DEVICE LOCK, UNA ALTERNATIVA A LA SEGURIDAD INFORMATICA EN EL ORGANO DE FISCALIZACIÓN SUPERIOR PERIODO 2013-2015

Raúl De La Fuente Izaguirre*
José Martín Cadena Barajas&

INTRODUCCIÓN

La administración pública es la actividad que se desarrolla en el organismo del estado para el cumplimiento de los fines del mismo. Los organismos adscritos tienen una relación de dependencia con un nivel central siendo las tecnologías de la información y comunicación (Tic's) un canal por medio del cual existe esa comunicación convirtiéndose la información en un activo muy importante para ambos.

Según (Chiavenato, 2006) el concepto de información representa mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones

Para (Ferrel & Hirt, 2004), la información comprende los datos y conocimientos que se usan en la toma de decisiones.

Desde la perspectiva de (Czinkota & Masaaki, 2001) la información consiste en datos seleccionados y ordenados con un propósito específico.

* Maestro en Tecnologías de la Información. Ingeniero en Sistemas Computacionales. radelafuente@uv.mx
& Maestro en Matemáticas. Licenciado en Matemáticas. jcadena@orfis.gob.mx

Desde un punto de vista informático la definición un dato es la unidad mínima de información, pero para (Toffler & Toffler, 2006) la diferencia radica en:

> Los datos suelen ser descritos como elementos discretos, huérfanos de contexto: por ejemplo, 300 acciones. Cuando los datos son contextualizados, se convierten en información: por ejemplo, tenemos 300 acciones de la empresa farmacéutica X.

Una de las principales problemáticas que enfrentan todas las organizaciones sean públicas o privadas es la administración de la seguridad de la información que viaja desde una red de área local (LAN) o bien tiene salida por medio de la Internet, desde una postura personal la seguridad de esta información es entendida como una ausencia de peligro o riesgo en la organización. Ante tal situación las Tic's son una pieza fundamental para evitar posibles amenazas hacia el principal activo de las instituciones.

Castells (1996) define a las Tic´s como el conjunto convergente de tecnologías de la microelectrónica, la informática, las telecomunicaciones, televisión, radio y la optoelectrónica.

Ávila (2007) define el concepto de internet como uno de los servicios principales y de más uso a nivel empresarial, el cual consiste de un conjunto de redes interconectadas a escala mundial con la particularidad de que cada una de ellas es independiente y autónoma.

Existen múltiples herramientas de tecnología que apoyan en la seguridad informática de la información, las cuales las podemos atacar desde cuestiones elementales como una configuración a los registro del sistema operativo, de manera física

desconectando componentes de la unidad centra de proceso (CPU) o de manera automatizada y remota vía una LAN o mediante servicios a través de internet, que no es otra cosa que la denominada nube informática.

EL ORFIS Y LA SEGURIDAD INFORMÁTICA

El Órgano de Fiscalización Superior es un organismo autónomo del Estado dotado de personalidad jurídica y patrimonio propios, autonomía técnica, presupuestal y de gestión, que apoya al Congreso en el desempeño de su función de fiscalización superior, y tiene la competencia que le confieren la Constitución Política de los Estados Unidos Mexicanos, la Constitución Política del Estado, la Ley de Fiscalización Superior y Rendición de Cuentas para el Estado y demás legislación aplicable (Orfis, 2016).

La visión del ORFIS es la consolidación de la imagen institucional con una dinámica estable y técnicamente fortalecida, que convalide la confianza de la Población y de los Entes Fiscalizables en los procesos y resultados de las auditorías, así como en las acciones posteriores que impactan favorablemente en la gestión pública. Su misión es hacer de la Fiscalización Superior el instrumento eficaz que estimule el control, la transparencia y la rendición de cuentas en los Entes Fiscalizables, dando cumplimiento al mandato legal que da origen a nuestra Institución (Orfis, 2016).

Además de contar con su política de integridad la cual garantiza la más alta probidad y confiabilidad en las funciones que desarrollan, dentro y fuera de la Institución, el personal del Órgano de Fiscalización Superior del Estado de Veracruz (ORFIS), deberá conducirse con independencia, objetividad y rigor técnico, enalteciendo la honestidad, la ética y el profesionalismo, debiendo ser intachables en el desempeño de su trabajo y preservar la transparencia de los asuntos que tienen bajo su encargo (Orfis, 2016).

El desarrollo tecnológico proporciona herramientas eficaces y seguras para la difusión de información, por lo que es de suma importancia para el ORFIS, las ventajas que ofrece la tecnología para garantizar que tanto la comunicación al interior como al exterior, se vea favorecida con el avance en dicha materia. En este sentido, el ORFIS dispondrá de la tecnología para desarrollar los procedimientos idóneos que nos permitan interactuar eficaz y oportunamente; primeramente al interior en el desarrollo de nuestras funciones, así como al exterior para lograr el cometido. Es por ello que en su plan estratégico 2012 -2019 señala los siguientes objetivos:

- Rediseñar e innovar la página web del ORFIS.
- Desarrollar una red interna de comunicación e información para las Unidades Administrativas del ORFIS. (Intranet)
- Implementar un "Sistema de Consulta Telefónica a Entes Fiscalizables", con registro de atención por Unidad Administrativa, mediante conmutador.
- Fomentar el uso de las tecnologías de información por parte de los Entes Fiscalizables para la transparencia y difusión de la información financiera.

El ORFIS se ha apoyado en la tecnología para desarrollar los procedimientos que permitan interactuar eficaz y oportunamente; para lograr el cometido de brindar seguridad en la información.

La seguridad informática mejora el sistema de información y el flujo de información de una organización. Los servicios están dirigidos a evitar los ataques de seguridad y utilizan uno o más

mecanismos de seguridad para proveer el servicio (UNAM, 2016).

La clasificación de la seguridad informática según la (UNAM, 2016) es:

- Confidencialidad
    - Servicio de seguridad o condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. También puede verse como la capacidad del sistema para evitar que personas no autorizadas puedan acceder a la información almacenada en él.

    - La confidencialidad es importante porque la consecuencia del descubrimiento no autorizado puede ser desastrosa. Los servicios de confidencialidad proveen protección de los recursos y de la información en términos del almacenamiento y de la información, para asegurarse que nadie pueda leer, copiar, descubrir o modificar la información sin autorización. Así como interceptar las

comunicaciones o los mensajes entre entidades.

- Autenticación
    - Es el servicio que trata de asegurar que una comunicación sea auténtica, es decir, verificar que el origen de los datos es el correcto, quién los envió y cuándo fueron enviados y recibidos también sean correctos.
- Integridad
    - Servicio de seguridad que garantiza que la información sea modificada, incluyendo su creación y borrado, sólo por el personal autorizado.
    - El sistema no debe modificar o corromper la información que almacene, o permitir que alguien no autorizado lo haga. El problema de la integridad no sólo se refiere a modificaciones intencionadas, sino también a cambios accidentales.
- No repudio
    - El no repudio sirve a los emisores o a los receptores para negar un mensaje transmitido. Por lo que cuando un mensaje es enviado, el receptor puede probar que el mensaje fue enviado por el presunto

emisor. De manera similar, cuando un mensaje es recibido, el remitente puede probar que el mensaje fue recibido por el presunto receptor.

- Control de acceso
    - Un control de acceso se ejecuta con el fin de que un usuario sea identificado y autenticado de manera exitosa para que entonces le sea permitido el acceso.

    - Los componentes básicos de un mecanismo de control de acceso son las entidades de red, los recursos de la red y los derechos de acceso. Estos últimos describen los privilegios de la entidad o los permisos con base en qué condiciones las entidades pueden tener acceso a un recurso de la red y cómo estas entidades son permitidas para tener acceso a un recurso de la red.

    - El control de acceso puede ejecutarse de acuerdo con los niveles de seguridad y puede ejecutarse mediante la administración de la red o por una entidad individual de

acuerdo con las políticas de control de acceso.

- Disponibilidad
    - En un entorno donde las comunicaciones juegan un papel importante es necesario asegurar que la red esté siempre disponible.
    - La disponibilidad es un servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información asociados en el lugar, momento y forma en que es requerido. Un sistema seguro debe mantener la información disponible para los usuarios. El sistema, tanto hardware como software, debe mantenerse funcionando eficientemente y ser capaz de recuperarse rápidamente en caso de fallo.

El uso de las Tecnologías de la Información y Comunicación (Tic's) representa radicalmente una forma en que los gobiernos administran y ejecutan sus procesos, abriendo la posibilidad de mejorar e incrementar los canales de comunicación entre los miembros de la organización o externos, es de vital importancia que no exista fuga de información y que cumplan cabalmente las características de la misma.

Las filtraciones de datos puede iniciarse por empleados sin querer o usuarios con malas intenciones, dedicados a la copia de información sensible o de propietario desde sus equipos a

unidades de memoria flash, smartphones, cámaras, PDA, DVD, CDROM, u otras formas viables de almacenamiento portátil. O bien, las filtraciones pueden deberse a correos electrónicos de usuarios, mensajería instantánea, formularios web, intercambios de redes sociales o sesiones telnet. Los puntos de intercambio inalámbrico como Wi-Fi, Bluetooth e infrarrojos, así como canales de sincronización de dispositivos, suponen riesgos adicionales de pérdida de datos. Del mismo modo, los equipos terminales pueden verse infectados con software dañino que aprovecha pulsaciones de teclado y envía los datos robados a través de canales SMTP o FTP para terminar en manos de criminales. Aunque algunas de estas vulnerabilidades pueden evadir soluciones de seguridad para redes y controles nativos de Windows (DeviceLock, 2016).

Está herramienta tecnológica permite el control de contenidos y contexto para la mayor prevención de filtraciones, su motor de intercepción e inspección de varias capas proporciona un control minucioso sobre una gran variedad de posibilidades de filtración de datos desde el nivel de contexto. Para mayor confianza en evitar la fuga de datos sensibles, es posible aplicar el filtrado y análisis de contenidos para seleccionar intercambios de datos de terminales con medios extraíbles y dispositivos punto a punto, así como dentro de la red. Resultando para el administrador del centro de cómputo la completa seguridad para ajustar con precisión los derechos de usuarios a cada rol por lo que respecta a la transferencia, recepción y almacenamiento de datos en equipos corporativos (DeviceLock, 2016).

La herramienta ofrece un enfoque sencillo sobre la gestión, que permite a los administradores de seguridad utilizar Objetos de directiva de grupos de Microsoft directorio activo y consolas remotas para la administración dinámica de agentes terminales distribuidos, e imponer directivas de dominio bien definidas de forma centralizada en sus equipos anfitrión.

La figura 1 representa la manera lógica en que trabaja herramienta, es decir la forma que opera la misma mediante red local y los agentes que intervienen en ella.

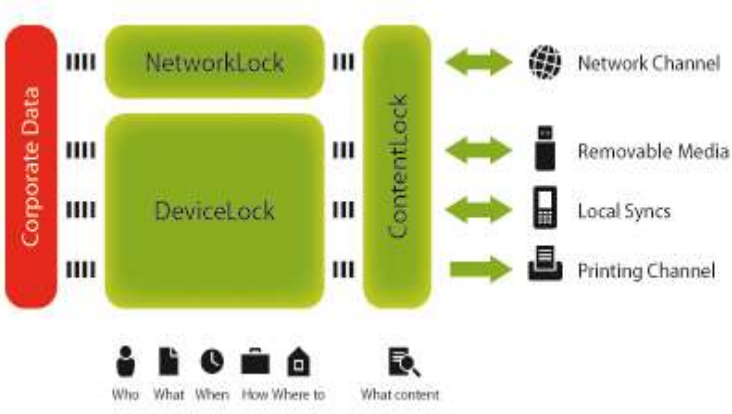

Figura 1
Fuente: http://www.devicelock.com/es/

La figura 2 describe cuales componentes son bloqueados por medio de DeviceLock asegurando así que se cumplan políticas de seguridad dentro de la organización, dichos elementos incluyen:

- Puertos USB
- Unidades Removibles
- Impresoras
- Tarjetas de Red Wifi
- Tecnología móvil.

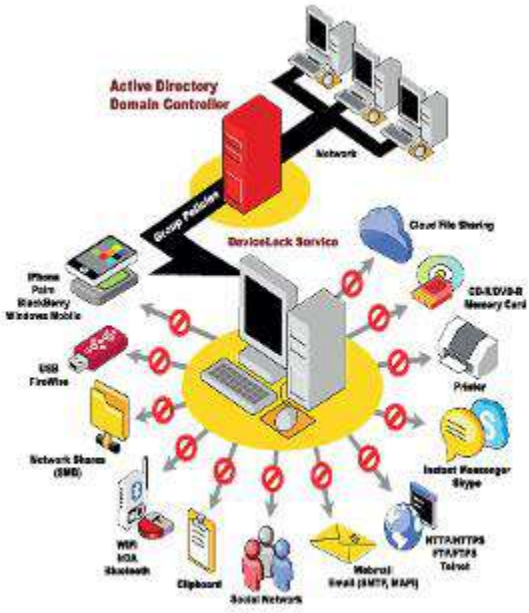

Figura 2
Fuente: http://www.devicelock.com/es/

Por lo antes mencionado el ORFIS opto por la implementación de dicho servicio tecnológico además que representa ventajas como:

- Control de acceso de dispositivos
- Control de comunicaciones de red.
- Filtrado de contenidos
- Protección de falsificación
- Integración con Active Directory
- True File Type Control
- Control del portapapeles
- Lista blanca USB
- Lista blanca de medios

- Lista blanca temporal
- Lista blanca de protocolos
- Auditoría
- Emulación

METODOLOGÍA

La metodología que se utilizó fue cualitativa, como indica su propia denominación, tiene como objetivo la descripción de las cualidades de un fenómeno. Adicionalmente se elaboraron figuras para la presentación y descripción de los resultados.

OBJETIVO GENERAL

Describir el uso de las Tic´s (DeviceLock) en proceso de seguridad informática en el Orfis durante el periodo 2013-2015.

RESULTADOS

Como antecedente a la seguridad informática en 2013, el ORFIS utilizaba la herramienta DeviceLock como parte de su protección y seguridad de la información, en esa fecha su uso era limitado, ya que se instalaba de manera independiente en cada equipo y no era administrada por una consola, además se bloqueaban puertos desde el bios de las computadoras limitando el uso de teclados y ratones usb (véase figura 3).

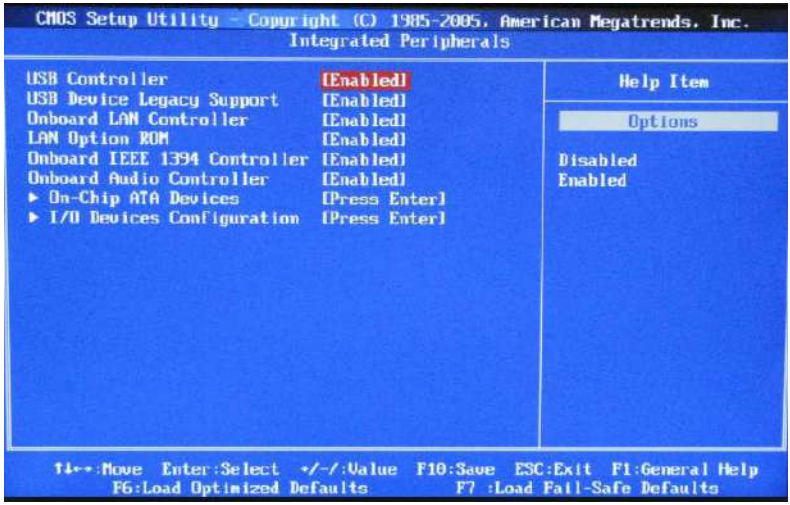

Figura 3
Fuente: Elaboración Propia

Otra herramienta que el ORFIS utilizó como parte de la seguridad informática era el antivirus, el cual fue administrado por 6 servidores instalados en distintas equipos de cómputo en el año 2013 y para el año 2015 se optimizo la administración de un solo servidor con 420 clientes (véase figura 4).

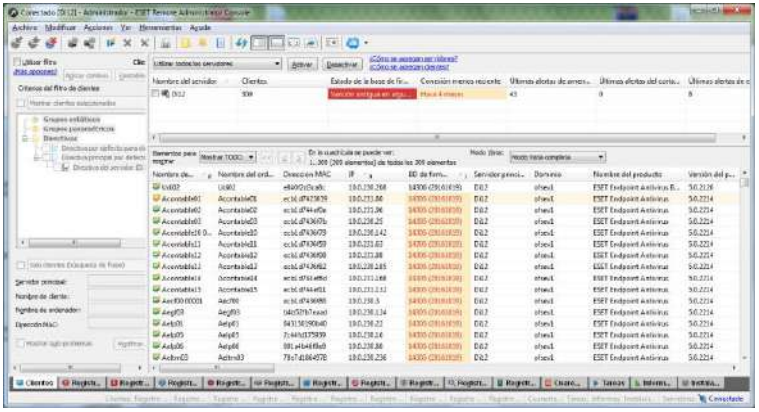

Figura 4
Fuente: Elaboración Propia

Para el año 2015 el ORFIS implementa la misma operación que se realizó con el antivirus con la herramienta DeviceLock la cual fue renovada y adquirida para 300 clientes, en su nueva implementación se incorporó al servidor principal del Directorio Activo de Windows y por medio del cual se realizan las operación de la seguridad informática, buscando que en todo momento dicha acción sea 100% transparente al usuario y no afecte sus actividades.

La figura 5 representa la consola de administración de DeviceLock, en la cual se busca a los equipos para bloquear determinados componentes.

La figura 6 indica los elementos que pueden ser bloqueados por el administrador de la herramienta de seguridad informática, así como el tipo de rol que cada usuario puede tener.

Figura 5
Fuente: Elaboración Propia

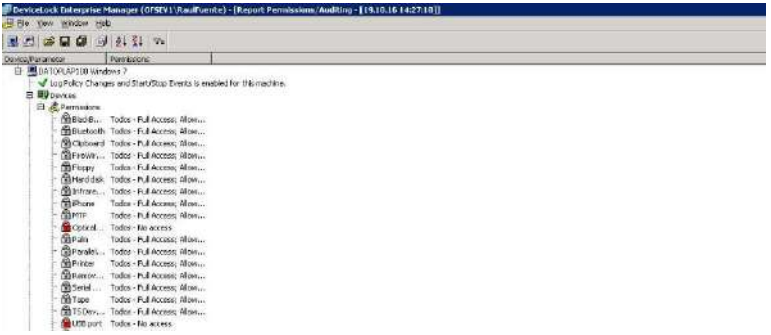

Figura 6
Fuente: Elaboración Propia

La figura 7 indica el permiso a cada uno de los usuarios, aunque esto podría considerarse repetitivo, bajo el esquema de red de dominio, cualquier usuario puede ocupar con su nickname y su contraseña un equipo de la organización. Por tal motivo se selecciona a quienes de estos se le aplica la política de seguridad.

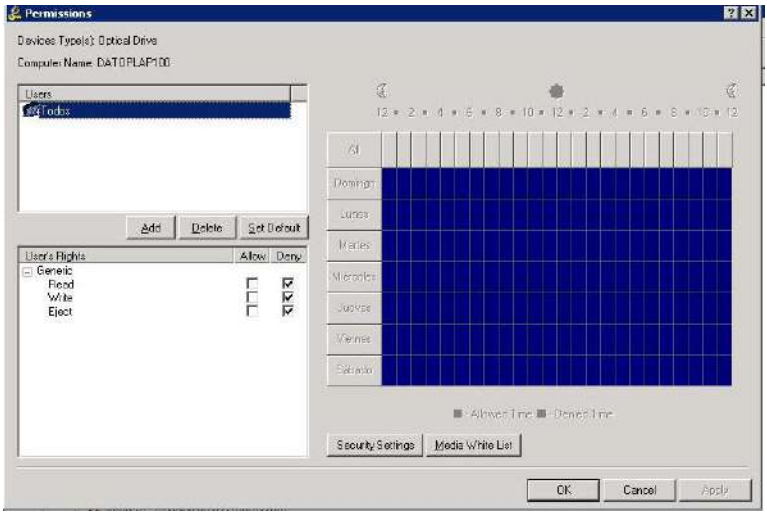

Figura 7
Fuente: Elaboración Propia

La figura 8 representa la posibilidad de permitir que dispositivos usb pueden utilizar los usuarios lo anterior porque en ocasiones hay dispositivos extraíbles que no representan una amenaza como el teclado, el ratón, etc.

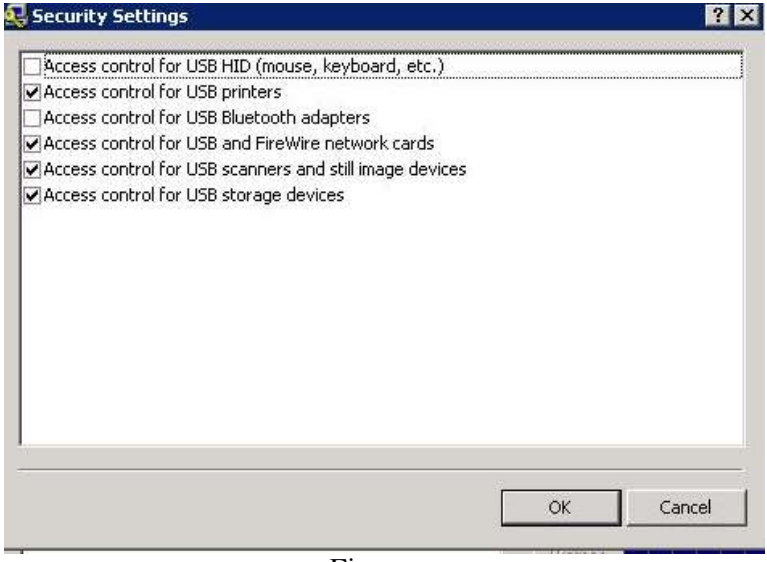

Figura 8
Fuente: Elaboración Propia

CONCLUSIONES

El Órgano de Fiscalización Superior (ORFIS) ha utilizado herramientas físicas tales como desconectar componentes del CPU y lógicas como lo ha sido el DeviceLock, el bloqueo por bios y modificación de registros del sistema operativo.
Los principales medios extraíbles que el ORFIS se ha preocupado por bloquear han sido los puertos USB, las unidades DVD y CD ROM así como también la tecnología móvil conectada al equipo de cómputo, lo anterior en un intento de salvaguardar la información de la organización.

La administración del antivirus es llevada a cabo por una sola persona, la cual es responsable de actualizar y verificar que las bases de datos de virus se encuentren al día para evitar que dichos fragmentos de código malicioso afecten la información y

se propaguen por la red, Actualmente se administran 420 clientes desde un solo servidor.
El 83% del equipo de cómputo del ORFIS tienen instaladas las seguridad informática por medio de políticas del DeviceLock y el 17% que no tiene instalada la herramienta de seguridad pertenece a la parte directiva de la institución.

Existe una diferencia entre el número total de clientes de antivirus y clientes de DeviceLock, lo anterior se debe a que todos los equipos de cómputo incluyendo la parte directiva y los servidores del site deben tener instalada la protección contra código malicioso.

De esta forma podemos concluir que las Tic's aunque no se apliquen de manera equivalente a todos los equipos de cómputo, las mismas benefician el proceso de seguridad informática

REFERENCIAS

Avila, A. (2007). *Iniciación a la red internet. Concepto, Servicios y Aplicaciones* . Vigo: IdeasPropias Ediciones.

Castells, M. (1996). *La Era de la Información. Economía Sociedad y Cultura.* Mexico: SigloXXI.

Chiavenato, I. (2006). *Introducción a la Teoría General de la Administración.* México: McGraw-Hill Interamericana.

Czinkota , M., & Masaaki, K. (2001). *Administración de Mercadotecnia.* International Thomson Editores.

DeviceLock. (19 de Octubre de 2016). *Seguridad y Control a Medios Extraibles* . Obtenido de http://www.devicelock.com/es/

Ferrel, O., & Hirt, G. (2004). *Introducción a los Negocios en un Mundo Cambiante.* México: McGraw-Hill Interamericana.

Orfis. (19 de Octubre de 2016). *Órgano de Fiscalización Superior del Estado de Veracruz.* Obtenido de http://orfis.gob.mx/orfis.html

Toffler, A., & Toffler, H. (2006). *La Revolución de la Riqueza.* Random House Mondadori.

UNAM. (19 de Octubre de 2016). *Seguridad Informatica.* Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad/ServiciosSeguridad.php