ETEA de ciberseguridad

0.- Antecedentes

Para manejar la información en el funcionamiento diario de la empresa se utilizan herramientas para su tratamiento en ordenadores, teléfonos móviles, tabletas, líneas de comunicaciones, teletrabajo, wifi, vpn, etc., por lo que asumimos una serie de riesgos que de forma genérica podemos resumir en fuga de información y ataques desde el exterior.

Entendemos que lo fundamental es que nuestra actividad, nuestro negocio, nuestra prestación de servicios no se quede desprotegido o indefenso.

Es cierto que pensamos que somos irrelevantes en el mercado y, en consecuencia, nadie pensará en dirigir un ciberataque contra Aussa. (¿quién va a querer robarnos información si no es valiosa?). Sin embargo, sí podrían bloquear la información e incluso pedir un rescate.

Sin embargo, sí es posible que se produzca, por lo que debemos **elaborar un plan** que contemple el análisis de la situación actual, adquirir conocimiento de los "agujeros" que tenemos, definir qué riesgos estamos dispuestos a asumir, adoptar las medidas correctoras necesarias y establecer las medidas preventivas y buenas prácticas que debamos incluir en nuestro trabajo diario.

A continuación describimos nuestra visión, pero desde el punto de vista del negocio, no desde la visión de un profesional TIC, que entendemos debe ceñirse a darnos soluciones para proteger y dar continuidad a nuestra actividad profesional y no fallarle a los clientes.

1.- Objeto

Los tres objetivos globales a lograr son:

1.1.- Realizar un análisis y evaluación de riesgos cibernéticos que nos permita determinar qué tiene nuestra organización, estimando lo que podría pasar.

1.2.- Decidir y aplicar el tratamiento de los riesgos que permita desplegar la defensa razonada y prudente, para que "no pase nada malo" y podamos seguir operando en las mejores condiciones para nuestros clientes. Se incluye la aportación de las opiniones necesarias y suficientes para que la dirección de Aussa decida el nivel residual de riesgo que está dispuesta a asumir.

Si expresamos los objetivos desde un punto de vista de la operativa del negocio, queremos tener una empresa segura con instrucciones de trabajo e informes que nos ayuden a tener criterio *para saber decidir en qué invertir y en qué gastar* en materia de

ciberseguridad tanto en el ámbito técnico como organizativo o procedimental, para garantizar la continuidad de nuestro negocio.

También aspiramos a que la información sobre nuestro estado se actualice periódicamente, es decir, dotarnos de un método de seguimiento caracterizado por la prevención.

En consecuencia, también deseamos:

- Trabajar con una arquitectura de sistemas clara, robusta y escalable, sobre la que se nos formularán recomendaciones.

- Lograr una ciberseguridad razonada de nuestras infraestructuras TIC materiales e inmateriales, a un coste aceptable.

- Mantener un nivel de disponibilidad de los sistemas y aplicaciones que no afecte a nuestros servicios externos (clientes), ni a los servicios internos de explotación ni a los procesos de tratamiento de datos o informes de gestión, incluidas las obligaciones legales, incluso ante un fallo de seguridad.

1.3.- Implantar un Sistema de Gestión de Seguridad de la Información (SGSI) de acuerdo con las directrices de la norma ISO 27001 y certificarlo por 3ª parte (estratégico para nuestro mercado). No se solicita consultoría para alcanzar esta meta, pero sí orientación metodológica para lograrla.

3.- Alcance

La asistencia técnica en ciberseguridad que se solicita será aplicable, dado que debemos conocer nuestra situación actual, respecto de todos los activos materiales e inmateriales que deban incluirse en la estrategia/táctica de ciberseguridad, a los siguientes activos que detallamos a continuación y a cualquier otro que pudiera afectar:

“PCs, portátiles, teléfonos móviles, tabletas, líneas de comunicaciones (wifi, vpn, fibra estándar de internet, etc), servidores, router, switch, aplicaciones, tráfico URL, contenidos, servicios a clientes, mail, web corporativa, ecommerce, cloud, usb, etc.”

Por tanto, aplicará a todo el inventario de activos, que forma parte de nuestro ecosistema TIC.

De hecho, no solo que afecta a los activos antes descritos, sino también a:

- Fuga de datos de la empresa: tanto por su importancia interna como para los clientes, por ejemplo, por los millones de transacciones de pago que realizamos anualmente.
- Los procesos de gestión y su criticidad, con posibilidad de parada de nuestra actividad.
- Comunicaciones por múltiples dispositivos y sistemas.
- Puntos de acceso a nuestra red que no controlamos.
- Personas: quién tiene acceso a la información, quién puede utilizarla.

4.- Proceso

Las ofertas que se presenten describirán de forma detallada las herramientas de trabajo que utilizarán así como la metodología que emplearán, debiendo dar respuesta de forma clara e inequívoca a las cuestiones planteadas en los puntos siguientes:

4.0.- Confidencialidad

Modelos redactados de las autorizaciones pertinentes para acceder a nuestros Sistemas de Información (SI) y propuesta de la empresa licitadora de un riguroso documento de confidencialidad, incluyendo las garantías que nos presentarán, ya que les daremos acceso a datos personales y a secretos profesionales.

4.1.- Herramientas

Se realizará la descripción de las herramientas se propone utilizar para la ejecución del análisis y evaluar los riesgos asociados al uso de nuestros sistemas de información según metodologías reconocidas internacionalmente.

Dado en principio hay varias, listamos algunas a continuación, sin ánimo de ser exhaustivos:

- Auditorías internas: para detectar y mitigar los riesgos y debilidades de nuestro SI. Para minimizarlo hay que ser muy riguroso con la norma interna que establezca la escala de privilegios de acceso.
- Auditorías externas: por encontrarnos en internet nuestra exposición crece exponencialmente, por lo que tenemos que detectar nuestras (debilidades (vulnerabilidades) e implantar soluciones de ciberseguridad.
- Evaluación de nuestros SI mediante un test de penetración / intrusión, tanto a nivel interno como externo, sobre nuestras aplicaciones y servicios TIC para detectar posibles debilidades, corregirlas, poner defensas, valorar la repercusión, etc.
- Monitorización continuada.
- Auditorías físicas, análisis manual de los sistemas, etc.
- Mapeo global de la red de la empresa.
- Campaña de phishing.
- Otras.

Se explicitará de forma inequívoca la tecnología de apoyo.

4.2.- Metodología

Se especificará y explicará, al menos lo siguiente:

4.2.1.- El diagrama de flujo de los elementos de la gestión de la seguridad de la información detallando, a partir de un activo, el proceso que incluya: amenazas, vulnerabilidades, riesgos con su impacto y probabilidad de que ocurra, tratamiento, controles, costes derivados y riesgos a asumir (ayuda a la decisión).

4.2.2.- Las etapas que se seguirán para el análisis de riesgo, como por ejemplo: identificación de activos, su valoración, amenazas, consecuencias, medidas de seguridad, etc.

4.2.3.- Si se utilizará como referencia Magerit u otras y en qué versión.

Seguiremos el criterio de implantar inmediatamente las medidas más sencillas y de menor coste para generar mejoras rápidamente.

4.3.- Informes

Con toda la información disponible estaremos en situación de que se nos facilite un informe que incluya: lista de todas las acciones correctoras y preventivas, un cronograma de implantación, prioridades para la implantación de cada acción y el presupuesto de hard y soft que necesitaríamos.

Se incluirán los formatos, tablas y diagramas que sean manejables y permitan el control y seguimiento fácil y riguroso de los distintos riesgos y de las medidas propuestas.

También se incluirá en el informe el índice a nivel de epígrafe y subepígrafe del futuro Plan de Ciberseguridad (PCS) de Aussa, que incluirá el conjunto de políticas, reglas, métodos y tecnología para proteger nuestro SI, así como el seguimiento periódico y valoración de nuestro estado de ciberseguridad y las actuaciones de recuperación de la información ante desastres según procedimientos.

4.4.- Plan de ciberseguridad

Continuando con lo adelantado en el punto anterior descripción de los contenidos del PCS a elaborar y entregar, que nos garantice el triple objetivo de reducir los riesgos, asegurar la continuidad del negocio y salvaguardar las responsabilidades corporativas. Incluirá el procedimiento de actuación ante un fallo de seguridad.

5.- Desarrollo

5.1.- Cronograma

Mediante un cronograma se describirán todas las actividades con sus tiempos de ejecución, explicitando los recursos que requerirán de Aussa y el detalle de la implantación de las acciones y medidas necesarias.

El plazo máximo de ejecución desde la firma del contrato será de seis (6) meses.

También incluirán los CV de los técnicos asignados a las actividades en el perímetro del contrato.

6.- Presupuesto

El presupuesto máximo a ofertar es de doce mil euros (12.000 €), excluido el IVA.

7.- Valoración de la oferta de ciberseguridad

La puntuación máxima será de 100 puntos, correspondiendo 51 a la valoración económica y 49 a la valoración técnica. (esta valoración no aplica al outsourcing)

7.1.- Valoración económica

a) Se calculará la Media Aritmética de las Ofertas (MAO) que se admitan.

b) Las ofertas que se encuentren fuera del intervalo comprendido entre + 25% y – 25% de la MAO serán excluidas automáticamente. El extremo de +25% del intervalo, sí superase el presupuesto máximo de licitación, será dicho presupuesto máximo.

c) Las admitidas se clasificarán de mayor a menos importe, dando 51 puntos a la de menor importe y cinco (5) puntos a la clasificada con mayor importe.

d) Los puntos de las demás ofertas se asignarán linealmente en el intervalo anterior entre los valores indicados de 51 y 5.

7.2.- Valoración técnica

a) A las garantías objetivas descritas en la oferta para alcanzar los objetivos plasmados en el epígrafe 1 de esta ETEA, modelos de confidencialidad (4.0) y herramientas (4.1).

b) A la descripción, fiabilidad y sencillez para entender la metodología a aplicar, como se expone en el epígrafe 4.2 de esta ETEA.

c) A los modelos de entregables como informes y documentos de acuerdo con lo descrito en el epígrafe 4.3 de esta ETEA.

d) A la calidad de la descripción que se solicita en el epígrafe 4.4 de esta ETEA.

e) A la calidad y detalle de lo indicado tanto respecto al cronograma como al resto de las cuestiones planteadas en el epígrafe 5.1 de esta ETEA, se le asignan 7 puntos.

8.- Plazo de presentación de ofertas

El plazo de presentación de ofertas finalizará el 23 de julio de 2022.

Deberán dirigir sus ofertas a la siguiente dirección de correo electrónico: avelazquez@aussa.com

Anexos.

A.- Outsourcing

Partiendo de que la función de ciberseguridad tiene una faceta técnica y otra jurídica, ésta última se acumulará al Responsable de Compliance de Aussa. Sin embargo, la técnica se externalizará, formalizando una asistencia técnica, que además de asistirnos en ciberseguridad coordinará para la dirección el sistema TIC de la empresa.

En un plazo de seis meses, está previsto realizar una contratación a medio plazo y flexible, cuyo alcance incluya: arquitectura de sistemas, ciberseguridad, mantener la disponibilidad de los SI, interlocutor con la empresa que gestiona y/o mantiene el hard y el soft que utilizamos.

Como anexo a la oferta que las empresas presenten al objeto de esta ETEA, recogido en el punto 1, deben incluir una propuesta de outsourcing con validez para un año, con los siguientes condicionantes:

- Se presentará un CV del candidato que proponen. La experiencia demostrable será superior a ocho años.
- Tendrá experiencia de gestión a nivel de dirección ya que buena parte de sus interlocutores serán del Comité de Dirección.
- Redactará un informe semestral de situación y avance.
- La estimación de horas anuales necesarias es la del intervalo entre 100 y 160 horas.
- El precio máximo a ofertar de 72 €/hora, excluido el IVA.

Valoración de la externalización

Cuando se proceda a la contratación del outsourcing, se valorará el precio más bajo ofertado de entre la empresas que hayan presentado oferta y se hayan admitido, sean adjudicatarias o no del proyecto de asistencia técnica de ciberseguridad, reservándose Aussa la potestad de desestimar una propuesta si no se acepta el CV presentado para el outsourcing y de no contratar a ninguna de las presentadas.