**PLANTILLA DE PLAN DE
SEGURIDAD DE DATOS**

**Pruebe Smartsheet GRATIS**

PLAN DE SEGURIDAD DE DATOS

NOMBRE DE LA EMPRESA

Domicilio

Ciudad, estado y código postal

webaddress.com

Versión 0.0.0

00/00/0000

| HISTORIAL DE VERSIONES |
| --- |
| VERSIÓN | APROBADO POR | FECHA DE REVISIÓN | DESCRIPCIÓN DEL CAMBIO | AUTOR |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. **IDENTIFICACIÓN DEL SISTEMA**

Detalles sobre el sistema, el propietario del sistema, cantidad de usuarios

1. **ENTORNO DEL SISTEMA**

Detalles sobre las interconexiones de sistemas, los dispositivos clave, los componentes de hardware y software

1. **REQUISITOS**

Detalles sobre los requisitos de seguridad de datos aplicables

* 1. **Control de acceso**

Garantice que el sistema limite el acceso a usuarios autorizados, establezca el tipo de transacciones permitidas, limite ciertas funciones a los usuarios que cuentan con privilegios, supervise el acceso remoto, controle la conexión de dispositivos móviles

* 1. **Sensibilización y capacitación**

Asegúrese de que todos en la organización conozcan los riesgos de seguridad del sistema, estén capacitados adecuadamente para realizar las actividades de una manera que proteja los datos, y comprendan los indicadores de amenazas o infiltraciones

* 1. **Auditoría y rendición de cuentas**

Asegúrese de que la organización tenga un sistema continuo que supervise cualquier actividad inusual o no autorizada en el sistema

* 1. **Gestión de configuraciones**

Establezca y mantenga configuraciones de referencia en todo el sistema, incluido el software de control y supervisión instalado por el usuario

* 1. **Identificación y autenticación**

Asegúrese de que el sistema pueda identificar a los usuarios y los dispositivos del sistema, aplique una complejidad mínima de contraseñas

* 1. **Respuesta a incidentes**

Establezca un sistema que realice un seguimiento, documente e informe los incidentes que pueden haber comprometido la seguridad y prueba la capacidad de la organización para responder a un incidente

* 1. **Mantenimiento**

Realice un mantenimiento continuo del sistema

* 1. **Protección de medios**

Limite el acceso a los medios digitales del sistema a los usuarios autorizados y asegúrese de que los medios digitales se mantengan seguros de otras maneras

* 1. **Seguridad del personal**

Examine a las personas antes de permitir el acceso al sistema y asegúrese de que el sistema esté protegido después de que las personas abandonen la organización

* 1. **Protección física**

Limite el acceso a los sistemas y equipos físicos a las personas autorizadas

* 1. **Evaluación de riesgos**

Evalúe periódicamente los riesgos de seguridad en el funcionamiento normal del sistema, analice las vulnerabilidades y realice correcciones cuando se encuentren vulnerabilidades

* 1. **Evaluación de seguridad**

Evalúe periódicamente los controles de seguridad para asegurarse de que son efectivos y realice correcciones cuando sea necesario

* 1. **Protección del sistema y las comunicaciones**

Supervise y proteja las comunicaciones que el sistema recibe desde fuera del sistema

* 1. **Integridad del sistema y la información**

Identifique, informe y corrija los defectos del sistema en tiempo y forma, proporcione protección contra códigos maliciosos y supervise las alertas y avisos de seguridad

|  |
| --- |
| **RENUNCIA**Todos los artículos, las plantillas o la información que proporcione Smartsheet en el sitio web son solo de referencia. Mientras nos esforzamos por mantener la información actualizada y correcta, no hacemos declaraciones ni garantías de ningún tipo, explícitas o implícitas, sobre la integridad, precisión, confiabilidad, idoneidad o disponibilidad con respecto al sitio web o la información, los artículos, las plantillas o los gráficos relacionados que figuran en el sitio web. Por lo tanto, cualquier confianza que usted deposite en dicha información es estrictamente bajo su propio riesgo. |