PROTECCIÓN DE LA INFORMACIÓN EN SUS 3 ESTADOS

DESARROLLO DE SOFTWARE SEGURO

- Jorge Ibarra Peña
- 20310025
- 7°P
- Desarrollo de Software
- 21/08/2023
- CETI COLOMOS

Existen 3 estados de la información las cuales son: “**Procesamiento, Almacenamiento** y **TRANSMISIÓN**”

EXPLICACIÓN

PROCESAMIENTO

Para implantar correctamente la protección de datos hay que seguir un proceso organizado.

Los procesos de protección de datos se realizan de forma ordenada y responsable, evaluando las características de la empresa en cuestión

- Elaboración de un cuestionario de conocimiento de la organización
- Enfoque de riesgos: Análisis-diagnóstico de los datos preexistentes
- Principios de responsabilidad activa.
- Medidas de responsabilidad activa:
  - 1.- Registro de actividades de tratamiento
  - 2.- Protección de datos desde el diseño y por defecto
  - 3.- Medidas de seguridad
  - 4.-Notificación de las violaciones de seguridad de los datos
  - 5.- Evaluación de impacto sobre la protección de datos
- Principio de transparencia e información a los afectados
  - 1.- Obligaciones para los responsables de tratamiento
  - 2.- Relaciones entre los responsables y los encargados del tratamiento
  - 3.- Recogida de la información
  - 4.- Ejercicio de los derechos de acceso, rectificación, cancelación, oposición, supresión, limitación del tratamiento y de portabilidad
- Análisis y elaboración de los contratos entre los responsables y encargados, personal con accesos y también con los servicios externalizados (informática, prevención de riesgos laborales, asesoramiento fiscal o laboral), ya sea directamente o por subcontratación.
- Funciones y obligaciones del delegado de protección de datos, si es preceptivo.
- Elaboración de documentación acreditativa de toda la implantación exigida por la legislación
- Auditoría final de implantación
- Asesoramiento técnico de mantenimiento
- Auditorías periódicas o bienales de verificación

ALMACENAMIENTO

Uno los aspectos que será necesario considerar desde el momento en que se planifique la investigación, es la forma en la cual se almacenarán los datos que serán generados o recopilados.

Al hacer esto, es importante tener en cuenta que los medios de almacenamiento y respaldo podrán variar dependiendo de las necesidades de los investigadores, y que las opciones utilizadas a lo largo del desarrollo de la investigación no necesariamente serán apropiadas para almacenar y dar acceso a los datos una vez que ésta haya finalizado.

Los medios de almacenamiento que se pueden utilizar no son excluyentes, por lo que pueden complementarse entre sí. Algunos de los tipos de solución más comunes que se pueden utilizar durante y después de la investigación son:

Almacén de datos personal o del proyecto (por ejemplo, utilizando discos USB, discos duros de laptops o unidades en red dentro de la institución)

- Repositorio institucional
- Almacén de datos institucional
- Infraestructura de almacenamiento nacional
- Almacén de datos en la nube
- Repositorio disciplinar

TRANSMISIÓN

Para proteger los datos cuando fluyen por una red que no sea de confianza, como Internet, debe aplicar las medidas de seguridad pertinentes. Estas medidas son la capa de sockets segura (SSL)

El establecimiento de una red de perímetro garantiza en parte una separación física entre la red interna e Internet. Esta separación disminuye los riesgos de Internet a los que son vulnerables los sistemas internos de la compañía. Al designar este nuevo sistema como servidor solo de Internet, la compañía también disminuye la complejidad que supone gestionar la seguridad de la red.

El protocolo SSL es un estándar del sector para proteger las comunicaciones entre clientes y servidores. SSL se desarrolló originalmente para las aplicaciones de navegador Web, pero son cada vez más las aplicaciones que pueden utilizar SSL. En el caso del sistema operativo i5/OS, son las siguientes:

- IBM HTTP Server para i5/OS (original y basado en Apache)
- Servidor FTP
- Servidor Telnet
- La arquitectura de bases de datos relacionales distribuidas (DRDA) y el servidor de gestión de datos distribuidos (DDM)
- Management Central de System i Navigator
- Servidor de servicios de directorio (LDAP)
- Aplicaciones IBM i Access for Windows, incluido System i Navigator, y aplicaciones escritas en el conjunto de interfaces de programación de aplicaciones (API) de IBM i Access for Windows
- Programas desarrollados con Developer Kit para Java™ y aplicaciones de cliente que utilizan IBM Toolkit para Java
- Programas desarrollados con las interfaces de programación de aplicaciones (API) de la capa de sockets segura (SSL), que sirven para habilitar SSL en las aplicaciones. En el tema Interfaces API de la capa de sockets segura (SSL) hallará más información sobre cómo escribir programas que empleen SSL.

FORMAS DE PROTECCIÓN

Procesamiento de Datos:

- **Acceso Restringido**: Limitar el acceso a los datos sensibles solo a personal autorizado mediante autenticación de dos factores.
- **Encriptación en Tránsito**: Utilizar conexiones seguras (HTTPS) para garantizar que los datos se transmitan de forma segura entre dispositivos durante el procesamiento.
- **Auditoría de Acceso**: Registrar y monitorizar todas las actividades relacionadas con el procesamiento de datos para detectar cualquier actividad sospechosa o no autorizada.
- **Pseudonimización**: Reemplazar identificadores de datos personales con identificadores únicos generados aleatoriamente durante el procesamiento para proteger la privacidad.
- **Políticas de Retención de Datos**: Establecer reglas claras sobre cuánto tiempo se pueden retener los datos y cuándo deben eliminarse de forma segura una vez que ya no sean necesarios.

Almacenamiento de Datos:

- **Encriptación de Datos en Reposo**: Almacenar datos sensibles en dispositivos o servidores encriptados para protegerlos de accesos no autorizados.
- **Acceso Basado en Roles**: Definir roles y permisos de usuario para controlar quién tiene acceso a qué datos almacenados.
- **Duplicación de Datos (Backups):** Realizar copias de seguridad regulares de los datos y almacenarlas de forma segura en ubicaciones separadas para la recuperación en caso de pérdida o daño.
- **Control de Acceso Físico**: Limitar el acceso físico a los servidores o sistemas de almacenamiento mediante medidas de seguridad física, como cerraduras y sistemas de alarma.
- **Evaluación de Vulnerabilidades:** Realizar análisis regulares de seguridad para identificar y mitigar posibles vulnerabilidades en el almacenamiento de datos.

Transmisión de Datos:

- **Encriptación de Datos en Tránsito**: Utilizar protocolos de encriptación (por ejemplo, SSL/TLS) para proteger los datos mientras se transmiten a través de redes públicas o privadas.
- **VPN (Red Privada Virtual**): Implementar una VPN para crear un túnel seguro a través del cual los datos se transmiten de forma protegida en redes no seguras.
- **Firewalls**: Configurar firewalls para controlar y filtrar el tráfico de red, evitando accesos no autorizados durante la transmisión.
- **Políticas de Eliminación de Datos**: Establecer políticas que requieran la eliminación segura de datos transmitidos una vez que se hayan entregado de manera segura.
- **Autenticación Mutua**: Utilizar autenticación de doble factor o autenticación mutua para garantizar que tanto el remitente como el receptor sean quienes dicen ser antes de la transmisión de datos críticos.

¿Cuál es el más inseguro?

Personalmente siento yo que el más inseguro es el procesamiento de datos debido a que hay más posibilidades de encontrar vulnerabilidades que en los otros, ya que por ejemplo, un acceso restringido es posible que con algunos trucos puedas acceder aunque la empresa no lo sepa y no tengas la autorización, como un hackeo y listo.

Más familiarizado y formas que protejo la información

Estoy más familiarizado con el almacenamiento, debido a que siempre suelo tener información en otros apartados como discos duros externos y USBS ya que antes solía tener mucha información y solía formatear mis dispositivos muy seguidos, por eso adopte la opción del almacenamiento ya que estoy más familiarizado. Dos ejemplos como anteriormente dije son discos duros, en este caso tengo el disco con sus fragmentaciones en el cual tengo Linux donde ahí guardo información importante, y en otro fragmento del disco guardo otra información donde desde el mismo Windows puedo entrar. Y suelo tener una USB normalmente conmigo con información no tan importante, pero si relevante o para alguna emergencia. Donde tengo todo realmente es en el Disco duro

CONCLUSIÓN

La forma en la que podemos proteger nuestra información varia mucho ya que depende de que es lo que realices es como las cosas te pueden Salir bien o mal, ya que todo tiene sus beneficios y sus contras ya que, en el procesamiento, no te salvas a ser hackeado; en el almacenamiento, no te salvas de tener algún apagón y perder tus datos, o en caso de USB, que se te extravíe y no vuelvas a ver esa información. Y la transmisión de datos tampoco debido a que es poco probable que burlen por ejemplo el firewall y puedan llegar a ti. Es complicado, pero no imposible y más si llegas a instalar algo y te pida que desbloquee el firewall para poder ser instalado. Todo es importante sin duda alguna, pero siempre hay que tener la precaución de que estamos en paginas seguras y de que la información esta completamente asegurada antes de ingresarla a la aplicación o a la página

BIBLIOGRAFÍA

Proceso de protección de datos | Prevedata. (s. f.). https://www.prevedata.com/los-procesos-de-proteccion-de-datos

Biblioguias: Gestión de datos de investigación: respaldo y almacenamiento. (s. f.). https://biblioguias.cepal.org/c.php?g=495473&p=4398069

IBM documentation. (s. f.). https://www.ibm.com/docs/es/i/7.2?topic=security-transmission-options