Mutua Montañesa
Mmuy fácil

Nº EXPEDIENTE 2022-002-021

PLIEGO DE PRESCRIPCIONES TÉCNICAS QUE HA DE REGIR LA CONTRATACIÓN, POR PROCEDIMIENTO ABIERTO SIMPLIFICADO SUMARIO, DEL SERVICIO DE SUSCRIPCIÓN Y MANTENIMIENTO DE LA PLATAFORMA DE CONCIENCIACIÓN Y FORMACIÓN EN MATERIA DE CIBERSEGURIDAD PARA LOS USUARIOS DE MUTUA MONTAÑESA, MUTUA COLABORADORA CON LA SEGURIDAD SOCIAL Nº 7.

ÍNDICE

1. INTRODUCCIÓN

Nuestras personas y los usuarios de nuestra plataforma son uno de los pilares fundamentales para minimizar los ataques de ciberseguridad.

Es esencial, y así lo indica nuestro SGSI adaptado al ENS, la incorporación y adaptación de nuestros procedimientos de seguridad, y la adopción de medidas y controles relacionados con la Concienciación y formación de nuestras personas en materia de Seguridad.

Es por tanto requerida la suscripción para el acceso a la plataforma de concienciación y formación a usuarios de Mutua Montañesa, así como su mantenimiento, que nos permita obtener resultados del nivel de concienciación actual, nos permita detectar y auditar nuestros puntos débiles y reforzarlos con formación específica.

En un momento en que las TIC (Tecnologías de la Información y la Comunicación) son tan necesarias para la conectividad y operatividad de muchas empresas, según los principales estudios relacionados con la ciberseguridad (protección de activos digitales) y la seguridad de la información en general (protección de activos corporativos, independientemente de su naturaleza), más del 80% de los ciber incidentes se debe a errores humanos, intencionados o no intencionados.

El comportamiento humano es un pilar esencial de la seguridad de la información. En un momento en que la tecnología de los productos para la protección de la información corporativa ha avanzado enormemente, los ciberdelincuentes han identificado que el eslabón más débil es ahora la persona. La definición de un Programa de Concienciación en este ámbito ya no es una opción, sino es una necesidad para todas las organizaciones que quieran definir un adecuado marco de protección de la información.

Además, Mutua Montañesa está actualmente inmersa en la adaptación de sus procedimientos de seguridad y en la adopción de las medidas y controles que el Esquema Nacional de Seguridad requiere para la obtención de la certificación de cumplimiento a nivel Alto. Una de las medidas de control que dicho marco normativo regula se encuentra la 5.2.3 Concienciación [mp.per.3] que indica que:

> *"Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.*
>
> *En particular, se recordará regularmente:*
>
> *a) La normativa de seguridad relativa al buen uso de los sistemas.*
> *b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.*
> *c) El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas."*

Con el fin de llevar a cabo esta tarea de concienciación de una manera profesional y acorde a las necesidades de la organización, el departamento de Sistemas llevo a cabo un análisis de mercado de las diferentes soluciones existentes con el fin de llevar a cabo un POC durante un año con la que resulto ser la más adecuada a las necesidades de la organización. De esta manera se optó por la implantación de la plataforma de concienciación líder en el mercado y mejor posicionada en el cuadrante mágico de Gartner, KnowBe4.

Durante este año de prueba la herramienta se ha demostrado, como de gran utilidad para la organización llevando a cabo con ella tanto la divulgación de la Normativa de Seguridad y de la Política de Seguridad, así como diversas campañas de formación y envío de correos de simulación de phishing que están siendo de gran utilidad para la seguridad de la empresa. Por lo tanto, se requiere la suscripción a la actual plataforma de formación.

2. REQUERIMIENTOS

Mutua Montañesa posee una suscripción a la plataforma KMSAT del fabricante KnowBe 4 en modalidad DIAMOND para 320 usuarios nominales activos.

Se requiere el servicio por un año prorrogable por otros dos periodos adicionales de 12 meses cada uno, de una subscripción idéntica a la descrita en este apartado:

- Producto: Knowbe4 KMSAT
- Modalidad: DIAMOND
- Usuarios: 320 Nominales activos (con una variación 10%)

Esta plataforma deberá ser en modo Cloud e incluir un programa completo de formación que observe como mínimo las siguientes tareas:

- Configuración de los sistemas de seguridad y correo de Mutua Montañesa para admitir los correos de la plataforma
- Sincronización con el DA de la organización
- Creación y distribución de una campaña para la aceptación de la Normativa y Política de Seguridad de la Organización
- Creación de una campaña de phishing trimestral dirigida a la totalidad de la organización con correos de simulación de escenarios típicos de este tipo de ataques. Dichas campañas irán acompañadas de píldoras formativas para aquellos usuarios que fallen en la detección de los correos de simulación
- Creación de una campaña de formación general dirigida a todos los usuarios y de al menos una campaña especifica para usuarios de dirección y contabilidad.
- Creación de un informe anual de cumplimiento en materia de concienciación y formación de seguridad a los usuarios de la organización.

3. GESTIÓN SOPORTE

El mantenimiento de este servicio por parte del fabricante de la solución cubrirá la corrección de bugs y errores detectados de la aplicación y su integración, así como cambios requeridos por actualizaciones de versión, durante el periodo de vida del presente contrato.

3.1. RESOLUCIÓN DE INCIDENCIAS

La plataforma deberá poseer modelo de gestión de incidencias, así como los niveles de servicio propuestos para éstas según los criterios de clasificación en función de la prioridad (alta, media y baja). En esta propuesta se debe poner a disposición de Mutua Montañesa una herramienta de ticketing o seguimiento de incidencias, para la gestión del servicio de mantenimiento, y garantizar los niveles de servicio presentados por la empresa adjudicataria.

A cada petición de soporte o incidencia, se le asignará una de las prioridades abajo descritas. El Adjudicatario utilizará la prioridad especificada por Mutua Montañesa, a menos que esté en clara discordancia con la naturaleza del problema, en cuyo caso la prioridad revisada se acordará entre las partes. El procedimiento de escalado se aplicará si las partes no son capaces de acordar la prioridad adecuada.

Prioridad alta: Esta prioridad debe asignarse a una petición de soporte por una parada del servicio de gestión de colas, impidiendo la ejecución total de alguno de ellos.

Prioridad media: Esta prioridad debe asignarse a una petición de soporte por una parada de una funcionalidad del servicio de gestión de colas, pero con la posibilidad de ejecutar parcialmente la funcionalidad de alguno de ellos.

Prioridad baja: Esta prioridad debe asignarse a una petición de soporte sobre el uso y la configuración de la aplicación de gestión de colas, que en ningún caso impide la ejecución de los procesos robotizados.

Las incidencias se clasificarán según el nivel de prioridad/criticidad antes indicando, y se exigirá un servicio mínimo en cuanto a la resolución de incidencias y tiempo de respuesta, en base a la siguiente definición:

- **Tiempo de respuesta:** Tiempo transcurrido desde que se comunica la incidencia al servicio de mantenimiento propuesto, hasta que dicho servicio se pone en contacto con el usuario o cliente

- **Tiempo de resolución:** Tiempo transcurrido desde el instante que se comunica la incidencia al servicio de mantenimiento propuesto, hasta el momento en que la incidencia o el servicio se ha restablecido o solucionado.

Teniendo en cuenta esta definición, estos son los tiempos máximos exigidos para la respuesta o resolución de incidencias, teniendo en cuenta la prioridad definida:

Prioridad	Tiempo de respuesta	Tiempo de resolución
Alta	4 hora	8 horas
Media	8 horas	24 horas
Baja	16 horas	80 horas

El adjudicatario pondrá a disposición de Mutua Montañesa un soporte estándar a través de web y correo.

3.2. SLA

La empresa adjudicataria deberá cumplir con los acuerdos de nivel de servicio para los tiempos de respuesta y los tiempos de resolución de incidencias que puedan surgir durante la ejecución de este contrato. Dado que existirá un registro en el momento del alta de la incidencia, así como de la respuesta y resolución, se establecerán unos indicadores objetivo (resolución en plazo) para el cumplimiento de los tiempos de respuesta y resolución mínimos por cada prioridad.

A continuación, definimos el indicador Nivel de cumplimiento:

*Nivel de cumplimiento (%) = Nº incidencias que cumplen en plazo *100 /Nº Total incidencias*

Se entiende que una incidencia cumple en plazo cuando el tiempo de respuesta y tiempo de resolución es igual o está por debajo del tiempo máximo establecido, en el cuadro anterior.

La empresa adjudicataria se responsabilizará de alcanzar estos niveles de cumplimiento establecido en el pliego de prescripciones técnicas, con independencia de los recursos técnicos y/o personales que tenga incorporar en el servicio.

Tiempo de respuesta:

En base a la definición de "Tiempo de respuesta" facilitado en el apartado anterior, cabe indicar que se diferenciará para su cálculo por la prioridad de la incidencia. El nivel de cumplimiento mínimo admitido según la prioridad será el siguiente

Prioridad	Nivel de Cumplimiento
Alta	90%
Media	85%
Baja	80%

Tiempo de resolución:

En base a la definición de "Tiempo de resolución" facilitado en el apartado anterior, cabe indicar que se diferenciará para su cálculo por la prioridad de la incidencia. El nivel de cumplimiento mínimo admitido según la prioridad será el siguiente

Prioridad	Nivel de Cumplimiento
Alta	80%
Media	85%
Baja	90%

Con la finalidad de garantizar los acuerdos de servicio detallados por parte del adjudicatario, y según se define y establece en el presente pliego de prescripciones técnicas, Mutua Montañesa se reserva el derecho de aplicar unas penalizaciones por el incumplimiento de estos ANS. En la cláusula de penalizaciones del pliego de condiciones particulares se establecen las deducciones por incidencias o faltas cometidas que sean imputables al adjudicatario, y que se clasificarán como faltas leves y faltas graves.

4. CUMPLIMIENTO ENS

El adjudicatario deberá garantizar la seguridad, disponibilidad, confidencialidad e integridad de la información de Mutua Montañesa a la que tenga acceso en el desarrollo del proyecto mediante el cumplimiento de las siguientes normas básicas:

- Cumplir con los estándares y políticas de seguridad de Mutua Montañesa.
- Garantizar la confidencialidad, integridad y disponibilidad de la información almacenada y transmitida por su red.
- Informar a Mutua Montañesa acerca de su política de seguridad, así como de la implementación y seguimiento por parte de su organización.
- Informar por escrito a Mutua Montañesa tan pronto como se detecten riesgos reales o potenciales de seguridad en su red o en el equipamiento del cliente.
- Acceso a cualquier equipamiento de red y/o sistemas de información mediante un control de acceso lógico, garantizando la restricción a los usuarios autorizados.
- Garantizar la estricta aplicación de las normas de seguridad por parte de su personal.