POLÍTICA DE ADQUISICIÓN DE LOS SISTEMAS DE INFORMACIÓN

DESYSWEB

Lima - Perú

CONTENIDO

1. OBJETIVO 3

2. ALCANCE 3

3. DEFINICIONES 3

4. POLÍTICA 3

4.1.1 Análisis y especificación de los requisitos de seguridad 3

4.1.2 Aseguramiento de los servicios de aplicación en las redes públicas 5

4.1.3 Transacciones en línea 6

1. OBJETIVO

El objeto de este apartado es la aplicación controles para la seguridad de la información al ciclo de vida completo de los sistemas de información, tanto propios como subcontratados.

2. ALCANCE

Aplica a todo el personal que labora en Desysweb S.A.C.

3. DEFINICIONES

Están detalladas en la Norma Internacional ISO/IEC 27000:2016 "Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Información general y vocabulario".

4. POLÍTICA

4.1.1 Análisis y especificación de los requisitos de seguridad

Desysweb S.A.C. analiza los requisitos y especificaciones de seguridad de la información. Cuando se diseña un sistema se presta gran atención a los requisitos funcionales y operativos. Desysweb S.A.C. deberá incluir requisitos para la seguridad de la información en la fase de especificación de condiciones para sistemas de información. Esto supone tener en cuenta la seguridad además de las funcionalidades requeridas por una aplicación o sistema.

Los requisitos de seguridad deben tener en cuenta valoraciones del impacto en el negocio de posibles fallos de seguridad (daño potencial)

Tenga en cuenta la principal ventaja de prever requisitos de seguridad en las fases tempranas es el ahorro de costes ya que un rediseño puede ser mucho más costoso sin contar con los daños potenciales de los fallos no previstos en la seguridad

Para ello podemos tener en cuenta factores como:

- ¿Qué nivel de confianza requiere la aplicación? Con ello podremos determinar los requisitos de autenticación.
- Especificaciones de la provisión de accesos para
    - Usuarios
- Usuarios privilegiados y técnicos de mantenimiento
- ¿Qué funciones y responsabilidades requiere de los usuarios?
- ¿Qué necesidades de protección tienen los activos involucrados? (análisis de riesgos)
- ¿Qué requisitos de seguridad se derivan de los procesos del negocio?
    - Registros de transacciones
    - Supervisión y monitoreo
    - Requisitos de no-repudio
    - Otros
- ¿Qué otros controles de seguridad son aplicables?
    - Interfaces para el registro y supervisión
    - Sistemas de detección de fugas de datos
    - Otros

En el caso de servicios a través de redes públicas hay controles específicos en los puntos siguientes 14.1.2 y 14.1.3

En el caso de compras de aplicaciones a terceros, Desysweb S.A.C. establecerá como control de seguridad:

- Procesos de compras formales que incluyan periodos de prueba y validación del producto
- Aplicar criterios de evaluación de riesgos para tomar medidas de control adicionales si el producto no satisface totalmente las necesidades de seguridad

- A la hora de integrar un software en aplicaciones o sistemas propios considere si es necesario configurar las aplicaciones, sistemas y Software a implantar en relación a la seguridad. Elabore procedimientos y asegúrese de que se implementan
- Defina protocolos de homologación y aceptación de productos de forma que se incluyan siempre criterios de seguridad de la información
- Aplique los criterios de aceptación de productos en actualizaciones de Software y en nuevas funcionalidades de productos en cuanto a criterios de seguridad. Una nueva funcionalidad puede ser muy interesante pero no debe vulnerar la seguridad de nuestros sistemas para que sea aceptable.

4.1.2 Aseguramiento de los servicios de aplicación en las redes públicas

Desysweb S.A.C. asegura los servicios de aplicaciones en redes públicas. Cuando las aplicaciones de la organización están accesibles mediante redes públicas, por ejemplo, Internet, están sujetas a mayores riesgos que cuando solo están accesibles a través de las redes controladas por la organización. Por ello es necesario considerar medidas de protección adicionales, como el cifrado de las comunicaciones, los mecanismos de autenticación a utilizar, la identificación válida del origen y del destino mediante el uso de certificados, etc.

Si utilizamos redes públicas para la transmisión de información sensible o para acceder a las aplicaciones deberemos tener en cuenta controles adicionales pues las redes públicas como internet suponen un riesgo adicional importante que debemos tener en cuenta si queremos salvaguardar nuestra información

En este caso hemos de valorar:

- El cifrado de las comunicaciones.
- Sistemas múltiples de autenticación.
- Uso de certificados digitales (Identificación segura de origen y destino).
- Sistemas de prevención de envío de información no permitida en redes públicas.

- Sistemas de protección para envíos involuntarios de archivos.

4.1.3 Transacciones en línea

Protección de las transacciones de servicios de aplicaciones. La información implicada en las transacciones en línea debe generarse y custodiarse de manera segura, evitando riesgos como la transmisión incompleta, errores de enrutamiento, mensajes no autorizados, alteración, divulgación, duplicación de mensajes o reproducción autorizada. Este tipo de información podría requerir validez legal siendo recomendable recurrir a terceros de confianza, por ejemplo, para la generación de certificados y firmas digitales.

Se trata de controles que garanticen la protección de las transacciones entre aplicaciones.

Los controles se han de aplicar para evitar

- Transacciones incompletas
- Errores de enrutamiento
- Mensajes no autorizados
- Alteración de los datos
- Divulgación de la información
- Duplicación de mensajes o reproducción no autorizada.

Para ello Desysweb S.A.C. deberá analizar la aplicabilidad de contar con controles tales como:

- Uso de firma digital para garantizar las comunicaciones extremo a extremo
- Validación y verificación de autenticación en toda la cadena de transmisión
- El canal de comunicación es cifrado para garantizar la confidencialidad de las transmisiones
- La utilización de protocolos seguros

- Los datos de las transacciones se guardan en lugares no accesibles desde la red (Intranet, Entornos CLOUD etc.)
- La obtención de firmas digitales se debe garantizar que la seguridad se integra e incorpora a través de todo el proceso completo de gestión del certificado o firma.
- De poco valdría trabajar con una autoridad confiable si para obtener los certificados lo vamos publicando al no contar con métodos seguros para obtenerlos.