AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

CYBEREDGE® CUESTIONARIO ADICIONAL SOBRE RANSOMWARE

Este cuestionario adicional es aplicable a la cobertura CyberEdge®. En el presente documento, **"Solicitante"** incluye a la Compañía que solicita la cobertura CyberEdge® y a sus filiales.

Nombre completo del **Solicitante** _____

INSTRUCCIONES PARA LAS SECCIONES SIGUIENTES:

Salvo que en la pregunta se indique expresamente que debe "escribir la respuesta" o "especificar un número entero", en la columna de respuesta, la selección desplegable solo permitirá la respuesta "Sí". Si el **Solicitante** deja la respuesta en blanco, se interpretará como "No" o "No tiene ese control", salvo que haya una opción de respuesta que indique concretamente "No", "No lo sé" o "Ninguno/a de las anteriores". Después de cada sección se incluyen secciones de comentarios que permitirán al **Solicitante** proporcionar comentarios adicionales si lo desea. (Las secciones de comentarios adicionales están limitadas a 1000 caracteres. Si se necesita espacio adicional, adjunte un documento por separado como anexo).

Las preguntas que se incluyen a continuación son importantes para la suscripción del riesgo del **Solicitante**. El cuestionario debe ser completado por la persona o personas responsables de la seguridad de los sistemas de información del **Solicitante**, o con la ayuda de esta persona o personas. Si la seguridad de la información se externaliza a un tercero (p. ej., proveedor de servicios de seguridad), se entiende que el **Solicitante** ha verificado sus respuestas con dicho tercero antes de enviar este cuestionario adicional.

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

Seguridad de datos y continuidad de negocio (DS/BC)

	PREGUNTA	RESPUESTA
	Seleccione únicamente una respuesta: ¿Cuál es el grado de centralización del programa de seguridad de la información del **Solicitante**?	
DS/BC N° 1	La seguridad de la información en el **Solicitante** se gestiona a nivel central y las políticas se aplican a todas las filiales del grupo. De haber excepciones, solo es a nivel de activo (y no a nivel de filial o entidad jurídica asegurada).	☐
	La seguridad de la información en el **Solicitante** se gestiona a nivel central, pero existen excepciones para determinadas filiales o entidades jurídicas aseguradas. Los controles, tal como se describen a continuación, se aplican al 98 % o más del total de los Endpoints.	☐
	La seguridad de la información en el **Solicitante** se gestiona a nivel central, pero existen excepciones para determinadas operaciones o entidades jurídicas. Los controles, tal como se describen a continuación, se aplican a menos del 98 % del total de los Endpoints.	☐
	La seguridad de la información en el **Solicitante** está descentralizada, pero los controles, tal como se describen a continuación, se aplican al 98 % o más del total de los Endpoints.	☐
	La seguridad de la información en el **Solicitante** está descentralizada, y los controles, tal como se describen a continuación, se aplican a más del 50 % del total de los Endpoints, pero a menos del 98 % del total de los Endpoints.	☐
	La seguridad de la información se gestiona a nivel individual para cada filial o unidad operativa. Los controles que se indican a continuación se basan en una encuesta de todas las filiales y unidades operativas.	☐
	Otro (indique a la derecha y describa en la sección de comentarios al final de la sección de Seguridad de datos y continuidad de negocio).	☐
	No lo sé.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con la gestión de los activos de tecnología de la información (hardware y software) que lleva a cabo el **Solicitante:**	
	El **Solicitante** tiene un inventario de todos los activos de hardware de la empresa (incluidos los dispositivos para usuarios finales, dispositivos de red, equipos, dispositivos del Internet de las cosas y servidores) en el que se incluye la dirección de red (de ser estática), la dirección del hardware, el nombre del equipo y el propietario del activo de la empresa, y que se actualiza, como mínimo, dos veces al año.	☐
	El **Solicitante** tiene un inventario de todos los activos de hardware de la empresa (incluidos los dispositivos para usuarios finales, dispositivos de red, equipos, dispositivos del Internet de las cosas y servidores) en el que se incluye la dirección de red (de ser estática), la dirección del hardware, el nombre del equipo y el propietario del activo de la empresa, y que se actualiza, como mínimo, una vez al año.	☐
	El **Solicitante** cuenta con un proceso para detectar e identificar activos de hardware en su red y lo hace, como mínimo, una vez al día.	☐

DS/BC Nº 2	El **Solicitante** cuenta con un proceso para detectar e identificar activos de hardware en su red y lo hace, como mínimo, una vez a la semana.	☐
	El **Solicitante** cuenta con un proceso para actualizar su inventario de activos de hardware, como mínimo, una vez a la semana, basándose en herramientas de detección o software de gestión de direcciones IP (IPAM).	☐
	El **Solicitante** tiene un inventario de todo el software con licencia instalado en activos de la empresa y lo actualiza, como mínimo, dos veces al año.	☐
	El **Solicitante** cuenta con un proceso para garantizar que todo el software está respaldado o es una excepción documentada con controles de mitigación, y el proceso se repite, como mínimo, una vez al mes.	☐
	Ninguna de las anteriores.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con la gestión de "Activos vitales" que lleva a cabo el **Solicitante:** "Activos vitales" se refiere a aquellos activos que son esenciales para el éxito y el funcionamiento de la organización, y que incluyen, a título enunciativo, pero no limitativo, aplicaciones que respaldan la producción empresarial, aplicaciones que almacenan datos confidenciales y/o fundamentales para el negocio, y servicios tecnológicos centrales, como servicios de directorio, repositorios de documentos y el correo electrónico.	
DS/BC Nº 3	El **Solicitante** cuenta con un inventario de todos los almacenes de datos, en el que se incluye el propietario de los datos, el activo en el que se almacenan, el grado de confidencialidad, los límites de conservación y los requisitos de eliminación, al menos para todos los datos confidenciales, y lo actualiza, como mínimo, una vez al año.	☐
	El **Solicitante** ha definido y documentado todos los "Activos vitales".	☐
	El **Solicitante** cuenta con un proceso para identificar de forma activa los "Activos vitales" y actualizar el inventario de "Activos vitales", como mínimo, una vez al trimestre.	☐
	El **Solicitante** prioriza los "Activos vitales" en función de su importancia para las operaciones de la empresa.	☐
	Ninguna de las anteriores.	☐
	¿Cuál es el "Tiempo de Recuperación Objetivo (RTO)" para los "Activos vitales"? "RTO" se refiere al periodo de tiempo en el que se espera que la organización restaure los "Activos vitales" tras un desastre o interrupción.	
DS/BC Nº 4	< 5 horas.	☐
	5-12 horas.	☐
	12-24 horas.	☐

	1-7 días.	☐
	> 7 días.	☐
	No hay un RTO definido/No lo sé.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con las capacidades de recuperación ante desastres del **Solicitante:**	
DS/BC Nº 5	Existe un proceso para crear copias de seguridad (backups) (aunque no esté documentado y/o sea ad hoc).	☐
	La Política de recuperación ante desastres documentada del **Solicitante** requiere que se realicen copias de seguridad automatizadas una vez a la semana, o con mayor frecuencia, e incluye estándares para copias de seguridad que se basan en la importancia de la información.	☐
	Como mínimo una vez al trimestre, el **Solicitante** prueba su capacidad de restaurar distintos "Activos vitales" de acuerdo con el Tiempo de recuperación objetivo (RTO).	☐
	Ninguna de las anteriores/No lo sé.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con las capacidades de backup del **Solicitante:**	
DS/BC Nº 6	La estrategia de backup del **Solicitante** incluye backups sin conexión (archivo) almacenadas onsite.	☐
	La estrategia de backup del **Solicitante** incluye backups sin conexión (archivo) almacenadas offsite.	☐
	La estrategia de backup del **Solicitante** incluye backups periódicas onsite.	☐
	La estrategia de backup del **Solicitante** incluye backups periódicas offsite (nube o lugar de continuidad de operaciones).	☐
	Los backups del **Solicitante** están aislados y separados del dominio de producción (es decir, se accede a ellos a través de un mecanismo de autenticación externo a Active Directory, o están disponibles de otro modo, incluso cuando el dominio de producción queda comprometido), o son inmutables.	☐
	Ninguna de las anteriores/No lo sé.	☐

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	Seleccione todas las respuestas que sean ciertas: En relación con las políticas del **Solicitante** sobre el uso del cifrado para proteger los datos:	
DS/BC Nº 7	El **Solicitante** requiere que todos los datos en los dispositivos portátiles, incluidos teléfonos, tabletas y portátiles, estén cifrados (a través del cifrado de disco completo o del cifrado basado en archivos)	☐
	El **Solicitante** requiere que todos los dispositivos para usuarios finales, aunque no sean portátiles, que contengan datos confidenciales utilicen el cifrado de disco completo.	☐
	El **Solicitante** requiere que todos los dispositivos extraíbles, memorias USB, CD, etc., estén cifrados.	☐
	El **Solicitante** requiere que todos los datos confidenciales almacenados estén cifrados, ya sea en la capa de almacenamiento o en la capa de aplicación.	☐
	Ninguna de las anteriores/No lo sé.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con la monitorización de "Activos vitales" que lleva a cabo el **Solicitante:**	
DS/BC Nº 8	El **Solicitante** cuenta con una función interna y/o un proveedor de servicios de seguridad gestionado ("MSSP") externo encargados de monitorizar las alertas de eventos de seguridad, incluidas las alertas sobre "Activos vitales" (un "Security Operations Center" o "SOC").	☐
	El SOC/MSSP del **Solicitante** recibe la lista actualizada de "Activos vitales", como mínimo, una vez al trimestre.	☐
	El SOC/MSSP del **Solicitante** utiliza una solución de información de seguridad y monitorización de eventos (SIEM) para automatizar la recopilación de registros de los "Activos vitales".	☐
	Ninguna de las anteriores/No lo sé.	☐
	Si el **Solicitante** quiere añadir comentarios adicionales sobre alguna pregunta o respuesta de esta sección, debe indicarlos aquí:	

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

Seguridad en la gestión de la identidad, las credenciales y el acceso (ICA)

	PREGUNTA	RESPUESTA
	Seleccione todas las respuestas que sean ciertas: ¿Cuáles de las siguientes herramientas utiliza el **Solicitante** para servicios de directorio, proveedores de identidad (IdP), federación y/o gestión de derechos?	
ICA Nº 1	Microsoft Active Directory (Active Directory)	☐
	Azure Active Directory (Azure AD)	☐
	Okta	☐
	Ping	☐
	Active Directory Federation Services	☐
	Google Workspaces	☐
	Otro (se requiere especificar; proporcione los detalles en la siguiente fila)	☐
	En caso de que la respuesta sea “Otro”, proporcione aquí los detalles	☐
	Ninguna de las anteriores/No lo sé.	☐

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	Seleccione una respuesta: ¿Cuál es la fuente de identidad para la mayoría de los usuarios del **Solicitante?**	
ICA Nº 2	Microsoft Active Directory (Active Directory)	☐
	Azure Active Directory (Azure AD)	☐
	Active Directory y Azure AD (Active Directory es autoritativo)	☐
	Azure AD y Active Directory (Azure AD es autoritativo)	☐
	Un proveedor de identidad ("IdP", p. ej., Okta o Ping)	☐
	Colaboración basada en la nube (p. ej., Google Workspaces)	☐
	Otro (se requiere especificar; proporcione los detalles en la siguiente fila)	☐
	En caso de que la respuesta sea *"Otro"*, proporcione aquí los detalles	☐
	Sin gestión de identidad centralizada o no la conozco.	☐

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	Seleccione todas las respuestas que sean ciertas: En relación con la gestión de cuentas del **Solicitante:**	
ICA Nº 3	El **Solicitante** tiene un inventario de todas las cuentas de administrador y de usuario.	☐
	El inventario de cuentas del **Solicitante** incluye el nombre, el nombre de usuario, las fechas de inicio y fin y el departamento del individuo.	☐
	El **Solicitante** valida que todas las cuentas activas estén autorizadas, como mínimo, una vez al año.	☐
	El **Solicitante** valida que todas las cuentas activas estén autorizadas, como mínimo, una vez al trimestre.	☐
	Ninguna de las anteriores.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con las políticas y controles técnicos del **Solicitante** sobre las contraseñas:	
ICA Nº 4	El **Solicitante** forma a los usuarios sobre los riesgos de reutilizar contraseñas y dispone de una política para evitarlo.	☐
	El **Solicitante** cuenta con una solución para evitar que los usuarios puedan utilizar contraseñas comunes e identificadas como vulnerables, aunque satisfagan los requisitos de complejidad (p. ej., "1q2w3e4r5t" y "Passw0rd!").	☐
	El **Solicitante** cuenta con un gestor de contraseñas para los empleados.	☐
	El **Solicitante** ha implementado una solución para establecer contraseñas aleatorias y diferentes en todos los ordenadores vinculados al dominio para las cuentas de administrador locales (p. ej., la solución de contraseña de administrador local. Referencia: https://support.microsoft.com/en-us/topic/microsoft-security-advisory-local-administrator-password-solution-laps-now-available-may-1-2015-404369c3-ea1e-80ff-1e14-5caafb832f53).	☐
	Ninguna de las anteriores.	☐

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	Seleccione todas las respuestas que sean ciertas: En relación con las medidas de protección de las cuentas de usuario con privilegios de administrador de dominio del **Solicitante** ("Cuentas de administrador de dominio"): "Cuentas de administrador de dominio" se refiere a las cuentas de usuario (excluyendo las "Cuentas de servicio") que pueden editar información en cualquier solución que el **Solicitante** esté utilizando para servicios de directorio, proveedor de identidad (IdP), gestión de derechos, etc. En un entorno de Active Directory, esto incluiría a los Administradores de empresa, Administradores de dominio y los grupos de Administradores (de dominio), así como a cualesquiera grupos y cuentas anidados. En Azure AD, el termino incluiría a los Administradores globales, Administradores de identidad híbrida y Administradores de roles con privilegios.	
ICA Nº 5	Los administradores de sistemas del **Solicitante** tienen credenciales únicas y con privilegios para las tareas administrativas (independientes de sus credenciales de usuario para el acceso diario, el correo electrónico, etc.).	☐
	Las "Cuentas de administrador de dominio" requieren autenticación multifactor.	☐
	Las "Cuentas de administrador de dominio" se gestionan y monitorizan a través del acceso "just in time", están sujetas a limitaciones temporales y requieren de aprobaciones para proporcionar un acceso con privilegios.	☐
	Las "Cuentas de administrador de dominio" se almacenan en un vault con contraseña que requiere que el usuario "verifique" las credenciales (que cambian después).	☐
	Además de almacenarse en un vault con contraseña, las "Cuentas de administrador de dominio" no quedan expuestas al usuario administrador cuando se "verifican", y el acceso queda registrado a través de un gestor de sesión.	☐
	Las "Cuentas de administrador de dominio" solo se pueden utilizar desde workstations de acceso privilegiado (workstations que no tienen acceso a Internet o al correo electrónico).	☐
	Existe un registro de todas las acciones realizadas desde las "Cuentas de administrador de dominio" durante, al menos, los últimos treinta días.	☐
	Ninguna de las anteriores/No lo sé.	☐
	Seleccione una respuesta: ¿Cómo se autentican los empleados del **Solicitante** para acceder a la red corporativa de forma remota?	
ICA Nº 6	El acceso remoto a la red corporativa normalmente solo requiere de un nombre de usuario y una contraseña válidos (autenticación de factor único).	☐
	La autenticación multifactor (MFA) está implementada para algunos tipos de acceso remoto a la red corporativa, pero no para todos.	☐
	La política requiere de MFA para todos los accesos remotos a la red corporativa, y todas las excepciones a la política están documentadas.	☐
	El **Solicitante** no proporciona acceso remoto a ningún empleado.	☐

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	Seleccione una respuesta: ¿Cómo se autentican los proveedores del **Solicitante** para acceder a la red corporativa de forma remota?	
ICA Nº 7	El acceso remoto a la red corporativa normalmente solo requiere de un nombre de usuario y una contraseña válidos (autenticación de factor único).	☐
	La MFA está implementada para algunos tipos de acceso remoto a la red corporativa, pero no para todos.	☐
	La política requiere de MFA para todos los accesos remotos a la red corporativa, y todas las excepciones a la política están documentadas.	☐
	El **Solicitante** no proporciona acceso remoto a ningún proveedor.	☐
	Seleccione una respuesta: ¿Cómo se autentican los empleados y proveedores del **Solicitante** para acceder a Activos vitales que son SaaS/aplicaciones de terceros?	
ICA Nº 8	El acceso a Activos vitales alojados externamente normalmente solo requiere de un nombre de usuario y una contraseña válidos (autenticación de factor único).	☐
	La MFA está implementada para algunos tipos de acceso a Activos vitales alojados externamente, pero no para todos.	☐
	La política requiere de MFA para todos los accesos a Activos vitales alojados externamente, y todas las excepciones a la política están documentadas.	☐
	El **Solicitante** no utiliza SaaS/aplicaciones de terceros que pudiesen considerarse Activos vitales.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con cómo protege el **Solicitante** las "Cuentas de servicio" "Privilegiadas": Las "Cuentas de servicio" son cuentas utilizadas para ejecutar aplicaciones y otros procesos. No suelen utilizarse más allá de la resolución de problemas. "Privilegiadas" significa que tienen privilegios elevados y, en el entorno de Active Directory, incluyen a título enunciativo, pero no limitativo, Administradores de empresa, Administradores de dominio y Administradores (dominio).	
ICA Nº 9	Hay un inventario de todas las "Cuentas de servicio" "Privilegiadas" que se actualiza, como mínimo, una vez al trimestre.	☐
	Las "Cuentas de servicio" "Privilegiadas" tienen contraseñas con una longitud de 25 caracteres como mínimo.	☐
	Las contraseñas de las "Cuentas de servicio" "Privilegiadas" cambian, como mínimo, una vez al año.	☐
	Las contraseñas de las "Cuentas de servicio" "Privilegiadas" cambian, como mínimo, una vez al trimestre.	☐
	Las "Cuentas de servicio" están divididas en capas, de modo que se utilizan cuentas diferentes para interactuar con workstations, servidores y servidores de autenticación, aunque sea para el mismo servicio.	☐

	Hay un proceso implementado para revisar, como mínimo una vez al año, los requisitos actuales para cada servicio asociado con las "Cuentas de servicio" "Privilegiadas", con el fin de comprobar si el servicio sigue requiriendo los permisos que la cuenta de servicio tiene (y reducirlos de no ser así).	☐
	Ninguna de las anteriores/No lo sé.	☐
	Seleccione una respuesta: Nivel de garantía de autenticador (AAL) que mejor representa la solución o soluciones de autenticación del **Solicitante.** La publicación especial de NIST 800-63B define los niveles de garantía de los autenticadores.	
ICA N° 10	AAL1	☐
	AAL2	☐
	AAL3	☐
	No lo sé.	☐
	Indique el número de cuentas activas que el **Solicitante** tiene para las siguientes categorías. Las cuentas no deberían incluir cuentas inactivas, pero sí todas las cuentas anidadas de todos los dominios/bosques.	
ICA N° 11	Número de "Cuentas de administrador de dominio":	
	Número de "Cuentas de servicio" "Privilegiadas":	
	NOTA: Para cada "Cuenta de servicio" "Privilegiada", utilice la tabla que se proporciona al final de este cuestionario adicional para indicar i) el nombre de la cuenta, ii) los privilegios que tiene, iii) el software que respalda, iv) en qué hosts se autentica la cuenta de servicio, y v) por qué son necesarios esos privilegios.	

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

Seleccione una respuesta: ¿Qué descripción refleja mejor la postura del **Solicitante** en relación con los controles de acceso para las workstations de cada usuario? A los efectos de esta pregunta, no se considerarán "accesos de administrador" aquellos casos en los que el Solicitante utilice un gestor de privilegios de los Endpoints, o alguna tecnología similar, para permitir a los usuarios solicitar acceso administrativo temporal para determinadas actividades.		
ICA Nº 12	Ninguna cuenta regular de uso diario se incluye en el grupo de administradores o tiene acceso de administrador local a su workstation.	☐
	La política del **Solicitante** es que los empleados, por defecto, no estén en el grupo de administradores y no tengan acceso de administrador local; todas las excepciones a la política están documentadas.	☐
	Algunos de los empleados del **Solicitante** pertenecen al grupo de administradores o son administradores locales.	☐
	No lo sé.	☐
Seleccione una respuesta: ¿Qué descripción refleja mejor la postura del **Solicitante** en relación con los controles de acceso para los servidores gestionados? La pregunta se refiere a las cuentas de usuario de los empleados de uso diario; los casos en los que el Solicitante proporcione a los empleados unas credenciales independientes para el acceso administrador no se deben tener en cuenta a los efectos de esta pregunta.		
ICA Nº 13	Ningún empleado está en el grupo de administradores o tiene acceso como administrador local a los servidores miembro.	☐
	La política del **Solicitante** es que los empleados, por defecto, no estén en el grupo de administradores y no tengan acceso de administrador local; todas las excepciones a la política están documentadas.	☐
	Algunos de los empleados del **Solicitante** pertenecen al grupo de administradores o son administradores locales.	☐
	No lo sé.	☐
¿Cuántos usuarios del **Solicitante** tienen acceso como administrador persistente a servidores y/o workstations que no sean propios? A los efectos de esta pregunta, "acceso como administrador" significa el acceso con privilegios para configurar, gestionar y dar respaldo de cualquier modo a estos Endpoints, incluyendo a través del uso de una cuenta de administrador única (independiente de la cuenta del usuario de uso diario). Los usuarios que deben "verificar" las credenciales para el acceso administrativo no deben incluirse.		
ICA Nº 14	Introduzca un número entero:	

	¿Integra el **Solicitante** los registros de seguridad de todos los controladores de dominio en su solución SIEM para fines de análisis?	
ICA Nº 15	Sí	☐
	No. El **Solicitante** no tiene una solución SIEM o no integra los registros de seguridad en su SIEM.	☐
	No se aplica. No utiliza servicios de directorio, IdP, gestión de derechos.	☐
	Seleccione todas las respuestas que sean ciertas: ¿Qué políticas de auditoría tiene el **Solicitante** habilitadas en los controladores de dominio?	
ICA Nº 16	Auditar validación de credenciales (Error)	☐
	Auditar creación de procesos (Éxito)	☐
	Auditar gestión de grupos de seguridad (Éxito y error)	☐
	Auditar gestión de cuentas de usuario (Éxito y error)	☐
	Auditar otros eventos de gestión de cuentas (Éxito y error)	☐
	Auditar el uso de privilegios delicados (Éxito y error)	☐
	Auditar inicios de sesión (Logon) (Éxito y error)	☐
	Auditar inicios de sesión (Logon) (Éxito y error)	☐
	Auditar inicios de sesión (Logon) especiales (Éxito)	☐
	Ninguna de las anteriores/No lo sé.	☐
	No se aplica (no se utiliza Active Directory)	☐

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	Si el **Solicitante** tiene comentarios adicionales sobre alguna pregunta o respuesta de esta sección, debe indicarlos aquí:	

Monitorización de seguridad y respuesta a incidentes (SMIR)

	PREGUNTA	RESPUESTA
	Seleccione una respuesta: ¿Qué descripción refleja mejor el programa de operaciones de seguridad del **Solicitante?**	
SMIR N° 1	El **Solicitante** no tiene personal (interno o externo) dedicado a monitorizar las operaciones de seguridad ("Security Operations Center" o SOC).	☐
	El **Solicitante** tiene un SOC, pero no está disponible en formato 24/7 (puede ser interno o externo).	☐
	El **Solicitante** dispone de una monitorización de las operaciones de seguridad en formato 24/7, por parte de un tercero (como un proveedor de servicios de seguridad administrados, "MSSP").	☐
	El **Solicitante** realiza internamente la monitorización de las operaciones de seguridad en formato 24/7 (independientemente de si también se utilizan los servicios de un tercero).	☐
	Seleccione todas las respuestas que sean ciertas: En relación con las capacidades de monitorización de la seguridad y la red del **Solicitante:**	
SMIR N° 2	El **Solicitante** utiliza una herramienta de "Información de seguridad y monitorización de eventos" (SIEM) para correlacionar el resultado de múltiples herramientas de seguridad.	☐
	El **Solicitante** monitoriza el tráfico de la red en busca de transferencias de datos anómalas y potencialmente sospechosas.	☐
	El **Solicitante** monitoriza los problemas de rendimiento y capacidad de almacenamiento en todos los servidores (como un elevado uso de la memoria o el procesador, o la falta de espacio libre en el disco).	☐
	El **Solicitante** tiene herramientas para monitorizar la pérdida de datos (DLP) y están en modo de bloqueo.	☐
	El **Solicitante** tiene herramientas para monitorizar la pérdida de datos (DLP) y no están en modo de bloqueo.	☐
	Ninguna de las anteriores/No lo sé.	☐

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	¿Cuál es el tiempo promedio que ha tardado el **Solicitante** en clasificar y contener los incidentes de seguridad en las workstations que se han producido en el trimestre finalizado más recientemente?	
SMIR Nº 3	<30 minutos	☐
	30 minutos-2 horas	☐
	2-8 horas	☐
	8 horas-3 días	☐
	> 3 días	☐
	El **Solicitante** no realiza un seguimiento de esta métrica/No lo sé.	☐
	¿Qué porcentaje de los "Activos vitales" del **Solicitante** se registran y envían a una solución SIEM?	
SMIR Nº 4	0-30 %	☐
	31-50 %	☐
	51-70 %	☐
	>= 71 %	☐
	No lo sé	☐
	No se aplica (no dispone de SIEM)	☐

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	¿Durante cuánto tiempo conserva los registros la solución SIEM del **Solicitante?**	
SMIR Nº 5	Menos de 30 días	☐
	30-59 días	☐
	60-89 días	☐
	90 días o más	☐
	No lo sé	☐
	No se aplica (no dispone de SIEM)	☐
	Seleccione todas las respuestas que sean verdaderas: En relación con cómo valida el **Solicitante** la eficiencia y eficacia de los controles de seguridad:	
SMIR Nº 6	El **Solicitante** utiliza software de Simulación de ataques y violaciones (BAS) para verificar la eficacia de los controles de seguridad.	☐
	El **Solicitante** dispone de un "red team" compuesto por personal para probar los controles de seguridad, o contrata, como mínimo una vez al año, a expertos para que lleven a cabo pruebas de penetración (pentest) centradas en los sistemas internos.	☐
	El **Solicitante** ha contratado a un tercero para simular a los actores de amenazas y probar los controles de seguridad en el último año.	☐
	Ninguna de las anteriores.	☐

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	Seleccione todas las respuestas que sean ciertas: En relación con los procedimientos y programas de respuesta a incidentes del **Solicitante:**	
SMIR N° 7	El **Solicitante** tiene un plan de respuesta a incidentes documentado.	☐
	El plan de respuesta a incidentes del **Solicitante** incluye un libro de tácticas específico para un incidente de ransomware en la organización.	☐
	El plan de respuesta a incidentes del **Solicitante** incluye un libro de tácticas específico para un incidente de ransomware de terceros/proveedor de servicios administrados.	☐
	El plan de respuesta a incidentes del **Solicitante** incluye el contacto con las autoridades policiales una vez se haya confirmado el incidente de ransomware.	☐
	El plan de respuesta del **Solicitante** incluye un proceso para reanudar las operaciones de la empresa a través de la restauración de backups que se sabe que no se han visto afectadas.	☐
	Ninguna de las anteriores.	☐
	¿Dispone el **Solicitante** de un proceso documentado para responder a los incidentes de phishing (ya sean dirigidos específicamente al **Solicitante** o a sus empleados, o no)?	
SMIR N° 8	Si	☐
	No	☐
	Si el **Solicitante** tiene comentarios adicionales sobre alguna pregunta o respuesta de esta sección, debe indicarlos aquí:	

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

Gestión de riesgos (RM)

	PREGUNTA	RESPUESTA
	¿Dispone el **Solicitante** de un programa de detección de vulnerabilidades que identifique y gestione las vulnerabilidades en todos los "Activos vitales"?	
RM N° 1	Si	☐
	No	☐
	Seleccione todas las respuestas que sean verdaderas: En relación con los factores que el **Solicitante** utiliza para priorizar las tareas de parcheado:	
RM N° 2	Puntuación del Common Vulnerability Scoring System (CVSS).	☐
	Correlación con el hecho de que la vulnerabilidad afecte a los "Activos vitales" del **Solicitante.**	☐
	Inteligencia sobre amenazas genéricas (p. ej., que los actores de amenazas están explotando una vulnerabilidad en concreto. Incluye herramientas como el Catálogo de vulnerabilidades explotadas conocidas de CISA).	☐
	Inteligencia sobre amenazas específicas para el **Solicitante** (incluida inteligencia sobre los actores de amenazas que podrían dirigirse específicamente al **Solicitante** a través de la explotación de una vulnerabilidad en concreto, o datos procedentes del entorno del **Solicitante** que indiquen cuál es el objetivo de los actores de amenazas).	☐
	Ninguna de las anteriores/No lo sé.	☐

	¿Cuál es el tiempo objetivo que tarda el **Solicitante** en implementar los parches de mayor prioridad?	
RM Nº 3	24 horas.	☐
	24-72 horas.	☐
	3-7 días.	☐
	7-29 días.	☐
	>= 30 días.	☐
	No hay una política definida sobre cuándo se deben implementar los parches/No lo sé.	☐
	¿Cuál es la tasa de cumplimiento del Solicitante con respecto a sus estándares de implementación de los parches de mayor importancia en el trimestre finalizado más recientemente?	
RM Nº 4	> 95 %	☐
	90-95 %	☐
	80-89 %	☐
	< 80 %	☐
	No se mide/No lo sé.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con las políticas del **Solicitante** sobre el uso de activos TI de la organización:	
	El **Solicitante** cuenta con una "Política de uso aceptable" (AUP) que recoge las obligaciones y restricciones de los usuarios.	☐
	La AUP describe las consecuencias de las violaciones de la política.	☐
	No se permite que los usuarios naveguen en plataformas de redes sociales desde los activos de la organización, salvo cuando sea una necesidad empresarial definida.	☐

RM N° 5	No se permite que los usuarios accedan a su correo electrónico personal desde los activos de la organización.	☐
	No se permite de manera rotunda que los administradores naveguen en Internet o accedan a sus correos electrónicos personales desde sus cuentas con privilegios.	☐
	Los usuarios y administradores son responsables de proteger sus cuentas y su ordenador de los problemas y riesgos más comunes.	☐
	Los usuarios y administradores deben notificar sospechas de violaciones.	☐
	Ninguna de las anteriores/No lo sé.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con las capacidades del **Solicitante** de monitorizar los comportamientos peligrosos y el personal interno malintencionado:	
RM N° 6	El **Solicitante** tiene un programa de amenazas internas.	☐
	El **Solicitante** monitoriza los casos en los que una cuenta de usuario o administrador establece una contraseña no segura.	☐
	El **Solicitante** monitoriza los casos en los que cuentas "Privilegiadas" acceden a sitios web y servicios no autorizados.	☐
	El **Solicitante** monitoriza el acceso remoto no autorizado a "Accesos vitales".	☐
	El **Solicitante** monitoriza las cuentas de usuario y administrador para detectar comunicaciones con sitios web y direcciones IP maliciosos conocidos, así como con otros recursos conocidos de grupos de amenazas.	☐
	Ninguna de las anteriores/No lo sé.	☐
	Si el **Solicitante** tiene comentarios adicionales sobre alguna pregunta o respuesta de esta sección, debe indicarlos aquí:	

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

Defensa ante phishing (PhD)

	PREGUNTA	RESPUESTA
	Seleccione todas las respuestas que sean ciertas: En relación con las capacidades para mitigar incidentes de phishing del **Solicitante:**	
PhD N° 1	El **Solicitante** proporciona cursos de concienciación sobre seguridad, incluidos cursos de concienciación sobre phishing, a los empleados, como mínimo, una vez al año.	☐
	El **Solicitante** utiliza ataques de phishing simulados para medir el nivel de concienciación de ciberseguridad de sus empleados, como mínimo, una vez al año.	☐
	Cuando el **Solicitante** realizó la última simulación de phishing, la tasa de éxito fue inferior al 15 % (menos del 15 % de los empleados fueron engañados).	☐
	El **Solicitante** "etiqueta" o marca de otro modo los correos electrónicos provenientes de un remitente externo a la organización.	☐
	El **Solicitante** dispone de un proceso documentado para informar sobre correos electrónicos sospechosos a un equipo de seguridad interno para que lo investigue, y publica el proceso para los usuarios.	☐
	Ninguna de las anteriores/No lo sé.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con las capacidades del **Solicitante** de bloquear páginas web y/o correos electrónicos potencialmente dañinos:	
PhD N° 2	El **Solicitante** utiliza una solución de filtrado de correo electrónico que bloquea los archivos adjuntos maliciosos conocidos y los tipos de archivos sospechosos, incluyendo los ejecutables.	☐
	El **Solicitante** utiliza una solución de filtrado de correo electrónico que bloquea los mensajes sospechosos en función de su contenido o los atributos del remitente.	☐
	El **Solicitante** utiliza una solución de filtrado web que evita que los empleados visiten páginas web sospechosas o maliciosas conocidas.	☐
	El **Solicitante** bloquea los dominios no categorizados y los dominios recientemente registrados mediante proxies web o filtros DNS.	☐
	El **Solicitante** utiliza una solución de filtrado web que bloquea las descargas sospechosas o maliciosas conocidas, incluidas las ejecutables.	☐
	La solución de filtrado de correo electrónico del **Solicitante** tiene la capacidad de ejecutar archivos adjuntos sospechosos en un entorno sandbox.	☐

	Las capacidades de filtrado web del **Solicitante** son efectivas en todos los activos de la organización, incluso si el activo no está en una red de la organización (por ejemplo, los activos están configurados para utilizar filtros web basados en la nube o requieren una conexión VPN para navegar por Internet).	☐
	Ninguna de las anteriores/No lo sé.	☐
	Si el **Solicitante** tiene comentarios adicionales sobre alguna pregunta o respuesta de esta sección, debe indicarlos aquí:	

Defensa ante malware (Mal)

	PREGUNTA	RESPUESTA
	Seleccione todas las respuestas que sean ciertas: En relación con las capacidades de las herramientas de seguridad de los Endpoints del **Solicitante:**	
Mal N°1	La solución de seguridad de los Endpoints del **Solicitante** incluye antivirus con capacidades heurísticas.	☐
	El **Solicitante** utiliza herramientas de seguridad con capacidades de detección de comportamiento y capacidades de mitigación de exploits en los Endpoints.	☐
	El **Solicitante** utiliza una herramienta de respuesta y detección de amenazas en los Endpoints (ETDR o EDR) que lleva a cabo lo siguiente: monitoriza indicadores de amenazas; identifica patrones que coinciden con amenazas conocidas; responde automáticamente eliminando o conteniendo amenazas; alerta de los incidentes al personal de seguridad; proporciona capacidades forenses y capacidades de análisis para que los analistas puedan llevar a cabo actividades de detección de amenazas.	☐
	El **Solicitante** implementa controles de aplicaciones en todas las workstations para que solo se ejecuten aplicaciones autorizadas. Las aplicaciones no autorizadas están bloqueadas y la lista de aplicaciones autorizadas se vuelve a evaluar, como mínimo, dos veces al año.	☐
	El **Solicitante** tiene un grupo interno y/o MSSP que monitoriza el resultado de las herramientas de seguridad de los Endpoints e investiga cualquier anomalía.	☐
	Ninguna de las anteriores/No lo sé.	☐

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	Seleccione todas las respuestas que sean ciertas: En relación con la implementación por parte del **Solicitante** de la herramienta o herramientas de seguridad de los Endpoints (tal como se describe arriba):	
Mal N° 2	La herramienta o herramientas de seguridad de los Endpoints del **Solicitante** están implementadas en todas las workstations y portátiles, y todas las excepciones están documentadas.	☐
	La herramienta o herramientas de seguridad de los Endpoints del **Solicitante** están implementadas en todos los servidores (salvo los hosts hipervisores), y todas las excepciones están documentadas.	☐
	La herramienta o herramientas de seguridad de los Endpoints del **Solicitante** están implementadas en todos los dispositivos móviles (incluidos teléfonos, tabletas, etc., pero excluyendo los portátiles), y todas las excepciones están documentadas.	☐
	Ninguna de las anteriores/No lo sé.	☐
	Seleccione todas las respuestas que sean ciertas: En relación con la configuración por parte del **Solicitante** de su herramienta o herramientas de seguridad de los Endpoints (tal como se describe arriba):	
Mal N° 3	En el caso de herramientas que requieren definiciones actualizadas, la actualización de las herramientas se realiza, como mínimo, una vez al día.	☐
	La herramienta o herramientas están configuradas para bloquear (y no solo notificar) procesos y archivos que se sospecha que son maliciosos.	☐
	La herramienta o herramientas están configuradas para detectar activos no administrados, que se abordan, como mínimo, una vez a la semana.	☐
	Hay habilitadas funciones anti-tamper (contra alteraciones).	☐
	Ninguna de las anteriores/No lo sé.	☐
	Identifique la herramienta o herramientas de seguridad de los Endpoints utilizadas (procure que su respuesta sea lo más específica posible, p. ej., "Falcon Prevent, Insight and Overwatch" y no "CrowdStrike"):	
Mal N° 4	*Escriba aquí:*	
	Seleccione todas las respuestas que sean ciertas: En relación con las capacidades para limitar los desplazamientos laterales del **Solicitante:**	
Mal N° 5	El **Solicitante** ha segmentado la red por geografía (por ejemplo, se deniega el tráfico entre oficinas en diferentes ubicaciones a menos que sea necesario para respaldar un requisito de negocio específico).	☐
	El **Solicitante** ha segmentado la red por funciones de negocio (por ejemplo, se deniega el tráfico entre activos que dan respaldo a diferentes funciones, como RR. HH. y Finanzas, a menos que sea necesario para responder a un requisito de negocio específico).	☐

	El **Solicitante** ha implementado reglas de firewall en los hosts que impiden el uso de RDP para iniciar sesión en las workstations.	☐
	El **Solicitante** ha configurado todas las cuentas de servicio para que no se permitan los inicios de sesión (logons) interactivos.	☐
	Ninguna de las anteriores/No lo sé.	☐
Ha llevado a cabo el **Solicitante** un ejercicio de simulación de las tácticas, técnicas y procedimientos de actores de ransomware en el último año?		
Mal N° 6	Si	☐
	No	☐
	Si el **Solicitante** tiene comentarios adicionales sobre alguna pregunta o respuesta de esta sección, debe indicarlos aquí:	

Defensa de terceros y proveedores de servicios administrados (TP & MSP)

	PREGUNTA	RESPUESTA
	Seleccione todas las respuestas que sean ciertas: En relación con los roles de terceros o de proveedores de servicios de administrador (MSP) para la red del **Solicitante,** incluido el acceso remoto a recursos como la nube y las VPN.	
TP & MSP N° 1	El **Solicitante** utiliza un MSP para la administración de "Activos vitales".	☐
	El **Solicitante** utiliza un MSP para operaciones de seguridad.	☐
	El **Solicitante** utiliza un MSP para copias de seguridad y recuperación de datos.	☐
	El **Solicitante** utiliza un MSP para transformación en la nube.	☐
	El **Solicitante** utiliza un MSP para el desarrollo de software.	☐

	El **Solicitante** proporciona acceso persistente ("siempre conectado") a terceros a los recursos corporativos (el acceso no requiere de la autorización del **Solicitante**).	☐
	Ninguna de las anteriores/No lo sé.	☐
	¿Cuenta el **Solicitante** con una solución técnica o proceso para identificar, evaluar, gestionar, monitorizar y reducir los riesgos de MSP y terceros?	
TP & MSP Nº 2	Sí	☐
	No	☐
	Si el **Solicitante** tiene comentarios adicionales sobre alguna pregunta o respuesta de esta sección, debe indicarlos aquí:	

Defensa de Internet y perímetro

	PREGUNTA	RESPUESTA
	Seleccione todas las respuestas que sean ciertas: En relación con las capacidades del **Solicitante** de proteger sistemas expuestos externamente, como sistemas expuestos a Internet:	
Perímetro Nº 1	El **Solicitante** tiene un inventario de activos expuestos al exterior.	☐
	El **Solicitante** lleva a cabo análisis de vulnerabilidades de forma periódica de los activos expuestos externamente.	☐
	El **Solicitante** tiene un firewall de aplicaciones web (WAF) en todas las aplicaciones expuestas externamente y está en modo de bloqueo.	☐
	El **Solicitante** lleva a cabo análisis en los activos expuestos externamente para detectar vulnerabilidades, como mínimo, una vez al mes.	☐
	El **Solicitante** utiliza un servicio externo para monitorizar su superficie de ataque (sistemas expuestos a Internet).	☐
	El **Solicitante** desactiva o bloquea, en sistemas expuestos externamente, aquellos puertos, servicios y protocolos que se conoce que difunden ransomware, incluidos, a título enunciativo, RDP, SMBv1 y SMBv2.	☐

	Los activos expuestos externamente del **Solicitante** están segmentados con una zona desmilitarizada (DMZ), y la DMZ no se puede rastrear directamente hasta la red corporativa. Los usuarios que necesitan acceder a los servicios DMZ son dirigidos a Internet para el acceso.	☐
	El Solicitante puede detectar amenazas y responder a ellas a través de las soluciones de monitorización de red y Endpoints.	☐
	Ninguna de las anteriores/No lo sé.	☐
	Si el **Solicitante** tiene comentarios adicionales sobre alguna pregunta o respuesta de esta sección, debe indicarlos aquí:	

Anexo sobre "Cuentas de servicio" "Privilegiadas" (si corresponde)

Instrucciones: Para cada "Cuenta de servicio" "Privilegiada", utilice la tabla que se proporciona para indicar:

i) el nombre de la cuenta,
ii) los privilegios que tiene,
iii) el producto de software al que da respaldo,
iv) en qué hosts se autentica la cuenta de servicio, y
v) por qué son necesarios esos privilegios.

ANEXO SOBRE "CUENTAS DE SERVICIO" "PRIVILEGIADAS"				
Nombre de la cuenta	**Privilegios que tiene**	**Producto de software al que da respaldo**	**En qué hosts se autentica**	**Por qué son necesarios esos privilegios**
SOLO EJEMPLO: svc_cyberark	*SOLO EJEMPLO: Administrador de dominio*	*SOLO EJEMPLO: Administrador de acceso privilegiado de CyberArk*	*SOLO EJEMPLO: Únicamente controladores de dominio*	*SOLO EJEMPLO: El Administrador de dominio necesita cambiar las contraseñas de cuentas delicadas*
	Administrador de dominio ("DA")		Únicamente controladores de dominio (DC)	

AIG Metropolitana
CIA. DE SEGUROS Y REASEGUROS S.A.

	Administrador de dominio ("DA")		Únicamente controladores de dominio (DC)	
	Administrador de dominio ("DA")		Únicamente controladores de dominio (DC)	
	Administrador de dominio ("DA")		Únicamente controladores de dominio (DC)	

Este cuestionario adicional se incorpora y pasa a formar parte de cualquier solicitud de cobertura CyberEdge® por parte del solicitante. Todas las declaraciones y garantías hechas por el solicitante en relación con dicha solicitud también se aplican a la información proporcionada en este cuestionario adicional.

En caso de que la aseguradora emita una póliza, el solicitante acepta que dicha póliza se emitirá en función de la veracidad de las declaraciones y manifestaciones de este cuestionario adicional incorporadas por su referencia aquí. Cualquier reserva o inexactitud, declaración falsa, omisión, encubrimiento o declaración incorrecta de un hecho o información incluido en este cuestionario adicional incorporado por su referencia aquí o de otra manera, será motivo para la rescisión de cualquier póliza emitida. A tales efectos, el abajo firmante declara, en la representación que ostenta, que las declaraciones e informaciones contenidas y comunicadas en este cuestionario son verdaderas y completas, así como que no ha omitido voluntariamente ni suprimido ningún dato, información o hecho relevante.

El abajo firmante declara y garantiza que es un representante debidamente autorizado del solicitante para representarle con relación a los asuntos de cualquier naturaleza o clase relativos al presente cuestionario y que está plenamente autorizado para responder, realizar declaraciones y completar el presente cuestionario en nombre del solicitante o por parte de este.

El solicitante se compromete a informar el asegurador de cualquier modificación relevante que se produjera, que afecte a las declaraciones contenidas en este cuestionario, que pudieran tener lugar entre la fecha de este cuestionario y la fecha de efecto de la póliza que en su caso se emita.

Firma del Solicitante: **Fecha:**

_____ _____

Cargo: _____