
CIUDAD
INTELIGENTE
Linea de Tiempo
@MaraCarlaSilve2
SIGESTIC'23

¿LOS SERVICIOS PÚBLICOS UTILIZADOS DE MANERA TRADICIONAL SON MÁS SEGUROS QUE EL USO DE SERVICIOS ELECTRÓNICOS?

¿PUEDEN LOS GOBIERNOS LOCALES O CUALQUIER PERSONA CONOCER TODA LA INFORMACIÓN DE LOS CIUDADANOS?

¿ESTÁN PROTEGIDAS LAS INFRAESTRUCTURAS CRÍTICAS DE LA CIUDAD?

¿TIENEN DISPOSITIVOS IOT CON SUFICIENTE SEGURIDAD?

¿EXISTEN LEYES QUE REGULAN LA SEGURIDAD DE LA INFORMACIÓN PERSONAL Y LAS INFRAESTRUCTURAS CRÍTICAS?

2

IMPLEMENTACIÓN

GARANTIZAR QUE LOS SISTEMAS FUNCIONAN DE MANERA SEGURA

OPERACIÓN Y MANTENIMIENTO

3

SOPORTE, SEGUIMIENTO Y SUPERVISIÓN

1

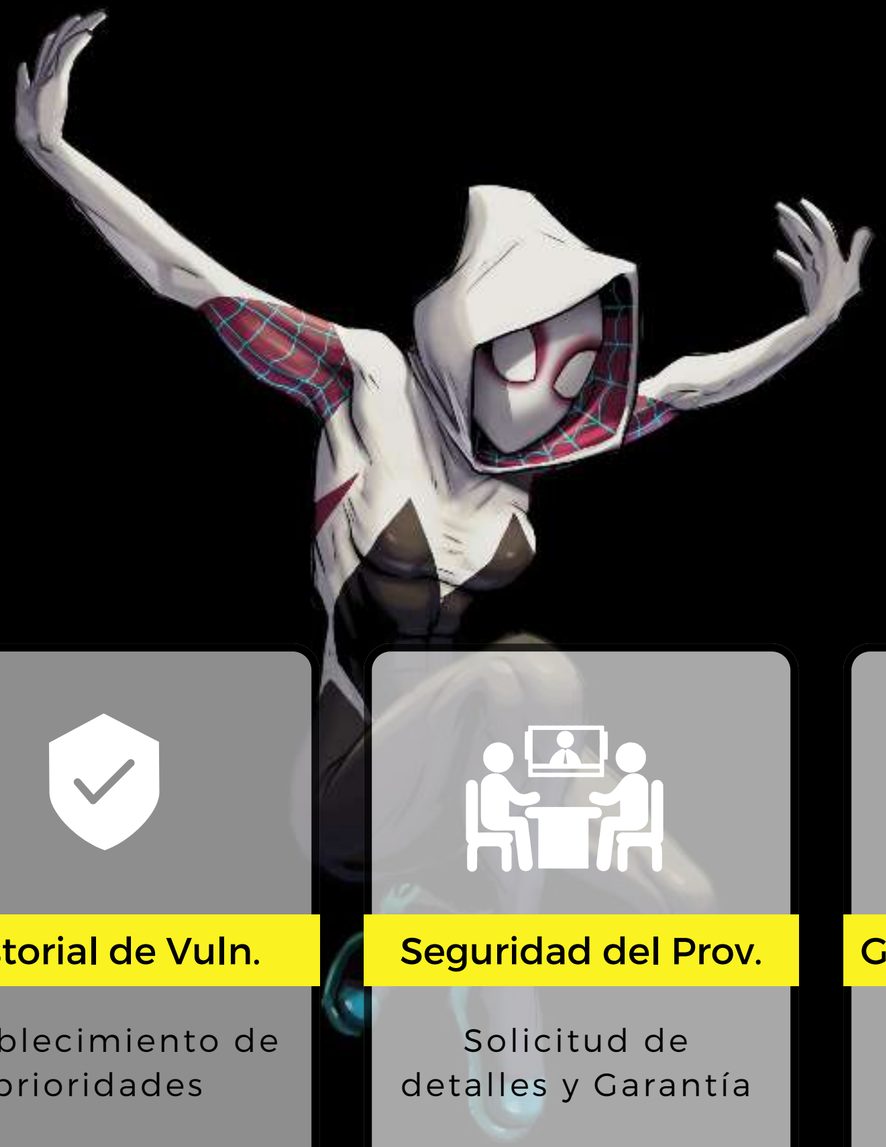
SELECCIÓN

CARACTERÍSTICAS DE SEGURIDAD ADECUADAS

DISPOSICIÓN

4

ELIMINACIÓN DE TECNOLOGÍA



SELECCIÓN

ESTABLECIMIENTO DE UNA LÍNEA BASE PARA AUDITAR EL COMPORTAMIENTO DEL SISTEMA.

Diseño y Planificación

Postura de seguridad de los productos y servicios

Historial de Vuln.

Establecimiento de prioridades

Seguridad del Prov.

Solicitud de detalles y Garantía

Gestión de Productos

Visibilidad

Pruebas

Verificación

ETAPA DE DISEÑO Y PLANIFICACIÓN

REQUISITOS BÁSICOS DE SEGURIDAD

1. CAPACIDADES DE:
   - Autenticación
   - Autorización
   - Auditoría
   - Alerta
   - Registro
   - contra Manipulación
2. CRIPTOGRAFÍA SÓLIDA PARA PROTEGER LOS DATOS
3. ACTUALIZACIÓN AUTOMÁTICA Y SEGURA DE SW, FW

ETAPA DE DISEÑO Y PLANIFICACIÓN

REQUISITOS BÁSICOS DE SEGURIDAD

4. A PRUEBA DE FALLAS /CIERRE

5. SIN CUENTAS DE PUERTA TRASERA/INDOCUMENTADAS /CODIFICADAS

6. ACUERDO A NIVEL DE SERVICIO:
   - características específicas de seguridad
   - demostración de cumplimiento
   - soluciones ante fallas

HISTORIAL DE VULNERABILIDADES

MADUREZ DE LOS PRODUCTOS

1. PREOCUPACIÓN DEL PROVEEDOR ANTE LA EXPOSICIÓN A LA SEGURIDAD DE SUS PRODUCTOS

2. TIEMPO QUE TARDA UN PROVEEDOR EN PARCHEAR LAS VULNERABILIDADES DE SEGURIDAD Y QUÉ TAN FÁCIL ES APLICAR LOS PARCHES.

3. HÁBITOS EN EL DESARROLLO DE SW

SEGURIDAD DEL PROVEEDOR

PRODUCTOS

1. REVISIONES DE CÓDIGO INDEPENDIENTES Y PRUEBAS DE PENETRACIÓN REGULARES EN SUS PRODUCTOS, REDES Y SISTEMAS

2. PROTECCIÓN DEL ENTORNO DE DESARROLLO Y PI CONTRA EL ESPIONAJE O LA MANIPULACIÓN.

3. APLICACIÓN DE LA SEGURIDAD EN LA CADENA DE SUMINISTRO

4. POLÍTICA DE DIVULGACIÓN Y NOTIFICACIÓN Y CANALES DE CONTACTO

11

GESTIÓN DE PRODUCTOS

PRODUCTOS

1. INTERFACES DE ADMINISTRACIÓN QUE:

- monitoreen el estado y la estabilidad de la operación
- correlacionen las actividades de registro
- sean compatibles con múltiples dispositivos y fuentes.

2. LA GESTIÓN CENTRALIZADA DE SOLUCIONES INTELIGENTES

PRUEBAS

PRODUCTOS

1. CUMPLIMIENTO DE LOS REQUISITOS BÁSICOS DE SEGURIDAD DEFINIDOS EN LA ETAPA DE PLANIFICACIÓN Y DISEÑO.
2. PRUEBAS DE PENETRACIÓN
3. ENDURECIMIENTO DEL SISTEMA
4. CERTIFICACIÓN
5. VERIFICACIÓN Y VALIDACIÓN DE LA SEGURIDAD OPERATIVA.

2

IMPLEMENTACIÓN

IMPLANTACIÓN DE LA TECNOLOGÍA

GARANTIZAR

1. Cumplimiento
2. Entrega
3. Cifrado
4. Administración
5. Contraseñas
6. Cuentas de usuarios innecesarias
7. Funciones y servicios no utilizados
8. Auditoría de eventos
9. Mecanismos contra la manipulación y el vandalismo

3

OPERACIÓN Y MANTENIMIENTO

SOPORTE, SEGUIMIENTO Y SUPERVISIÓN

1. Monitoreo
2. Parches
3. Evaluación y auditoría periódica
4. Protección del entorno de registro
5. Control de acceso
6. Reacción de compromiso y recuperación

4

DISPOSICIÓN

POLÍTICAS ESPECÍFICAS PARA DESECHAR LA TECNOLOGÍA DE FORMA SEGURA

1. Evitar la reutilización de la tecnología por parte de la misma organización o de terceros.

2. Borrar de forma segura los datos del almacenamiento de los sistemas o destruir el almacenamiento.

3. El reemplazo del proveedor, se espera que estos proporcionen una eliminación segura de la tecnología como parte de sus servicios y contrato de mantenimiento con la organización del cliente.

4

CIUDAD INTELIGENTE

Linea de Tiempo

@MaraCarlaSilve2