SERVICIO DE CORREDURÍA DE SEGUROS PARA LA PÓLIZA DE RIESGOS CIBERNÉTICOS DE IFEMA MADRID

EXP.: 21/113 – 2000019609

-. RESPUESTAS A CONSULTAS Y ACLARACIONES .-

CONSULTAS REALIZADAS

Les informamos de las consultas realizadas por las empresas interesadas y de las respuestas facilitadas por IFEMA, relacionadas con el expediente de referencia:

- ¿El número de datos personales de terceros almacenados en su sistema supera el millón de personas?

  Esta información se encuentra en el apartado "Protección de datos" del anexo "CONFIDENCIAL anexo situación actual".

- ¿Actualiza sus sistemas informáticos, incluidos antivirus, sistemas operativos y firewall, máximo 30 días después del lanzamiento de las actualizaciones por parte del fabricante?

  Esta información se encuentra en el apartado "Seguridad aplicable a los empleados de la compañía" y "Seguridad implementada en los sistemas de la compañía" del anexo "CONFIDENCIAL anexo situación actual".

- ¿No usa sistemas operativos SIN soporte del fabricante (por ejemplo Windows 7, Microsoft Server 2008 o Windows XP?

  Esta información se encuentra en el apartado "Seguridad implementada en los sistemas de la compañía" del anexo "CONFIDENCIAL anexo situación actual".

- ¿Realiza copias de seguridad de sus sistemas e información crítica para su negocio al menos cada siete días, dispone de dos copias, y al menos una de ellas la guarda en dispositivos externos desconectados de sus sistemas (sin conexión entre el dispositivo de copias de seguridad y su sistema), y/o bien en en alguna de las siguientes soluciones de copias de seguridad en la nube con el multifactor de autenticación habilitado (Microsoft OneDrive, Google Drive, iCloud, AWS S3 Glacier, AWS EFS Infrequent Access o Azure Recovery Services Vault).?

  Esta información se encuentra en el apartado "Protección de datos" y "Seguridad implementada en los sistemas de la compañía" del anexo "CONFIDENCIAL anexo situación actual"

- ¿Tiene activada la autenticación multifactor en todos los sistemas que sean accesible remotamente (por ejemplo GSuite, Microsoft 365, conexiones VPN, CRM, o cualquier solución en la nube?

  Esta información se encuentra en el apartado "Protección de datos" y "Seguridad implementada en los sistemas de la compañía" del anexo "CONFIDENCIAL anexo situación actual"

- ¿Disponen los usuarios con *privilegios de administrador con dos perfiles, siendo uno de ellos para aquellas tareas que no necesiten *privilegios de administrador (por ejemplo leer el correo electrónico)?

  Esta información se encuentra en el apartado "Seguridad aplicable a los empleados de la compañía" del anexo "CONFIDENCIAL anexo situación actual".

- Confirmar si su proveedor en nube ALTIA tiene calificación TIER III y/o certificado ISO 270001

  La información proporcionada por el proveedor es que el datacenter que concentra los servicios alojados de IFEMA MADRID tiene clasificación TIER III. Asimismo, está certificada en la Norma UNE-ISO/IEC 27001 por AENOR.

- Confirmar si cumplen con el Reglamento General de Protección de Datos
  Sí.

- ¿han llevado a cabo una auditoria en materia de privacidad de datos durante el último año? De ser así, han aplicado las recomendaciones de la misma?

  Esta información se encuentra en el apartado "Protección de datos" del anexo "CONFIDENCIAL anexo situación actual".

- En relación a su página web, si dispone de al menos dos proveedores de Internet, y si el hosting contratado por usted o el que usa vuestro proveedor para su sitio web está alojado en Google, Telefónica, Amazon Web Services, Microsoft Azure o Salesforce. Respecto a su proveedor de la plataforma de pagos, confirmar si cumple con la normativa PCI DSS, así como que la información de las tarjetas bancarias nunca pasa por, ni es alojada, en los servidores de Ifema.

  Sí, nuestro proveedor de hosting dispone de más de un proveedor a Internet. El hosting contratado por IFEMA MADRID para su sitio web está alojado en los propios datacenter de ALTIA, estando previsto usar también a medio plazo servicios de nube pública en Microsoft Azure, Amazon Web Services, Google Cloud y Salesforce.

  Igualmente confirmamos que el proveedor de plataforma de pagos cumple con la normativa PCI DSS. La información de las tarjetas bancarias nunca pasa por, ni es alojada en los servidores de IFEMA MADRID.

- ¿Han sido objeto de investigación o reclamaciones por parte de la Agencia de Protección de datos, interrupción no programada de sus sistemas, cyber ataque?. En su caso, por favor facilitar detalles en cuanto a fechas, causas, consecuencias, circunstancias y medidas correctoras aplicadas para evitar situaciónes similares en el futuro.

  Esta información se encuentra en el apartado "Siniestros y circunstancias" del anexo "CONFIDENCIAL anexo situación actual".

- En relación a su uso de SSH. por favor indique las opciones que usa como parte de su proceso de autenticación:
  1. Pares de claves
  2. Token de verificación de autenticación basada en tiempos
  3. Contraseña de un solo uso

  Se usa como mínimo alguna de las tres, según el caso.

- Mediante herramienta de vulnerabilidades Bitsight, se detectan múltiples vulnerabilidades por falta de actualizaciones de software.

  La red Business de IFEMA MADRID está complemente aislada, también de forma física, de la red corporativa de IFEMA MADRID. Esta red Business soporta los servicios de conectividad comercializados a clientes de IFEMA MADRID, y se rige por políticas de control de riesgos distintas a la del resto de redes internas de IFEMA MADRID (Corporativa e IoT). Consideramos que las vulnerabilidades que se mencionan se han detectado en la red Business.

- Se ha detectado mediante herramienta Bitsight malware "CrossRider" instalado en IP 195.69.254.26. Instrucciones para eliminarlo en Microsoft.com

  La red Business de IFEMA MADRID está complemente aislada, también de forma física, de la red corporativa de IFEMA MADRID. Esta red Business soporta los servicios de conectividad comercializados a clientes de IFEMA MADRID, y se rige por políticas de control de riesgos distintas a la del resto de redes internas de IFEMA MADRID (Corporativa e IoT). Consideramos que las vulnerabilidades que se mencionan se han detectado en la red Business.

- Algunos servidores de su red soportan versiones obsoletas de TLS (Transport Layer Security). ¿Se necesita este TLS antiguo por razones empresariales válidas y, si no es así, cuáles son sus planes para eliminar estas versiones antiguas?

  La red Business de IFEMA MADRID está complemente aislada, también de forma física, de la red corporativa de IFEMA MADRID. Esta red Business soporta los servicios de conectividad comercializados a clientes de IFEMA MADRID, y se rige por políticas de control de riesgos distintas a la del resto de redes internas de IFEMA MADRID (Corporativa e IoT).

  La vulnerabilidad que se menciona se ha detectado en la red Business y debe necesariamente obedecer a la existencia de un servidor temporal de alguno de los clientes usuario de esta red durante algún evento. IFEMA MADRID no tiene servidores con versiones obsoletas de TLS.

EL PRESENTE DOCUMENTO PASA A FORMAR PARTE INTEGRANTE DEL PLIEGO DE BASES, QUEDANDO AFECTOS EN LOS TÉRMINOS PREVISTOS EN EL CITADO PLIEGO.

Dirección de Compras y Logística
26 de noviembre de 2021