Fomento de la cultura de ciberseguridad	
Código identificativo	CBP 80/2023
Categoría	Tecnología / Servicios digitales
Órgano responsable	Organismo Autónomo Informática del Ayuntamiento de Madrid gerenciaiam@madrid.es

Fomento de la cultura de ciberseguridad

Descripción

En marzo de 2019 se ejecutó en el Ayuntamiento de Madrid un proyecto de renovación de todos los servicios de comunicaciones que llevaba aparejada la transformación innovadora de las telecomunicaciones y el modelado del puesto de trabajo corporativo. Dicho proyecto permitió que los empleados municipales pudieran desempeñar sus actividades profesionales a distancia, sin restricciones de horario y haciendo uso de cualquier dispositivo. Apenas un año después, la crisis sanitaria provocada por la pandemia de COVID-19 sometió a prueba este modelo de trabajo, imponiendo el teletrabajo de forma global para la totalidad del personal del Ayuntamiento de Madrid.

Esta adaptación y transformación del puesto de trabajo, que aceleraba e incrementaba el uso de los servicios digitales, requería acciones de formación y concienciación en materias digitales para todos los empleados municipales; dicha formación que se llevó a cabo a través de un plan de capacitación y acompañamiento en habilidades digitales. A pesar de todos estos esfuerzos, no todos los usuarios pudieron adquirir habilidades suficientes como para permitirles conocer todos los riesgos de ciberseguridad en que puede incurrir durante la prestación de sus servicios a la organización y ocasionalmente esto genera ciberincidentes que deben ser atendidos por el Centro de Ciberseguridad del Ayuntamiento de Madrid.

El fomento de la cultura de la ciberseguridad pretende reducir el número de ciberincidentes en la organización municipal provocados por prácticas desaconsejables por parte de los usuarios, ampliando los conocimientos en este ámbito. También se pretende reducir especialmente la reincidencia, para ello se define una ruta específica de concienciación para usuarios que ya se han visto envueltos en un incidente de ciberseguridad.

Esta buena práctica promueve la seguridad del entorno digital municipal y la capacitación de sus usuarios.

Fomento de la cultura de ciberseguridad

Implantación y desarrollo

Los usuarios implicados en ciberincidentes antes de la puesta en marcha del proyecto no recibían notificación alguna más allá de las propias requeridas por los equipos de resolución, en las que ocasionalmente se les indicaban las acciones que se realizaban con sus activos para el restablecimiento de los servicios, sin explicaciones adicionales detalladas sobre las posibles causas o consecuencias derivadas. En ocasiones, tan solo eran informados sobre la retirada parcial o definitiva del acceso a sus equipos corporativos o servicios digitales.

El proyecto dio comienzo en julio de 2022. La primera fase del proyecto se ha desarrollado mediante interacciones de Teams directas con los propios usuarios, indicando la existencia de la incidencia en curso, sus posibles causas, los pasos a seguir para restablecer el servicio y los tiempos previstos.

Una vez finalizada la fase de contención y respuesta, se realiza una evaluación sobre la necesidad de concienciación de los usuarios implicados en el incidente y en caso de considerarlo necesario, se les notifica mediante correo electrónico que van a ser incluidos de forma voluntaria en una futura sesión específica sobre los temas relacionados con la seguridad de la información desde el punto de vista del usuario.

Fomento de la cultura de ciberseguridad

Impacto

Debido a que el proyecto dio comienzo en julio de 2022, por extrapolación de los resultados se estimó una horquilla de proyección anual aproximada de entre 40 y 60 usuarios anuales.

Está prevista la puesta en marcha de una medida de los incidentes de ciberseguridad originados por los usuarios, y observar tendencias de crecimiento o decrecimiento, así como el nivel de reincidencia que permita valorar la eficacia de las actividades de concienciación realizadas. Esto se realiza a través de la inclusión del flujo en una herramienta de *ticketing* que permite hacer seguimiento de los indicadores clave de rendimiento (KPIs) y de otros indicadores relevantes.

Con fecha 31 de enero de 2023 se han realizado un total de 57 notificaciones a usuarios diferentes implicados en incidentes de seguridad, haciendo que las estimaciones iniciales estuvieran muy por debajo de los valores encontrados, si bien es cierto que en ese período se han incorporado mecanismos de detección que han ampliado la superficie de observación por parte de los equipos de monitorización y respuesta. La mitad de las notificaciones (34) se produjeron en el último mes del año, lo cual es coherente con la pauta esperada de comportamiento en este tipo de acciones.

Fomento de la cultura de ciberseguridad

Actores

Se requiere la participación combinada de:

- Unidades de soporte a usuarios dependientes del Organismo Autónomo Informática del Ayuntamiento de Madrid, actuando mediante las figuras de técnicos de zona y técnicos de soporte, que contactan con el usuario para recabar información sobre el ciberincidente y mantenerle informado.
- Centro de Ciberseguridad del Ayuntamiento de Madrid, que coordina la monitorización, detección y respuesta ante los incidentes, recibe de los técnicos la información que han recabado a través de los usuarios implicados y evalúan la necesidad de impartir una sesión de concienciación, definiendo los contenidos y proponiendo como participantes a los usuarios implicados.
- Escuela de Formación del Ayuntamiento de Madrid, que coordina la realización de las sesiones de concienciación en el Plan Anual de Formación a través de las peticiones que el Centro de Ciberseguridad Ayuntamiento de Madrid les hace llegar.

Fomento de la cultura de ciberseguridad

Replicabilidad

En otros organismos con competencias sobre seguridad de la información se puede replicar esta medida. Para ello se requieren los siguientes medios:

- Monitorización de la ciberseguridad: de forma que se puedan detectar las alertas de seguridad de responsabilidad de los usuarios. Otra opción es la realización de auditorías de hacking ético y técnicas similares que permitan detectar usuarios con necesidades de formación en ciberseguridad.
- Trazabilidad y seguimiento: basado en una herramienta informática.
- Sistema de formación online con seguimiento de la actividad de los usuarios y posibilidad de realización de encuestas de satisfacción.

Como condiciones necesarias se requiere del apoyo y compromiso de la dirección por la ciberseguridad, siendo la principal amenaza la resistencia al cambio de los usuarios.

Fomento de la cultura de ciberseguridad

Difusión y documentación

La fase de concienciación mediante sesiones formativas está previsto que comience en el segundo semestre del año 2023, de forma que se haya completado un ciclo de toma de datos anual casi completo, que permita elaborar material didáctico lo más orientado posible a las acciones detectadas.