ni pedido de rescate.
3. Se está trabajando con las bases de datos de respaldo que se tenía.

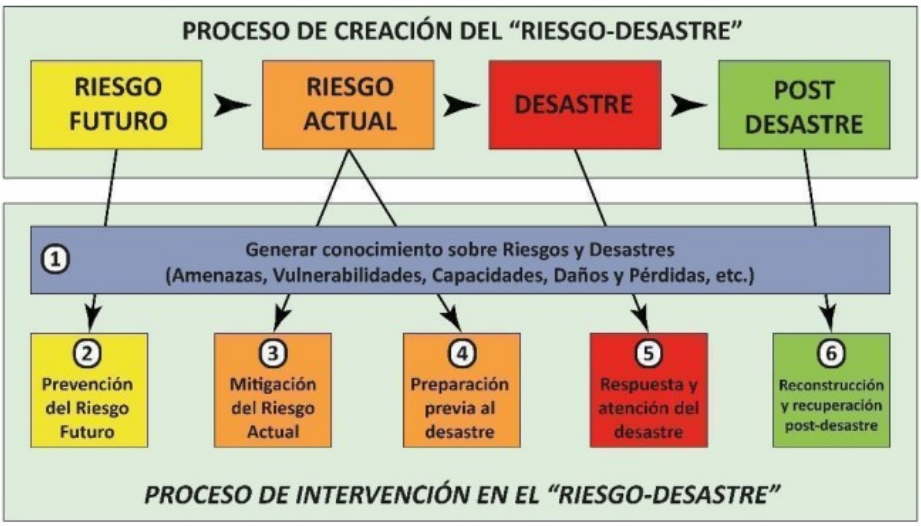
Otros aspectos sobre el suceso informático de 16 de abril

En complemento al informe presentado por la DMI, es oportuno que la Comisión de Conectividad considere, además, los siguientes aspectos que pueden ayudar a tener un panorama completo sobre el ataque informático, así como la mejor manera de prevenir futuros nuevos ataques:

1. **Enfoque** general sobre el riesgo informático
   1. Al igual que en riesgos de desastres o de enfermedades, es necesario incorporar un enfoque transversal de gestión de los riesgos informáticos a la gestión municipal, no solamente de manera reactiva sino también de manera preventiva.

2. El propio Plan Metropolitano de Desarrollo y Ordenamiento Territorial enumera actividades que forman parte del proceso de gestión de riesgos:

Ilustración 10: Procesos de creación e intervención en el Riesgo - Desastres



Fuente: Procesos de Creación y de Intervención del "Riesgo-Desastre" (Modificado de Narváez y otros, 2009)

3. En consecuencia, no es suficiente estudiar las actividades cumplidas **a partir** del evento ocurrido, sino también las actividades cumplidas antes.

2. Observaciones a las **medidas de prevención** previas
    1. El 18 de febrero de 2015 se creó la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL), con la promulgación de la Ley Orgánica de Telecomunicaciones (LOT, art. 142).
    2. ARCOTEL tiene atribución para "Establecer las regulaciones necesarias para garantizar la seguridad de las comunicaciones y la protección de datos personales" (LOT art. 144.28).
    3. Para este propósito, su estatuto de gestión por procesos ha establecido una dirección técnica de área de control de seguridad de redes de telecomunicaciones (Resolución No. 04-03-ARCOTEL-2017 sección 1.2.13.3, RO EE 13, 14 junio 2017), también denominada EcuCERT: www.ecucert.gob.ec, parte del Foro de equipos de respuesta a incidentes y seguridad (FIRST).[1]
    4. Otros Centros de Respuesta a incidentes con sede en Ecuador y afiliación al foro FIRST son (aparte de EcuCERT):
        1. CSIRT de la EPN: https://www.first.org/members/teams/csirt-epn
        2. CSIRT de la red CEDIA: https://www.first.org/members/teams/csirt-cedia
        3. Blue Hat Corp: https://www.first.org/members/teams/blue_hat_cert
        4. CSIRT de GMS: https://www.first.org/members/teams/csirt-gms
        5. CSIRT de Telconet: https://www.first.org/members/teams/csirt_telconet
        6. CERT Radical: https://www.first.org/members/teams/cert_radical
        7. CSIRT de Maint: https://www.first.org/members/teams/maintlatam_csirt
    5. En febrero de 2022, EcuCERT ha publicado en su página web un documento denominado "Ciber consejos Protégete del Ransomware", donde sugiere como medidas de protección:
        1. En caso de ser víctima de ransomware, lo más importante es NO PAGAR el rescate.

1 EcuCERT es una de las 605 integrantes de FIRST: https://www.first.org/members/teams/ecucert

2. Realizar periódicamente copias de respaldo de información crítica.
3. No abrir, manipular o interactuar con correos altamente sospechosos o mensajes en redes sociales.
4. Implementar técnicas de navegación segura en toda institución, como por ejemplo: visita únicamente sitios con certificados SSL y de origen seguro.
5. Mantener actualizados y bajo licencia todos y cada uno de los sistemas y subsistemas de software y hardware de toda la infraestructura incluido a nivel de *firmware*[2] de todos los componentes.
6. Capacitar a todos los usuarios mediante concientización y simulaciones para reconocer e informar intentos de *phishing*[3] e ingeniería social.

3. Observaciones sobre la contención **durante** el incidente
    1. La documentación presentada por DMI ante el Concejo Metropolitano en sesión 216 incluye la denuncia 170101822043050 presentada el lunes 18 de abril ante la Fiscalía General del Estado.
    2. De acuerdo al informe presentado por DMI en la sesión de la comisión de conectividad, se desprende que el Municipio ha reportado oportunamente este incidente ante el EcuCERT de ARCOTEL.
    3. Sin embargo, cuando ocurre un incidente informático, no solo interviene la DMI en cuanto a contención del incidente, sino también el resto de entidades municipales de cara al usuario (brindar información y atención) y de cara al trabajo mismo frente a las computadoras y sistemas municipales. Probablemente hizo falta más preparación para los servidores públicos municipales, pues se han reportado que algunas entidades o administraciones zonales han negado atención en servicios que ya están habilitados.
4. Observaciones sobre la gestión **post** incidente:
    1. La descripción del virus BlackCat realizada por la DMI es consistente con la información que sobre este virus se ha encontrado en portales especializados:
        1. La empresa especializada Varonis encontró este virus a fines de 2021. Debido a que atrae a atacantes en ruso, existe la teoría de que ALPHV pueda ser el sucesor de grupos de hackeo ruso como BlackMatter o REvil, que teóricamente habían sido desmantelados por autoridades rusas en 2020: https://www.varonis.com/blog/blackcat-ransomware
        2. BlackCat también se llama ALPHV. Surgió en noviembre 2021 y funciona como *Ransomware as a software* (es decir, aplica el ataque a una presa previamente seleccionada por quien usa el programa). En foros de la dark web (Ransomware Anonymous Market Place, RAMP), los "operadores" del ransomware atraen a atacantes "free lance" ofreciéndoles entre el 80% a 90% del rescate que logre cobrarse: https://unit42.paloaltonetworks.com/blackcat-ransomware/
        3. Otros nombres: ALPHV-ng o Noberus. Permite hacer una triple extorsión al robar datos y encriptarlos:
            1. Primero reclama un pago a cambio de no encriptar la data.
            2. Luego pide rescate para no liberar la información al público.
            3. Y después pide rescate mediante bloquear acceso a las páginas.

---

2 Firmware o soporte lógico inalterable es un programa informático que controla a nivel más básico un aparato electrónico. En computadoras, su firmware es el programa BIOS, que administra el hardware. En electrodomésticos antiguos de línea blanca y de línea café, el firmware es la totalidad del software.

3 Phishing es una práctica para engañar a usuarios haciéndose pasar por otra entidad, para hacerse entregar información personal o hacer click en enlaces no seguros.

4. BlackCat fue usado para atacar dos empresas alemanas de hidrocarburos, afectando cientos de estaciones de servicio en el norte de Alemania a inicios de 2022: https://www.securezoo.com/2022/02/blackcat-a-new-ransomware-as-a-service-threat/
5. Este ransomware es manejado completamente desde la línea de comandos, operado humanamente y extremadamente programable: https://heimdalsecurity.com/blog/alphv-blackcat-a-new-ransomware/
6. ¿Cuánto puede representar un rescate? En diciembre 2021 se conoció que la entidad financiera CNA pagó $40 millones por rescatar su información de BlackCat: https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/
7. En diciembre 2021, la entidad especializada S2W publicó en Medium una explicación detallada sobre las similitudes y diferencias entre BlackCat y su antecesora BlackMatter: https://medium.com/s2wblog/blackcat-new-rust-based-ransomware-borrowing-blackmatters-configuration-31c8d330a809

2. El Plan progresivo y priorizado de restauración de servicios presentado por la DMI prevé tres semanas hasta la recuperación de todos los servicios.
3. Una vez gestionado el actual incidente, se debería estudiar la adopción de alguna de las siguientes normas sobre seguridad de la información:
   1. El INEN aprobó con el carácter de Voluntario su Norma Técnica Ecuatoriana INEN-ISO/IEC 27000.
   2. En caso de que el Municipio no se haya inscrito en la Red Nacional de Confianza de EcuCERT, debiera explorar la posibilidad de inscribirse: https://www.ecucert.gob.ec/proceso-registro-de-centros/
   3. Mediante Acuerdo Ministerial 025-2019, se emitió el Esquema gubernamental de seguridad de la información (EGSI), el cual es de implementación obligatoria en las instituciones de la Función Ejecutiva (RO EE N.º 128 de 10 de enero de 2020). El Municipio podría rescatar de esta normativa las mejores prácticas para gestionar el próximo incidente.
4. Los nodos de gobierno electrónico en cada entidad municipal debieran desarrollar mecanismos para enseñar al personal municipal sobre cómo identificar amenazas, disminuir riesgos y reportar incidentes.
5. Para aportar a la investigación de Fiscalía, toda reparación o adecuación debiera precaver conservar elementos probatorios sobre el incidente ocurrido.

Sobre la relación entre el tipo de licencias del software utilizado y el nivel de riesgo

En los distintos análisis sobre el incidente, se ha abordado la calidad de las licencias del software que utiliza el Municipio, por lo que conviene analizar este aspecto.

El Municipio de Quito fue la entidad pionera en regular el uso de software de código abierto en el sector púbico en Ecuador, con su Ordenanza Metropolitana 169 de 2005.

Le siguió la Función Ejecutiva, que abordó este asunto en el Decreto 1014 de 2008.

Posteriormente, en 2016, se aprobó el Código Ingenios, que dispone el uso de software libre en todas las instituciones del sector público en Ecuador.

Como expuso la DMI, actualmente se ha superado la aparente separación entre licencias privativas y licencias abiertas en el uso de programas. De hecho, Microsoft utiliza el lenguaje de programación Phyton (que es de código abierto) para desarrollar las herramientas de inteligencia artificial que detectan virus en sus programas: https://www.securezoo.com/2022/02/blackcat-a-new-ransomware-as-a-service-threat/

Microsoft es un actor importante en el ecosistema del software de código abierto, especialmente a partir de 2018, cuando adquirió GitHub, que es un portal donde se alojan muchos proyectos de software de código abierto: https://news.microsoft.com/announcement/microsoft-acquires-github/

Los principales cambios en materia de propiedad intelectual en el sector público se establecieron en 2016 mediante el Código Ingenios[4]:

1. Art. 33: El Municipio y sus empresas públicas pueden ser entidades receptoras para formación dual y formación técnica.
2. Art. 40: Obligación de municipios de ofrecer internet inalámbrico gratuito en espacios públicos de concurrencia masiva.
3. Art. 60: El Municipio puede postular a fondos concursables para financiar investigaciones.
4. Art. 114: Los establecimientos educativos tienen derecho de uso no comercial de las creaciones de su alumnado o magisterio, para fines académicos.
5. Art. 116: Regulación de la titularidad de derechos de autor en el sector público:
    1. Toda obra creada por servidores públicos en el desempeño de su trabajo pertenece a la entidad pública.
    2. En contratación pública: la entidad contratante es titular de los derechos patrimoniales de las consultorías bienes o servicios que hubiere contratado, mientras los derechos morales son del autor.
    3. La información y contenido de bases de datos financiadas con fondos públicos son de acceso abierto.
6. Art. 144: Las instituciones educativas deben enseñar las distintas licencias de software, de modo que el conocimiento no se agote en meramente usar tecnología, sino también comprenderla o si es posible, crearla.
7. Art. 145: Las instituciones públicas deben evaluar la factibilidad de migrar a tecnologías digitales libres, considerando cuatro criterios.
8. Art. 146: Las instituciones públicas deben alojar sus datos con proveedores que garanticen estándares internacionales de seguridad y protección. En particular, sobre determinados tipos de datos:
    1. Datos de seguridad nacional y sectores estratégicos sólo se alojan en Ecuador.
    2. Datos *"de relevancia para el Estado"* pueden estar, o en el país o en países con normas de protección de datos iguales o más exigentes que la norma ecuatoriana.
    3. Otros datos pueden estar indistintamente en o fuera del país.
9. Art. 147: Todos los programas informáticos del sector público cuya licencia puede compartirse están disponibles para cualquier otra entidad (o persona) en el repositorio de software público: https://minka.gob.ec/users/sign_in En esta página, cualquier entidad

4 Formalmente: Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, Registro Oficial Suplemento N° 899. 9 de diciembre de 2016.

puede acceder al código fuente de programas como Quipux u otros, para utilizarlos libremente.

10. Art. 148: Normas para contratación pública de software:
    1. Contratar software en el sector público requiere seguir un orden de prelación que considera la producción nacional y el tipo de licencia.
    2. El Ministerio de Telecomunicaciones autoriza la adquisición tras un pedido de cada entidad contratante.
    3. Para renovar software ya en uso, basta solamente solicitar autorización al Ministerio, quien responde en un plazo de 30 días.
    4. Tras la adquisición de tecnologías no libres, la entidad contratante debe presentar al Ministerio un plan de factibilidad de migración a tecnologías libres.
    5. Es factible una migración que requiera un plazo de hasta 5 años.
    6. El reglamento determina con qué periodicidad volver a evaluar la factibilidad de migración de un determinado programa o necesidad.
11. Art. 232-236: Derechos reservados en materia de radiodifusión (aplica a las radios municipales).
12. Art. 573: Formas y excepciones a las autorizaciones necesarias para espectáculos públicos de difusión de obras artísticas.
13. Art. 610: En contratación pública, se otorga puntaje adicional a oferentes que participen en programas de: formación dual, pasantías o contratación de becarios por al menos un año.
14. Art. 612: Al contratar eventos artísticos, se debe privilegiar la producción nacional.
15. Art. 620: Normas sobre asignación no reembolsable de capital **semilla**. Si el proyecto financiado resulta en ganancias económicas, la entidad estatal que aporta el capital semilla participa entre 5% y 10% de la titularidad y beneficios económicos del emprendimiento.
16. Art. 621: Normas sobre asignación no reembolsable de capital **de riesgo**.
17. Art. 627: Los emprendimientos incubados en espacios acreditados por el Estado acceden a puntaje adicional en compras públicas.[5]
18. Disposición General 21ª: Si ocurre obsolescencia programada en bienes adquiridos por la entidad contratante, el proveedor quedará impedido de contratar con el Estado de manera permanente.
19. Disposición General 24ª: Entidades públicas están obligadas a reciclar sus residuos electrónicos y destinar los ingresos que ello genere a financiar proyectos de investigación.
20. Disposición General 26ª: La página web de toda entidad pública debe informar el tratamiento que da a los datos personales y tener un botón para poder solicitar correcciones o supresiones.
21. Disposición General 31ª: Principios que rigen los procesos para acceder a beneficios o incentivos para la investigación.
22. Disposición Transitoria 13ª: Cada entidad pública tiene un plazo para elaborar un plan de migración a software libre (en 180 días) y ejecutarlo (en 5 años).

Por motivos de espacio, este informe abarca únicamente los tres asuntos subrayados.

El plazo de 180 días para elaborar el plan de migración a software libre venció en julio de 2017. En 2019 se llevó a cabo una migración en el programa encargado de gestión documental, pasando del anterior sistema GDOC al actual SITRA, que es un programa

5 Actualmente son 20 las incubadoras reconocidas por el Estado, incluyendo a Conquito: http://www.bancodeideas.gob.ec/incubadora/index

de software libre basado en el programa QUIPUX (su código fuente está disponible en www.minka.gob.ec).

Los portales de la Secretaría General de Coordinación Territorial y Participación Ciudadana: decide.quito.gob.ec y zonales.quito.gob.ec funcionan en código abierto.

Tal vez el mejor indicador de un plan de migración a software libre no sea el número de herramientas migradas, sino el número de servidores públicos que están utilizando las herramientas libres migradas.

El plan de restauración de servicios enumera 32 programas informáticos de uso municipal (SIGEN, SIPARI, SKELTA, etc.), pero no todos estos sistemas son utilizados con la misma frecuencia o por la misma cantidad de personal que el sistema de gesitón documental SITRA.

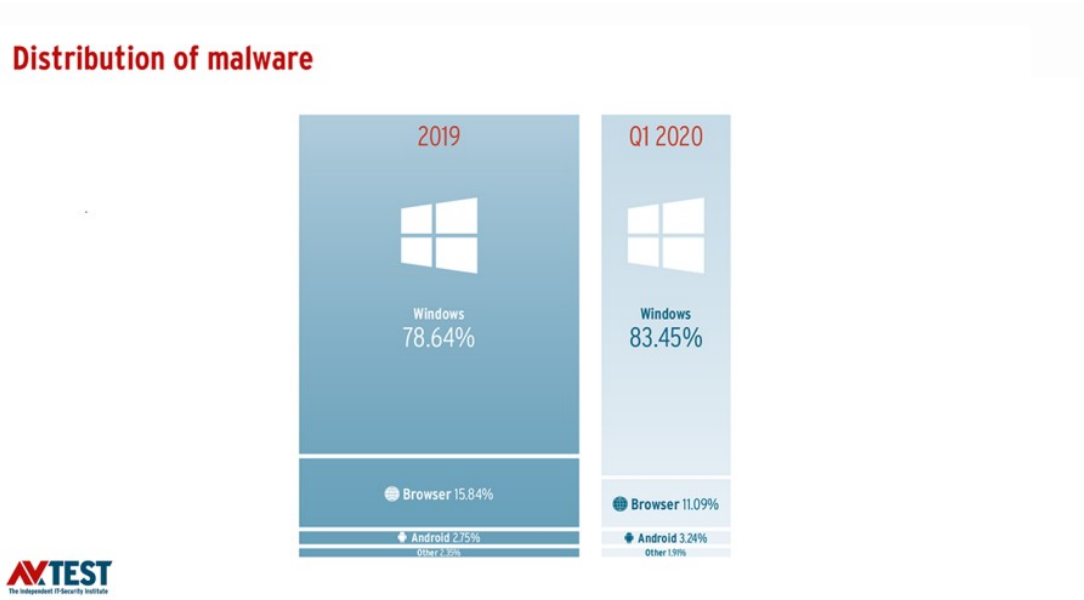
En cualquier caso, la seguridad informática depende de varios factores: el tipo de licenciamiento es uno, pero otros factores incluyen: el nivel de conocimiento o capacidades de los usuarios, la calidad o vigencia tecnológica del hardware que se utilice y la existencia o no de soporte técnico disponible. Bajo esta premisa, para incrementar la seguridad informática puede ser más crítico capacitar a los usuarios, tener contratado soporte técnico externo para aspectos de seguridad informática que no puedan gestionarse al interior del Municipio y observar periódicamente el funcionamiento del hardware.

El portal especializado SecureBlitz enumera como aspectos que brindan seguridad informática a: la educación del usuario, firewalls seguros para evitar tráfico negativo, alto sentido de vigilancia, actualización frecuente de programas, un antivirus confiable, entre otras: https://secureblitz.com/most-secure-operating-systems/

En cuanto a la relación entre el tipo de licencia (tipo de sistema operativo) y el nivel de riesgo de verse afectado por ataques informáticos, se ha encontrado lo siguiente:

1. Hasta 2011, el sistema operativo Mac OS se consideraba inmune a virus, pero desde entonces se han creado virus multi plataforma: https://news.softpedia.com/news/Security-Expert-Explains-Why-Windows-Is-the-Most-Attacked-Operating-System-445834.shtml
2. Por diseño, el sistema operativo Linux exige que el usuario expresamente autorice actualizar o ejecutar archivos, mientras que Windows permite actualizaciones “sin el consentimiento” del usuario. Este es otro factor que incide en la menor exposición a virus: https://www.malwarefox.com/windows-virus-attacks/ BlackCat enciende Windows Restart Manager para apagar la computadora mientras está encriptando los datos que pretende secuestrar. Una actividad equivalente no es posible en Linux (o en Mac OS).[6]
3. El portal especializado IGTIC describía que 61% de las campañas de ataque informático registradas entre julio a noviembre 2019 apuntan al sistema operativo Windows. El autor atribuye esta frecuencia a que existe más usuarios de Windows. Otros sistemas operativos afectados han sido: Chrome OS (22%), macOS (10,5%) y Linux (0,3%): https://itigic.com/the-most-and-least-attacked-operating-systems/oo
4. Esta tendencia se mantuvo en 2020 según PC Magazine. En el primer cuatrimestre, 83% del malware que circuló apuntaba a atacar a Windows: https://www.pcmag.com/news/windows-computers-account-for-83-of-all-malware-attacks-in-q1-2020

6 https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/



5. La lista oficial de vulnerabilidades que lleva el gobierno de EE.UU. Puede consultarse en: https://nvd.nist.gov/vuln , donde se describe cada vulnerabilidad, qué hace y cómo enfrentarla. A su vez, la comunidad de expertos informáticos lleva su lista de debilidades en: https://cwe.mitre.org/index.html
6. Mientras por un lado hay un número de amenazas, por otro lado, también debe considerarse el número de personas especialistas que pueden enfrentar la amenaza o corregir la vulnerabilidad. En los programas de código cerrado (código propietario), por su definición, sólo pueden corregir las vulnerabilidades quienes trabajan en/con la empresa fabricante, pues solo ellos conocen el código fuente. En cambio, en programas de código abierto, cualquier persona con conocimiento suficiente, puede involucrarse en ayudar a corregir. Probablemente esto explica que las vulnerabilidades en programas abiertos como Debian demoran menos en ser corregidas que aquellas encontradas en programas de código propietario: https://thebestvpn.com/vulnerability-alerts/

En definitiva, actualmente todo sistema operativo es, más o menos, susceptible de un ataque. Al momento de seleccionar un sistema operativo, conviene entonces analizar otros criterios también:

1. Se usa código abierto para ganar credibilidad o confianza de parte de terceros. Así, por ejemplo, al anunciar la compra de Twitter esta semana, Elon Musk ha anunciado que dicha red social usará algoritmos de código abierto “para incrementar la confianza”: https://twitter.com/elonmusk/status/1518677066325053441
2. Se usa código abierto para permitir a terceros trabajar en un mismo proyecto. Por ejemplo, en 2015 se creó OpenAI para desarrollar inteligencia artificial de manera abierta: https://money.cnn.com/2015/12/12/technology/openai-elon-musk/

Independientemente de qué sistema operativo se utilice, los expertos[7] recomiendan medidas de prevención como:

1. Se debe dejar de usar HTTP. Se debe usar HTTPS que es más seguro.
2. Por tanto, el Municipio deberá adquirir certificaciones de HTTPS o usar certificaciones gratuitas como Let’s Encrypt.

7 https://autonomia.digital/2022/02/11/fundamental-security-recommendations-for-critical-infrastructure.html

3. Muchas veces las páginas web tienen incrustadas en su interior imágenes o líneas de código de JavaScript. Ambos debieran ser enviados mediante una conexión segura. Muchas páginas web omiten este detalle.
4. Uno de los principales problemas de seguridad informática es la autenticación de los usuarios:
    1. Para mitigar este riesgo, es indispensable enseñar (educar) a los usuarios a usar contraseñas seguras. Preferiblemente, se nos debiera enseñar a utilizar gestores de contraseñas (pasword managers).
    2. Se debería programar un límite de intentos de autenticación. Una persona puede hacer varios intentos de ingresar con una contraseña equivocada, pero una computadora puede hacer cientos de intentos por minuto.
    3. Se debería establecer autenticación “de doble factor” para ingreso a plataformas delicadas. Algunas páginas envían un SMS al teléfono o un código al email, como factor de autenticación adicional al ingreso de una contraseña. Otras páginas generan una contraseña “de un solo uso”, lo que además reduce el riesgo de que usuarios “se presten” entre sí su clave.
5. Cada servidor debiera tener un espacio de memoria separado para llevar registro de las acciones realizadas (*logging*). Es importante asegurar que el logging sea confiable y registre toda instrucción que reciba el servidor. El dispositivo de logging debiera estar en una red separada y con suficientes seguridades.
6. Segmentar y autorizar la red: Quien diseñe o administre las redes debiera poder programar qué actividades o tareas se pueden autorizar sólo si el usuario está físicamente en instalaciones municipales, qué actividades podrían realizarse remotamente o cuáles actividades estén disponibles para cualquier ubicación (en el caso de servicios utilizados por la ciudadanía). Un ejemplo de esto es la actual implementación de SITRA, que es accesible solo desde la red municipal.
7. Se debe mantener actualizados los programas. Frecuentemente surgen ataques y las actualizaciones sirven para enfrentar tales ataques. Quien no actualiza el software queda a merced de virus o riesgos que seguramente ya tienen solución. En definitiva, no actualizar software equivale a no querer vacunarse habiendo como. Utilizar software “pirata” o “crackeado” es un riesgo en toda institución.
8. Se requiere respaldo de las autoridades. Muchas veces la seguridad informática no se nota cuando funciona, sino que se vuelve importante cuando falla. Es necesario que las autoridades tengan entre sus prioridades la seguridad informática, y esto se refleja en el acceso o no a recursos para este ámbito.
9. Es necesario ser transparente sobre lo ocurrido. No es buena idea ocultar información o minimizar su impacto: la credibilidad de la institución puede afectarse peor. Además, al informar con transparencia, se puede lograr que terceros puedan aportar soluciones.

Conclusiones y recomendaciones

Conclusiones

1. En términos generales, la Dirección Metropolitana de Informática ha llevado bien la gestión del incidente hasta el momento. Sin embargo, debe considerarse que esta Secretaría no emite un criterio técnico informático.

2. En términos generales, el resto de servidores municipales requerimos preparación tanto en el plan de contingencia como para evitar nuevos ataques.

3. El Municipio de Quito fue la institución pionear en el país en regular el uso de software de código abierto en el país, por parte de instituciones públicas.
4. La transición de GDOC a SITRA es un ejemplo de migración a software libre.

Recomendaciones

1. La Dirección Metropolitana de Informática debiera considerar algunas de las recomendaciones para incrementar las seguridades de los sistemas informáticos.
2. Aquellos aspectos de seguridad informática que no puedan ser abordados internamente, requieren soporte profesional o garantía técnica de los proveedores. Es necesario considerar estas actividades en la planificación de la DMI.
3. Cada servidor público municipal debería conocer más sobre cómo cuidar sus contraseñas, como verificar que una página es auténtica o segura (https), cómo reportar correos o información sospechosa, entre otras tareas. Una institución está tan ciber segura como el menos preparado de sus integrantes.
4. El Municipio podría aprovechar otras de las normas del Código Ingenios para cumplir sus actividades o introducir nuevas actividades, como ser entidad receptora de becarios, estudiantes de formación dual u otras modalidades de aprendizaje.

Aprobación del documento

Nombre	Dependencia	Fecha de aprobación	Firma

Elaborado por:

Firmado electrónicamente por:
SANTIAGO DAVID OCHOA BELTRAN

David Ochoa
SDPC Legal

Anexos

Código anexo	Fecha vigencia	Descripción del anexo
1	2022-04-27	ARCOTEL: Ciberconsejos protégete del ransomware
2	2022-04-27	Catálogo y priorización de programas
3	2022-04-27	Acuerdo ministerial MINTEL 025-2019 Esquema gubernamental de seguridad de la información EGSI para la Función Ejecutiva
4	2022-04-27	Norma técnica ecuatoriana NTE INEN-ISO/IEC 27000: Sistemas de gestión de seguridad de la información