ISAudit - Cuestionario de Auditoría

Nivel de Confidencialidad : Restringida
Version : 202507.1
Audit Level : General

Total of Questions: 65
Report Date : 2025-07-23

El presente documento es un esfuerzo realizado por MasterBase® para informar sobre temas de seguridad específicos. Para esto se ha escogido el formato de cuestionario por ser el de mayor utilidad en auditorías desde nuestros clientes. Para una máxima claridad se define los siguientes conceptos, a los cuales se hará referencia en el cuestionario:

- Proveedor: Empresa MasterBase®.
- Cliente: La empresa que tiene contratado algún servicio brindado por MasterBase®.
- Tercero: Alguna empresa que provee servicios relacionados a MasterBase®.

Los siguientes son los tópicos involucrados:
1 : Políticas y Estándares
2 : Autenticación, autorización y acceso (personal del proveedor)
3 : Autenticación, autorización y acceso al servicio (usuarios del cliente)
4 : Confidencialidad e Integridad
5 : Detección y Respuesta de Incidentes
6 : Seguridad del Personal
7 : Concientización y Entrenamiento
8 : Firewalls y Sistemas de Detección de Intrusión
9 : Desarrollo y Mantenimiento de Sistemas
10 : Riesgo Operacional
11 : Seguridad Física
12 : Continuidad de Negocio
13 : Proveedores
14 : Cumplimiento / Leyes y Regulaciones
15 : Transporte de Medios Electrónicos
16 : Transporte documentos Valorados/Confidenciales
17 : Internet Web Hosting
18 : Gestión de Control Financiero Contable
19 : Administración de Operaciones y Comunicaciones
20 : Respecto de los servicios

Cuestionario y Respuestas

ID	Question	Answer	Comment	File
G001.001	¿El proveedor ha creado una política de seguridad de la información con una frecuencia periódica de revisión?	SI		
G002.001	¿Se eliminan o desactivan las cuentas por defecto de los fabricantes o se cambian sus contraseñas inciales en los sistemas y/o dispositivos antes de su puesta en producción?	SI		
G002.002	¿Se les obliga a los empleados del proveedor a cambiar periódicamente sus contraseñas?	SI	Para las labores críticas definidas	
G002.003	¿Existen reglas de seguridad para la construcción de las contraseñas para los sistemas y aplicaciones del proveedor?	SI	Se siguen las mejores prácticas apoyados en un administrador de contraseñas institucional	
G002.004	¿Se ha establecido un procedimiento para la administración de perfiles de acceso del proveedor ?	SI	Se siguen las mejores prácticas apoyados en un administrador de contraseñas institucional	
G002.005	¿Se requiere autenticación para los sistemas que almacenen, procesen o transporten datos del cliente?	SI		
G002.006	¿Existe un procedimiento formal y documentado para otorgar/eliminar/modificar acceso lógico a los sistemas y aplicaciones del proveedor que contienen o procesan información del cliente?	SI		
G003.001	¿El reiniciar las contraseñas de usuario está restringida a personas autorizadas y/o a una herramienta automatica?	SI	El servicio lo ofrece de manera automática	
G003.002	¿A los nuevos usuarios se les proporciona una contraseña inicial generada de manera aleatoria?	SI		
G003.003	¿A los nuevos usuarios se les fuerza el cambio de contraseña tras el primer acceso?	SI		
G003.004	¿Existen reglas de seguridad para la construcción de las contraseñas para acceder a los servicios?	SI		
G003.005	¿Existe un procedimiento de administración de usuarios en el que se garantice que el acceso se otorga de acuerdo a roles? funcionalidades y privilegios mínimos?	SI	El servicio ofrece al cliente toda la granularidad que requiere para que él haga su propia definición	
G003.006	¿Los usuarios disponen de identificadores únicos para el acceso a las aplicaciones?	SI		
G003.007	¿Existe una política de control de accesos que incluya la finalidad de la misma, alcance, distintos roles y responsabilidades y compromiso de la dirección?	SI		
G003.008	¿Se requiere el uso de contraseñas complejas (mezcla de mayúsculas, minúsculas, números y caracteres especiales) para acceder al servicio?	SI		
G004.001	¿Se proporcionan mecanismos de devolución/regresión para el servicio y los datos en caso de finalización del contrato?	N/A	Sus datos están bajo la administración del cliente	
G004.002	¿Existen acuerdos de confidencialidad firmados entre el proveedor y el cliente?	SI		
G004.003	¿Existe un procedimiento para la liberación de parches y actualizaciones para los sistemas y aplicaciones del proveedor?	SI		

ID	Question	Answer	Comment	File
G004.004	¿El proveedor encripta toda la información electrónica del cliente que transmite o transporta?. Describa la encriptación utilizada o los controles que la reemplazan si la encriptación no se usa.	SI	Protocolo HTTPS	
G004.005	¿El proveedor ha adoptado medidas que aseguren razonablemente la privacidad de la información que reciben de sus clientes y usuarios de servicios, conforme a la normatividad vigente sobre la materia?	SI	https://www.es.masterbase.com/privacidad.html	
G004.006	¿Tiene el proveedor un esquema de clasificación de la información(Restringida/Confidencial / /Interna/ Pública) u otra similar?	SI		
G004.007	¿Tiene el proveedor procedimientos para desechar, eliminar y reutilizar equipos y medios de respaldo, de manera que cualquier dispositivo o medio de almacenamiento que se dé de baja, se bote o remate no contenga información del cliente, ni tampoco la información pueda ser recuperada por terceras personas?	SI	Incluye borrado lógico y destrucción física del medio de almacenamiento	
G005.001	¿El proveedor ha establecido un procedimiento formal para la atención de incidentes de seguridad, que además considere planes de resolución conforme a la criticidad del evento/problema detectado?	SI		
G005.002	¿Dispone de una política formalizada de gestión de incidentes de seguridad (incluyendo un plan documentado de identificación, respuesta, escalado y solución) ?	SI		
G005.003	¿La documentación relativa a los incidentes y soluciones a los mismos es registrada y almacenada?	SI		
G005.004	¿Se encuentran claramente identificadas las responsabilidades respecto a revisión y monitoreo de los incidentes de seguridad?	SI		
G006.001	¿El proveedor tiene políticas, normas y/o procedimientos para la selección del personal?	SI		
G006.002	¿Se ha definido claramente los roles y responsabilidades en seguridad de la información por parte del proveedor?	SI		
G007.001	¿Personal interno del proveedor y tercerizado recibe regularmente entrenamiento apropiado del conocimiento y actualización sobre políticas de Seguridad de la Información?	SI		
G007.002	¿Se proporciona capacitación en ciberseguridad al personal? ¿Con qué periodicidad?	SI	Anualmente	
G008.001	¿Existen medidas para asegurar el nivel de servicio ante ataques de denegación de servicio DoS/DDoS?	SI	Nuestros servicios se ofrecen a través de CloudFlare	
G008.002	¿El proveedor ha protegido sus redes internas de conexiones externas a través de firewall?	SI		
G009.001	En caso que el proveedor desarrolle sistemas o aplicaciones que sean ocupados para entregar el servicio al cliente, responda ¿Existe metodología para el desarrollo, pruebas (Quality Assurance)? Ejemplo, autorización de paso a producción, etc.	SI		
G009.002		SI		

ID	Question	Answer	Comment	File
	¿Esta prohibido dentro de la organización proveedora usar una base de datos con información del cliente para ser usada en ambiente de desarrollo o pruebas?			
G009.003	¿Los desarrolladores tienen restringido el acceso al entorno de producción?	SI		
G010.001	¿El proveedor puede desarrollar investigaciones de fraudes , ya sea interno o externos, como apoyo para investigaciones por parte del cliente?	SI		
G010.002	¿El proveedor tiene controles de prevención de fraude interno y/o Externo, para evitar posibles daños económicos al cliente?	SI		
G011.001	¿El proveedor tiene procedimientos formales de control de seguridad física para sus instalaciones?	SI		
G011.002	¿El proveedor mantiene registro de los ingresos a su(s) Datacenter(s)?	SI		
G011.003	¿Las instalaciones del proveedor están protegidas por alarmas de detección de intrusos?	SI		
G011.004	¿El proveedor posee controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales?	SI		
G011.005	¿El proveedor tiene CCTV Interno / Externo con sistema de almacenamiento de imágenes en su(s) Datacenter(s)?	SI		
G011.006	¿El proveedor tiene procedimientos formales de control de seguridad física para su(s) Datacenter(s)?	SI		
G011.007	¿El proveedor mantiene controles físicos para su(s) Datacenter(s) y controles ambientales conforme a las especificaciones de los equipos (por ejemplo: valores de humedad, temperatura, eléctricas, entre otros)?	SI		
G012.001	¿Ha sufrido algún incidente de seguridad que requiriese la activación del Plan de Recuperación ante Desastres en los últimos 3 años?	NO		
G012.002	¿El Plan de Continuidad de Negocio del proveedor incluye todos los procesos principales que soportan el procesamiento del cliente?	SI		
G012.003	¿El proveedor cuenta con una política, modelo y gestión formal de continuidad de negocio implementado y actualizado?	SI		
G012.004	¿Existe un calendario anual de pruebas de Recuperación ante Desastres?	SI		
G013.001	¿El proveedor tiene controles que aseguren que los contratos con sus proveedores incluyan cláusulas de confidencialidad, Auditibilidad, de continuidad de negocio, niveles de servicio, multas y otras de cumplimiento de la industria?	N/A	No existen terceros involucrados para la prestación del servicio	
G014.001	¿La empresa cuenta con un área definida de Seguridad de la Información?	SI		
G014.002	¿El proveedor tiene organismos reguladores o de reglamentación que lo rigen en el ámbito del cumplimiento? (por ejemplo, SOX, OSFI, etc.)	SI	Certificación ISO 27001 vigente como referencia normativa principal para la gestión de seguridad de la información	

ID	Question	Answer	Comment	File
G015.001	¿El proveedor tiene un procedimiento para el Transporte de Medios Electrónicos (Cintas, CD, DVD, etc.) que contengan información del cliente?	N/A	No se transporta información del cliente	
G016.001	¿El proveedor tiene un procedimiento para el Transporte de documentos Valorados o Confidenciales del cliente?	N/A	No se transporta información del cliente	
G017.001	¿A sus aplicaciones e infraestructura de Internet WebHosting, el proveedor les realiza pruebas de calidad (Quality Assurance) antes de salir a producción?	SI		
G017.002	¿El proveedor tiene procedimientos para identificar y solucionar fallas en el ambiente de red (routers, switches, firewalls, DNS, servers, etc.)?	SI		
G017.003	¿En el servicio ofrecido, utiliza certificados emitidos por una autoridad de certificación (CA certified)? Describa su uso	SI	El servicio se ofrece con certificados HTTPS generados en CloudFlare, luego sigue hacia servidores proxy (HAProxy) y finalmente el request es pasado a servidores backend	
G019.001	¿El proveedor ha establecido la política del buen uso de los equipos, entre ellos el correo electrónico?	SI		
G019.002	¿El proveedor cuenta con sistema antivirus con administración centralizada y con las últimas firmas?	SI	Antivirus actualizado aunque se ha definido sin administración central	
G019.003	¿El proveedor tiene procedimientos documentados para el uso de plataformas específicas que tengan impacto con los servicios brindados al cliente?	SI		
G019.004	¿Los sub-contratantes del proveedor están alineados en temas de seguridad y de acuerdo a sus estándares?	SI		
G019.005	¿El proveedor de servicios administra y hace seguimiento de sus recursos informáticos?	SI		
G019.006	¿Se documenta la instalación, configuración y operación de los sistemas? (ej. manuales de instalación, manuales de usuario, etc.)	SI		
G020.001	¿Los sistemas en donde se procesan o almacenan datos del cliente son monitorizados para asegurar la disponibilidad del servicio?	SI		
G020.002	¿El servicio requiere de conexión con la infraestructura del cliente?	NO		
G020.003	¿El servicio es 24x7? ¿Cómo se realiza el mantenimiento de la plataforma, hay una programación?	SI	Nuestra plataforma fue diseñada con redundancia en sus múltiples componentes para entregar alta disponibilidad, debido a esto se realizan mantenciones y actualizaciones sin bajar el servicio, ahora bien en casos muy puntuales en que si se requiera bajarlo, se programará la interrupción y se avisará con la debida anticipación	