INFORME DE AUDITORIA INTERNA AI JPS 22-2012

ÁREA DE AUDITORIA DE SISTEMAS

NOMBRE DEL ESTUDIO

VERIFICACIÓN DE LA SEGURIDAD DE LOS SISTEMAS INFORMATICOS RELACIONADOS CON LAS APUESTAS DEPORTIVAS QUE COMERCIALIZA LA JUNTA DE PROTECCION SOCIAL POR MEDIO DE LOS SOCIOS COMERCIALES

PREPARADO POR:

LIC. ANDRES MARTÍNEZ PORRAS
PROFESIONAL II

LIC. JOSÉ A. WONG CARRIÓN
JEFE DE ÁREA

20 DE DICIEMBRE DEL 2012

DIRIGIDO A:

GERENCIA
SUBGERENCIA FINANCIERA CONTABLE
DEPARTAMENTO DE INFORMÁTICA

Contenido

RESUMEN EJECUTIVO
Informe de Auditoría Interna AI JPS N° 22-2012

Esta Auditoría Interna, en cumplimiento al Programa de Trabajo del Área de Sistemas para el año 2012 realizó una verificación de la seguridad de los sistemas informáticos relacionados con las apuestas deportivas que comercializa la Junta de Protección Social por medio de los socios comerciales. Para llevar a cabo el estudio, se contrató en calidad de asesora a la empresa Price Waterhouse Cooper Consultores, S.A

El Objetivo General fue evaluar la seguridad existente en las transacciones que llevan a cabo los socios comerciales, relacionados con la comercialización de las apuestas deportivas, así como la seguridad (controles existentes), exactitud, integridad y veracidad de la información en el servidor de la Junta de Protección Social, donde se operan dichas apuestas. Este objetivo implicó la revisión del ambiente de seguridad general existente en el Departamento de Informática tanto en equipos como ambiente físico, de la seguridad del sistema informático por medio del cual se llevan a cabo las apuestas deportivas y de los equipos de cómputo (de una muestra de socios comerciales) donde se confeccionan las apuestas que se comercializan.

Dentro de los aspectos observados relacionados con la seguridad física y lógica del Departamento de Informática, se determinó:

a. Inexistencia de monitoreo de equipos que tienen alguna relación con la Internet. Las paredes de ese departamento representan inseguridad al ser de un vidrio no resistente a impactos.
b. No existen detectores de humedad, lo cual eventualmente puede afectar a los equipos y,
c. Una inadecuada distribución del cableado conectado a los equipos de las salas de cómputo y comunicaciones.

En relación con los servidores se determinó,

d. Uso de protocolos de comunicación inseguros como Telenet y FTP.
e. El atributo de autocompletado de la contraseña se encuentra habilitado.

f. Uso de una versión de sistema operativo obsoleta y

g. Debilidades de control en funciones como DNZ Zone, en Adoble Cold Fusion y en los IDs de sesiones de usuario.

En relación con la seguridad de la aplicación de apuestas deportivas (sistema informático) se pudo determinar una debilidad en las contraseñas permitidas por el sistema para uso de los socios comerciales tales como:

h. Un solo factor de autenticación.

i. Falta de requerimientos de complejidad de las contraseñas e

j. Inexistencia de controles de expiración de las mismas.

Finalmente, en los equipos de cómputo utilizados por los socios comerciales según muestra escogida, se observaron aspectos tales como:

k. Protector de pantalla deshabilitado, lo cual, en ausencia del vendedor la aplicación utilizada para la venta queda expuesta a personas ajenas.

l. Herramientas instaladas en los equipos por medio de las cuales puede haber un acceso al sistema en forma remota.

m. Antivirus desactualizado y

n. Uso compartido de nombres de usuario y contraseñas con otros vendedores del juego Progol.

Las recomendaciones emitidas en este informe están dirigidas a fortalecer el control interno a través del monitoreo de las comunicaciones de Internet, la eliminación de protocolos de comunicación inseguros, actualización de software, protección general del ambiente físico del Departamento de Informática, fortalecimiento del sistema informático de apuestas deportivas a través de mejores credenciales para el ingreso a la aplicación y una mejor regulación de los usuarios y el fortalecimiento de la seguridad en las actividades habituales de control aplicadas por los socios comerciales.

1. INTRODUCCIÓN

1.1 Antecedentes

Esta Auditoría incluyó dentro del Programa de Trabajo del 2012, un estudio relacionado con la *"Verificación de la seguridad de los sistemas informáticos relacionados con las apuestas deportivas que comercializa la Junta de Protección Social por medio de los socios comerciales"*, para llevar a cabo el estudio, se contrató en calidad de asesora a la empresa Price Waterhouse Cooper Consultores, S.A., mediante Contratación Directa N° 2012 CD-000153-PROV-01.

1.2 Objetivo general

Realizar una evaluación de la seguridad existente en las transacciones que llevan a cabo los socios comerciales, relacionadas con la comercialización de las apuestas deportivas, así como la seguridad (controles existentes), exactitud, integridad y veracidad de la información en el servidor de la Junta de Protección Social, donde se operan dichas apuestas.

1.3 Objetivos específicos

Con base en las especificaciones técnicas solicitadas para llevar a cabo el estudio en mención, se contemplaron los siguientes objetivos específicos:

- Evaluar la seguridad de los dispositivos de comunicación utilizados en la conexión entre los socios comerciales y la Junta de Protección Social, tanto física como lógicamente.

- Valorar la seguridad de la aplicación (sistema informático) y la seguridad alrededor de la misma, para realizar apuestas deportivas a través de los Entes Externos (socios comerciales).

- Hacer un estudio completo de la distribución física de las conexiones de internet utilizadas en la Junta de Protección Social, para brindar el servicio a los socios comerciales.

- Valorar la seguridad e integridad de los datos almacenados en la base de datos institucional, en el momento de llevarse a cabo las apuestas deportivas por parte de los socios comerciales.

- Determinar y verificar la capacidad de respuesta ante una posible contingencia en el momento de llevarse a cabo las apuestas deportivas por parte de los socios comerciales.

- Evaluar mediante pruebas de penetración la seguridad de los servidores utilizados en el proceso de apuestas deportivas, así como el equipo de cómputo utilizado por los socios comerciales.

1.4 Metodología utilizada

La metodología utilizada en la confección de este estudio fue la siguiente:

- ✓ Se entrevistaron a los funcionarios de la Junta de Protección Social involucrados en los procesos de comercialización del juego Progol en el Departamento de Informática con la finalidad de revisar el sistema y los equipos donde se llevan a cabo las transacciones de dicho juego.

- ✓ Se efectuó una inspección general del ambiente físico donde se encuentran los servidores (sala de comunicación y sala de servidores).

- ✓ Se visitaron 12 puestos donde se comercializa el juego Progol seleccionados por la Auditoría Interna (6 dentro del Gran Área Metropolitana y 6 fuera de ella, incluida la Sucursal de Alajuela y el puesto de ventas en caja ubicado en el mezanine del Departamento de Tesorería).

- ✓ Se solicitó la información necesaria para la verificación de cada una de las actividades antes mencionadas.

- ✓ Se realizaron apuestas de Progol en diferentes puestos de socios comerciales con la finalidad de verificar la integridad de la información en las bases de datos institucionales.

Las actividades fueron realizadas de acuerdo con la normativa aplicable al ejercicio de la Auditoría Interna.

1.5 Alcance

Para llevar a cabo el estudio se realizaron visitas a los siguientes socios comerciales:

Socio Comercial	Ubicación
Díaz Miranda Felipe	Centro Comercial Santa Ana 2000 (GAM)
Juan Luis Ávila	El Roble Puntarenas, Ventanita (Puntarenas)
Carlos Artavia Prada	Local costado oeste del Mercado Municipal, venta y cambio, La Bolsita (Pérez Zeledón)
Mynor Bermúdez Solano	Cartago, Stand, costado N.O, del parque de la Basílica, Cartago (GAM - Cartago)
Jorge Alexander Venegas Rojas	Paraíso, Puesto en Brumas, Exclusividades Americanas, local costado sur de la Clínica de CCSS (GAM - Cartago)
Gerardo Sojo Flores	Santo Domingo de Heredia, Costado oeste de Palí (Heredia)
Arnulfo Montero Castro	Guápiles, local frente al Banco Nacional (Limón)
Stephanie García Del Valle	Frente al BCR, Centro Comercial Sofía (Liberia - Guanacaste)
Alejo Ramírez Campos	Costado norte del Redondel de Toros Chorotega en el Punto de la Suerte (Cañas - Guanacaste)
Graciela Salazar Ramírez	Barrio Jardín contiguo a Funeraria El Milagro de la Fe 150 mts norte de CCSS (Ciudad Quesada -Alajuela)

Asimismo, se realizaron revisiones en los siguientes puntos de venta de la Institución:

Carlos Artavia Soto	Junta de Protección Social (Sucursal Alajuela)
William Hernández Díaz	Oficinas Centrales Junta de Protección Social (GAM)

Aspectos evaluados en los equipos de los puestos de venta de los socios comerciales:

- Sistema operativo, tipo de procesador, cantidad de memoria RAM y disco duro.
- Versión y tipo de navegador.
- Longitud de caracteres de las contraseñas utilizadas por los socios comerciales.
- Cantidad de personas que tienen acceso al punto de ventas (para realizar ventas)
- Antivirus instalados y actualización de los mismos.
- Cantidad de tiempo predeterminado para la activación del protector de pantalla.
- Contraseña del protector de pantalla.
- Existencia de instalación de aplicaciones riesgosas en los equipos utilizados para la venta de Progol.
- Existencia de conexiones de hardware riesgoso en los equipos utilizados para la venta de Progol.

Además, se incluyeron los siguientes equipos, ubicados en el Departamento de Informática, que soportan la comunicación y las transacciones del juego de apuestas denominado Progol:

- Cluster Firewall Checkpoint RG65
- Switch 3Com Core Capa 3
- Servidor Proxy (10.0.0.80 - proxy.jps.go.cr)
- Servidor de Base de Datos (10.0.0.200)
- Servidor de Capa de Negocios (10.0.0.135)
- Servidor de Capa de Presentación (192.168.1.2, 196.40.67.146)

1.6 Disposiciones de la Contraloría General de la República sobre los informes emitidos por las Auditorías Internas

De conformidad con el recordatorio enviado vía correo electrónico el 17 de marzo del 2003, por parte del Centro de Relaciones para el Fortalecimiento del Control y la Fiscalización Superiores de la Contraloría General de la República, se transcriben los artículos Nº 36, 37, 38 y 39 de la Ley General de Control Interno Nº 8292, publicada en La Gaceta Nº 169 de 4 de setiembre del 2002:

> ***"Artículo 36.- Informes dirigidos a los titulares subordinados***
>
> *Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*
>
> *a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*
>
> *b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.*
>
> *c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.*
>
> ***Artículo 37.- Informes dirigidos al jerarca***
>
> *Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente.*

Artículo 38.- Planteamiento de conflictos ante la Contraloría General de la República

Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.

La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994.

Artículo 39.- Causales de responsabilidad administrativa

El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios..."

2. RESULTADOS DEL ESTUDIO

Se clasificó cada uno de los hallazgos según la ponderación de riesgo que pudiera causar algún daño o perjuicio a la Junta de Protección Social si se llegara a materializar, tal como se muestra a continuación:

Riesgo alto:

El hallazgo se clasificó de riesgo alto si el sistema, equipo o plataforma es de carácter crítico para el negocio así como el nivel de gravedad o deficiencia.

Riesgo medio:

Es de riesgo medio si el sistema, equipo o plataforma es de carácter importante para el negocio pero que no implica la detención de las actividades más críticas del negocio, así como el nivel de gravedad del hallazgo o deficiencia.

Riesgo bajo:

Es de riesgo bajo si el sistema, equipo o plataforma es alternativa y no detiene las actividades del negocio

Asimismo, la solución de los hallazgos se clasificó de acuerdo a la facilidad de la resolución según la siguiente escala:

Solución compleja:

- Implica involucrar no sólo recursos humanos del Área de Tecnología, sino de otras áreas relacionadas con el hallazgo.
- Implica una inversión económica significativa.
- Implica una inversión de tiempo significativa.
- La solución requiere un alto nivel de planificación.
- Está dentro de las prioridades que la empresa si desea atender de manera inmediata.

Solución moderada

- Implica una inversión económica manejable.
- Implica una inversión de tiempo manejable.
- La solución requiere de algún nivel de planificación o ejecución, que demanda cierto nivel de atención especial a los planes de acción.

Solución trivial

- Se disponen de los recursos técnicos y tecnológicos para resolverlo.
- Solución a bajo o ningún costo.
- Solución rápida de aplicar.
- Poca o mediana inversión de tiempo.
- Implica recurso humano del área de tecnología, lo cual facilita la asignación de tareas.

A continuación se muestran los hallazgos determinados en el informe emitido por la empresa Price Waterhouse Cooper.

A. Hallazgos relacionados con la seguridad lógica y física de los dispositivos de comunicación entre Socios Comerciales y la Junta de Protección Social.

A.1 Seguridad lógica

Descripción del hallazgo	Nivel de riesgo	Facilidad de resolución
1. Se identificó que actualmente no existen mecanismos de monitoreo para el control de los equipos involucrados en las conexiones de internet. La falta de monitoreo constante puede provocar que una alta cantidad de tráfico no deseado viaje a través de la red, además existe la dificultad de controlar el desempeño de los diferentes dispositivos de la infraestructura de red.	Medio	Moderada
2. Durante el proceso del estudio se pudo observar que no existen comentarios que definan o describan de forma general las interfaces de switch[1] capa 3. En el momento que se de alguna eventualidad, la capacidad de reacción y cambio va a ser un proceso más lento por motivo de que las interfaces no tienen descripción y es difícil identificarlas.	Bajo	Trivial

A.2 Seguridad y distribución física

Descripción del hallazgo	Nivel de riesgo	Facilidad de resolución
3. Durante la revisión de la seguridad física en el Departamento de Informática, se observó que la tarjeta magnética usada por los funcionarios de ese departamento para acceder a la sala de cómputo, se encuentra adherida al carnet que identifica como funcionario de la Junta de Protección Social. Esta situación podría ocasionar que en caso de que el carnet sea extraviado por algún funcionario del Departamento de Informática, un tercero pueda tener acceso de igual manera a la tarjeta magnética, conocer a donde pertenece y eventualmente tener acceso a la sala donde se encuentran los servidores y equipos de comunicación.	Medio	Trivial

[1] *Switch* es un dispositivo digital lógico de interconexión de redes de computadoras que opera en la capa de enlace de datos del modelo OSI

Descripción del hallazgo	Nivel de riesgo	Facilidad de resolución
4. Las salas de cómputo y comunicaciones del Departamento de Informática, poseen paredes de vidrio, no resistentes a impactos por lo que podrían ser fácilmente violentadas. Las paredes de vidrio incrementan el riesgo de acceso a los equipos por parte de personas no autorizadas.	Medio	Moderada
5. Se observó que dentro del Departamento de Informática, no existe una bitácora de acceso para ingresar a las salas de cómputo y comunicaciones. Esta situación impide que se lleve un mejor control acerca de las personas que ingresan a la sala de cómputo diluyendo la responsabilidad si eventualmente ocurre un problema o incidente en dicha sala.	Medio	Trivial
6. Durante la revisión a la sala de cómputo y comunicaciones del Departamento de Informática se observó la inexistencia de dispositivos detectores de humedad. La ausencia de estos detectores puede retardar la detección de altos o bajos niveles de humedad que pudieren afectar el normal funcionamiento de los equipos que se encuentran en la sala de cómputo y comunicaciones.	Medio	Trivial
7. Durante la revisión a las salas de cómputo y comunicaciones, se logró observar que existen objetos que no corresponden a esas salas como por ejemplo un mueble con papeles (licencias de software). La papelería encontrada en las salas descritas por ser material combustible, podría provocar posibles conatos de incendio.	Bajo	Trivial
8. La distribución del cableado conectado a los equipos de las salas de cómputo y comunicaciones no es la adecuada, dichos cables no se encuentran rotulados. La falta de identificación del cableado dificulta la identificación de éste en caso de alguna irregularidad que se presente o en labores de soporte, al tener que ubicar a que equipo pertenece el cableado.	Medio	Moderada

B. Hallazgos relacionados con la seguridad de la aplicación de apuestas deportivas.

Descripción del hallazgo	Nivel de riesgo	Facilidad de resolución
9. La aplicación utilizada por los socios comerciales para realizar apuestas deportivas hace uso de un solo factor de autenticación para validar el ingreso al mismo por parte de dichos usuarios (utiliza solo contraseña del usuario), adicionalmente existen socios comerciales que comparten dicha contraseña para hacer uso de la aplicación citada. La práctica de compartir contraseñas, aunada a que existe un sólo factor de autenticación, puede eventualmente provocar que personas ajenas al socio comercial o a sus autorizados, tengan acceso a la contraseña y realizar apuestas.	Alto	Compleja
10. La aplicación de apuestas deportivas no posee controles para cumplir con los requerimientos de complejidad de las contraseñas utilizadas por los socios comerciales. En este sentido, de una muestra de 50 cuentas se observó que 13 tenían como contraseña el mismo nombre de la cuenta (nombre de usuario). Estas contraseñas se encuentran en detalle en el informe emitido por la empresa Price Waterhouse Cooper. Esta situación permite a los socios comerciales definir contraseñas de fácil deducción, lo que podría ocasionar que un intruso pueda obtener la contraseña y accesar al sistema de apuestas.	Alto	Moderada
11. La aplicación de apuestas deportivas no posee un control para la expiración de la contraseña de los usuarios. El hecho de que una contraseña permanezca invariable por un período prolongado podría aumentar la probabilidad de que un intruso pueda identificarla.	Medio	Moderada

C. Estudio completo de la distribución física de las conexiones de Internet.

Según estudio realizado, durante la evaluación de la seguridad Física y Ambiental de las conexiones de Internet, la comprobación de la existencia de redundancia de enlaces y fuentes eléctricas, y la verificación de la existencia de un sitio alterno no se encontraron hallazgos que tuvieran impacto sobre el juego Progol.

D. Seguridad e integridad de los datos de la base de datos en el momento de hacerse las apuestas deportivas.

En relación con el estudio elaborado, para cada una de las apuestas efectuadas en los puestos de los Socios Comerciales se revisó la integridad de dichas transacciones en la base de datos y no se obtuvieron hallazgos que impactaran en la seguridad del juego Progol.

E. Capacidad de respuesta ante una posible contingencia en el momento de realizarse las apuestas deportivas.

Según estudio ejecutado, durante la verificación de los planes de contingencia ante posibles fallas no se encontraron hallazgos relevantes que pudieran ocasionar la caída del servicio.

F. Pruebas de penetración de la seguridad de los servidores y equipos de cómputo involucrados en las apuestas deportivas.

F.1 Servidores de la Junta de Protección Social

Descripción del hallazgo	Nivel de riesgo	Facilidad de resolución
12. Se identificó la existencia de un mecanismo de autenticación el cual se realiza en texto claro (sin encriptar) ubicado en el servidor de base de datos "obrenes1". Un intruso con acceso a la red y al equipo podría obtener las credenciales de acceso realizando un "sniffing"[2] en el tráfico de la red.	Medio	Moderada
13. Se identificó el uso de protocolos de comunicación inseguros como Telnet y FTP[3], los cuales permiten el envío de las credenciales de autenticación en texto claro (sin encriptar) a través de la red. Al igual que en el hallazgo anterior mediante un "sniffing" un intruso podría obtener credenciales de acceso al tráfico de la red.	Medio	Moderada

[2] El sniffer es un software que permite capturar tramas de la red. Generalmente utilizado con fines maliciosos para capturar textos de emails, chats, datos personales, contraseñas, etc.

[3] Telnet es un programa que permite acceder a ordenadores distantes en Internet a los cuales se tiene acceso FTP siglas de File Transfer Protocol. Método muy común para transferir uno o más ficheros de un ordenador a otro.

Descripción del hallazgo	Nivel de riesgo	Facilidad de resolución
14. Se identificó la posibilidad de generar una lista de los servicios RPC (Remote Procedure Call)[4] que están siendo ejecutados. Un intruso podría generar una lista de los servicios RPC que están siendo ejecutados en el servidor con el fin de identificar las vulnerabilidades que puedan ser explotadas.	Bajo	Moderada
15. Se identificó que la secuencia de números en el proceso de establecimiento de conexión TCP[5] es de fácil aproximación. Los puertos que se ven afectados por esta vulnerabilidad son puerto 111 (RPC) y puerto 21 (Telnet). El servidor es "obrenes1". Algún intruso que pueda explotar esta vulnerabilidad podría realizar un ataque de denegación en el servicio TCP del servidor mencionado.	Bajo	Moderada
16. Se identificó que se encuentra habilitado el método de comunicación HTTP TRACE[6] el cual es inseguro debido a que es vulnerable a ataques "cross-site tracing"[7] los servidores involucrados son: "obrenes1" y " Servidor Web". Si esta vulnerabilidad es explotada por personas inescrupulosas, las credenciales de autenticación de usuarios del servidor podrían ser comprometidas, de manera que se podrían detectar contraseñas e información sensible que viaja a través de la red.	Bajo	Moderada
17. El atributo de autocompletado de la contraseña no está deshabilitado los servidores que validan esta característica son "obrenes1" y "Servidor Web". Con este atributo habilitado, la contraseña ingresada por un usuario podría ser almacenada en el sistema operativo y ser recuperada por otro usuario que utilice el computador.	Medio	Moderada

[4] El **Remote Procedure Call (Llamada a Procedimiento Remoto)** es un protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.

[5] TCP/IP (Transmission Control Protocol) es el lenguaje que rige todas las comunicaciones entre todos los ordenadores en Internet.

[6] Http trace, es un método de solicitud usado para la depuración de aplicaciones.

[7] **Cross-site tracing** es una vulnerabilidad de la seguridad de la web expotada por medio del método HTTP Trace

Descripción del hallazgo	Nivel de riesgo	Facilidad de resolución
18. Se identificó que se está haciendo uso de la versión 8 del sistema operativo Solaris, la cual está obsoleta y ya no es soportada por el proveedor desde Abril de 2012. Con una versión del sistema operativo obsoleta, el sistema se encuentra en riesgo de ser expuesto a vulnerabilidades de seguridad debido a que el proveedor ya no liberara parches de actualización de seguridad.	Alto	Moderada
19. La función DNS Zone Transfer[8] no está restringida y puede ser ejecutada por cualquier usuario. La falta de restricción del DNS[9] podría provocar que un usuario no autorizado tenga acceso a nombres y direcciones IP de otros servidores de la organización con lo cual podría eventualmente realizar intentos maliciosos de robo y modificación de información.	Medio	Trivial
20. La aplicación Adobe ColdFusion[10] está expuesta a múltiples vulnerabilidades de tipo cross-site scripting. Lo anterior puede permitir a un atacante a través de una conexión remota, ejecutar código malicioso tales como virus, malware y spyware en el navegador del usuario.	Medio	Trivial
21. Las IDs de sesiones de usuario, al momento de autenticarse en el servidor donde radica el sistema de apuestas deportivas, son predecibles. Esta situación podría permitir a un atacante deducir fácilmente el ID de sesión de un usuario y por consiguiente tener acceso de forma no autorizada a la aplicación de apuestas deportivas.	Medio	Trivial

[8] DNS Zone transfer, es uno de muchos mecanismos para replicar las bases de datos DNS a través de un grupo de servidores.
[9] DNS es un sistema que asocia direcciones IP con nombres de dominio.
[10] **Adobe ColdFusion** es un servidor de aplicaciones y un lenguaje de programación usado para desarrollar aplicaciones de Internet.

F.2 Equipos de cómputo de los Socios Comerciales

Descripción del hallazgo	Nivel de riesgo	Facilidad de resolución
22. Según revisión efectuada a los equipos de los socios comerciales según muestra seleccionada, se observó que los equipos que se mencionan a continuación, no tenían el protector de pantalla configurado con contraseña. Juan Luis Ávila Morales El Roble de Puntarenas (1 equipo) Oficinas Centrales JPS -San José (1 equipo) Carlos Artavia Prada -Perez Zeledón (1 equipo) Gerardo Sojo Flores -Heredia (3 equipos) Carlos Cruz Chan -Guápiles (3 equipos) Stephanie García del Valle -Liberia (2 equipos) Alejo Ramírez Campos -Cañas Guanacaste (1 equipo) Jorge Venegas Rojas -Cartago (1 equipo) En caso de que el protector de pantalla se encuentre deshabilitado por un periodo de tiempo prolongado, puede facilitarle a un intruso el acceso al equipo y por consiguiente al sistema de apuestas deportivas.	Medio	Trivial
23. Se observaron ocho equipos de socios comerciales que tenían instaladas herramientas que permiten acceder a éstos de manera remota, tal como el Team Viewer[11], a continuación el detalle: Carlos Artavia Prada -Perez Zeledón (1 equipo) Jorge Venegas Rojas -Cartago (1 equipo) Gerardo Sojo Flores -Heredia (3 equipos) Carlos Cruz Chan -Guápiles (3 equipos)	Medio	Trivial
24. Se observó en dos equipos de socios comerciales que los programas antivirus estaban desactualizados, estos son: Carlos Cruz Chan -Guápiles (1 equipo) Stephanie García del Valle -Liberia (1 equipo) La no actualización de los programas antivirus aumenta la posibilidad de que el equipo sea infectado con un virus informático pudiendo eventualmente comprometer las credenciales de acceso de la aplicación de apuestas deportivas.	Medio	Trivial

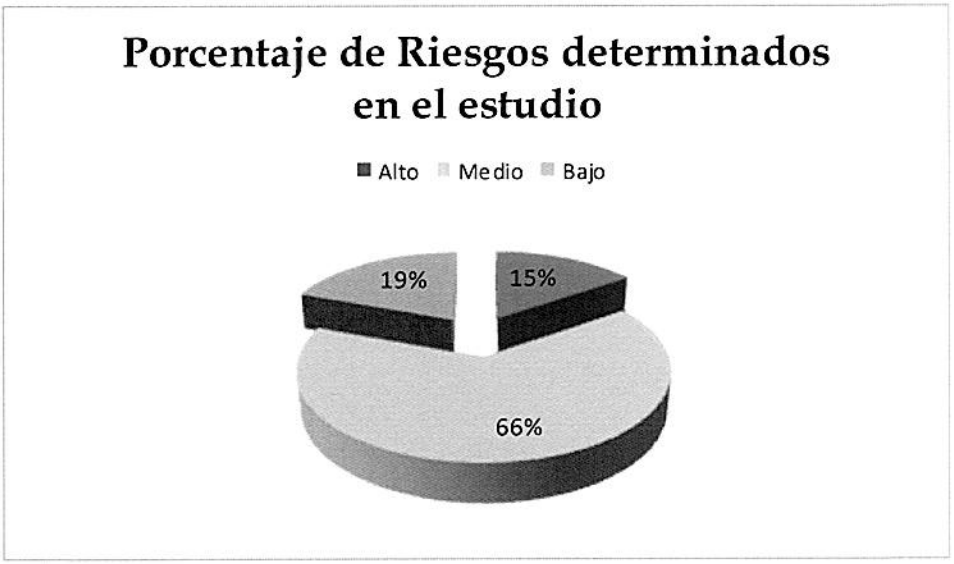
[11] Teamviewer, es un software que permite accesar a los computadores desde otro equipo, sin tener que pensar en direcciones IP

Descripción del hallazgo	Nivel de riesgo	Facilidad de resolución
25. De los socios comerciales visitado se observó que dos de ellos tenían sus nombre de usuario y contraseña escritas en un papel ubicado en lugares de fácil acceso a terceros, dichos socios comerciales son: Carlos Cruz Chan -Guápiles Gerardo Sojo Flores -Heredia Esta situación podría facilitar que un intruso tenga al alcance las credenciales de acceso al sistema de apuestas deportivas de forma no autorizada.	Alto	Trivial
26. Se observó el uso compartido de cuentas y contraseñas en 14 equipos utilizados por los socios comerciales donde comercializan el juego Progol, dichos equipos son: Carlos Cruz Chan -Guápiles (4 equipos) Gerardo Sojo Flores -Heredia (2 equipos) Juan Luis Ávila Morales -El Roble Puntarenas (1 equipo) Carlos Artavia Prada -Perez Zeledón (1 equipo) Mynor Bermúdez Solano -Cartago (1 equipo) Jorge Venegas Rojas -Cartago (1 equipo) Stephanie García del Valle -Liberia (2 equipos) Alejo Ramírez Campos -Cañas Guanacaste (1 equipo) Felipe Díaz Miranda -Santa Ana (1 equipo) Esta práctica usada por los socios comerciales dificulta el seguimiento de las acciones ejecutadas por dichos usuarios y atribuir las responsabilidades en caso de ocurrir alguna eventualidad.	Medio	Trivial

3. RESUMEN PORCENTUAL DE LOS HALLAZGOS IDENTIFICADOS EN TERMINOS DE RIESGOS

Como resultado de los servicios dados por la empresa Price Waterhouse Cooper Consultores S.A. a la Auditoría Interna de la Junta de Protección Social, se identificaron veintiséis hallazgos, los cuales como se indicó al principio, fueron clasificados en tres niveles de riesgo: Alto, Medio y Bajo, siendo esta categoría establecida por el impacto que puede ocasionar en el cumplimiento de los objetivos institucionales. A continuación el detalle:

✓	Riesgo Alto:	4	hallazgos
✓	Riesgo Medio:	17	hallazgos
✓	Riesgo Bajo.	5	hallazgos
	Total	26	hallazgos



Asimismo se grafica la "facilidad de resolución" de los hallazgos detectados con la finalidad de visualizar que tan complejo podría ser el cumplimiento de las recomendaciones, para determinar lo anterior, cada resolución fue clasificada en Trivial, Moderada y Compleja:

✓	Trivial:	13	recomendaciones
✓	Moderada:	12	recomendaciones
✓	Compleja:	1	recomendación
	Total	26	recomendaciones

Nótese que en su mayoría las recomendaciones están dentro de las clasificaciones de Moderada y Trivial para la resolución correspondiente, sólo una de ellas fue calificada como compleja de cumplir.

En relación con los aspectos observados durante la ejecución del estudio y descritos en los puntos anteriores, las "Normas técnicas para la gestión y el control de las tecnologías de información" emitidas mediante circular de la Contraloría General de la República N-2-2007-CO-DFOE citan:

1.4.1 Implementación de un marco de seguridad de la información

La organización debe implementar un marco de seguridad de la información, para lo cual debe:

a. *Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.*
b. *Mantener una vigilancia constante sobre todo el marco de seguridad y definir y ejecutar periódicamente acciones para su actualización.*

1.4.3 Seguridad física y ambiental

La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos. Como parte de esa protección debe considerar:

a. Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.
b. La ubicación física segura de los recursos de TI.
...
g. El acceso de terceros.
h. Los riesgos asociados con el ambiente.

1.4.4 Seguridad en las operaciones y comunicaciones

La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe:

a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.
...
c. Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus.

4.2 Administración y operación de la plataforma tecnológica

La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:

c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.

4.3 Administración de los datos

La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura.

4. CONCLUSIONES

De acuerdo a la categorización dada a los hallazgos determinados en el estudio, en cuanto a su nivel de riesgo, se tiene que: un 66% de los mismos se consideran de riesgo medio, un 19% de riesgo bajo y un 15% de riesgo alto, aunque el porcentaje de riesgos altos es bajo, la cantidad de riesgos medios supera el 50% del total, los cuales en conjunto pueden vulnerabilizar el control interno en general y en el entorno que involucra el juego Progol, desde los procedimientos y equipos empleados por los socios comerciales hasta los procedimientos y equipos utilizados en la Institución para finalmente comercializar ese producto.

Los resultados del estudio, demuestran la necesidad de fortalecer los controles en el área de la seguridad y distribución física del Departamento de Informática en aspectos como bitácoras de acceso, paredes con poca seguridad y dispositivos detectores de humo, procurando con ello fortalecer y proteger los recursos de la Junta de Protección Social.

Además, con el diseño de la aplicación Web Transaccional para los socios comerciales, la Junta de Protección Social debe fortalecer la seguridad de la aplicación y su imagen en Internet, con la implementación de métodos de seguridad de ingreso al sistema por parte de los socios aplicando requerimientos en las contraseñas tales como complejidad y expiración.

Otra de las áreas donde existen hallazgos de nivel de riesgo medio, es en aspectos relacionados con los servidores de la Junta ubicados en el Departamento de Informática, en éstos se identificaron protocolos de comunicación inseguros, método de comunicación vulnerable, una versión de sistema operativo obsoleta lo cual es de riesgo alto y uso de IDs de sesiones de usuario predecibles.

En cuanto a los equipos de los socios comerciales, en su mayoría, los niveles de riesgo son medios y es importante destacar, entre otros aspectos, que las versiones de antivirus usados por estos socios están desactualizadas, el protector de pantalla no está configurado para activarse cuando el equipo esté sin usar por algunos

segundos o minutos, las cuentas y contraseñas de usuario son compartidas con otras personas y además cuando éstas son escritas en papel, son dejadas en lugares de fácil acceso. Lo anterior, son aspectos que debilitan el control interno existente alrededor de la venta de productos promocionados por la Junta a través de los socios comerciales.

Es importante indicar además que, para lograr niveles de seguridad razonables, se debe continuar con el proceso de fortalecimiento de los equipos de seguridad, monitoreo constante de transacciones e incentivar la cultura del riesgo tanto en el personal de Informática como en los socios comerciales, todo lo anterior, alineado a los procesos de negocio y la estrategia global de la Institución.

5. RECOMENDACIONES

Al señor Ronald Ortiz Méndez, Jefe del Departamento de Informática: (el número de recomendación hace referencia al número de hallazgo)

1. Se recomienda tener equipo destinado para el monitoreo continuo de las comunicaciones, especialmente en los equipos utilizados para las conexiones a Internet.

2. Se recomienda agregar comentarios informativos en la configuración del switch de capa 3.

3. Se recomienda que los funcionarios del Departamento de Informática, porten el carné de identificación y la tarjeta magnética utilizada para el ingreso a dicho Departamento, en lugares separados, con el fin de evitar de que en caso de que la tarjeta magnética sea extraviada, el tercero que la encuentre desconozca el lugar donde pertenece.

4. Se recomienda proteger las paredes de la sala de cómputo y comunicaciones con un material no vulnerable a agresiones externas o rompimiento por accidente.

5. Se recomienda la utilización de bitácoras de acceso para controlar el ingreso a las salas de cómputo y comunicaciones.

6. Se recomienda utilizar detectores de humedad dentro de la sala de servidores, así como monitorearlos periódicamente.

7. Se recomienda trasladar el mueble ubicado en las salas de cómputo y comunicaciones y su contenido (papelería), en un lugar distinto a dichas salas, donde no exista la posibilidad de incendio.

8. Se recomienda optimizar la distribución del cableado de las salas de cómputo y comunicaciones de manera organizada y rotularlo de acuerdo a un estándar preestablecido que permita identificar a qué equipos se encuentran conectados.

9. Debido a la sensibilidad de las transacciones realizadas en la aplicación para realizar apuestas deportivas, se recomienda hacer uso de un segundo factor de autenticación como por ejemplo certificados digitales instalados en los puntos de ventas autorizados.

10. Se recomienda que en la aplicación para realizar apuestas deportivas, se definan controles para el cumplimiento de los requerimientos de complejidad de las contraseñas, impidiendo al usuario definir contraseñas de fácil deducción como por ejemplo el mismo nombre de la cuenta, números consecutivos, números de cédula de identidad, entre otros. Se recomienda el uso de combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales. Previo a la implantación de este control, se recomienda la concientización hacia los usuarios.

11. Se recomienda la definición dentro del sistema de apuestas de Progol, de un control que obligue al usuario (socios comerciales) a cambiar la contraseña al menos cada 90 días acorde a las mejores prácticas de seguridad.

12. Se recomienda la implementación de un mecanismo que permita cifrar las credenciales de acceso antes de ser enviadas del cliente al servidor a través del uso de un puerto seguro como 443 (https) o cifrados a nivel de la aplicación a través del uso del algoritmo MD5.

13. Se recomienda el uso de protocolos de comunicación seguros como SSH, el cual cifra las credenciales de acceso antes de ser enviadas a la red.

14. Se recomienda remover cualquier servicio RPC (Remote procedure call) que no sea estrictamente necesario para las funciones de la organización.

15. Se recomienda filtrar el puerto *portmapper* (puerto 111) a través de un firewall o cerrar los puertos mencionados en el punto N° 15 de este estudio, que no sean estrictamente necesarios para las funciones de la organización.

16. Se recomienda deshabilitar el método de comunicación HTTP TRACE en caso de no ser requerido. De lo contrario, solo habilitarlo temporalmente en el momento en que se requiera, ya que con este método de comunicación eventualmente se pueden detectar contraseñas e información sensible que viaje a través de la red.

17. Se recomienda deshabilitar el atributo *AutoComplete* para el campo de texto correspondiente a la contraseña en el servidor Web y en el equipo "obrenes1". Del mismo modo, se recomienda deshabilitar este atributo para el campo de texto correspondiente al nombre del usuario.

18. En cumplimiento a la Norma 1.4.4 Seguridad en las operaciones y comunicaciones de las Normas técnicas para la gestión y el control de las tecnologías de información emitido por la Contraloría General de la República se recomienda el uso de software no obsoleto.

19. Se recomienda restringir el *Zone Transfer* únicamente a servidores DNS del mismo dominio. Si se usa un solo servidor de DNS, se recomienda deshabilitar el *Zone Transfer*.

20. Se recomienda actualizar la aplicación Adobe ColdFusion con los parches liberados por el proveedor.

21. Se recomienda usar un algoritmo de cifrado robusto que genere ID de sesiones de usuario de forma aleatoria, de tal manera que no sean tan predecibles como los citados en el punto 21 de este informe.

22. Se sugiere recomendar a los Socios Comerciales la activación del protector de pantalla con contraseña, debido a que la no activación del mismo representa un riesgo para la aplicación de la Junta de Protección Social.

23. Se recomienda sugerir a los Socios Comerciales no instalar aplicaciones que representen un riesgo para la seguridad del equipo desde donde se realizan las apuestas deportivas.

24. Recomendar a los Socios Comerciales mantener actualizado sus programas de antivirus a fin de mantener protegido el equipo de código malicioso.

25. Recomendar a los Socios Comerciales dejar la práctica de tener la contraseña y nombre de usuario escritas en papel en lugares visibles, indicándoles los riesgos asociados de mantener dicha práctica.

26. Recomendar a los Socios Comerciales no compartir las cuentas y contraseñas y asignar por parte de Informática una cuenta y contraseña por usuario.

Realizado por:
Lic. Andres Martínez Porras
Profesional II

Revisado por:
Lic. José Alberto Wong Carrión
Jefe de Área

Aprobado por:
M.Sc. Doris María Chen Cheang
Auditora Interna