

Capítulo V

Seguridad de un portal

Seguridad del Portal

Los portales WEB se ven expuestos a un creciente número de amenazas y vulnerabilidades que pueden afectar la imagen institucional, la disponibilidad de los servicios brindados, la integridad y la confidencialidad de la información que se trasmite a través del mismo, entre otros. En este capítulo se presenta un conjunto de controles para mitigar los riesgos de seguridad a los cuales se ven expuesto los portales WEB. Los controles expuestos no constituyen una lista exhaustiva y el organismo puede considerar que se necesitan controles adicionales.

Los controles presentados en este capítulo implican funciones de hardware y software, pero cabe señalar que la seguridad que puede lograrse a través de estos medios técnicos es limitada y por esto debería apoyarse en una gestión y en procedimientos adecuados. Los controles seleccionados deberían estar alineados con las buenas prácticas de seguridad definidas por el organismo y en particular con la Política de Seguridad del mismo (ver Política de Seguridad modelo de AGESIC www.agesic.gub.uy).

En esta oportunidad hemos seleccionado un conjunto de controles enfocados en la estructura del sitio y en la confidencialidad, integridad y disponibilidad de la información que albergan.



Protección contra divulgación de información no autorizada

No necesariamente toda la información que ponemos a disposición a través de nuestro portal es de carácter público, en consecuencia debemos proteger la divulgación no autorizada de la misma. Podemos contar, por ejemplo, con secciones reservadas para personal autorizado y servicios interactivos que realicen trasiego de datos sensibles que requieren adecuada protección.

Adicionalmente nuestros portales pueden revelar, involuntariamente, información sobre su configuración, su funcionamiento interno, e incluso violar la privacidad de personas físicas. Los atacantes pueden usar estas vulnerabilidades para obtener datos delicados o realizar ataques más serios.

Protección contra Robots – No ponga a disposición más de lo necesario

Dado el gran número de sitios Web que pueblan Internet la única forma viable de realizar búsquedas de contenidos pasó a ser los motores de búsqueda y sin duda debe ser el mecanismo por el cual los usuarios acceden mayoritariamente a nuestro portal. Para alimentar a estos motores de búsqueda se utilizan los llamados robots¹, programas generados por los distintos buscadores que atraviesan la estructura de un sitio Web recuperando los enlaces del mismo.

No necesariamente toda la información disponible a través de nuestro portal tiene carácter público, podemos desear preservar la confidencialidad de ciertos directorios de nuestro sitio destinados sólo para uso interno o privilegiado. Para evitar que los robots identifiquen, analicen y registren estos directorios debemos generar un archivo de texto llamado “robots.txt” el cual debemos alojar en el directorio raíz de nuestro portal.

Cada vez que un robot visita un sitio, primero revisa si existe ese archivo, si no lo encuentra, registra la página en el motor de búsqueda que lo haya enviado; si lo encuentra, analiza su contenido.

Ejemplo

Fuente: basado en el ejemplo presentado en la Guía de pruebas de OWASP ver.3.0 [3]

A continuación, se presenta a modo de ejemplo, el archivo robots.txt del portal gubernamental del Estado de Nuevo León en México: <http://www.nl.gob.mx>

```
http://www.nl.gob.mx/robots.txt :
# Robots.txt file from http://www.nl.gob.mx
#
# Bans from tesoreria
#
# Disallow /tesoreria/
```

¹Los robots también son conocidos bajo los términos crawler o spider web

```
User-agent: *  
Disallow: /tesoreria/  
Disallow: /stats/  
Disallow: /servicios/  
Disallow: /protegido/  
Disallow: /skins/  
Disallow: /Eventos/  
Disallow: /buscador/  
Disallow: /apps/  
Allow: /protegido/buscador/
```

La directiva *User-Agent* hace referencia al robot de búsqueda. Por ejemplo, con *User-Agent: Googlebot* se hará referencia al robot de búsqueda de Google, mientras que utilizando *User-Agent: ** como en el ejemplo anterior, se aplicarán las reglas a todos los robots de búsqueda:

La directiva *Disallow* especifica que recursos no deberán ser inspeccionados por los robots. En el ejemplo anterior, se prohíben los siguientes directorios:

```
...  
Disallow: /tesoreria/  
Disallow: /stats/  
Disallow: /servicios/  
Disallow: /protegido/  
Disallow: /skins/  
Disallow: /Eventos/  
Disallow: /buscador/  
Disallow: /apps/  
...
```

Se puede utilizar la directiva *Allow* para permitir incluir ciertos directorios. En el ejemplo citado se emplea:

```
Disallow: /protegido/  
...  
Allow: /protegido/buscador/
```

En la primera línea se indica con *Disallow* que no está permitido ingresar al directorio protegido, pero a través de *Allow* se indica que se puede registrar el directorio buscador dentro de protegido.

Analizar nuestro robots.txt utilizando las Herramientas para webmasters de Google

Google proporciona una función de “Análisis de robots.txt” como parte de sus “Herramientas para webmasters de Google”, que puede resultar de ayuda para probar si nuestro archivo robots.txt está funcionando según lo esperado.

Instrucciones de uso

1. Acceder a las Herramientas para webmasters de Google
<http://www.google.com/webmasters/tools/?hl=es> (requiere cuenta de Google/Gmail)
2. Añadir su portal y verificar que usted tiene derechos de administración sobre el mismo, luego podrá seleccionar su portal desde el Panel, haciendo clic en la URL del mismo.
3. Hacer clic en Información del sitio y seguidamente en “Acceso de rastreadores”

Algunos robots de búsqueda pueden ignorar intencionadamente las directivas *Disallow* que se especifiquen en el archivo “robots.txt”, por lo cual no debe tomarse este control como un mecanismo que impone restricciones en cómo el contenido Web deba ser accedido o distribuido. En particular para aquellas secciones restringidas sólo a personal autorizado deben implementarse controles de acceso.

Visite la página <http://www.robotstxt.org/faq.html> para obtener información sobre cómo dirigir el comportamiento de los robots que visiten su portal.

Manejo adecuado de errores

Nuestros portales frecuentemente generan mensajes de error durante su operación normal. Estos errores deben ser manejados de acuerdo a un esquema bien pensado que provea al usuario de un mensaje con sentido, información de diagnóstico para quienes mantienen el sitio, y ninguna información útil para un atacante.

El manejo de errores debe contemplar tanto las entradas generadas por el usuario, así como cualquier error que pueda ser generado por componentes internos como ser: llamadas al sistema, consultas a base de datos o cualquier otra función interna.

La amenaza de no realizar un correcto manejo de errores radica en revelar información detallada a través del mensaje de error, como el contenido de

variables, nombres de directorios e información sobre la base de datos, la cual puede ser explotada por un usuario malintencionado para generar un ataque contra nuestro portal.

Ejemplo

Un claro ejemplo de un mal manejo del error sería, presentar, ante un intento fallido de acceso a una sección reservada de nuestro portal, un mensaje de error especificando qué ha fallado, si ha sido la identificación (usuario) o la autenticación (contraseña). Por el contrario la forma correcta sería simplemente notificarle al usuario que hay un error en los datos proporcionados sin otorgar mayor detalle.

Para evitar un manejo inadecuado de los errores se recomienda:

Fuente: basado en la protección de la vulnerabilidad A6 del OWASP Top Ten 2007 [4]

Exigir al equipo de desarrollo un esquema común para el tratamiento de errores o bien asegurar que la herramienta de administración del portal prevea un manejo adecuado de los errores.

No mostrar mensajes de error que presenten información detallada del mismo.

Estandarizar los mensajes de error.

Por mayor información visite el Capítulo de Manejo de Errores de OWASP:
http://www.owasp.org/index.php/Error_Handling

Galletas de la fortuna - Usar cookies de forma segura

Las cookies son archivos creados por los sitios Web para almacenar en los equipos de sus visitantes información específica sobre estos. La principal utilidad de las cookies radica en almacenar datos y preferencias de los usuarios a fin de que nuestro portal pueda reconocer un navegador (usuario) específico.

Dado que las cookies se envían generalmente en texto claro (no cifrado) y se almacena de igual forma en el equipo del usuario, son vulnerables a ataques que comprometen su integridad. Por lo tanto, las cookies que genere nuestro portal no deberían contener datos que pueden ser utilizados directamente por un atacante (por ejemplo, las credenciales de un usuario).

Algunas de las operaciones que se pueden realizar mediante el uso de cookies pueden ser suplantadas por otros mecanismos más seguros, por ejemplo para mantener la información de sesión, el identificador de sesión se pueden pasar

como parte de la dirección URL del portal en lugar de almacenarse en una cookie.

El uso de cookies debería reforzarse con la implementación de canales seguros (ver sección Canales seguros de comunicación)

Se recomienda al utilizar cookies en nuestro portal considerar lo siguiente:

- Evaluar cifrar la información almacenada en las cookies;
- Evitar cookies longevas, limitando su tiempo de vigencia a lo mínimo imprescindible;
- Evitar almacenar información confidencial en una cookie.

Por información adicional sobre las precauciones necesarias al asignar cookies puede consultar el apartado 4.5.2 Pruebas para atributos de cookies (OWASP-SM-002) del OWASP Testing Project [3]

Control de acceso y comunicación segura

Hemos visto evolucionar las prestaciones de los portales del Estado, de portales puramente institucionales con información estática hasta portales que ofrecen una importante gama de servicios. Con esta creciente oferta de servicios surgió la necesidad de brindarle a los usuarios y las organizaciones las garantías de que la información brindada para la prestación de dichos servicios no sea accedida por terceros no autorizados. Como respuesta a esta necesidad irrumpen los mecanismos de control de acceso y el establecimiento de canales seguros de comunicación entre el usuario y nuestro portal.



Pasará, pasará... - Control de acceso

La organización debe examinar periódicamente toda la información accesible desde su portal para determinar los requisitos de seguridad necesarios. Como se menciona anteriormente muchos portales ofrecen diversos servicios los cuales involucran en su gran mayoría información sensible, para la cual la organización debe determinar los usuarios o grupos de usuarios que deben tener acceso.

Este control de acceso se apoya en una gama de tecnologías para autenticar y autorizar a los usuarios con diferentes privilegios de acceso a la información.

Sin autenticación de usuarios, las organizaciones no podrán restringir el acceso a información específica, destinada sólo a usuarios autorizados. Toda la información que reside en un servidor Web público será accesible por cualquiera con acceso a Internet.

Para aquella información de acceso restringido disponible en el portal, la organización deberá identificar que mecanismo de autenticación es el más adecuado. A continuación presentamos una lista con mecanismos recomendados:

- Autenticación basada en formulario Web;
- Autenticación basada en la dirección;
- Autenticación HTTP básica;
- Autenticación HTTP *digest*;
- Autenticación del cliente mediante Certificado Digital;

Autenticación basada en formulario Web

Este mecanismo implica una implementación en nuestro portal de un formulario Web que recoja las credenciales de un usuario (identificación y clave) y las coteje contra un sistema de control de usuarios, el cual puede ser una base de datos. Esta implementación debería complementarse con protocolos seguros de comunicación (ver sección canales seguros de comunicación).

Autenticación basada en la dirección

El mecanismo más simple de autenticación, soportado por la mayoría de los servidores Web, está basada en la dirección del usuario. El control de acceso se basa en la dirección IP o el nombre del *host* del usuario que solicita la información. Aunque es fácil de implementar para pequeños grupos de usuarios, la autenticación basada en la dirección puede ser difícil de gestionar para los sitios Web que tienen una gran población de usuarios potenciales. Este mecanismos de autenticación se debe utilizar sólo cuando se requiere una seguridad mínima, salvo que se emplee en conjunto con otros métodos de autenticación más fuertes.

Autenticación HTTP básica

La autenticación básica HTTP utiliza la estructura de directorios del servidor Web. Normalmente, todos los archivos de un mismo directorio cuentan con los mismos privilegios de acceso. El mecanismo se instrumenta a través de una

identificación de usuario y una clave que le permiten acceder al usuario autenticado a un determinado directorio de archivos. El método y la sintaxis para definir y utilizar este mecanismo depende del servidor Web en el cual este alojado nuestro portal. La debilidad de este mecanismo reside en que la clave del usuario es transferida desde el usuario al servidor Web codificada en lugar de viajar cifrada.

Autenticación HTTP *digest*

La autenticación *digest* puede verse como una versión mejorada de la autenticación básica, ambas incorporadas dentro de la definición del protocolo HTTP. La diferencia radica en cómo se comunican las credenciales que otorga el usuario. En este caso se codifican los datos del usuario mediante el algoritmo criptográfico MD5 al cual se añade una marca de tiempo generada por el servidor y la URL solicitada, esta última también cifrada. Este mecanismo es más seguro que la autenticación básica sin embargo no está soportado por todos los navegadores.

Autenticación del cliente mediante Certificado Digital

Los protocolos SSL/TLS permiten a un servidor Web confirmar la identidad de un usuario, validando su Certificado Digital y confirmando que el mismo fue emitido por una CA que figuran en la lista de entidades emisoras de certificados de confianza. Este mecanismo debe ser considerado sólo en aquellos casos que la información que va a ser accedida reviste de una sensibilidad importante.

Puede encontrar información adicional sobre control de acceso en el capítulo 11 de la Norma UNIT-ISO/IEC 27002:2005.



Dime con quién hablas y te diré quién eres - Canales seguros de comunicación

Se debe preservar también la confidencialidad y la integridad de la información sensible que mencionábamos anteriormente, para ello resulta necesario establecer canales de comunicación seguros.

Se pueden utilizar técnicas criptográficas para proteger la información que atraviesa la conexión entre un usuario y nuestro portal, en particular se recomienda el empleo de los protocolos SSL y TLS para el cifrado de la comunicación. Sin el cifrado, cualquier persona con acceso al tráfico de la red puede determinar y posiblemente alterar el contenido de la información sensible, incluso si el usuario se ha autenticado adecuadamente.

Se debe verificar que aquellas páginas o secciones de nuestro portal para las cuales se haya decidido establecer acceso mediante SSL/TLS sólo sean accesibles por este mecanismo.

La dirección URL de las páginas protegidas mediante SSL o TLS deberían comenzar con *https://*. Otra manera de identificar una página Web protegida por SSL, es a través de la imagen del "candado" que exhiben la mayoría de los navegadores en su parte inferior, tal como se muestra en la figura debajo para el caso del navegador Mozilla Firefox.



Los protocolos mencionados anteriormente, además de proveer cifrado de la información en tránsito, permite la identificación de los clientes y de los servidores mediante certificados digitales. El caso de la identificación de los clientes se presentó en el apartado control de acceso, por otra parte, la identificación del servidor garantiza a los usuarios que se está ante el portal "auténtico" y no una versión falsificada operada por una entidad maliciosa.

La identificación mediante certificados digitales debe, siempre que corresponda, estar alineada a las disposiciones de la Ley N° 18.600 sobre Documento Electrónico y Firma Electrónica que regula los servicios de certificación.

La implementación de los canales seguros reside en el administrador de nuestro servidor Web.

Protegiendo la integridad de su portal

Como comentamos en la sección anterior dada la creciente oferta de servicios que se brindan desde nuestros portales, los mismos tienden en gran medida a transformarse en aplicaciones Web con complejas implementaciones de funciones de software.

Quizás una de las principales amenazas que enfrentan en la actualidad los portales Web es la explotación de vulnerabilidades en dichas aplicaciones Web y la forma en que la información se procesa en los servidores Web. Estos ataques explotan los elementos interactivos de nuestros portales Web.

Más vale malo conocido... - Validación de los datos de entrada

En aquellos casos que contemos con elementos interactivos en nuestros portales Web y siempre que estos requieran ingreso de datos por parte de los usuarios, como por ejemplo formularios de contacto, debemos adoptar como regla general, nunca dar por sentado que estas entradas son confiables.

Si nuestro portal no tiene establecido un mecanismo adecuado para restringir la entrada de datos, un atacante podría entrar cierto tipo de información afectando negativamente nuestro portal y comprometiendo su seguridad. La ausencia de controles que validen las entradas de los usuarios constituye una de las mayores debilidades de los portales interactivos. Esta debilidad conduce a las principales amenazas en aplicaciones Web, como por ejemplo, inyección SQL o Cross Site Scripting (XSS).

A fin de protegerse de entradas de datos malintencionadas, se recomienda que su portal contemple las siguientes indicaciones:

- Para los formularios de entrada de datos, determinar una lista de caracteres posibles y filtrar los caracteres inesperados de los datos de entrada introducidos por un usuario antes de procesar un formulario. Por ejemplo, en la mayoría de los formularios se esperan como datos de entrada, letras de la “a” a la “z”(minúsculas o mayúsculas) y números del 0 al 9.
- Si debemos desplegar en pantalla una entrada del usuario, por ejemplo para confirmar sus datos, debemos previamente filtrar dicha entrada. En particular en el caso de admitir elementos HTML estos deben ser codificados. Por ejemplo, a fin de evitar una ventana emergente con el texto “Soy pasible de un ataque de XSS” deberíamos convertir la entrada del usuario “<script>alert('Soy pasible de un ataque de XSS');</script>” en “<script>alert('Soy pasible de un ataque de XSS');</script>”. De esta manera convertimos cualquier secuencia de comandos potencialmente peligrosa en cadenas visibles, pero no ejecutables.
- No almacene nunca información proporcionada por el usuario sin filtrar en una base de datos.
- Tenga en cuenta que la información que el navegador envía al servidor puede ser suplantada, por tanto desconfíe de todo parámetro de entrada, incluyendo URLs, cadenas de consulta, encabezados HTTP, “cookies” o campos de formularios.

Se describen a continuación algunas de las principales amenazas relacionadas con la falta de validación de datos de entrada.

Inyección SQL

En este tipo de ataque, una entidad maliciosa envía a través de una entrada un comando o cadena SQL específica a la base de datos de nuestro portal, que al no pasar por la validación correspondiente, podría llegar a devolver al atacante cualquier información almacenada en dicha base de datos. Las fallas de inyección SQL, también permiten al atacante crear, modificar o borrar cualquier información arbitraria disponible en la base de datos de nuestro portal.

Por información detallada sobre fallas de inyección y mecanismos de protección consulte la vulnerabilidad A2 del OWASP Top Ten 2007 [4].

Secuencia de comandos en Sitios Cruzados [del inglés *Cross Site Scripting*] (XSS)

La secuencia de comandos en sitios cruzados, más conocida como XSS, es una amenaza que afecta aplicaciones Web interactivas que permite inyección de código malicioso de usuarios de Internet en las páginas Web visitadas por otros usuarios. XSS permite a los atacantes ejecutar secuencias de comandos que pueden secuestrar sesiones de usuario, modificar sitios Web, insertar contenido hostil, realizar ataques de phishing y tomar control del navegador Web del usuario.

Por mayor información sobre *Cross Site Scripting* y mecanismos de protección consulte la vulnerabilidad A1 del OWASP Top Ten 2007 [4]

Destino incierto – Redirección de dominios (*Pharming*)

La amenaza de redirección de dominio aparece ante las vulnerabilidades de los sistemas de administración y asignación de nombres de dominio (DNS)², los cuales se utilizan para asociar nombres en lenguaje natural a las direcciones IP de nuestros servidores Web, o mediante la alteración de los archivos *host* del equipo del cliente que utiliza para resolver localmente (asociar IP a lenguaje natural) los nombres de dominio de Internet. En cualquier caso, el sistema afectado va a dirigir nombres legítimos de nuestros portales Web a direcciones de sitios Web malintencionados.

²En el capítulo Normativa a cumplir se profundiza sobre Nombres de dominios

A continuación se describen algunas prácticas para evitar la redirección de dominios:

Fuente: basado en las técnicas anti-Pharming presentadas en el apartado 6.3.2 de la Norma NIST SP 800-44 [2]

- Asegurar la utilización de la versión vigente del software DNS con los últimos parches de seguridad aplicados.
- Instalar mecanismos de protección contra *pharming* en el servidor DNS.
- Monitorear los dominios de la organización y el registro de dominios similares. En el caso de existencia de nombres de dominio similares los atacantes podrían tomar ventaja de los errores de los usuarios al digitar la dirección.
- Simplificar la estructura y el número de nombres de dominio de nuestra organización. Si una organización tiene una estructura de nombres complicados para sus servidores, se hace cada vez más difícil para los usuarios discernir si están en un sitio ilegítimo.
- Usar canales seguros de comunicación para inicios de sesión, que permitan a los usuarios verificar que los certificados del servidor son válidos y están asociados con un sitio Web legítimo.

Protegerse contra amenazas de negación de servicio

Los ataques de negación de servicios buscan deshabilitar un servicio o dejar completamente fuera de línea un portal. La idea tras estos ataques radica en saturar un equipo, aplicación, servicio o canal de comunicación, de forma tal que se impide la prestación de los servicios e incluso la caída del equipo que alberga nuestro portal por tiempo indeterminado.

Este tipo de ataque generalmente va más allá de lo que se puede evitar en la implementación de nuestro portal. Sin embargo existen tipos de vulnerabilidades dentro de las aplicaciones Web que permiten a un usuario malicioso provocar que algunas funcionalidades o en ocasiones el portal en su conjunto queden no disponibles. Estos problemas son causados por errores en la aplicación, a menudo como resultado de entradas maliciosas o valores de entrada no esperados.

Se presentan a continuación algunas pautas para prevenir ataques de negación de servicios.

Limitar consultas a bases de datos

En caso de portales interactivos con manejo de base de datos, se recomienda limitar las consultas a la base de datos para protegerse frente a consultas grandes que consuman los recursos del sistema.

Un ejemplo de consultas maliciosas lo constituye el uso de “comodines” en los formularios de búsqueda de nuestros portales. Consultas que incluyan caracteres como "[", "[^", "_" y "%", interpretados por la mayoría de los motores de base de datos como “comodines”, pueden requerir un uso intensivo del procesador.

Algunas de las técnicas que se pueden implementar para limitar las consultas a bases de datos son:

- Contar con un listado de caracteres aceptados (ver apartado Validación de los datos de entrada);
- Implementar CAPTCHA³ en formularios de búsqueda avanzada⁴;
- Limitar el tiempo de ejecución de las consultas SQL;
- Limitar el número de registros devueltos por una consulta a la base de datos;

Evitar bloqueos de cuentas de usuarios de forma malintencionada

Una defensa comúnmente usada para evitar el descubrimiento de contraseñas de usuarios por fuerza bruta es bloquear el uso de una cuenta después de varios intentos fallidos de autenticación. Eso significa que incluso si un usuario legítimo proporcionase su contraseña válida, no podría registrarse en el sistema hasta que su cuenta haya sido desbloqueada. Este mecanismo de defensa puede convertirse en un ataque de negación de servicio contra nuestro portal Web si el atacante conoce o puede deducir nombres de cuentas válidos.

³<http://es.wikipedia.org/wiki/Captcha>

⁴Las técnicas de CAPTCHA implementadas deben cubrir los requisitos de accesibilidad (ver capítulo Accesibilidad)

En caso de contar con secciones que requieran autenticación y se utilice este mecanismo de bloque de cuentas, es necesario asegurar que un atacante no podrá recolectar identificadores de usuarios válidos, con los cuales lanzar un ataque de negación de servicios. Tener presente que para evitar esto es preciso:

- Realizar un adecuado manejo de los errores presentados al usuario ante intentos fallidos de autenticación, evitando divulgar cualquier información que pueda servir para identificar cuentas válidas.
- Si el portal permite crear cuentas nuevas eligiendo el nombre de usuario, los controles de redundancia de usuarios revelarán la existencia de cuentas válidas.
- En los casos que el portal prevea el reinicio de claves, asegurar los mensajes desplegados para cuentas inexistentes.

Evitar desbordamientos de *buffer*

Un desbordamiento de *buffer* es un error de software causado por un defecto de programación que se produce cuando se copia una cantidad de datos sobre un área que no es lo suficientemente grande para contenerlos, sobrescribiendo de esta manera otras zonas de memoria. Si se produce la escritura fuera de una zona de memoria protegida esto dará lugar a la terminación del programa.

Esto puede afectar nuestros portales interactivos, produciendo la no disponibilidad de los servicios. Para evitar ataques de este tipo se recomienda:

Validar los datos de entrada (ver sección correspondiente);

Verificar que los servidores Web, de aplicaciones y de bases de datos se encuentren con las últimas actualizaciones tanto a nivel de sistema operativo como en las aplicaciones de seguridad(antivirus, malware, etc.).

Limitar la escritura a disco

Un atacante podría afectar la disponibilidad de nuestro portal valiéndose de la inexistencia de límites en la carga de archivos o almacenaje de datos de registro. Una vez más este tipo de ataque afecta sólo aquellos portales con características interactivas.

Para evitar el llenado de los discos de forma maliciosa, se recomienda:

- Comprobar los límites de tamaño de la entrada del usuario antes de usarla o almacenarla.
- Si se le permite al usuario cargar archivos establecer un límite de tamaño para los mismos.

Resguardo de la información

Con el fin de mantener la integridad y disponibilidad de nuestro portal resulta necesario realizar regularmente copias de seguridad del software y la información que lo constituyen.

Los respaldos deberían garantizar que toda la información esencial y el software puedan recuperarse tras un acto malicioso o accidental o de un error de hardware o software.

Deberían considerarse los siguientes elementos para el respaldo de la información y el software de nuestro portal:

Fuente: basado en la Guía de implementación presentada en el apartado 10.5.1 de la Norma UNIT-ISO/IEC 27002:2005 [1]

- El grado (por ejemplo, respaldo completo o diferencial) y la frecuencia de los respaldos deberían reflejar los requisitos del negocio y los requisitos de seguridad de la información implicada;
- Los respaldos deberían almacenarse en un lugar apartado, a una distancia adecuada que garantice que cualquier daño en el sitio principal no los afecte;
- La información de respaldo debería tener un nivel apropiado de protección ambiental y físico consistente con las normas aplicadas en el sitio principal;
- Los controles aplicados a los soportes en el sitio principal se deben ampliar para cubrir el sitio de respaldo;
- Debería probarse periódicamente la correcta restauración de las copias de seguridad;

- En caso de información confidencial, los respaldos deberían protegerse por medio del cifrado.

Monitoreo

El registro de las actividades en nuestro portal es vital para detectar acciones no autorizadas y fallas en el mismo. Es importante recoger los datos correctos en los registros de auditoría (*logs*) y dar seguimiento a los mismos.

A la hora de identificar que registros mantener deberían considerarse los *logs* del servidor Web y evaluar la necesidad de que las aplicaciones Web (implementaciones de servicios) mantengan sus propios registros de las acciones. Por ejemplo una sección restringida debería incluir en sus registros de auditoría, cuando sea relevante:

- Identificación del usuario que accede;
- Fechas, horas, y los detalles de acontecimientos claves, por ejemplo inicio y fin de una sesión;
- Identidad del equipo y ubicación, si es posible;
- Registros de los intentos aceptados y rechazados de acceso a la sección;
- Archivos accedidos y la clase de acceso;

Muchas veces la revisión de *logs* es trivial y reactiva, la misma es considerada mayoritariamente como tediosa, sin embargo, es importante señalar que los *logs* a menudo son el único registro de un comportamiento sospechoso. Es recomendable valerse de procedimientos y herramientas para procesar y analizar los *logs* y revisar las notificaciones de alerta.

Los registros de auditoría pueden contener datos personales confidenciales e indiscretos. Deberían tomarse medidas de protección de privacidad.

De ser posible, los administradores de sistema no deberían tener el permiso de borrar o desactivar los registros de sus propias actividades.

Lista de Verificación de Seguridad de un Portal

Acción	Completada
Generar el archivo “robots.txt”	<input type="checkbox"/>
En caso de producirse errores se despliegan mensajes adecuados que no brindan información detallada del mismo	<input type="checkbox"/>
Prohibir el uso de cookies persistentes	<input type="checkbox"/>
Usar la cookie de sesión sólo si está claramente identificada en la política de privacidad	<input type="checkbox"/>
No se almacena en las cookies información confidencial en claro	<input type="checkbox"/>
Para los recursos del portal que requieren una protección mínima y para los cuales hay una pequeña y claramente definida audiencia, se ha configurado “Autenticación basada en la dirección”	<input type="checkbox"/>
Para los recursos del portal que requieren protección adicional y para los cuales hay una pequeña y claramente definida audiencia, se ha configurado “Autenticación basada en la dirección” como segunda línea de defensa complementada con “Autenticación basada en formulario Web”	<input type="checkbox"/>
Para los recursos del portal que requieren una protección mínima pero no tienen definido una audiencia clara, se ha configurado Autenticación HTTP básica o <i>digest</i> (mejor opción)	<input type="checkbox"/>
Para los recursos del portal que requieren protección adicional pero no tienen definido una audiencia clara, se ha configurado Autenticación basada en formulario Web y Autenticación HTTP básica o <i>digest</i> (mejor opción) como segunda línea de defensa	<input type="checkbox"/>
Para los recursos del portal que requieren máxima protección, se ha configurado SSL / TLS	<input type="checkbox"/>

Acción	Completada
Para las configuraciones que requieran un nivel de seguridad medio en la autenticación de clientes, se ha configurado el servidor para exigir el nombre de usuario y la contraseña a través de SSL/TLS	<input type="checkbox"/>
Para las configuraciones que requieren un nivel de seguridad alto en la autenticación de clientes, se ha configurado el servidor para requerir certificados digital de cliente a través de SSL/TLS	<input type="checkbox"/>
En los casos que se autentique mediante certificados digitales se ha verificado la alineación con las disposiciones de la Ley N° 18.600	<input type="checkbox"/>
Toda entrada de usuario es validada	<input type="checkbox"/>
Se ha personalizado el contenido Web para ayudar a los usuarios ha identificar los sitios Web fraudulentos	<input type="checkbox"/>
Se utilizan las versiones actuales del software DNS con los últimos parches de seguridad	<input type="checkbox"/>
Se han Instalado del lado del servidor mecanismos de protección de DNS	<input type="checkbox"/>
Se realiza el seguimiento de los dominios de la organización y dominios similares	<input type="checkbox"/>
Se ha simplificado la estructura de nombres de dominio de la organización	<input type="checkbox"/>
Las consultas a bases de datos que requieren entradas de usuarios cuentan con listas de caracteres aceptados	<input type="checkbox"/>
En aquellos casos que sea factible, se han implementado técnicas CAPTCHA en los formularios de búsqueda avanzada	<input type="checkbox"/>
Se han establecido límites temporales a la ejecución de consultas SQL	<input type="checkbox"/>
Se ha limitado el número de registros devueltos por una consulta a nuestra base de datos	<input type="checkbox"/>
Se han asegurados las cuentas de usuarios	<input type="checkbox"/>

Acción	Completada
Se ha verificado que los servidores Web, de aplicaciones y de bases de datos se encuentren con las últimas actualizaciones tanto a nivel de sistema operativo como en las aplicaciones de seguridad (antivirus, malware, etc.)	<input type="checkbox"/>
Se verifican los tamaños de las entradas de usuario antes de almacenarlas en disco	<input type="checkbox"/>
Se ha establecido una sistemática de respaldo periódica para el software y la información del portal	<input type="checkbox"/>
Se ha verificado la recuperación exitosa de los respaldos del software y la información del portal	<input type="checkbox"/>
Los respaldos del portal se almacenan en un lugar apartado del sitio principal	<input type="checkbox"/>
Se cifran los respaldos de la información confidencial del portal	<input type="checkbox"/>
Se mantienen los registros de auditoría (<i>logs</i>) adecuados a los requisitos de la organización	<input type="checkbox"/>
Se revisan periódicamente los <i>logs</i>	<input type="checkbox"/>
Se protegen adecuadamente los <i>logs</i> contra modificaciones	<input type="checkbox"/>

Tabla de Contenido

Seguridad del Portal	261
Protección contra divulgación de información no autorizada	261
Protección contra Robots – No ponga a disposición más de lo necesario.....	262
Manejo adecuado de errores	264
Galletas de la fortuna - Usar cookies de forma segura	265
Control de acceso y comunicación segura	266
Pasaré, pasará... - Control de acceso.....	266
Dime con quién hablas y te diré quién eres - Canales seguros de comunicación.....	268
Protegiendo la integridad de su portal.....	269
Más vale malo conocido... - Validación de los datos de entrada	270
Destino incierto – Redirección de dominios (<i>Pharming</i>).....	271
Protegerse contra amenazas de negación de servicio	272
Limitar consultas a bases de datos.....	273
Evitar bloqueos de cuentas de usuarios de forma malintencionada	273
Evitar desbordamientos de <i>buffer</i>	274
Limitar la escritura a disco.....	274
Resguardo de la información	275
Monitoreo	276
Lista de Verificación de Seguridad de un Portal.....	277
Tabla de Contenido	280