Información General (Contratante)					
Nombre o Razón Social:					
Persona Física o Moral:		RFC:		CURP:	
Nombre del Representante Legal:					
ID del Representante Legal:					
Giro de la Empresa:					
Fecha de creación de la empresa:		Experiencia en el giro (En años):			
Domicilio Fiscal:		No. Exterior:		No. Interior:	
C.P.:		Ciudad:		Estado:	
Teléfono:		Correo Electrónico:			

Datos del Solicitante (Sólo si es diferente al Contratante)			
Nombre:		RFC:	
CURP:		Relación con el Contratante:	

1. Vigencia del Seguro			
Inicio de Vigencia a las 12 horas. del:		Término de Vigencia a las 12 horas. del:	
Duración de la Obra en Meses:		Periodo de Cobertura Esperada (Años):	

Datos Generales del Proyecto

2 PERFIL DE LA COMPAÑÍA/COMPAÑÍAS A SER ASEGURADAS

2.1 Actividades del Asegurado

[Por favor describa las actividades principales de la compañía/compañías a ser aseguradas. Si estas actividades incluyen comercio electrónico, por favor indicar el porcentaje de los ingresos que se generan por este concepto]|

2.1 Alcance

[Liste por favor las compañías y subsidiarias a ser aseguradas. Si la compañía tiene subsidiarias en Estados Unidos, por favor detallar la actividad de la misma]

2.3 Criticidad de los Sistemas de Información

[Por favor indique el periodo de interrupción sobre el cual su compañía sufriría un impacto significativo en su negocio]

Aplicación (o Actividad)	Periodo de interrupción máximo antes de un impacto adverso en el negocio				
	Inmediato	> 12 h	> 24 h	> 48 h	> 5 días

3 SISTEMAS DE INFORMACIÓN

	< 100	101 – 1000	> 1000
Número de Usuarios			
Número de portátiles			
Número de Servidores			

	SI	NO
¿Realiza usted comercio electrónico o provee un servicio online en su sitio web?	☐	☐

De ser positivo : ¿Cuál es el porcentaje de ingresos generado o soportado por el sitio web? (estimado)	(% o COP)

4 SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN (ISS)

	4.1 Políticas de seguridad y Manejo del Riesgo	SI	NO
1	Hay una política de Seguridad de los Sistemas de Información formalizada y aprobada por la Dirección y/o normas de seguridad definidas y comunicadas a los empleados, y aprobados por los mismos?	☐	☐

2	¿Se provee regularmente Capacitación y Entrenamiento en Seguridad de los Sistemas de Información a los usuarios?	☐ ☐
3	¿Ha identificado usted los riesgos críticos de los Sistemas de Información y ha implementado controles apropiados para su mitigación?	☐ ☐
4	¿Se realizan auditorías periódicas a los sistemas de Información y se implementan las recomendaciones generadas?	☐ ☐
5	¿Realiza usted un inventario y clasificación de la información de acuerdo con su criticidad y sensibilidad, definiendo los requerimientos de seguridad según lo anterior?	☐ ☐
	4.2 Protección de los Sistemas de Información	SI NO
1	¿El acceso a los sistemas de información requiere la identificación del usuario, el cambio periódico de claves y la construcción de una contraseña segura?	☐ ☐
2	¿Las autorizaciones de acceso están basadas en roles de usuario y se ha implementado un procedimiento para el manejo de las autorizaciones de acuerdo con el principio de menor privilegio?	☐ ☐
3	¿Referencias de configuración seguras están definidas para portátiles, estaciones de trabajo, servidores y dispositivos móviles?	☐ ☐
4	¿Cuenta con un manejo centralizado y realiza monitoreo de la configuración de los sistemas?	☐ ☐
5	¿Las computadoras portátiles cuentan con un firewall personal?	☐ ☐
6	¿Un antivirus está instalado en todos los sistemas y se monitorea la actualización de los mismos?	☐ ☐
7	¿Los parches de seguridad se instalan periódicamente?	☐ ☐
8	¿Tiene implementado un Plan de Recuperación de Desastres que es actualizado periódicamente?	☐ ☐
9	¿Se realizan back ups de manera diaria, se prueban periódicamente y una copia de seguridad se guarda periódicamente en un sitio remoto?	☐ ☐
	4.3. Operaciones y Seguridad de la Red	SI NO
1	¿Se actualizan los filtros de tráfico entre la red interna e internet y se monitorea de manera periódica?	☐ ☐
2	Tiene implementado un sistema de detección/prevención de intrusiones, el cual se actualiza y monitorea periódicamente?	☐ ☐

3	¿Los usuarios internos tienen acceso a los sitios de Internet navegando a través de un dispositivo de red (proxy) equipado con antivirus y filtros de red?	☐ ☐
4	Se ha realizado una segmentación de la red para separar las áreas críticas (servidores, administración…) de las menos criticas (como las áreas de usuarios...)	☐ ☐
5	¿Se realizan pruebas de penetración periódicamente y se implementa el plan de remediación?	☐ ☐
6	¿Se realizan asesorías de vulnerabilidad periódicamente y se implementa el plan de remediación?	☐ ☐
7	¿Se tienen implementados procedimientos para manejo de incidentes y gestión de modificaciones?	☐ ☐
8	¿Los incidentes de seguridad (como detección de virus, intentos de acceso…) son registrados y monitoreados periódicamente?	☐ ☐
9	¿Se ha implementado un monitoreo preventivo en contra de intrusiones en la red y las alertas e incidentes de seguridad se priorizan y manejan de acuerdo con su criticidad?	☐ ☐
	4.4. Seguridad Física en el Centro de Cómputo (Site o Datacenter)	SI NO
1	¿Los sistemas críticos son ubicados en un Centro de Cómputo exclusivo, con acceso restringido y niveles de seguridad ambiental y eléctricos?	☐ ☐
2	¿El Centro de Cómputo en el que se alojan los sistemas críticos posee infraestructura resilente? (redundancia con respecto a la generación de energía, aire acondicionado, conexiones de red …)	☐ ☐
3	Los sistemas críticos son duplicados de acuerdo con arquitectura Activa/Pasiva o Activa/Activa	☐ ☐
4	¿Los sistemas críticos son duplicados en 2 predios físicamente separados?	☐ ☐
5	¿Se ha implementado un sistema de detección de incendios y extinción automática de incendios en las áreas críticas?	☐ ☐
6	¿El suministro de energía está protegido con UPS y baterías? ¿Se realiza un mantenimiento periódico de los mismos?	☐ ☐
7	¿El suministro de Energía está respaldado por un generador de energía al cual se le realizan mantenimiento y pruebas periódicas?	☐ ☐
	4.5. Outsourcing	SI NO
	[Por favor completar si una función de los sistemas de información es contratada por outsourcing]	
1	¿El contrato de outsourcing incluye requerimientos de seguridad que deben ser observados por parte del proveedor del servicio?	☐ ☐

2	¿Se acuerdan niveles de servicio con el outsourcing, que impliquen controles en el manejo de incidentes y de solicitud de cambios? ¿Se aplican penalizaciones al proveedor en caso en que no cumpla con dichos acuerdos?	☐	☐
3	¿Se realiza monitoreos y reuniones periódicas con el proveedor del servicio para revisar la gestión y mejoramiento del servicio?	☐	☐
4	En sus contratos ha renunciado usted a reclamar en contra de su(s) proveedor(es) de servicios	☐	☐

¿Cuáles son las funciones de los Sistemas de información que maneja por outsourcing?	SI	NO	Proveedor de Servicios (Outsourcing)
Desktop management	☐	☐	
Server management	☐	☐	
Network management	☐	☐	
Network security management	☐	☐	
Application management	☐	☐	
¿Use of cloud computing or Software as a service)? Uso de servicios en la nube o de software	☐	☐	
Otro - por favor especifique			

5 DATOS PERSONALES

5.1. Tipo de Datos y número de registros

Cuál es el número de registros manejado por el asegurado : Total :

Por región : Europa(EU): | EU/Canadá: | Resto del mundo:

Categorías de datos personales recolectados/procesados	SI	NO	Número de Registros
Información comercial y de marketing	☐	☐	
Información financiera o de Tarjetas de Pago	☐	☐	
Información de salud	☐	☐	

Otros, por favor especificar :	
Usted procesa datos para:	☐ ¿Usted? ☐ en nombre de un tercero?

	5.2. Política de Protección de Datos Personales	SI	NO
1	Existe una política de privacidad formalizada y aprobada por el Consejo de Administración de la empresa y/o existen reglas de seguridad referente a datos personales definidos y comunicados a los empleados que tienen acceso a esta información.	☐	☐
2	¿Capacita y concientiza a los empleados con acceso autorizado o que procesa datos personales?	☐	☐
3	¿Existe un oficial de protección de datos personales designado por su organización?	☐	☐
4	¿Existen acuerdos de confidencialidad o cláusulas de confidencialidad en los contratos de trabajo del personal que maneja o tiene acceso a datos personales o información confidencial?	☐	☐
5	¿Los aspectos legales de su política de protección de datos han sido validados por un abogado y el cumplimiento con las leyes y regulaciones de protección de datos personales se monitorean periódicamente?	☐	☐
6	¿Sus prácticas frente al manejo de información personal han sido auditadas por un auditor externo en los últimos 2 años?	☐	☐
7	¿Ha implementado usted un plan de respuesta a incidentes y ha comunicado dicho plan al equipo de respuesta?	☐	☐

	5.3. Recolección de Datos Personales	SI	NO
1	¿Ha notificado Usted a la Autoridad de Protección de Datos el procesamiento de datos personales involucrado en su actividad y obtenido las autorizaciones por parte de esta? (Conteste sólo en caso en que esta notificación o autorización sea parte de las Regulaciones de Privacidad)	☐	☐
2	¿La política de privacidad publicada en su sitio web ha sido revisada por un abogado o su departamento legal?	☐	☐
3	¿Ha solicitado usted el consentimiento de los titulares en los casos en que la Ley Federal de Protección de Datos Personales en posesión de los Particulares establece, antes de recolectar datos personales? ¿Y los titulares de los Datos Personales pueden ejercer los derechos ARCO conforme lo dispone dicha Ley?	☐	☐
4	En caso en que realicen operaciones de marketing, los titulares tienen a su disposición un medio adecuado para des registrarse (opt out)	☐	☐
	¿Transfiere usted Datos Personales a terceros?	☐	☐

Si la respuesta es positiva por favor responda las siguientes preguntas:

5	¿El tercero (ej. procesador) tiene la obligación contractual de procesar los datos personales solo en su nombre y bajo sus instrucciones?	☐	☐
6	¿El tercero tiene la obligación contractual de mantener medidas de seguridad suficientes para proteger los datos personales?	☐	☐

	5.4. Medidas de Protección de Información Personal	SI	NO
1	¿El acceso a Datos personales está restringido solo a esos usuarios que así lo requieren para desarrollar sus labores y las autorizaciones de acceso son revisadas periódicamente?	☐	☐
2	¿Los datos personales están encriptados cuando se guarda en los sistemas de información y los back ups de los datos personales están encriptados?	☐	☐
3	¿Los datos personales están encriptados cuando se transmiten a través de la red?	☐	☐
4	¿Los dispositivos móviles y los discos duros de los computadores personales se encuentran encriptados?	☐	☐
5	¿Están prohibidas las copias en dispositivos de almacenamiento o transmisiones por correo electrónico de datos personales no encriptados?	☐	☐

	Si los registros que manejan contienen información de tarjetas de pago - **Payment Card Information** (PCI), por favor conteste lo siguiente:	SI	NO
1	Si nivel de PCI DSS es (por favor diríjase a la sección de definiciones al final de este documento)	☐ Nivel1 ☐ Nivel 2 ☐ Nivel 3 ☐ Nivel 4	
2	El procesador de pago (ustedes. o el tercero) cumple con los estándares PCI DSS Si la respuesta es No, por favor conteste lo siguiente :	☐	☐
3	La información PCI es almacenada encriptada o solo se almacena una parte del número de tarjeta	☐	☐
4	El almacenamiento de la información PCI no excede la duración del proceso de pago y los requerimientos legales y regulatorios.	☐	☐
5	¿El procesamiento de datos para pagos a través de tarjeta se externaliza? Si la respuesta es Si, por favor conteste lo siguiente	☐	☐
6	¿Usted requiere del procesador de pago una indemnización en caso de una brecha de seguridad?	☐	☐

Por favor indique el nombre del procesador de pago, tiempo de retención de la información PCI y cualquier medida de seguridad adicional:

	5.5. Contenido Electrónico	SI	NO
1	¿Su Departamento Legal o un abogado revisa el contenido electrónico antes de que este sea publicado?	☐	☐
2	¿Utiliza usted material suministrado por otros, como el contenido, música, gráficas o video por internet, en su software o en su página web?	☐	☐
3	En caso afirmativo, confirmar que usted obtiene siempre licencias por escrito y acuerdos de consentimiento para el uso de tales materiales	☐	☐
4	Tiene un procedimiento establecido para editar o remover de su página web; y chat room o tablón de anuncios contenidos injuriosos o calumniosos, o contenidos que infrinjan derechos de propiedad intelectual u otros (derechos de autor, maracas comerciales, marcas de nombres, etc.)	☐	☐

6	INCIDENTES Y/O EVENTOS

Fecha	Descripción del Incidente

Comentario:

Nombre de quien realiza la supervisión:	

Pago de Primas	
Tipo de Moneda: Pesos (MXN) ☐ Dólares (USD) ☐ Otra (Especificar) ☐	
Forma de Pago	Instrumento de cobro
Elija un elemento.	Elija un elemento.

Otros Seguros			
¿Cuenta con otros seguros o le ha sido rechazada o pospuesta una solicitud de seguro?		Si ☐	No ☐
Compañía	Tipo de Seguro	Suma Asegurada Solicitada	Motivo

Nota importante (Leer antes de firmar)

El contratante o solicitante debe declarar tal y como los conozca todos los hechos importantes para la apreciación del riesgo que se ampara en esta solicitud.

En caso de que el Contratante y/o Asegurado y/o representante de éstos, incurra en falsas e inexactas declaraciones u omisiones, la Compañía podrá rescindir el Contrato de pleno derecho en los términos de lo previsto en el artículo 47 de la Ley sobre el Contrato de Seguro, en relación con los Artículos 8, 9 y 10 de la citada Ley.

Declaración de Veracidad

Hago constar que la información y respuestas proporcionadas en esta solicitud son exactas, veraces y completas, reconozco que estos datos constituyen la base del Contrato de Seguro y que en caso de que la Aseguradora demostrase cualquier inexactitud u omisión implicaría la nulidad automática de la solicitud.

Lugar y fecha	Firma del Solicitante

Información del Agente

De conformidad con el artículo 96, fracción I, de la Ley de Instituciones de Seguros y de Fianzas, el Agente está obligado a informar de manera amplia y detallada el alcance real de la cobertura del seguro, así como la forma de conservarla o darla por terminada. Le informamos que el Agente de Seguros recabará información y documentación personal, realizará una entrevista y dará cumplimiento a las medidas y procedimientos implementados por la Compañía Aseguradora para detectar actos, omisiones u operaciones que pudieran favorecer, prestar ayuda, auxilio o cooperación de cualquier especie para la comisión de los delitos previstos en los artículos 139 o 148 Bis del Código Penal Federal, o que pudieran ubicarse en los supuestos del artículo 400 Bis del mismo Código, por tal motivo, en caso de que pudiera ubicarse en alguno de los actos señalados anteriormente, generará la improcedencia en el pago, nulificando el seguro de forma automática.

Nombre Completo del Agente:

RFC: Clave del Agente:

Correo electrónico: Teléfono:

Firma

Este documento sólo constituye una solicitud de seguro y, por tanto, no representa garantía alguna de que la misma será aceptada por la Institución de Seguros, ni de que, en caso de aceptarse, la aceptación concuerde totalmente con los términos de la solicitud.

En cumplimiento a lo dispuesto en el artículo 202 de la Ley de Instituciones de Seguros y de Fianzas, la documentación contractual y la nota técnica que integran este producto de seguro, quedaron registradas ante la Comisión Nacional de Seguros y Fianzas, a partir del día 23 de junio de 2021, con el número CNSF-S0128-0243-2021/ CONDUSEF-004942-01.