Política Modelo
Política de rendición de cuentas de ciberseguridad

G20 Global Smart Cities Alliance

Esta política se considera fundamental para los principios de **seguridad y resiliencia** de la guía de políticas de la Alianza Global de Ciudades Inteligentes del G20**.** Puede encontrar contenido complementario en nuestro sitio web[1] para encontrar apoyo práctico para la adopción y aplicación de esta política.

Prólogo

Las ciudades se enfrentan a crecientes amenazas por ataques cibernéticos. En 2016, una cuarta parte de las ciudades en los EE.UU. enfrentaron cada hora intentos de ataques de seguridad cibernética[2]. Tres años después, los gobiernos reportaron 163 ataques exitosos de *ransomware* con más de US$1.8 millones en rescates pagados y decenas de millones de dólares gastados en costos de recuperación, un aumento de casi 150 por ciento en ataques reportados desde 2018[3].

[1] Visite https://globalsmartcitiesalliance.org/

[2] Deloitte, Lograr que las Ciudades Inteligentes sean Ciberseguras.

[3] ¿Deberían las ciudades hoy pagar a los cibercriminales?

Las tecnologías utilizadas en la creación de ciudades inteligentes plantean tanto beneficios sociales como riesgos únicos de seguridad cibernética. La convergencia de los Sistemas de Tecnologías de la Información (IT) con los Sistemas de Tecnología Operativa (OT) proporcionan numerosas "puertas de ingreso" para los ciberatacantes que buscan impactar la ciudad, y las distintas plataformas tecnológicas y dispositivos utilizados por las ciudades pueden crear vulnerabilidades ocultas. Esto se ve exacerbado por la falta de estándares comunes que rigen los dispositivos críticos e interconectados, lo que resulta en el uso de dispositivos de varios proveedores con diferentes protocolos de comunicación y seguridad.

El valor añadido de los servicios gubernamentales mejorados debido a la tecnología avanzada impulsa la adopción de dispositivos IoT a nivel mundial. Este crecimiento extraordinario de dispositivos interconectados aumenta exponencialmente la exposición al ciberataque, y se espera que el número de estos dispositivos en el mundo pase de 8.400 millones, en 2019, a 20.000 millones a finales de 2020[4]. Como resultado, los gobiernos enfrentan un desafío creciente para aumentar su preparación y capacidad de resistencia a la seguridad cibernética, al tiempo que reconocen que la alternativa podría dar lugar a algo más que la pérdida de datos, el impacto financiero y los riesgos de daño a la reputación. En cambio, los costos sociales podrían incluir un efecto en cascada entre los sistemas gubernamentales que provoque la interrupción total de los servicios, desde la respuesta de emergencias y el transporte, hasta las redes eléctricas, la educación y más.

Además de aumentar los servicios a los ciudadanos, las ciudades también se enfrentan a las nuevas realidades operativas de una fuerza de trabajo altamente distribuida en todo el territorio. Los enfoques tradicionales de seguridad cibernética basados en supervisión de redes en silos, no son eficaces en estos entornos altamente distribuidos donde todo se conecta con todo. El resultado de las importantes iniciativas tecnológicas que se están llevando a cabo las ciudades, es que el balance general de los ciberataques sigue creciendo y los sistemas gubernamentales son cada vez más vulnerables a éstos.

Las ciudades ofrecen una multitud de servicios que dependen de una infraestructura crítica digital dispersa y variada. Estos sistemas, a menudo denominados sistemas OT, han estado tradicionalmente en redes aisladas y contienen hardware y software sensibles, a menudo heredados, controlando la infraestructura que puede tener implicaciones físicas significativas si se interrumpen. Cada vez más, estas áreas de infraestructura crítica están abarcando

[4] Foro Económico Mundial, 2018. Nuestra exposición a los ciberataques está creciendo – necesitamos transformarnos en ciudades preparadas para enfrentar los riesgos cibernéticos (Cyber Risk Ready)

soluciones IoT, la nube y las integraciones digitales de terceros. Debido a esta combinación de factores, estos sistemas son áreas de alto riesgo.

A medida que los gobiernos se vuelven más sofisticados en su respuesta, hemos visto a varias ciudades nombrar el cargo de director de Seguridad de la Información (CISO, en inglés), o similar. Esta persona es responsable, independientemente del título, de evaluar, dirigir y supervisar el diseño y la implementación efectiva de la seguridad de la información de los servicios inteligentes, y es responsable de los errores en la seguridad. Independientemente de si una ciudad tiene un cargo CISO específico, tener un modelo robusto para la responsabilidad de la seguridad cibernética crea las bases para un cargo de seguridad cibernética mejorado y, por lo tanto, una ciudad más cibersegura.

El objetivo de esta política es definir las áreas clave para un modelo de rendición de cuentas para la seguridad cibernética que sea aplicable a todas las ciudades del mundo, protegiendo así los activos informativos y operativos de la ciudad y sus ciudadanos. Estas medidas proporcionan una estructura para que las ciudades puedan priorizar su ejecución operativa de ciberseguridad.

Se trata de una política aspiracional que pretende crear líneas de responsabilidad más claras dentro del contexto de una ciudad, a pesar de los diferentes ejemplos de estructuras de gobierno de la ciudad.

Cómo utilizar esta política modelo de rendición de cuentas (*Accountability*)

Hemos encontrado a través de investigaciones y entrevistas, que los CISO de las ciudades pueden ser responsables de los sistemas sobre los que no tienen control directo, ya que estos pueden ser adquiridos o gestionados por departamentos que no tienen las funciones centrales de IT. Creemos que la rendición de cuentas (*accountability*) se ajusta mejor dentro del dominio de una sola persona, aunque entendemos que cambiar las estructuras de gobierno dentro de las ciudades lleva tiempo, reconocemos que la rendición de cuentas de una sola persona, podría ser algo para trabajar. Esta política está escrita para la responsabilidad de una sola persona, sin embargo, un paso intermedio puede ser tener un modelo de *accountability* compartido entre un equipo central de TI / la oficina de CISO y los departamentos de operaciones.

Las ciudades tienen flexibilidad para implementar este modelo de rendición de cuentas de diferentes maneras, y la rendición de cuentas podría estar en poder de varios altos funcionarios, siempre y cuando todas las responsabilidades estén cubiertas y las ciudades puedan mostrar quién tiene la responsabilidad en última instancia de cada una de estas áreas. Estos roles (si son más de uno) deben tener un nivel claramente definido de cooperación/coordinación para asegurar que todas las responsabilidades sean compartidas entre ellos y que se realicen actualizaciones regulares, incluyendo, sin limitarse a; indicadores clave de desempeño (KPIs), cronogramas asociados de la autoridad entre dominios, y una clara jerarquía de escalabilidad.

Esta política podría ser un documento de política interno o externo publicado, y/o la base para una o más descripciones de trabajo para aquellos responsables de la seguridad cibernética en la ciudad.

Contenido

Política Modelo

Definiciones

¿Qué es la ciberseguridad?

Se trata de la preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio.

El ciberespacio es un entorno complejo que resulta de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos y redes conectadas, que no existen en ninguna forma física[5].

¿Qué es la ciber-resiliencia?

La seguridad cibernética desempeña un papel fundamental en la mitigación del impacto de una interrupción cibernética al proteger la confidencialidad, integridad y disponibilidad (comúnmente abreviado como CIA por sus siglas en inglés) de los datos y la infraestructura habilitada para datos. Sin embargo, la seguridad por sí sola no es suficiente. La ciber-resiliencia va un paso más allá al garantizar que los sistemas de tecnología de la información y las comunicaciones (TICs) sigan ofreciendo servicios en caso de un incidente cibernético[6].

[5] Nota 1: Además, también pueden participar otras propiedades, como la autenticidad, la redición de cuentas, el no repudio y la fiabilidad.
Nota 2: Adaptado de la definición de seguridad de la información encontrada en ISO/IEC 27000:2009.

[6] McKinsey, 2018. Resilencia de Ciudades Inteligentes: Empoderar digitalmente a las ciudades para sobrevivir, adaptarse y prosperar.

¿Qué es la ciberseguridad y la ciber-resiliencia en el contexto de la ciudad inteligente?

Para las ciudades, la ciber-resiliencia se puede entender a través de su capacidad de preparación, respuesta y reinvención. Los esfuerzos para construir la ciber-resiliencia son críticos para sobrevivir e incluso prosperar ante los ciberataques o desastres físicos[7].

La convergencia de la infraestructura física y digital, la consecuente interoperabilidad y la interconexión entre los sistemas urbanos y los datos son un esfuerzo continuo en muchas ciudades. Los objetivos de seguridad de una ciudad inteligente (confidencialidad, integridad, disponibilidad, seguridad y resiliencia) deben basarse tanto en los objetivos de las TI tradicionales (para asegurar los datos) como en los de las Tecnologías Operacionales (OT) (para garantizar la seguridad y la resiliencia de los sistemas y procesos). Estos objetivos de seguridad combinados pueden ayudar a las ciudades a mantener un entorno operativo más seguro y resiliente[8].

La rendición de cuentas de ciberseguridad en este contexto puede incluir a una sola persona, tanto para la tecnología de la información (IT) como para la tecnología operativa (OT) o una persona para cada dominio (IT y OT) – cada ciudad puede decidir lo más apropiado para que la persona responsable tenga el control sobre tales actividades.

¿Qué es la responsabilidad y la rendición de cuentas en un contexto de ciudad inteligente?

La buena gobernanza en lo que se refiere a la seguridad cibernética en una ciudad, en donde un funcionario superior o un grupo de personas estratégicas de una ciudad son los responsables finales de cualquier infracción de la seguridad cibernética. La(s) persona(s) responsable(s) debe(n) evaluar, dirigir y monitorear el diseño e implementación de la seguridad de la información efectiva de los servicios *smart* (inteligentes), y ser responsable de responder y recuperarse de cualquier incidente cibernético.[9]

[7] Ibíd

[8] Deloitte, Lograr que las Ciudades Inteligentes sean Ciberseguras.

[9] Principios de gobernanza del COBIT 5

1. Introducción al modelo de rendición de cuentas de ciberseguridad

1. Esta política puede ser citada como la "Política de rendición de cuentas de ciberseguridad", y entrará en vigor al publicarse en el [documento oficial de la ciudad o documento interno];

2. Objetivos

1. La [ciudad] se compromete a garantizar la ciberseguridad y la resiliencia de toda la información e infraestructura física, incluyendo, pero no limitándose a la infraestructura física y en la nube, dispositivos, redes, datos, aplicaciones y usuarios.

2. El objetivo de esta política es proporcionar un modelo de rendición de cuentas para la ciberseguridad con el fin de garantizar que un funcionario de alto nivel (o varios) tenga la supervisión, rendición de cuentas, responsabilidad, autoridad y los recursos necesarios para tomar decisiones sobre la ciberseguridad y proteger a [la ciudad] de posibles daños, incluyendo, sin limitarse, temas relacionados a impactos negativos de la marca, interrupción operativa, pérdida financiera, responsabilidades legales, y la pérdida de confianza pública como resultado de ataques cibernéticos.

3. Responsabilidades críticas (esenciales)

1. Liderazgo y rendición de cuentas

a. La ciberseguridad, incluida la seguridad cibernética de las ciudades inteligentes, es la responsabilidad, se rige y se entrega a nivel del liderazgo *senior*.

b. Un funcionario de alto rango (*senior*) tiene la responsabilidad de rendición de cuentas y la autoridad para ejecutar la ciberseguridad para todas las infraestructuras de tecnología de la información (TI) y tecnología operativa (OT) (usuarios, dispositivos, redes, datos y aplicaciones).

c. El funcionario *senior* es miembro del equipo de liderazgo de alto rango o depende directamente del mismo.

d. El funcionario *senior* es responsable de informar sobre todos los asuntos relacionados con la ciberseguridad de conformidad con los indicadores de desempeño definidos por las ciudades.

e. El funcionario *senior* establece el marco general de gobernanza y la política sobre ciberseguridad, que es revisada y aprobada por el liderazgo de alto rango, por lo menos una vez al año.

f. El funcionario *senior* debe trabajar con los equipos jurídicos para garantizar que todas las políticas y directivas cumplan con las normas y leyes locales, regionales, nacionales e internacionales aplicables.

g. El funcionario *senior* tiene la autoridad final para tomar decisiones sobre los aspectos de ciberseguridad de todos los productos, servicios, adquisiciones y desarrollo de aplicaciones internas de IT/OT existentes, incluyendo cualquier inversión significativa en productos o servicios de IT/OT adquiridos por la ciudad.

h. El funcionario *senior* es responsable de garantizar que se ha hecho un inventario de la infraestructura existente, incluidos los dispositivos, usuarios, redes, datos y aplicaciones, y debe tener entendimiento sobre el inventario y el panorama actual para poder garantizar la seguridad de los activos existentes. El funcionario debe tener un nivel de comprensión del panorama de amenazas de esa infraestructura, dependencias de varios sistemas, derechos de acceso de los usuarios y quién es la persona responsable del inventario (incluyendo propietarios y administradores).

i. Para los nuevos sistemas que se adquieren, el grupo de liderazgo superior o de alto rango, o equivalente, debe tener un contrato de servicio (SLA, *Service Level Agreement*) por escrito. Cualquier programa de tecnología, que utilice recursos internos o externos, debe registrarse ante el funcionario *senior* previo de la aprobación de la financiación. Si la solicitud se encuentra dentro de las políticas usuales, entonces el funcionario senior firma y es responsable. En casos excepcionales en los que una necesidad empresarial es primordial y anula una preocupación de seguridad (p. ej COVID), los procesos de adquisición pueden quedar fuera de los procedimientos estándar. En esta circunstancia, el equipo de liderazgo *senior* puede firmarlo y los departamentos serán responsables conjuntamente.

j. El funcionario *senior* tiene la autoridad para ejecutar la informática forense y la ejecución técnica de las regulaciones de privacidad (por ejemplo, realizar evaluaciones de impacto de privacidad e implementar los principios de privacidad por diseño, dentro de los procesos de negocio y soluciones tecnológicas).

2. Seguridad de los activos de información

a. El funcionario *senior* es responsable de hacer cumplir la política pertinente que garantice el cumplimiento de las normas mínimas (incluida la adquisición de nuevas implementaciones TIC) y aprobar todas las decisiones operativas relativas a ciberseguridad, incluidas las cuestiones relativas a la gestión de los activos de información de la ciudad, para toda la infraestructura IT/OT tal como se define en la Sección 1.

3. Seguridad de los activos físicos, incluidos los sensores y otros dispositivos IoT

a. El funcionario *senior* no es directamente responsable de la seguridad física de la infraestructura TI, incluidos, entre otros, los dispositivos de recolección de datos en espacios públicos, centros de datos, oficinas, trabajadores itinerantes y dispositivos remotos, sin embargo, debe trabajar estrechamente con quien, dentro de la ciudad, tiene la responsabilidad de esto, incluyendo a terceros y propietarios de infraestructura del sector privado, para garantizar que la seguridad se mantenga de acuerdo con la política.

4. Revisión de las medidas de seguridad de la información

a. Un funcionario responsable bajo la supervisión del funcionario *senior* debe revisar anualmente los documentos relativos a la seguridad de la información (incluyendo, sin limitarse a la política de seguridad de la información) (o más frecuentemente si la ciudad determina que es necesario) teniendo en cuenta los resultados de las auditorías o siguiendo las normas internacionales de seguridad que se elaboran y/o revisan.

5. Prevención de incidentes de seguridad

a. El funcionario *senior* es responsable de poner en marcha la gobernanza, procesos, políticas, sistemas y tecnologías que se centran en la prevención de incidentes cibernéticos.

b. El funcionario *senior* es responsable de la concienciación de toda la ciudad y la capacitación para los funcionarios de la ciudad, el consejo, los empleados

y contratistas en las prácticas más importantes de ciberseguridad. La formación de los usuarios finales debe registrarse/rastrearse y, como mínimo, debe reevaluarse anualmente.

6. Respuesta a incidentes

a. La política de seguridad cibernética deberá tener un plan específico para la respuesta a incidentes, con diferentes respuestas para acciones operativas y de comunicación basadas en la gravedad del incidente con contratos SLA definidos para las partes responsables.

b. El funcionario *senior* es responsable de garantizar que se establezca un programa adecuado de recuperación ante desastres que incluya aplicaciones para la recuperación, es decir, funcionalidad de copia de seguridad en línea/fuera de línea para todos los sistemas principales, estas estrategias de copia de seguridad deben probarse, al menos una vez al año, para determinados sistemas.

c. El funcionario *senior* debe examinar todos los incidentes de seguridad y adoptar las medidas necesarias para evitar incidentes futuros que utilicen el mismo vector de ataque.

d. El funcionario *senior* informará inmediatamente al equipo de liderazgo de alto rango por escrito cuando se produzca cualquier incidente de seguridad que se considere significativo, según lo definido por la política.

e. Tras la confirmación de un incidente de ciberseguridad, el funcionario responsable debe mantener un registro del ataque cibernético y comunicarse de manera apropiada con las autoridades supervisoras y las organizaciones pertinentes.

f. El funcionario *senior* trabajará con la oficina de comunicaciones y relaciones con los medios de comunicación, y será el contacto interno y externo clave durante un incidente importante.

4. Responsabilidades importantes (adicionales)

1. Formación en seguridad de la información y gestión de riesgos

a. Un funcionario responsable, bajo la responsabilidad del funcionario *senior*, debe llevar a cabo y mantener un registro de la capacitación en seguridad de la información y gestión de riesgos [anualmente] (o con más frecuencia si la ciudad determina que es necesario).

2. Auditoría de seguridad

a. Se requiere que un funcionario responsable, bajo la supervisión del funcionario *senior*, lleve a cabo o designe a un tercero para que realice auditorías periódicas de la aplicación de las medidas de seguridad de la información, y trabaje en estrecha colaboración con otros equipos de cumplimiento en toda la ciudad.

3. Estándares de ciberseguridad para terceros

a. Un funcionario responsable, bajo la supervisión del funcionario *senior*, debe establecer una política de evaluación de riesgos y de investigación a terceros con los que se subcontraten actividades.

4. Educación para la ciudadanía en torno a temas básicos de ciberseguridad

a. Un funcionario responsable, bajo la supervisión del funcionario *senior*, tendrá como responsabilidad crear una fácil referencia a los recursos en línea, asegurando que el sitio web de la ciudad tenga información que los ciudadanos puedan encontrar y utilizar.

Agradecimientos

Lead

Yalena Coleman Datos Aplicados y Tecnología, Connected Places Catapult

Miembros del grupo de trabajo:

Abhik Choudhury Chevening Fellow, Tata Consulting

Daniel Dobrygowksi Jefe de Gobernanza y Confianza, Plataforma para la Seguridad Cibernética y la Confianza Digital, Foro Económico Mundial

Eleri Jones Jefe del Centro Nacional DE Excelencia de PETRAS para la ciberseguridad en IoT, UCL

Gökay Bekşen Asesor Principal, municipio Metropolitano de Estambul

Greg McCarthy Director de Seguridad de la Información, Ciudad de Boston

Saj Huq Director, Oficina de Londres para el Rápido Avance de la Ciberseguridad

Sandy Tung Director del programa, Greater London Authority

Xiadong Lee Fundador y CEO, Fuxi Institution

Michael Lake CEO, Leading Cities

Murray Rosenthal Analista Superior de Políticas (Seguridad), Ciudad de Toronto

Tadashi Kaji Miembro del Foro Económico Mundial, Hitachi

Thad Eidman Gerente de Operaciones, Acreto Security

Colaboradores y revisores:

Kush Sharma CISO, Ciudad de Toronto

Mirel Sehic Director de Ciberseguridad, Honeywell

Acerca de la Alianza Global de Ciudades Inteligentes del G20

Creada en junio de 2019, la Alianza Global de Ciudades Inteligentes del G20 sobre Gobernanza Tecnológica reúne a los gobiernos municipales, regionales y nacionales, a los socios del sector privado y a los residentes de las ciudades en torno a un conjunto compartido de principios para el uso responsable y ético de las tecnologías de las ciudades inteligentes. El Foro Económico Mundial, Organización Internacional para la Cooperación Público-Privada, actúa como Secretaría de la Alianza.

A través de la Alianza, expertos globales del gobierno, socios del sector privado y la sociedad civil, están recopilando y analizando políticas de todo el mundo para identificar políticas modelo necesarias para ciudades inteligentes y éticas exitosas.

Puede encontrar más políticas modelo y más detalles sobre la Alianza en:
https://globalsmartcitiesalliance.org/

Foro Económico Mundial
91–93 route de la Capite
CH-1223 Cologny/Ginebra
Suiza
Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744
info@globalsmartcitiesalliance.org
https://globalsmartcitiesalliance.org/

Portada: Imágenes de stock del