INFORME DE NECESIDAD PARA LA CONTRATACIÓN DEL "SERVICIO DE DESARROLLO DE FUNCIONALIDADES PARA EL PORTAL DE CIBERSEGURIDAD DE LA DIRECCIÓN GENERAL DE TRANSFORMACIÓN DIGITAL"

Contexto organizativo y competencial

Desde la Dirección General de Transformación Digital (DGTD) se pretende prestar soporte al Comité de Seguridad de la Información (Orden de 28 de marzo de 2017, del Consejero de Hacienda y Administración Pública por la que se establece la política de seguridad de la información en la Administración Regional), mediante un sistema de información que facilite el cumplimiento de la normativa que lo regula, en concreto:

- Artículo 8 Misión
  ..
  f) *Concienciación y formación en materia de seguridad. Todo el personal al servicio de los organismos a los que es de aplicación esta Orden deberán recibir la información y formación necesaria de forma que sean conscientes de los riesgos, sus obligaciones y responsabilidades en la interacción con los sistemas de información.*"

- Artículo 11.- Comité de Seguridad de la Información
  ..
  h) Informar la aprobación de las normas de seguridad de la información.
  k) Velar por la adecuada divulgación de la normativa en materia de seguridad de los sistemas de información.

Estas funciones obligan, para ser eficientes, a disponer de canales específicos de comunicación, almacenamiento y difusión de información sobre Ciberseguridad que sea de interés y apropiada a cada persona ya sea técnico o usuario, propio o perteneciente a empresas prestadoras de servicios.

Contexto normativo en ciberseguridad

Directivas Europeas como la Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2) establece medidas que tienen por objeto alcanzar un elevado nivel común de ciberseguridad en toda la Unión con el objetivo de mejorar el funcionamiento del mercado interior, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS), Orden de 28 de marzo de 2017, del Consejero de Hacienda y Administración Pública por la que se establece la política de seguridad de la información en la Administración Regional, el REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), la Ley

Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, o la DIRECTIVA (UE) 2016/1148 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión y sus normas de transposición son ejemplos de la importancia que los poderes públicos le prestan a la protección de los activos digitales.

Contexto técnico

Los equipos de ciberseguridad deben hacer frente al creciente volumen y sofisticación de las amenazas. La falta de visibilidad de la red, el volumen de datos a analizar, la escasez de personal y la necesidad de filtrado y rápida respuesta en forma de alertas lleva consigo que para cualquier organización ya no es posible hacer este análisis de forma manual.

Los sistemas de información actuales, tienen una consideración estratégica, por lo que son activos a proteger de manera especial. El tamaño de los mismos, así como su altísima complejidad, hacen que ya no sean suficientes con las herramientas tradicionales que hasta ahora se han venido usando, sino que se requiere de herramientas y profesionales de una capacitación muy alta, para poder hacer frente a las cada vez más sofisticadas amenazas, tanto internas como externas.

La cantidad de malware en la última década ha crecido de manera sostenida año tras año, situando a los equipos de seguridad ante un escenario con cada vez mayor cantidad de herramientas maliciosas e incidentes de seguridad.

Mención aparte merece el aumento exponencial de los ataques de phishing y ransomware, técnica que secuestra los datos de la organización solicitando un rescate por desbloquearlos. Este tipo de ataques inutilizan los sistemas de información impidiendo acceder a la información que contienen. Obligando a cualquier organización afectada a trabajar manualmente, prescindiendo de sus equipos informáticos.

Sin duda los factores de mayor impacto sobre la seguridad de los sistemas de información y, sobre los que podemos actuar para prevenir ciberataques, impedir su progreso y/o limitar los daños son **las personas** técnicas que los gestionan y los usuarios propios (empleados públicos y personal contratado) que los usan.

En el contexto y para cubrir las necesidades de gestión y comunicación de información sobre ciberseguridad, facilitar contenidos de concienciación y soporte a equipos técnicos de otras áreas de la DGTD, el área de seguridad de la DGTD inicio con medios propios el desarrollo de un portal en la intranet bajo la tecnología de Sharepoint. Este portal hoy desarrolla las funciones con evidentes carencias funcionales y de soporte técnico que hacen que su eficacia se vea limitada y no cubra los objetivos descritos, sin que el conocimiento y recursos disponibles permitan mejorarla.

Con la propuesta que acompaña a este documento se pretenden finalizar los trabajos iniciados por el Área de seguridad sobre el portal de seguridad con tecnología Sharepoint (M265) y corregir las carencias existentes, alcanzando en la función de soporte técnico,

gestión documental y comunicación en materia de ciberseguridad, niveles de eficacia aceptables y perdurables.

Los abajo firmantes, conforme a lo dispuesto en el artículo 64 de la LCSP y en el apartado V. "Principios y normas de conducta internas" del Acuerdo de Consejo de Gobierno de aprobación del código de conducta en la contratación pública de la Región de Murcia, adoptado en su sesión de 5 de noviembre de 2020, publicado por Resolución de 10 de noviembre de 2020 de la Secretaria General de la Consejería de Transparencia, Participación y Administración Pública, (BORM nº 266, de 16 de noviembre de 2020), declaramos que no concurre en nosotros ningún conflicto de interés que pueda comprometer nuestra imparcialidad e independencia durante el procedimiento, y nos comprometemos a poner en conocimiento, de forma inmediata, cualquier potencial conflicto de intereses que pudiera producirse con posterioridad, ya sea durante el desarrollo del procedimiento de adjudicación o en la fase de ejecución, y así lo suscribimos en el presente documento firmado y fechado electrónicamente al margen.

EL JEFE DE SERVICIO DE PLANIFICACIÓN INFORMÁTICA CORPORATIVA
Fdo.: Manuel Frutos Mirete

CONFORME. EL SUBDIRECTOR DE INFRAESTRUCTURAS DIGITALES
Fdo.: Diego Pedro García García