INSTRUCCIÓN 3/2021

Ciberseguridad en las relaciones y comunicaciones informáticas con OMIE

19 – Octubre - 2021

INSTRUCCIÓN 3/2021

Ciberseguridad en las relaciones y comunicaciones informáticas con OMIE

1. PREÁMBULO

La seguridad en las relaciones y comunicaciones informáticas, incluso antes del COVID-19, ha sido siempre un tema clave para las empresas, especialmente aquellas como OMIE con un alto componente de utilización de medios electrónicos, por las características y debilidades que supone trabajar en un entorno sometido a la aplicación de tecnologías emergentes. Este entorno abre la puerta a ataques que pueden minar la operación y continuidad de los negocios.

Con la aparición del COVID-19, los principales ataques informáticos que se han suscitado durante la pandemia se han incrementado presentándose de formas diversas tales como correos supuestamente provenientes de fuentes conocidas y aparentemente debidamente acreditadas, mensajes con información específica y especialmente sensible, (petición o intento de ejecución de transacciones económicas), virus, malware, cibercriminalidad, spyware y un sinnúmero de amenazas existentes, todo ello con el objetivo de obtener fraudulentos efectos económicos, hacerse con información o secuestrar o corromper sistemas informáticos.

Adicionalmente, el nuevo modelo de trabajo remoto ha sido un gran desafío para las compañías, y ha incrementado significativamente los riesgos, entre ellos la vulnerabilidad de ser víctimas de ataques y fraudes cibernéticos.

A la vista de las circunstancias mencionadas, OMIE, en su calidad de operador del mercado, debe proceder a atender en todo momento esta relevante cuestión con el objetivo de configurar una estrategia que proteja activos, agentes e información que sustenten una pacifica continuidad del negocio.

De conformidad con lo anteriormente expuesto, esta Instrucción pretende responder a los riesgos de ciberseguridad existentes en las infraestructuras de los agentes y del mercado, proporcionando una guía para la gestión y solución de futuros escenarios de riesgos con el objetivo de asegurar la integridad y buen funcionamiento de los equipos informáticos de los agentes y de las plataformas del mercado, así como de las comunicaciones con los agentes, ante posibles problemas de actuaciones fraudulentas, pérdidas o interceptación de datos

2. DESARROLLO

El adecuado funcionamiento del mercado de electricidad requiere, como una de sus características esenciales, el cumplimiento por parte del operador del mercado y por parte de los agentes de medidas e instrucciones de ciberseguridad en los sistemas de información y comunicación utilizados en las comunicaciones con OMIE.

El incremento del número de ciberataques a las empresas y particulares, así como los tipos de ataques, requieren el establecimiento de medidas a todos los niveles (técnicos, organizativos, de concienciación) para evitar incidentes de ciberseguridad que alteren el funcionamiento de los procesos.

En los últimos tiempos se están observando diferentes tipos de ataques a las infraestructuras de las empresas (virus, malware, spyware, …). Destacan entre ellos aquellos que utilizan los mecanismos de correo electrónico, los cuales, a partir de información obtenida de manera fraudulenta mediante ingeniería social o interceptando correos electrónicos de cuentas comprometidas por terceros no autorizados, suplantan la identidad de los remitentes de los mensajes y solicitan la realización de acciones u operaciones inadecuadas.

Es por ello necesario mantener constante atención y seguimiento de las normas básicas de ciberseguridad, siendo un requerimiento esencial que debe ser aplicado en las infraestructuras utilizadas por los agentes para la negociación, y en las relaciones y comunicaciones informáticas entre OMIE y los agentes del mercado.

Plataformas de OMIE y comunicaciones informáticas con OMIE

OMIE tiene establecidas medidas de ciberseguridad de carácter técnico, procedimental y organizativas que garantizan el funcionamiento correcto y seguro de sus sistemas de información y de las plataformas de mercado.

El acceso a las plataformas de mercado utilizado por los agentes (www.mercado.omie.es) se realiza a través de una conexión segura, requiriendo el uso de certificados digitales personales que garantizan la identidad del usuario, impidiendo el acceso en caso de no disponer de un certificado autorizado. El certificado digital se utiliza también para la firma de las operaciones que realice el agente en el web de agentes y permite la trazabilidad de dichas operaciones. Las acciones realizadas por los agentes en su relación con el mercado deben ser exclusivamente llevadas a cabo a través de dichas plataformas y mediante el adecuado uso de los certificados personales.

Toda la información confidencial suministrada por los agentes o requerida para sus actuaciones en el mercado está accesible exclusivamente a través del web de agentes (www.mercado.omie.es) utilizando los certificados digitales emitidos por OMIE.

En caso de modificación del contenido de la información, OMIE sustituirá la información accesible a través del web, pudiendo notificar a los agentes su modificación, indicando que se vuelva a acceder al web para obtener los nuevos valores, pero nunca enviando los valores modificados vía correo electrónico.

OMIE no facilita información sensible (datos de ofertas, resultados del mercado, facturas de entrega de energía o notas de abono o cargo) por correo electrónico.

En caso que el agente reciba correos electrónicos, que puedan aparentemente haber sido enviados por OMIE, en los que se requiera la realización de acciones atípicas, no habituales, con carácter excepcional o de emergencia, el agente deberá revisar adecuadamente el mensaje y, si tiene alguna sospecha sobre su autenticidad, debe inmediatamente contactar con OMIE por los medios establecidos para confirmar la autenticidad del mismo.

Obligaciones de los agentes

Los agentes deben tomar todas las precauciones razonables y propias de una diligencia profesional adecuada para proteger su infraestructura informática y evitar el uso o acceso fraudulento o no autorizado a los datos y a las plataformas de negociación del mercado. Asimismo, deberán ponerse en contacto de inmediato con OMIE si tienen motivos para sospechar que se ha producido un acceso indebido a su infraestructura informática que haya podido comprometer a la información intercambiada con el mercado, a los equipos informáticos del agente que se comunican con el mercado, a los certificados digitales de acceso al mismo, o se han divulgado indebidamente datos confidenciales o de seguridad de los accesos a las plataformas de mercado.

En caso de duda ante una información aparentemente recibida de OMIE, el agente debe remitirse siempre a la información publicada en el web de agentes, o en caso de necesidad, proceder a confirmar la autenticidad de dicha información mediante llamada a los teléfonos de contacto de OMIE.

En lo relacionado con los certificados digitales emitidos por OMIE para el acceso de los agentes al web del mercado, el agente está obligado a su custodia y a su mantenimiento, debiendo revocar y solicitar la emisión de nuevos certificados digitales en caso de pérdida del certificado, ante la duda de que se estén realizando accesos externos no autorizados con algún certificado del agente o ante la sospecha de que hayan podido ser accedidos de manera indebida.

En lo relativo a la infraestructura de acceso y a las comunicaciones digitales con OMIE, el agente debe tener establecidos los mecanismos y los procedimientos de ciberseguridad y de vigilancia sobre el uso e intercambio de la información sensible, atendiendo a las mejoras prácticas en ciberseguridad, que garanticen que los mencionados procesos se realizan de manera segura.

Los agentes deben garantizar en todo momento que sus infraestructuras informáticas no causan ningún impacto en el correcto funcionamiento de las

plataformas del mercado, así como colaborar con OMIE para gestionar y solventar estas situaciones.

Actuación ante un incidente de ciberseguridad interna en las instalaciones de un agente

En el caso que un agente del mercado detecte algún incidente de ciberseguridad interna que pueda poner en riesgo la información intercambiada con OMIE, los equipos informáticos del agente que se comunican con el mercado, o los certificados digitales de acceso a las plataformas de negociación, aparte de los procesos internos que tenga establecidos para el tratamiento de los incidentes de ciberseguridad, el agente debe cooperar con OMIE durante todo el proceso de gestión del incidente.

En cuanto se detecte el incidente, el agente deberá notificarlo inmediatamente a OMIE mediante los medios oficiales de comunicación establecidos, según se indica en la “Información de contacto” accesible en el web de agentes, descrita en el ANEXO I.

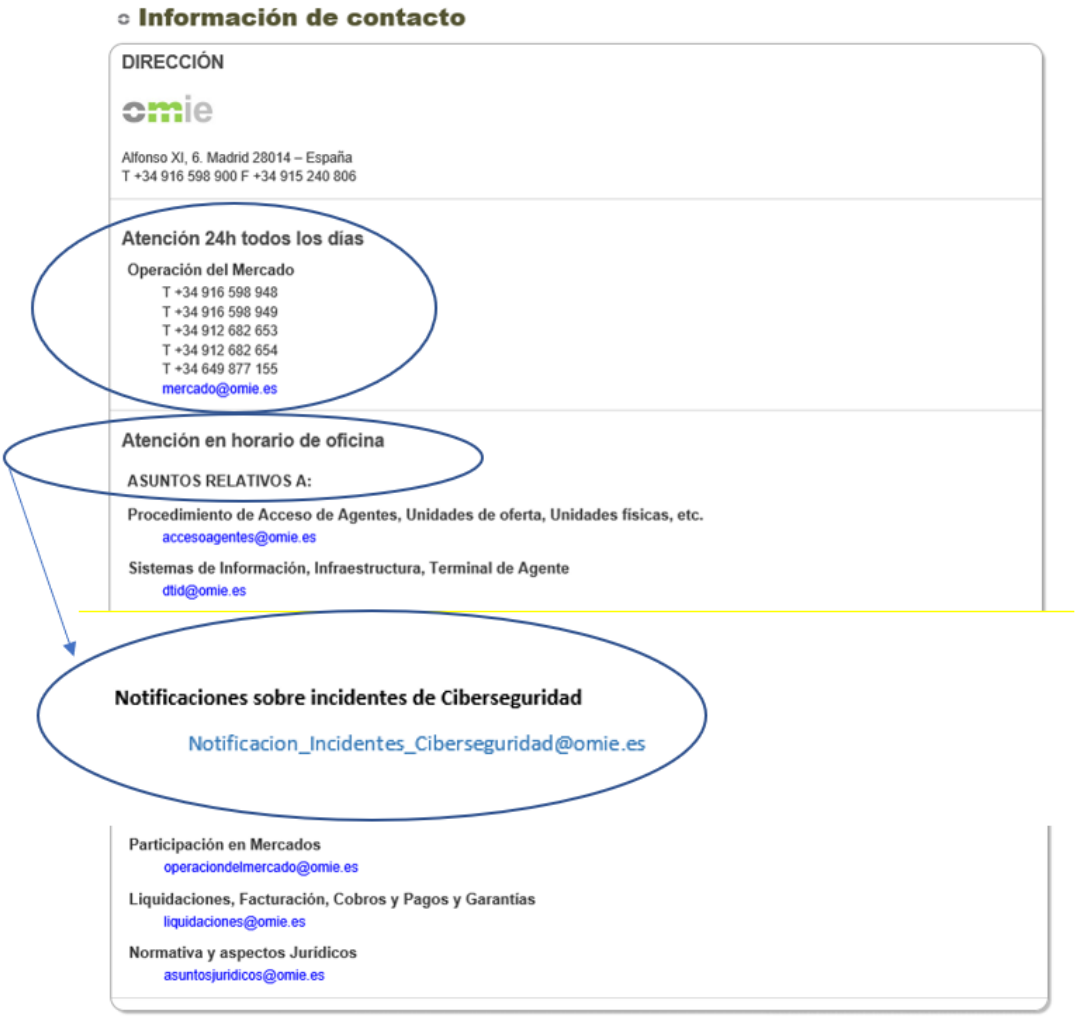
La notificación debe contener el detalle del tratamiento del incidente por parte del agente en aquellos aspectos relevantes del incidente que puedan afectar al mercado, especialmente en todo lo referente a los equipos del agente que se comunican con el mercado o en los que se almacena la información del mismo, con especial referencia a los certificados digitales de acceso.

El agente está obligado a proporcionar la información adicional relevante que le pueda ser requerida por OMIE en relación al incidente y a las posibles actuaciones en la infraestructura del agente que tenga relación con el mercado, para que, de manera coordinada, se avance en el establecimiento de las medidas necesarias hasta la completa resolución del incidente, o, al menos, se asegure completamente la ausencia de ningún riesgo para el mercado, momento en el que se deberá informar nuevamente a OMIE, proporcionando la información asociada al cierre total o parcial del incidente. El agente debe comunicar la información relevante asociada a los apartados de detección, contención y mitigación y, finalmente, recuperación del incidente.

Durante este proceso, en caso de riesgo para el mercado, OMIE podrá en cualquier momento interrumpir el acceso del agente o exigir acciones tales como la revocación de certificados, la renovación o modificación de claves de cifrado o elementos similares que utilice el agente a fin de proteger el correcto funcionamiento del mercado.

Con objeto que todo el proceso de gestión del incidente se realice de manera adecuada y la comunicación entre OMIE y el agente sea ágil y efectiva, el agente está obligado a mantener actualizados, en el web de agentes, los datos de las personas de contacto designadas por el agente para la interlocución con OMIE, accesibles según la ruta indicada en el ANEXO II

ANEXO I



ANEXO II

www.mercado.omie.es

Datos de Agentes - Datos operativos - Agentes y **Personas de contacto**