SEGUROS

# Protección Digital - Cuestionario de evaluación Cyber

## Introducción

Este cuestionario no es una oferta ni un contrato de seguro vinculante. Además, su diligenciamiento no obliga a la compañía de seguros a ofrecerle cobertura alguna. Las respuestas a este cuestionario son muy importantes para evaluar el riesgo con el fin de proporcionar un seguro cibernético para su compañía en base a esta información. Por lo tanto, confiamos en sus declaraciones hechas en el cuestionario, que son la base del contrato de seguro. Si no tiene un recurso de seguridad de la información, entonces el cuestionario debe ser complementado por un representante principal (propietario o miembro de la junta).

¿Adjuntan alguna información o detalles adicionales con respecto a su seguridad informática como anexo?

Sí ☐ No ☐

Moneda de las cifras en este cuestionario: USD ☐ EUR ☐ GBP ☐ Otros: ☐

## 1. INFORMACIÓN DEL SOLICITANTE

Nombre de la compañía

| Dirección | País |
|---|---|
| Correo electrónico | |
| Filiales | Teléfono |
| Nombres de todos los sitios web ( cubiertos por este seguro) | |

### 1.1 ACTIVIDAD(ES) INDUSTRIAL(ES)

Por favor marcar todas las actividades industriales aplicables. Detalles y explicaciones se encuentran en el anexo.

- ☐ Alimentación y Agricultura
- ☐ Autoridad pública; ONG sin fines de lucro
- ☐ Defensa / Contratista militar
- ☐ Educación
- ☐ Entretenimiento & Medios
- ☐ Fabricación
- ☐ Productos farmacéuticos
- ☐ Propiedad inmobiliaria & Construcción
- ☐ Salud
- ☐ Otros
- ☐ Servicios Financieros - Seguros
- ☐ Servicios profesionales
- ☐ Tecnología de la información - Hardware
- ☐ Tecnología de la información - Servicios
- ☐ Tecnología de la información - Software
- ☐ Telecomunicaciones
- ☐ Transporte / Aviación / Aeroespacial
- ☐ Turismo & Hospitalidad
- ☐ Venta al por menor

En caso de “Otros”, por favor especificar

Por favor especificar detalles de sus actividades

## 1.2 FACTURACIÓN / INGRESOS Y HUELLA REGIONAL

| | LOCAL | EEUU | UNIÓN EUROPEA | RESTO DEL MUNDO |
|---|---|---|---|---|
| Su facturación / ingresos durante el último año fiscal | | | | |
| Parte de su facturación / ingresos **creados en línea** durante el último año fiscal | | | | |

| | ULTIMO AÑO | AÑO ANTERIOR | DOS AÑOS ANTERIORES |
|---|---|---|---|
| Su beneficio bruto (o equivalente) | | | |

| | | | | |
|---|---|---|---|---|
| Por favor indicar número de empleados | | Servidores | | Computadores de escritorio |
| Por favor indicar número (estimado ) de dispositivos de Ti implementados | | Ordenadores portátiles | | Dispositivos móviles |

## 1.3 TIPO Y CANTIDAD DE DATOS

Por favor estimar el tipo y volumen de las siguientes categorías de datos sensibles que su compañía maneja/procesa según su conocimiento:

| TIPO DE DATOS | N° DE REGISTROS UNICOS | N° DE REGISTROS UNICOS DE CIUDADANOS DE EEUU | N° DE REGISTROS UNICOS ALMACENADOS EN CENTROS DE DATOS EN EEUU |
|---|---|---|---|
| ☐ Información de Identificación Personal (PII) | | | |
| ☐ Información de Tarjetas de pago (PCI) | | | |
| ☐ Información de salud personal (PHI) | | | |
| ☐ Propiedad Intelectual (IP) | | | |

## 1.4 COBERTURA DE SEGURO SOLICITADO

| | | |
|---|---|---|
| Período de la Póliza | Desde | Hasta |
| Límite Agregado solicitado | | |

## Secciones de cobertura

| Daños Propios | Deducible para casa uno de los eventos asegurados | Sub-Límite para cada uno de los eventos asegurados y en el agregado |
|---|---|---|
| ☐ Respuesta a incidentes | | |
| ☐ Restauración de datos | | |
| ☐ Interrupción de negocio | Período de espera = (  ) horas | |
| ☐ Extorsión cibernética | | |
| ☐ Ciber crimen | | |
| ☐ PCI-DSS | | |

| Reclamaciones de Terceros | Deducible para casa uno de los eventos asegurados | Sub-Límite para cada uno de los eventos asegurados y en el agregado |
|---|---|---|
| ☐ Responsabilidad por violación de la confidencialidad y privacidad | | |
| ☐ Responsabilidad por seguridad de la red | | |
| ☐ Responsabilidad por contenido multimedia | | |

## 1.5 SEGURO ANTERIOR

1. ¿Actualmente tiene o ha tenido un seguro de ciber con la misma cobertura o cobertura similar a la solicitada actualmente?

Sí ☐ No ☐

2. ¿Alguna aseguradora ha cancelado o no ha renovado una póliza que proporcione la misma cobertura o cobertura similar a la que solicita el seguro?

Sí ☐ No ☐

## 1.6 INCIDENTES DE SEGURIDAD E HISTORIAL DE PÉRDIDAS

Por favor responda a las siguientes preguntas considerando cualquier momento durante los últimos tres años.

1. ¿Ha tenido algún incidente, reclamo o demanda que involucren el acceso no autorizado o el uso indebido de su red, incluyendo malversación, fraude, robo de información de propiedad exclusiva, violación de información personal, robo o pérdida de computadoras portátiles, denegación de servicio, vandalismo electrónico o sabotaje, virus informático u otro incidente?

Sí ☐ No ☐

2. ¿Ha experimentado una interrupción de negocio no planeada de más de cuatros horas causada por un incidente cibernético?

Sí ☐ No ☐

3. ¿Ha experimentado un intento o demanda de extorsión con respecto a sus sistemas informáticos?

Sí ☐ No ☐

4. ¿Ha recibido alguna reclamación o queja con respecto a denuncias de difamación, invasión o lesión de la privacidad, robo de información, violación de la seguridad de la información, transmisión de malware, participación en un ataque de denegación de servicio, solicitud para notificar a personas debido a un hecho real o sospecha de divulgación de información personal?

Sí ☐ No ☐

5. ¿Ha estado sujeto a alguna acción, investigación o citación gubernamental con respecto a cualquier (supuesta) violación de alguna ley o regulación (de privacidad)?

Sí ☐ No ☐

6. ¿Está consiente de cualquier publicación, pérdida o divulgación de información de identificación personal en su cuidado, custodia o control, o en el control de cualquier persona que ––tenga dicha información en su nombre?

Sí ☐ No ☐

7. ¿Está consiente de algún hecho, circunstancia, situación, error u omisión real o alegado, o un problema potencial que pueda dar lugar a una pérdida o reclamación en su contra en virtud de la presente póliza de seguro cibernético o cualquier otro seguro similar actual o anterior?

Sí ☐ No ☐

Si se responda "sí" a una o más preguntas de esta sección 1.6, por favour adjuntar una descripción incluyendo detalles completos (causa, costos, notificación, tiempo hasta descubrimiento, tiempo de recuperación y pasos tomados para mitigar futuras exposiciones) de cada evento (incidente, reclamación, etc.).

## 1.7 MARCOS Y ESTÁNDARES

Por favor marcar todos los marcos legales a los que tiene que cumplir.

| | |
|---|---|
| ☐ Reglamento General de Protección de Datos (GDPR) de la Unión Europea (EU) | ☐ US Federal Privacy Act |
| ☐ US Health Insurance Portability and Accountability Act (HIPAA) y US Health Information Technology for Economic and Clinical Health (HITECH) Act | ☐ Otros |

Por favor marcar todos los estándares para los que haya sido auditado con éxito o tenga una certificación válida.

| | | | |
|---|---|---|---|
| ☐ Payment Card Industry Data Security Standard (PCI DSS) | | | |
| ☐ Mercantil 1 | ☐ Mercantil 2 | ☐ Mercantil 3 | ☐ Mercantil 4 |
| ☐ ISO 27001:2013 Information security management systems | | ☐ NIST (US National Institute of Standards and Technology) Cybersecurity Framework | |
| ☐ Critical Security Controls | | ☐ Otros | |

Si aplican otros estándares, por favor detallar:

_____

## 2. SEGURIDAD INFORMATICA

Las siguientes preguntas nos ayudan a evaluar la madurez de su seguridad informática. Por favor responda todas las preguntas y proporcione evidencia donde esté disponible (p.ej. informes, presentaciones, documentos, etc.).
Las preguntas están estructuradas de acuerdo con las cláusulas de la norma ISO 27000. Por lo tanto, las preguntas centradas en un mismo objetivo de seguridad pueden aparecer en diferentes secciones de este cuestionario. Con el fin de crear una mejor comprensión acerca de por qué hacemos las preguntas, cada sección comienza con el objetivo de las categorías de seguridad de ISO.

### 2.1 POLÍTICAS DE SEGURIDAD INFORMÁTICA

**Objetivo:** Proporcionar dirección de gestión y soporte para la seguridad de la información de acuerdo con los requisitos del negocio y las leyes y regulaciones relevantes.

1. ¿Usted tiene una política formal de seguridad de la información desarrollada, implementada a nivel corporativo y permanentemente disponible para todos los empleados y partes externas relevantes?

Sí ☐ No ☐

### 2.2 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

**Objetivo:** : Establecer un marco de gestión para iniciar y controlar la implementación y el funcionamiento de la seguridad de la información dentro de la organización. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.

1. Tiene su compañía una persona responsable para la seguridad informática (p.ej. Chief Information Security Officer "CISO")?

Sí ☐ No ☐

2. ¿Tiene una lista actualizada de autoridades y contactos externos, que deben ser informados en caso de un incidente de seguridad de la información?

Sí ☐ No ☐

### 2.3 POLÍTICAS DE SEGURIDAD INFORMÁTICA

**Objetivo:** Garantizar que los empleados y contratistas entiendan sus responsabilidades y sean adecuados para las funciones para las que se los considera. Garantizar que empleados y contratistas conozcan y cumplan sus responsabilidades de seguridad de la información. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.

1. ¿Usted provee formación por lo menos anual para aumentar la conciencia de sus usuarios (empleados y contratistas) hacia la seguridad y para preparar a los usuarios a ser más resilientes y vigilantes contra el phishing?

Sí ☐ No ☐

### 2.4 MANEJO DE ACTIVOS

**Objetivo:** Identificar los activos de la organización y definir las responsabilidades de protección apropiadas. Asegurar que la información reciba un nivel apropiado de protección de acuerdo con su importancia para la organización. Evitar la divulgación, modificación, eliminación o destrucción no autorizada de información almacenada en los medios.

1. ¿Usted mantiene un inventario actualizado de dispositivos de software (incl. sistemas operativos) y hardware en sus redes?

Sí ☐ No ☐

2. ¿Usted clasifica información con respecto a su confidencialidad?

Sí ☐ No ☐

3. ¿Se implementan y aplican los procedimientos de etiquetado de información de acuerdo con el esquema de clasificación?

Sí ☐ No ☐

4. ¿Usted brinda orientación sobre cómo manejar la información clasificada?

Sí ☐ No ☐

5. ¿Usted o limita el acceso o encripta la información confidencial almacenada en medios extraíbles, como dispositivos de almacenamiento externos (p.ej. memorias USB, discos duros)?

Sí ☐ No ☐

6. ¿Usted desecha de forma segura los medios que contienen información confidencial si ya no se utilizan?

Sí ☐ No ☐

## 2.5 CONTROL DE ACCESO

**Objetivo:** Limitar el acceso a la información y a las instalaciones de procesamiento de información. Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios. Hacer responsables a los usuarios por salvaguardar su información de autenticación. Evitar el acceso no autorizado a sistemas y aplicaciones.

1. ¿Usted restringe los privilegios de empleados y usuarios externos en función de las necesidades comerciales (especialmente los permisos administrativos y el acceso a datos sensibles como datos personales)?

2. ¿Usted tiene un proceso formal de aprovisionamiento de acceso para asignar y revocar los derechos de acceso?

Sí ☐ No ☐

3. ¿Usted prohíbe los derechos de administrador local en las estaciones de trabajo para los usuarios?

Sí ☐ No ☐

4. ¿Usted revisa los derechos de acceso de los usuarios al menos una vez al año?

Sí ☐ No ☐

5. ¿Usted revoca todo el acceso al sistema, las cuentas de usuarios y los derechos asociados después de la terminación de los usuarios (incl. a empleados, empleados temporales, contratistas y proveedores)?

Sí ☐ No ☐

6. ¿Usted ha implementado una política de contraseñas que impone el uso de contraseñas largas y complejas en su compañía? Contraseñas largas y complejas se definen como: 8 caracteres o más; no consiste en palabras incluidas en los diccionarios; libre de caracteres idénticos, numéricos o alfabéticos consecutivos.

Sí ☐ No ☐

## 2.6 CRIPTOGRAFÍA

**Objetivo:** Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.

1. ¿Está encriptada toda la información confidencial cuando se almacena en dispositivos móviles como laptops o móviles?

Sí ☐ No ☐

2. ¿Usted ha desarrollado e implementado una política sobre el uso, la protección y la duración de las claves criptográficas?

Sí ☐ No ☐

## 2.7 SEGURIDAD FÍSICA Y AMBIENTAL

**Objetivo:** Evitar acceso físico no autorizado, daño e interferencias a la información y a las instalaciones de procesamiento de información. Evitar la pérdida, el daño, el robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

1. ¿Usted mantiene una lista del personal (empleados, proveedores y visitantes) con acceso autorizado a sus predios y áreas de seguridad sensible?

Sí ☐ No ☐

## 2.8 SEGURIDAD OPERACIONAL

**Objetivo:** Garantizar operaciones correctas y seguras de las instalaciones de procesamiento de información. Garantizar que la información y las instalaciones de procesamiento de información estén protegidos contra el malware. Proteger contra la pérdida de datos. Registrar eventos y generar evidencia. Garantizar la integridad de los sistemas operativos. Evitar la explotación de vulnerabilidades técnicas. Minimizar el impacto de las actividades de auditoría en los sistemas operativos.

1. ¿Usted ha implementado procedimientos de gestión de cambios para los sistemas críticos?

Sí ☐ No ☐

2. ¿Está separado el entorno de TI de desarrollo y prueba del entorno de TI productivo?

Sí ☐ No ☐

3. ¿Usted utiliza protección contra malware en proxy web, puerta de enlace de correo electrónico (email-gateway), estaciones de trabajo y computadoras portátiles?

Sí ☐ No ☐

4. ¿Usted realiza copias de seguridad periódicas de datos críticos para el negocio al menos una vez a la semana?

Sí ☐ No ☐

5. ¿Usted produce y revisa regularmente registros de eventos que registran las actividades de los usuarios, excepciones, fallas y eventos de seguridad de la información (al menos desde sus firewalls y controlador de dominio)?

Sí ☐ No ☐

6. ¿Usted ha implementado un proceso de instalación de software centralizado?

Sí ☐ No ☐

7. ¿Usted aplica oportunamente - al menos dentro de un mes del lanzamiento – actualizaciones a sistemas aplicaciones de TI críticos ("parches de seguridad")?

Sí ☐ No ☐

8. ¿Usted garantiza técnicamente y organizativamente que los usuarios no deben instalar software en sus estaciones de trabajo por sí mismo?

Sí ☐ No ☐

## 2.9 SEGURIDAD DE LA COMUNICACIÓN

**Objetivo:** Garantizar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.

1. ¿Están protegidos todos los puntos de acceso a Internet por firewalls apropiadamente configurados?

   Sí ☐ No ☐

2. ¿Usted monitorea su red e identifica eventos de seguridad?

   Sí ☐ No ☐

3. ¿Están todos sus sistemas accesibles por Internet (p.ej. servidores web/de correo electrónico) segregados de su red de confianza (p.ej. dentro de una zona desmilitarizada "DMZ" o en un proveedor externo)?

   Sí ☐ No ☐ No aplica ☐

4. ¿Está encriptada la comunicación confidencial (p.ej., correos electrónicos seguros con SMIME (Secure Multipurpose Internet Mail Extensions) o SMTP-over-TLS (Simple Mail Transfer Protocol Secure))?

   Sí ☐ No ☐

## 2.10 ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

**Objetivo:** Garantizar que la seguridad de la información sea una parte integral de los sistemas de información en todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que brindan servicios a través de redes públicas. Garantizar que la seguridad de la información se diseñe e implemente dentro del ciclo de vida de desarrollo de los sistemas de información. Garantizar la protección de los datos utilizados para las pruebas.

1. ¿Su servidor web encripta los datos confidenciales (p.ej. HTTPS)?

   Sí ☐ No ☐ No aplica ☐

2. ¿Usted hace pruebas de las funcionalidades de seguridad durante el ciclo de vida de desarrollo de los sistemas de información, incluyendo actualizaciones de seguridad de TI?

   Sí ☐ No ☐ No aplica ☐

3. ¿Usted está considerando aspectos de confidencialidad al utilizar datos operacionales para pruebas para garantizar que todos los detalles sensibles estén protegidos por eliminación o modificación?

   Sí ☐ No ☐ No aplica ☐

## 2.11 RELACIONES CON PROVEEDORES

**Objetivo:** Garantizar la protección de los activos de la organización a la que pueden acceder los proveedores. Mantener un nivel acordado de seguridad de la información y entrega de servicios en línea con los acuerdos con los proveedores.

1. ¿Usted ha identificado y documentado todos sus proveedores importantes (incluyendo a proveedores de servicios externos)?

   Sí ☐ No ☐

2. ¿Los acuerdos con proveedores externos de servicios requieren niveles de seguridad proporcionales al nivel de seguridad de su información?

   Sí ☐ No ☐

3. ¿Usted monitorea las actividades de los proveedores de servicios externos para detectar eventos de seguridad a fin de mantener un nivel acordado de seguridad de la información?

   Sí ☐ No ☐

## 2.12 GESTIÓN DE INCIDENTES DE LA SEGURIDAD INFORMÁTICA

**Objetivo:** Garantizar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

1. ¿Usted tiene implementado un plan de respuesta a incidentes de la seguridad de la información?

Sí ☐ No ☐

2. ¿Es conocida por todos los empleados y proveedores externos la línea de informes de un evento de seguridad de la información?

Sí ☐ No ☐

3. ¿Se requiere a los empleados y contratistas que informen una debilidad de seguridad de la información (aún no un incidente o evento) en sistemas o servicios?

Sí ☐ No ☐

4. ¿Usted ha establecido un proceso de escalación para incidentes de la seguridad de la información?

Sí ☐ No ☐

5. ¿Usted utiliza el conocimiento adquirido al analizar y resolver incidentes de seguridad dela información para reducir la probabilidad o el impacto de incidentes futuros?

Sí ☐ No ☐

## 2.13 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

**Objetivo:** La continuidad de la seguridad de la información debe integrarse en los sistemas de gestión de la continuidad del negocio de la organización.

1. ¿Usted ha realizado un análisis de impacto de negocio ("BIA")?

Sí ☐ No ☐

2. ¿Usted tiene implementado un plan de continuidad de negocio que se dirija específicamente a los incidentes cibernéticos?

Sí ☐ No ☐

3. ¿Usted prueba por lo menos anualmente sus planes de continuidad de la seguridad informática (p.ej. Continuidad de negocio, Recuperación de desastre?

Sí ☐ No ☐

4. ¿Sus instalaciones de procesamiento de información (i.e. cualquier sistema, servicio o infraestructura o ubicación física que lo albergue) están implementadas con redundancia?

Sí ☐ No ☐

## 2.14 COMPLIANCE

**Objetivo:** Evitar incumplimientos de obligaciones legales, reglamentarias o contractuales relacionadas a la seguridad de la información y con los requisitos de seguridad. Garantizar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos de la organización.

1. ¿Usted tiene implementado un procedimiento para cumplir de manera permanente con requisitos legales (o contractuales) y regulaciones de privacidad?

Sí ☐ No ☐

2. ¿Usted tiene pautas emitidas sobre la retención, almacenamiento, manejo y eliminación de registros e información?

Sí ☐ No ☐

3. ¿Usted tiene una persona responsable para brindar orientación y garantizar el conocimiento de los principios de privacidad (p. ej. Oficial de Privacidad)?

Sí ☐ No ☐

4. ¿Usted escanea periódicamente los sistemas críticos (incl. pruebas de seguridad, pruebas de penetración) - ya sea por su cuenta o con el apoyo de terceros - en particular cuando se introducen nuevos sistemas y los cambios subsecuentes?

Sí ☐ No ☐

## 3. MANEJO DE VULNERABILIDADES CONOCIDAS (Como por ejemplo Log4shell)

¿Usted revisa periódicamente con proveedores de tecnología internos y/o externos en búsqueda de vulnerabilidades conocidas del estilo Log4Shell o similares?

Sí ☐ No ☐

¿Usted realiza los parches necesarios en forma inmediata referentes a estas Vulnerabilidades Conocidas e implementa medidas correctivas en el corto plazo en caso de que los parches aún no estén disponibles?

Sí ☐ No ☐

¿Usted escanea si sus sistemas han sido vulnerables contra los Indicadores de Compromiso (IoC) y tomó las acciones necesario si usted encuentra cualquier IoC (por ejemplo volver a instalar desde la copia de seguridad y parche)?

Sí ☐ No ☐

## 4. COMENTARIOS ADICIONALES Y FIRMAS (S)

¿Desea agregar más información o detalles sobre su seguridad de la información?

Al firmar este documento (debe ser firmado por el funcionario, el propietario o el gerente), confirmo que soy un representante debidamente autorizado de la empresa con las habilidades técnicas suficientes para proporcionar, según mi mejor conocimiento, respuestas ciertas y completas con respecto a las preguntas dentro de este cuestionario en nombre de la empresa. El cuestionario completado y los anexos opcionales son la base de la cobertura y, por lo tanto, serán parte del contrato de seguro.

| | |
|---|---|
| Fecha | Fecha |
| Firma | Firma |
| Nombre | Nombre |
| Cargo | Cargo |
| Correo electrónico | Correo electrónico |

## ANEXO 1: RESUMEN – ACTIVIDADES INDUSTRIALES

| | |
|---|---|
| Alimentación & Agricultura | Compañías involucradas en la industria alimentaria, incluyendo la producción, transformación, distribución y suministro al por mayor. |
| Autoridad pública; ONG, sin fines de lucro | Agencias gubernamentales nacionales o locales, organizaciones no-gubernamentales y sin fines de lucro |
| Defensa / Contratista Militar | La industria de la defensa incluye el gobierno y la industria comercial, incluyendo la investigación, el desarrollo, la producción y el servicio del material, del equipo y de las instalaciones militares. |
| Educación | Colegios y universidades, distritos escolares independientes y unificados, préstamos a estudiantiles y colegiaturas |
| Energía | Empresas involucradas en la exploración, extracción y desarrollo de reservas de petróleo o gas, perforación de petróleo y gas o empresas de energía integrada. |
| Entretenimiento & Medios | Empresas que ofrecen noticias, información y entretenimiento: radio, televisión, cine, teatro. |
| Fabricación | Compañías fabricando o procesando bienes, sobre todo en grandes cantidades y a través de maquinaría industrial. |
| Minería & Industrias Primarias | Empresas involucradas en la minería, extracción y procesamiento de extracción de minerales, carbón, materias primarias y recursos naturales. |
| Productos farmacéuticos | La industria farmacéutica desarrolla, produce y comercializa fármacos para su uso como medicamentos. Las compañías farmacéuticas pueden tratar medicamentos genéricos o de marca y dispositivos médicos. |
| Propiedad Inmobiliaria & Construcción | Empresas que administran, desarrollan y realizan transacciones de propiedades que consisten en terrenos y edificios, junto con sus recursos naturales, como cultivos, minerales o agua. |
| Salud | Empresas proveedoras de bienes y servicios para el tratamiento de pacientes con atención curativa, preventiva, rehabilitadora y paliativa. |
| Servicios Financieros – Bancos | Empresas dedicadas a banca comercial, instituciones de ahorro, cooperativas de crédito, emisión de tarjetas de crédito, financiamiento, compañías y corredores de hipotecas y préstamos, procesamiento de transacciones financieras, actividades de reserva y cámara de compensación y banca central. |
| Servicios Financieros – Gestión de inversiones | Empresas dedicadas a la gestión de inversiones, negociación y corretaje de valores, negociación de contratos de productos básicos y corretaje, bolsas de valores e inversiones, fondos de inversión y capital de riesgo, adminis- tración de carteras, asesoramiento sobre inversiones y fondos y fideicomisos de entidades legales. |
| Servicios Financieros – Seguros | Aseguradoras directas, compañías de reaseguro y agencias de seguros y corredurías. |
| Servicios profesionales | Ocupaciones que ofrecen asesoramiento y servicios especializados de negocios. Algunos servicios profesionales requieren la tenencia de licencias o cualificaciones profesionales, tales como arquitectos, auditores, ingenieros, médicos y abogados. |
| Tecnología de la información – Hardware | Empresas dedicadas a la fabricación y/o montaje de ordenadores (mainframes, ordenadores personales, estaciones de trabajo, ordenadores portátiles y servidores) y equipos periféricos (p. ej. dispositivos de almacenam iento, impresoras, monitores, etc.) |
| Tecnología de la información – Servicios | Empresas proveedoras de servicios de almacenaje o de procesamiento de datos (incluyendo servicios cloud y streaming); Publicación en internet y contenido de radiodifusión (incluyendo medios sociales); Portales de búsqueda en Internet; Servicios relacionados con el diseño de sistemas informáticos, gestión de instalaciones informáticas, servicios de programación informática y consultoría en hardware o software informático. |

## ANEXO 1: RESUMEN – ACTIVIDADES INDUSTRIALES

| | |
|---|---|
| Tecnología de la información – Software | Empresas que participan en el diseño, desarrollo, documentación y publicación de programas informáticos. |
| Telecomunicaciones | Empresas que facilitan el intercambio de información a través de distancias significativas por medios electrónicos |
| Transporte / Aviación / Aerospacial | Empresas que facilitan el transporte de bienes o clientes. El sector del transporte está compuesto por aerolíneas, ferrocarriles y compañías de transporte. |
| Turismo & Hospitalidad | Empresas que prestan servicios de turismo, viajes, alojamiento, restauración y hostelería. |
| Utilidades | Este sector contiene empresas tales como empresas de electricidad, gas y agua y proveedores integrados. |
| Venta al por menor | Minoristas para el público en general, vendedores de bienes y servicios tanto en tiendas minoristas como en línea, mayoristas y distribuidores. |
| Otros | |