**FORMULARIO DE MUESTRA DEL CUESTIONARIO DE EVALUACIÓN DE RIESGOS DEL PROVEEDOR**

|  |  |
| --- | --- |
| NOMBRE DEL PROVEEDOR | DIRECCIÓN DEL PROVEEDOR |
|   |   |
| PUNTO DE CONTACTO | INFORMACIÓN DE CONTACTO |
|   |   |

INSTRUCCIONES: Por favor, complete este cuestionario en su totalidad, dejando notas y adjuntando documentación de respaldo cuando sea necesario.

**Naturaleza de los datos El proveedor tendrá acceso para** *verificar todo lo que corresponda*

|  |  |  |
| --- | --- | --- |
| **X** | **TIPO DE DATO** | **NOTAS** |
|  | Sin intercambio de datos |  |
|  | Datos demográficos |  |
|  | Datos financieros |  |
|  | Datos personales (por ejemplo, nombre, dirección, número de teléfono) |  |
|  | Datos personales no públicos (por ejemplo, SSN, médicos, propietarios) |  |
|  | Otro:  |  |  |

**POLÍTICAS Y PROCESOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sí** | **No** | **N/A** | **PREGUNTA** | **NOTAS** |
|  |  |  | ¿Su organización documenta, publica y aplica directivas de seguridad? |  |
|  |  |  | ¿Su organización documenta y hace cumplir las políticas de recursos humanos? |  |
|  |  |  | ¿Su organización documenta y aplica directivas para el uso autorizado de servicios en red? |  |

**POLÍTICAS Y PROCESOS continuados**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sí** | **No** | **N/A** | **PREGUNTA** | **NOTAS** |
|  |  |  | ¿Su organización documenta y aplica directivas para el uso autorizado del correo electrónico, Internet e intranet de la empresa? |  |
|  |  |  | ¿Su organización documenta y aplica políticas y estándares de cifrado? |  |
|  |  |  | ¿Su organización documenta y aplica políticas con respecto al almacenamiento, uso y eliminación de datos confidenciales? |  |
|  |  |  | ¿Su organización documenta y aplica políticas con respecto al almacenamiento, uso y eliminación de datos confidenciales por parte de terceros? |  |
|  |  |  | ¿Su organización subcontrata funcionalidades relacionadas con la gestión de la seguridad? |  |
|  |  |  | ¿Las políticas y procedimientos se adhieren y cumplen con las leyes y regulaciones de privacidad relacionadas con la seguridad, ocultación y protección de los datos de los clientes? |  |
|  |  |  | ¿Están bien documentadas las sanciones asociadas con el incumplimiento de las políticas de su organización? |  |
|  |  |  | [Inserte la pregunta Políticas y Procesos Aquí] |  |
|  |  |  | [Inserte la pregunta Políticas y Procesos Aquí] |  |
|  |  |  | [Inserte la pregunta Políticas y Procesos Aquí] |  |

**MEDIDAS DE SEGURIDAD FÍSICAS Y DEL CENTRO DE DATOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sí** | **No** | **N/A** | **PREGUNTA** | **NOTAS** |
|  |  |  | ¿Su organización revisa y evalúa regularmente los riesgos físicos y ambientales? |  |
|  |  |  | ¿Los controles perimetrales del centro de datos implican el uso de tarjetas de acceso? |  |
|  |  |  | ¿Los controles perimetrales del centro de datos implican el uso de controles de teclado? |  |
|  |  |  | ¿Los controles perimetrales del centro de datos implican el uso de guardias de seguridad? |  |
|  |  |  | ¿Los controles perimetrales del centro de datos implican el uso de \_\_[agregue la medida aquí]\_\_? |  |
|  |  |  | ¿Tiene procedimientos de continuidad del negocio implementados si la oficina es inaccesible por cualquier motivo? |  |
|  |  |  | ¿Todos los equipos de red están físicamente protegidos? |  |
|  |  |  | ¿Su organización utiliza proveedores de centros de datos? |  |
|  |  |  | ¿Su organización utiliza registros de visitantes? Si es así, ¿se mantienen durante más de 30 días? |  |
|  |  |  | ¿Su organización mantiene una política escrita con respecto a los requisitos de seguridad física para la oficina? |  |
|  |  |  | [Inserte la pregunta de seguridad física y del centro de datos aquí] |  |
|  |  |  | [Inserte la pregunta de seguridad física y del centro de datos aquí] |  |

**MEDIDAS DE SEGURIDAD CONTRA MALWARE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sí** | **No** | **N/A** | **PREGUNTA** | **NOTAS** |
|  |  |  | ¿Se analizan todos los correos electrónicos en busca de virus? |  |
|  |  |  | ¿Se requiere y habilita el software antivirus en todos los equipos de la red? |  |
|  |  |  | ¿El software antivirus tiene una frecuencia establecida de análisis en los equipos de la red? |  |
|  |  |  | ¿Su organización permite la instalación de software no aprobado en equipos de red? |  |
|  |  |  | [Inserte la pregunta de seguridad de malware aquí] |  |
|  |  |  | [Inserte la pregunta de seguridad de malware aquí] |  |
|  |  |  | [Inserte la pregunta de seguridad de malware aquí] |  |

**MEDIDAS DE SEGURIDAD DE LA INFORMACIÓN**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sí** | **No** | **N/A** | **PREGUNTA** | **NOTAS** |
|  |  |  | ¿Su organización cuenta con un programa de seguridad de la información? (En la columna de notas, proporcione un enlace a todas las políticas de seguridad y privacidad relevantes de cara al público). |  |
|  |  |  | Si su organización tiene un programa de seguridad de la información, ¿se aplica a todas las operaciones y sistemas que procesan datos confidenciales? |  |
|  |  |  | ¿El personal y los gerentes relevantes están certificados profesionalmente en seguridad de la información? |  |
|  |  |  | ¿El acceso a nivel de administrador está limitado en la infraestructura de red? |  |
|  |  |  | ¿Existen controles estrictos para acceder a los registros de seguridad? |  |
|  |  |  | [Inserte la pregunta de seguridad de la información aquí] |  |
|  |  |  | [Inserte la pregunta de seguridad de la información aquí] |  |
|  |  |  | [Inserte la pregunta de seguridad de la información aquí] |  |

**MEDIDAS DE SEGURIDAD DE LA INFRAESTRUCTURA DE RED**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Sí** | **No** | **N/A** | **PREGUNTA** | **NOTAS** |
|  |  |  | ¿Su organización mantiene una directiva de seguridad de red? |  |
|  |  |  | ¿Todos los routers están sistematizados con listas de control de acceso para sofocar el tráfico no autorizado? |  |
|  |  |  | ¿Los sistemas operativos de servidor están parcheados al último nivel? |  |
|  |  |  | ¿Tiene su organización un proceso para rastrear y comunicar parches de vulnerabilidad? |  |
|  |  |  | ¿Su organización realiza una copia de seguridad de sus datos? |  |
|  |  |  | ¿Se almacenan y prueban las copias de seguridad? |  |
|  |  |  | ¿Los dispositivos de los empleados están encriptados? |  |
|  |  |  | ¿Se utiliza un tercero para probar la seguridad de la infraestructura de red? |  |
|  |  |  | ¿Emplean sistemas de detección de intrusos? |  |
|  |  |  | [Inserte la pregunta de seguridad de la infraestructura de red aquí] |  |
|  |  |  | [Inserte la pregunta de seguridad de la infraestructura de red aquí] |  |
|  |  |  | [Inserte la pregunta de seguridad de la infraestructura de red aquí] |  |

|  |
| --- |
| **INFORMACIÓN ADICIONAL** |
|  |

|  |  |  |
| --- | --- | --- |
| NOMBRE Y TÍTULO DEL EVALUADOR DE RIESGOS | FIRMA | FECHA |
|  |  |  |

|  |
| --- |
| **RENUNCIA**Cualquier artículo, plantilla o información proporcionada por Smartsheet en el sitio web es solo para referencia. Si bien nos esforzamos por mantener la información actualizada y correcta, no hacemos representaciones o garantías de ningún tipo, expresas o implícitas, sobre la integridad, precisión, confiabilidad, idoneidad o disponibilidad con respecto al sitio web o la información, artículos, plantillas o gráficos relacionados contenidos en el sitio web. Por lo tanto, cualquier confianza que deposite en dicha información es estrictamente bajo su propio riesgo. |