MR – SPEL. MARCO DE REFERENCIA PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE PAGOS EN LÍNEA DE UNIVERSIDADES OFICIALES EN COLOMBIA

ANEXOS

YOHANA ANDREA TRUJILLO CAIPE
FIDEL CAMILO HIDALGO ZAMBRANO

Director: Ing. SILER AMADOR DONADO

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Sistemas
Área de Investigación: Seguridad Informática
Popayán, Junio de 2010

TABLA DE CONTENIDO

ANEXO A PLAN DE ACTIVIDADES PROPUESTO POR ACH COLOMBIA

En este anexo se presenta el cronograma que propone ACH Colombia para el desarrollo del SPEL.

ENTIDAD COMERCIAL: _____

Líder de Proyecto _____

Contacto en Sistemas: _____

Contacto en otras áreas: _____

Día para reuniones de seguimiento: _____

Fecha producción estimada: _____

ACTIVIDADES	
	FASE 1 - PREPARACION DEL PROYECTO
1.1	PRESENTACION GENERAL DEL SERVICIO
1.2	PRESENTACION ANTE PSE
1.3	CARTA PRESENTACION ENTIDAD FINANCIERA
1.4	ASIGNACION LIDER DEL PROYECTO
1.5	ENTREGA DE INFORMACION TECNICA Y OPERATIVA(FORMATOS, ETC)
1.6	SOLICITUD CODIGO GLN(IAC)
1.7	PRESENTACCION TECNICA DEL PROYECTO
1.8	REUNION DE SEGUIMIENTO
	FASE 2 - DESARROLLOS DE SOFTWARE
2.1	INSTALAR SERVIDOR DE PRUEBAS
2.2	INSTALAR SOFWARE AMBIENTAL

2.3	Resolver dudas con el coordinador asignado EN pse
2.4	Web Services "getbanklist"
2.5	Web Services "createtransactionpayment"
2.6	Web Services "Finalizetransactionpayment"
2.7	Sonda "getTransactioninformation"
2.8	DESARROLLO O AJUSTE AL SITIO TRANSACCIONAL
2.9	CONCILIACION
2.10	REUNION DE SEGUIMIENTO
	FASE 3 - SEGURIDAD Y COMUNICACIONES AMBIENTE DE PRUEBAS
3.1	DEFINIR E INFORMAR IP PUBLICAS PARA SITIO WEB Y TERMINADOR VPN
3.2	CONSECUCION E INSTALACION DE CERTIFICADOS DE PRUEBA
3.3	CONSECUSION TERMINADOR VPN*
3.4	INSTALACION Y CONFIGURACION TERMINADOR VPN
3.5	ESTABLECER CONEXIÓN Y SEGURIDADES CON PSE
3.6	DEFINIR PERMISOS EN LOS FIREWALL
3.7	REUNION DE SEGUIMIENTO
	FASE 4 - ETAPA FUNCIONAL
4.1	ELABORACION DE PROCEDIMIENTOS (Internos y con Clientes)
4.2	PARAMETRIZACION MODULOS ADMINISTRATIVO
4.3	DEFINICION DECK DE PRUEBAS INTERNO
4.4	ENTREGA DOCUMENTOS FUNCIONALES
4.5	REUNION DE SEGUIMIENTO
	FASE 5 - PRUEBAS INTERNAS
5.1	PRUEBAS SITIO WEB
5.2	PRUEBAS TRANSACCIONALES CLIENTE
5.3	PRUEBAS RECAUDOS
5.4	PRUEBAS DE CONCILIACION
5.5	PRUEBAS INTEGRALES:CLIENTE - COMERCIO - PSE - BANCO
5.6	REUNION DE SEGUIMIENTO
	FASE 6 - PRUEBAS PSE
6.1	Fase I. Pruebas a Nivel de Aplicativo como Entidad Comercial
6.2	Fase II. Pruebas Integrales de Ciclo Completo Simulado en PSE
6.3	Fase III. Verificaciones Ambientales
6.4	CERTIFICACION PSE

6.5	REUNION DE SEGUIMIENTO
	FASE 7 - PREPARACION PRODUCCION
7.1	ENTREGA DE FORMULARIOS OPERATIVOS DEFINITIVOS CODIGO GLN
7.2	ENTREGA DE FORMULARIO ADMINISTRADORES(DE CUENTAS Y DE USUARIOS)
7.3	ENTREGA ACTA DE PRUEBA FINAL
7.4	SOLICITUD DE CERTIFICADO DEFINITIVO CERTICAMARA
7.5	DEFINICION DE AREA Y FUNCIONARIOS RESPONSABLES DE LA OPERACIÓN
7.6	DEFINICION ESTRATEGIA COMERCIAL
7.7	CAPACITACION MODULO ADMINISTRATIVO
7.8	REUNION DE SEGUIMIENTO
	FASE 8 - SEGURIDAD Y COMUNICACIONES AMBIENTE DE PRODUCCION
8.1	DEFINIR E INFORMAR IP PUBLICAS PARA SITIO WEB Y TERMINADOR VPN
8.2	INSTALACION DE CERTIFICADOS DE PRODUCCION
8.3	CONFIGURACION TERMINADOR VPN
8.4	ESTABLECER CONEXIÓN Y SEGURIDADES CON PSE PRODUCCION
8.5	DEFINIR PERMISOS EN LOS FIREWALL
8.6	REUNION DE SEGUIMIENTO
	FASE 9 - MIGRACION A PRODUCCION
9.1	INSTALAR SERVIDOR DE PRODUCCION
9.2	INSTALAR SOFWARE AMBIENTAL
9.3	INSTALAR SOFTWARE APLICATIVO
9.4	CONFIGURACION PARAMETROS APLICATIVOS
9.5	REUNION DE SEGUIMIENTO
	FASE 10 - PRODUCCION TOTAL
10.1	**MARCHA BLANCA**
10.2	DIVULGACION CLIENTES
10.3	CAPACITACIONES A GRUPO COMERCIAL
10.4	REUNION DE SEGUIMIENTO

Funcionarios de apoyo en ACH COLOMBIA S. A.
Jaime Martínez - Director de Sistemas;
Edgar Avila Perdomo- Director Unidades de Negocio,
Recomendamos enviar un reporte semanal a jmartinez@achcolombia.com.co informando los adelantos y los inconvenientes presentados en el desarrollo.

ANEXO B ACUERDO DE CONFIDENCIALIDAD

UNIVERSIDAD DEL CAUCA

DIVISION DE SISTEMAS

Yo, _____, identificada con cédula de ciudadanía número _____, en calidad de miembro activo de la DIVISIÓN DE SISTEMAS de la UNIVERSIDAD DEL CAUCA, he conocido y tenido acceso, y conoceré o tendré acceso a ciertos datos e informaciones confidenciales de todos y cada uno de los miembros de la DIVISION DE SISTEMAS y de su director técnico y coordinador. Que la voluntad mía, es que tales datos e informaciones permanezcan confidenciales. Que por lo anterior, la DIVISION DE SISTEMAS y yo hemos estimado conveniente regular el alcance de esta carta de compromiso de confidencialidad.

En consecuencia, las partes han decidido celebrar este Acuerdo, que se regirá por las siguientes Cláusulas:

PRIMERA: Yo, _____, mantendré bajo reserva y no podré propagar, difundir o usar en beneficio propio o de terceros la totalidad o parte de y cualquier dato o información considerada por la DIVISION DE SISTEMAS y el SPEL como “información confidencial”, que pertenezca u obtenga de la DIVISION DE SISTEMAS y el SPEL, al igual que de sus integrantes, sus empleados, sus representantes, su director o coordinador que maneje información acerca de: resultados, conocimiento, las soluciones o métodos de operaciones, procedimientos, ideas, equipos, productos, diseños y estrategias de mercado de la DIVISION DE SISTEMAS, así como todo el secreto en I + D + I de la DIVISION DE SISTEMAS y el SPEL. Los conocimientos reservados de sobre ideas, desarrollos, métodos, productos o procedimientos investigativos con aplicaciones industriales que la DIVISION DE SISTEMAS y el SPEL por su valor competitivo desean mantener confidenciales, y en especial, los productos, procesos, Know-how, técnicas, diseños y cualquier otro mecanismo o métodos de propiedad intelectual desarrollados o manejados por la DIVISION DE SISTEMAS y el SPEL.

PARAGRAFO N° 1: Así mismo, la DIVISION DE SISTEMAS y el SPEL desean mantener en secreto sus bases de datos e informaciones propias de su trabajo, tales como métodos, resultados, análisis de laboratorio, proyectos, actividades, proveedores, negocios, contratos, asuntos de interés privado, y otras actividades inherentes a su específica actividad investigativa, de desarrollo e innovación, o comercial por lo cual quedan contenidos en esta Carta de Confidencialidad.

PARAGRAFO Nº 2: Yo, _____, no podré apropiarme, revelar o utilizar el contenido del secreto de la DIVISION DE SISTEMAS y el SPEL descrito para ellos, para mi beneficio directo o indirecto o de terceros, excepto la DIVISION DE SISTEMAS mismo, salvo autorización previa y por escrito de la DIVISION DE SISTEMAS.

PARÁGRAFO Nº 3: Sin perjuicio de lo anterior, yo debo guardar especial diligencia en el cumplimiento de las obligaciones de este acuerdo tratándose de aquellos datos e informaciones que la DIVISION DE SISTEMAS y el SPEL designe expresamente como "CONFIDENCIALES" al momento que en representación de la DIVISION DE SISTEMAS vaya a exponerlos o hacerlos conocer de los clientes, demás personas o interesados en investigaciones, negociaciones, acuerdos o actividades en I+D+I o comerciales con la DIVISION DE SISTEMAS.

SEGUNDA: Este acuerdo tendrá un término de vigencia exactamente igual a mi permanencia como miembro activo de la DIVISION DE SISTEMAS, quien observaré las obligaciones contenidas en el presente acuerdo durante el término de vigencia de este, más un año contado a partir de la fecha en la cual el presente acuerdo haya expirado, a menos que la DIVISION DE SISTEMAS acuerde por escrito otra cosa conmigo, sin perjuicio de la protección de la información confidencial que haya sido conocida con anterioridad a la suscripción del presente documento. Adicionalmente, debo solicitar autorización de la DIVISION DE SISTEMAS para hacer uso de la información para cualquier fin, una vez termine el tiempo total estipulado de duración del presente acuerdo.

TERCERA: Salvo advertencia en contrario de la DIVISION DE SISTEMAS, yo debo entender que todo documento, modelo, diseño, presentación o cualquier otro método que conozca o al que tenga acceso en relación o con ocasión de la ejecución de proyectos, negociación, celebración y ejecución de este acuerdo son de propiedad exclusiva de la DIVISION DE SISTEMAS y están amparados, en lo

pertinente, por toda la legislación vigente en autoría de derechos de autor y propiedad intelectual de la Universidad del Cauca.

CUARTA: Este acuerdo se celebra en consideración a la calidad de las personas que en él intervinieron, por lo tanto sólo podrá cederse, modificarse o terminarse, en todo o en parte, mediante mutuo acuerdo consignado por escrito y firmado por ambas partes.

En constancia de lo anterior, en la ciudad de Popayán, a los ____ días del mes de _____ del año _____.

Integrante DIVISION DE SISTEMAS	Jefe DIVISION DE SISTEMAS
_____	_____
C.C.	C.C.

ANEXO C CONTROL DE INGRESO A LA SALA DE SERVIDORES

FECHA	HORA ENTRADA	NOMBRE	CARGO	MOTIVO DE INGRESO	HORA DE SALIDA	FIRMA

SUPERVISADO POR:

FIRMA:

CC:

ANEXO D ENCUESTA SPEL UNIVERSIDADES OFICIALES DE COLOMBIA

Teniendo en cuenta su intención de colaborar con el desarrollo del proyecto *MR – SPEL. MARCO DE REFERENCIA PARA LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL SISTEMA DE PAGOS EN LÍNEA DE UNIVERSIDADES OFICIALES EN COLOMBIA*, solicitamos realizar esta encuesta por las personas idóneas, con el fin de conocer y analizar el estado actual del sistema de pago en línea SPEL[1] con respecto a la seguridad de la información SI[2] que se maneja en las diferentes Universidades Oficiales de Colombia.

1. ¿Cuánto tiempo lleva funcionando el SPEL de su Universidad? _____
2. ¿Por qué decidieron implementar el SPEL? _____ _____ _____
3. ¿Qué servicios se pueden cancelar mediante el botón de pagos?
   Matricula no__ si__
   Multas no__ si__
   Citas Médicas no__ si__
   Cursos no__ si__
   Certificaciones no__ si__
   Otro. ¿Cuál? _____
4. ¿De los servicios mencionados anteriormente cuál es el más pagado? _____

[1] Sistema de Pago en Línea (SPEL): medio por el cual se puede realizar un pago, directamente desde el sitio web de una organización. Autorización de transferencia de dinero en línea, desde la entidad financiera del usuario, hasta la entidad financiera de la organización.

[2] La protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

5. ¿Quiénes son los posibles usuarios del sistema?
   Estudiantes no__ si__
   Docentes no__ si__
   Administrativos no__ si__
   Otro. ¿Cuál? _____

6. ¿Qué acogida ha tenido por los usuarios el sistema de pagos en línea?
   Mala __ Buena __ Excelente __

7. ¿Cuál es el número promedio de usuarios que utiliza el servicio?
   Estudiantes ___ Docentes ___ Administrativos ___
8. ¿Qué porcentaje del presupuesto de la Universidad se asigna para el departamento encargado de la Infraestructura Tecnológica de la Institución? _____

9. ¿Del presupuesto asignado al departamento que porcentaje se invierte en seguridad de la información? _____

10. ¿Quién desarrollo el SPEL? Universidad __ Empresa Outsourcing __

11. ¿Cuáles de los siguientes estándares o referencias en seguridad de la información se tuvieron en cuenta en el desarrollo del SPEL?
    ISO 27001 no__ si__
    ISO 27002 no__ si__
    ISO 27005 no__ si__
    ISO 15408 no__ si__
    TIA 942 no__ si__
    RFC 2196 no__ si__
    OSSTMM no__ si__
    OWASP no__ si__
    ISSAF no__ si__
    Otro. ¿Cuál? _____

12. ¿Existen políticas de seguridad específicas del SPEL en?
    Parches no__ si__
    Antivirus no__ si__
    Seguridad Física no__ si__
    Control de Acceso no__ si__

Creación de Contraseñas no__ si__
Administración del Sistema no__ si__
Almacenamiento de Datos de Usuario no__ si__
Otro. ¿Cuál? _____

13. La Revisión y Actualización de las Políticas se realiza:
    Mensual no__ si__
    Trimestral no__ si__
    Semestral no__ si__
    Anual no__ si__
    Otro. ¿Cuál? _____

14. ¿El SPEL se ha visto afectado por:
    Ataques de denegación del servicio no__ si__
    Suplantación del sitio de pagos no__ si__
    Fraude de transacciones no__ si__
    Robo de información con ingenierita social no__ si__
    Phishing no__ si__
    Pharming no__ si__
    Implantación de keylogger no__ si__
    Otro. ¿Cuál? _____

15. ¿Las fallas o problemas del SPEL se solucionan:
    Proactivamente con Procedimientos establecidos no__ si__
    Reactivamente con Procedimientos establecidos no__ si__
    Reactivamente con Habilidades del administrador encargado no__ si__
    Otro. ¿Cuál? _____

16. ¿Existe un plan de contingencia específico para el SPEL? no__ si__

17. El código fuente de la aplicación del SPEL:
    Ha sido evaluado no__ si__
    Se tiene respaldo no__ si__
    Se encuentra protegido del acceso público no__ si__

18. El SPEL cuenta con:
    Servidor de pruebas no__ si__
    Servidor de producción dedicado al servicio no__ si__
    Servidor de producción con otras aplicaciones no__ si__

19. ¿El servidor del SPEL cuenta con certificado de servidor seguro valido? no__ si__

20. El SPEL implementa tecnologías de seguridad como:
    SSL – https no__ si__
    WS-Security no__ si__
    VPN internas (intranet) no__ si__
    VPN externas no__ si__
    IP/Certificado no__ si__
    Canal de respaldo no__ si__
    Otro. ¿Cuál? _____

21. ¿Qué algoritmos de cifrado utiliza el SPEL?
    RSA no__ si__
    DES no__ si__
    RC2 no__ si__
    RC4 no__ si__
    AES no__ si__
    Otro. ¿Cuál? _____

22. ¿Qué funciones hash se utilizan en le SPEL?
    MD5 no__ si__ SHA no__ si__

23. ¿Existe un registro de acceso a las instalaciones donde se encuentra el SPEL?
    no__ si__

24. El control de acceso a las instalaciones del SPEL se realiza por:
    Candados no__ si__
    Chapas de seguridad no__ si__
    Lectores de tarjetas (barras, magnéticas, rfid) no__ si__
    Otro. ¿Cuál? _____

25. Las instalaciones donde se encuentra el SPEL cuenta con:
    Extractores calor no__ si__
    Ventilación no__ si__
    Circuito cerrado de TV no__ si__

Detectores de incendio no__ si__
Extintores de incendio adecuados no__ si__
Piso falso no__ si__
Fuente de energía alternativa no__ si__
Adecuaciones eléctricas adecuadas no__ si__
Adecuaciones de cableado estructurado no__ si__
Otro. ¿Cuál? _____

26. La autenticación del usuario ante el SPEL se realiza por:
Numero de cedula no__ si__
Código estudiante no__ si__
Clave privada no__ si__
Otro. ¿Cuál? _____

27. El SPEL almacena datos de usuarios como:
Nombres no__ si__
Cedulas no__ si__
Números de cuentas no__ si__
Contraseñas no__ si__
Otro. ¿Cuál? _____

28. ¿El acceso a la base de datos de usuarios es restringido? no__ si__

29. La información de los pagos a realizar en el SPEL se encuentra en:
Base de datos estática (información introducida manualmente) no__ si__
Base de datos dinámica (información introducida por un sistema) no__ si__
Archivos planos no__ si__
Archivos cifrados no__ si__
Otro. ¿Cuál? _____

30. ¿El SPEL genera al usuario, el resultado de la operación mediante comprobación:
Ninguna no__ si__
Física, imprime comprobante no__ si__
Digital, descarga de comprobante no__ si__
Digital, envió del comprobante correo electrónico no__ si__

Visual, en línea mientras realiza la operación no__ si__
Otro. ¿Cuál? _____

31. ¿Cuántos equipos conforman la Intranet de la Universidad? _____

32. ¿EL servidor del SPEL se encuentra en una subred protegida? no__ si__

33. ¿El SPEL se encuentra protegido con :
Firewall no__ si__
Antivirus no__ si__
Antispyware no__ si__
Otro. ¿Cuál? _____

34. La configuración de routers y firewall es evaluada cada :
Mes __ Tres meses __ Seis meses __ Año __ Otro. ¿Cuál? ___

35. ¿Existe un documento u archivo que tenga la configuración de los diferentes dispositivos de la red informática que se relacionan con el SPEL? no__ si__

36. La Revisión y actualización de sistemas operativos, software de servidores, software del SPEL se realiza cada:
Mes __ Tres meses __ Seis meses __ Año __ Otro. ¿Cuál? ___

37. La disponibilidad del servicio de pago en línea es:
Temporalmente para pago de un servicio no__ si__
Durante todo el semestre no__ si__
Otro. ¿Cuál? _____

38. ¿Cuántas transacciones se realizan semestralmente? _____

39. ¿Cuál es el promedio semestral en dinero realizado en el total de las transacciones?

_____
_____

40. ¿El SPEL genera reportes de:
    Eventos no__ si__
    Transacciones no__ si__
    Ninguno no__ si__
    Otro. ¿Cuál? _____

41. ¿Con que frecuencia realizan auditoría interna?
    Mes __ Tres meses __ Seis meses __ Año __ Otro. ¿Cuál? ___

42. Se realizan pruebas de funcionamiento y vulnerabilidad:
    Del Sitio Web no__ si__
    De Transacciones Cliente no__ si__
    De Recaudos no__ si__
    De Conciliación no__ si__
    Integrales: CLIENTE - COMERCIO - PSE – BANCO no__ si__

OBSERVACIONES: