GOBIERNO DEL ESTADO DE CAMPECHE
FONDO DE APORTACIONES PARA LA SEGURIDAD PÚBLICA
(FASP 2015)

EN CAMPECHE VAMOS POR NUESTRO PROGRESO
GOBIERNO DEL ESTADO • 2009-2015

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UN SERVIDOR DE CÓMPUTO DE SEGURIDAD FIREWALL"

ACTA No. SAIG-164/2015

ESTADO: **CAMPECHE**
MUNICIPIO: **CAMPECHE**
LOCALIDAD: **SAN FRANCISCO DE CAMPECHE**

PROGRAMA: **SISTEMA NACIONAL DE INFORMACIÓN.**

CONCEPTO: **ADQUISICIÓN DE UN SERVIDOR DE CÓMPUTO DE SEGURIDAD FIREWALL.**

CONTRATO: 023/2015 FECHA: 20 DE MAYO DE 2015

EN LA CIUDAD DE SAN FRANCISCO DE CAMPECHE, ESTADO DE CAMPECHE, SIENDO LAS 12:00 HORAS DEL DÍA 14 DE JULIO DEL AÑO DOS MIL QUINCE, SE HACE CONSTAR QUE SE RECIBIÓ DE CONFORMIDAD EL EQUIPO DE CÓMPUTO CONFORME A LAS CARACTERÍSTICAS Y ESPECIFICACIONES CONTRATADAS, EN PRESENCIA DE LOS REPRESENTANTES DE LAS ENTIDADES QUE INTERVINIERON EN LA ENTREGA-RECEPCIÓN DEL PROYECTO.

ENTREGA EL PROVEEDOR: *ESTRATEGIAS EN TECNOLOGÍA CORPORATIVA, S.A. DE C.V.*

RECIBE (QUIEN OPERA EL PROYECTO)

GOB. DEL ESTADO:	X	NOMBRE:	**I.C.E. FERNANDO JOSÉ BOLIVAR GALERA**
GOB. MUNICIPAL:		CARGO:	**SECRETARIO EJECUTIVO**
GOB. FEDERAL:		DEPENDENCIA:	**CONSEJO ESTATAL DE SEGURIDAD PÚBLICA**

DESCRIPCIÓN DEL PROYECTO

CANT.	DESCRIPCIÓN	PRECIO UNITARIO	IMPORTE
1	TRADE-IN EQUIPO 4600 NEXT GENERATION FIREWALL APPLIANCE. INCLUYE: WEB FILTERING, ANTIVIRUS PERIMETRAL, ANTI-SPAM, ANTI-BOT. NÚMERO DE SERIE: 1442B00667. INCLUYE: • INSTALACIÓN DE EQUIPO 4600 APPLIANCE CON 7 NAVAJAS OPCIÓN EQUIVALENTE (NGFW). • SOPORTE DE MANTENIMIENTO DE ASISTENCIA EN SITIO CHECK POINT 7X24 POR 12 MESES PARA EQUIPO 4600 APPLIANCE CON 7 NAVAJAS OPCIÓN EQUIVALENTE (NGFW). INCLUYE INSTALACIÓN BÁSICA Y GARANTÍA DE 1 AÑO.	$ 343,348.00	$ 343,348.00
		SUBTOTAL	$ 343,348.00
		16% I.V.A.	$ 54,935.68
		TOTAL	$ 398,283.68

INVERSIÓN EJERCIDA PARA LA REALIZACIÓN DEL PROYECTO	AÑO	TOTAL
	2015	**$398,283.68**

FASP OPERADO CON RECURSOS 2015

ISO 9001:2008 SAIG

GOBIERNO DEL ESTADO DE CAMPECHE

FONDO DE APORTACIONES PARA LA SEGURIDAD PÚBLICA

(FASP 2015)

EN **CAMPECHE** VAMOS POR NUESTRO **PROGRESO**

GOBIERNO DEL ESTADO • 2009-2015

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UN SERVIDOR DE CÓMPUTO DE SEGURIDAD FIREWALL"

ACTA No. SAIG-164/2015

UNA VEZ VERIFICADO EL EQUIPO DE CÓMPUTO RECIBIDO POR PARTE DE LOS QUE INTERVIENEN EN ESTE ACTO, SE CONCLUYE QUE DICHA ADQUISICIÓN, SE ENCUENTRA TERMINADA Y EN CONDICIONES DE SER RECIBIDA POR LA UNIDAD RESPONSABLE.

LA PRESENTE ACTA NO EXIME AL PROVEEDOR DE LOS DEFECTOS O VICIOS OCULTOS QUE RESULTAREN EN LOS MISMOS Y SE OBLIGA A CORREGIR LAS DEFICIENCIAS DETECTADAS SIN COSTO ALGUNO PARA EL GOBIERNO DEL ESTADO DE CAMPECHE.

EL GOBIERNO DEL ESTADO DE CAMPECHE, A TRAVÉS DEL TITULAR DEL CONSEJO ESTATAL DE SEGURIDAD PÚBLICA, HACE ENTREGA DEL EQUIPO ANTES DESCRITO, AL CENTRO DE ENLACE INFORMÁTICO, QUIEN RECIBE A SU ENTERA SATISFACCIÓN.

NO HABIENDO OTRO ASUNTO QUE TRATAR, SE DA POR CONCLUÍDA LA PRESENTE ACTA, SIENDO LAS 13:00 HORAS DEL MISMO DIA DE SU INICIO, FIRMANDO AL CALCE LOS QUE EN ELLA INTERVINIERON.

ENTREGA POR "EL PROVEEDOR"

ING. JUAN GUALBERTO CABRERA PÉREZ

RECIBEN

I.C.E. FERNANDO JOSÉ BOLIVAR GAMERA
SECRETARIO EJECUTIVO DEL CONSEJO ESTATAL DE SEGURIDAD PÚBLICA

LIC. RÓMULO FERNANDO LEAL DOMÍNGUEZ
DIRECTOR DEL CENTRO DE ENLACE INFORMÁTICO

FASP 2015 OPERADO CON RECURSOS

ISO SAIG

GOBIERNO DEL ESTADO DE CAMPECHE

FONDO DE APORTACIONES PARA LA SEGURIDAD PÚBLICA

(FASP 2015)

EN **CAMPECHE** VAMOS POR NUESTRO **PROGRESO**

GOBIERNO DEL ESTADO • 2009-2015

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UN SERVIDOR DE CÓMPUTO DE SEGURIDAD FIREWALL"

ACTA No. SAIG-164/2015

ANEXO ÚNICO

RENOVACIÓN DE PLATAFORMA DE SEGURIDAD CHECKPOINT

ACTUALIZACIÓN DE CHECKPOINT CON LA FUNCIONALIDAD DE FIREWALL, VPN Y SERVICIOS DE IPS.
ACCOUNT ID: 0006283082
NOKIA IP390 IPS SENSOR. CK 093064901720
CHECKPOINT SECURITY GATEWAY. CPSG-P202-CPSM-P303-F-CKP. CK C7022771F671

- DEBIDO AL FIN DE SOPORTE PRÓXIMO DE LA SOLUCIÓN ACTUAL CHECKPOINT SE SOLICITA LA RENOVACIÓN Y ACTUALIZACIÓN DE LA SOLUCIÓN.
- "EL PROVEEDOR" CONSIDERA LA MIGRACIÓN DEL EQUIPO Y LICENCIAS ACTUALES A UN PRODUCTO QUE PERMITA CONSERVAR Y SUPERAR EL NIVEL DE SERVICIO ACTUAL DE SEGURIDAD DE LA RED, CALCULADO PARA AL MENOS 150 DISPOSITIVOS SIMULTÁNEOS.
- LA ACTUALIZACIÓN CONSERVA EL MISMO NÚMERO DE ACCOUNT ID CHECKPOINT.
- SE CONSIDERA LA ACTUALIZACIÓN DEL EQUIPO CHECKPOINT NOKIA IP390 A UN EQUIPO SECURITY GATEWAY 4600.
- EL EQUIPO SECURITY GATEWAY TIENE INCLUIDA UNA CONSOLA DE ADMINISTRACIÓN QUE PERMITE CONFIGURAR LAS FUNCIONES DEL EQUIPO Y LAS DE UN EQUIPO ADICIONAL.
- INCLUYE FUNCIONES ADICIONALES DE RUTEO, GESTIÓN DE USUARIOS PARA LA GENERACIÓN DE POLÍTICAS Y ACCESO VPN SSL PARA AL MENOS 5 DISPOSITIVOS MÓVILES.
- ACTUALIZACIÓN DE MÓDULO CON LA FUNCIONALIDAD IPS DE FIRMAS DE ATAQUES Y BASES DE DATOS DE ACCIONES DE ATAQUES INFORMÁTICOS A LOS SISTEMAS DE COMUNICACIÓN PERIMETRAL. SE INCLUYE SERVICIO DE CONTROL DE APLICACIONES.
- SERVICIO DE FILTRADO DE CONTENIDO WEB, SERVICIOS DE ANTIVIRUS PERIMETRAL, SERVICIO DE ANTI-SPAM Y SERVICIOS DE ANTI-BOT.
- PÓLIZA DE SOPORTE DE FABRICANTE EL CUAL DA DERECHO A UPGRADE DEL SISTEMA OPERATIVO O DE VERSIÓN DE CHECKPOINT SIN COSTO ALGUNO ASÍ COMO ACCESO A LA BASE DE CONOCIMIENTO TÉCNICO ILIMITADO. INCLUYE ACCESO A LOS PARCHES O FIXES QUE EL FABRICANTE LIBERE PARA LA CORRECCIÓN DE FALLAS DEL SISTEMA. INCLUYE ESCALACIÓN DE SOPORTE AL FABRICANTE PARA LA APERTURA DE TICKETS POR MEDIO DE UN CANAL DE SOPORTE LOCAL CON 4 HORAS DE TIEMPO DE RESPUESTA.
- PÓLIZA DE MANTENIMIENTO CHECKPOINT CATEGORÍA PREMIUM PARA SECURITY GATEWAY 4600, EL CUAL DA DERECHO A REEMPLAZO DEL EQUIPO EN CASO DE FALLA. SOPORTE PARA HW Y SW 7X24 DIRECTO DE FABRICANTE PARA DIAGNÓSTICO DE FALLAS. INCLUYE ESCALACIÓN DE SOPORTE AL FABRICANTE PARA LA APERTURA DE TICKETS POR MEDIO DE UN CANAL DE SOPORTE LOCAL.
- SOPORTE TÉCNICO DEL "EL PROVEEDOR" CON PRESENCIA LOCAL TIPO 7X24 TELEFÓNICO, CORREO ELECTRÓNICO ILIMITADO Y ASISTENCIA DE INGENIERO EN SITIO CON UN PERIODO DE RESPUESTA DE 6 HORAS. INCLUYE SISTEMA DE MESA DE AYUDA PARA APERTURA Y SEGUIMIENTO DE CASOS DE SOPORTES, ATENCIÓN VÍA TELÉFONO 01-800 SIN COSTO. INCLUYE MANO DE OBRA E INGENIERÍA PARA REEMPLAZO DE REFACCIONES Y/O EQUIPOS EN CASO DE FALLAS.
- LA ACTUALIZACIÓN CONSIDERA TODOS LOS SERVICIOS DE INGENIERÍA REQUERIDOS PARA LA MIGRACIÓN DE LA SOLUCIÓN A UN EQUIPO CHECKPOINT SECURITY GATEWAY 4600 INCLUYENDO INSTALACIÓN FÍSICA, MIGRACIÓN DE LICENCIAS, POLÍTICAS Y CONFIGURACIONES DE RED, ASESORÍA PARA LA OPTIMIZACIÓN DE LA SOLUCIÓN Y LA APLICACIÓN DE MEJORES PRÁCTICAS DE SEGURIDAD, SALIDA A PRODUCCIÓN, TRANSFERENCIA DE CONOCIMIENTOS Y ENTREGA DE MEMORIA TÉCNICA.

FASP OPERADO CON RECURSOS 2015

ISO SAIG

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UN SERVIDOR DE CÓMPUTO DE SEGURIDAD FIREWALL"

ACTA No. SAIG-164/2015

LA ACTUALIZACIÓN CONSIDERA LAS SIGUIENTES CARACTERÍSTICAS:

CARACTERÍSTICAS DE RENDIMIENTO:

- ✓ EL EQUIPO GARANTIZA AL MENOS 9 GBPS DE DESEMPEÑO EN FIREWALL
- ✓ EL EQUIPO TIENE AL MENOS 8 INTERFACES 10/100/1000 RJ45
- ✓ EL EQUIPO GARANTIZA AL MENOS 1.5 GBPS EN DESEMPEÑO VPN EN AES-128
- ✓ EL EQUIPO GARANTIZA AL MENOS 50,000 CONEXIONES POR SEGUNDOS
- ✓ EL EQUIPO GARANTIZA AL MENOS 1,200,000 CONEXIONES CONCURRENTES
- ✓ EL EQUIPO GARANTIZA COMO MÍNIMO 1 GBPS EN IPS
- ✓ EL HARDWARE DEL EQUIPO DEBE SER EXPANDIBLE MEDIANTE AL MENOS 1 RANURA DE EXPANSIÓN PARA TARJETAS DE RED; ESTO CON EL FIN DE ASEGURAR EL CRECIMIENTO DE LA RED Y LA COMPATIBILIDAD CON FUTUROS ESTÁNDARES DE COMUNICACIÓN A NIVEL DE CAPA FÍSICA.
- ✓ EL EQUIPO CUENTA CON AL MENOS 250 GB DE ALMACENAMIENTO LOCAL PARA GARANTIZAR LAS BITÁCORAS Y LOGS.
- ✓ CON EL FIN DE MANTENER LA SEGMENTACIÓN DE LA RED, EL EQUIPO DEBE SER CAPAZ DE VIRTUALIZAR COMO MÍNIMO 10 SISTEMAS ADICIONALES DE FIREWALLS.
- ✓ CUENTA CON UNA FUENTE DE PODER AC.

FIREWALL

- ✓ ALTA DISPONIBILIDAD EN UN ESQUEMA REDUNDANTE
- ✓ EL EQUIPO TIENE LA ÚLTIMA VERSIÓN LIBERADA POR EL FABRICANTE.
- ✓ PERMITE CREAR CONTROLES DE ACCESO A POR LO MENOS 150 APLICACIONES/SERVICIOS/PROTOCOLOS PREDEFINIDOS.
- ✓ PROTEGE IMPLEMENTACIONES DE VOIP, SOPORTANDO H323 V2/3/4 (INCLUIDO H.225 V.2/3/3 Y H.254 V3/5/7), SIP. MGCP Y SCCP.
- ✓ INCLUYE LA POSIBILIDAD DE CREAR NATS DINÁMICOS (N-1 O HIDE) Y ESTÁTICOS, PERMITIENDO TRASLADAR DIRECCIONES IP Y PUERTOS ORIGEN Y DESTINO, EN UN MISMO PAQUETE Y EN UNA SOLA REGLA
- ✓ TIENE LA OPCIÓN DE NEGAR LOS PARÁMETROS DE ORIGEN O DESTINO, ES DECIR QUE PARA UNA REGLA DADA PERMITE TODAS LAS CONEXIONES DE ORIGEN / DESTINO EXCEPTO LA ESPECIFICADA EN LA REGLA.
- ✓ PERMITE IMPLEMENTAR REGLAS APLICADAS A INTERVALOS DE TIEMPO ESPECÍFICOS.
- ✓ LA COMUNICACIÓN ENTRE LOS SERVIDORES DE ADMINISTRACIÓN Y LOS GATEWAYS, DEBE SER CIFRADA Y AUTENTICADA.
- ✓ LOS SIGUIENTES ESQUEMAS DE AUTENTICACIÓN DEBEN SER SOPORTADOS POR LOS MÓDULOS DE FIREWALL Y VPN: TOKENS (POR EJEMPLO, SECUREID), TACACS, RADIUS, CERTIFICADOS DIGITALES.

FASP OPERADO CON RECURSOS '2015-

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UN SERVIDOR DE CÓMPUTO DE SEGURIDAD FIREWALL"

ACTA No. SAIG-164/2015

- ✓ PERMITE ALMACENAR UNA BASE DE USUARIOS LOCAL QUE PERMITA REALIZAR AUTENTICACIÓN, SIN DEPENDER DE UN DISPOSITIVO EXTERNO.
- ✓ ES COMPATIBLE CON ACTIVE DIRECTORY.
- ✓ EL FIREWALL PUEDE CONECTARSE MODO TRANSPARENTE (TRANSPARENT MODE).
- ✓ PERMITE EL CONTROLAR EL ACCESO A ARCHIVOS COMPARTIDOS DE MICROSOFT USANDO CIFS, Y QUE EL ADMINISTRADOR DECIDA QUE CARPETAS SE PUEDEN ACCEDER Y CUÁLES NO.
- ✓ SOPORTE ALTA DISPONIBILIDAD Y BALANCEO DE CARGA DE GATEWAYS CON SINCRONIZACIÓN DE ESTADOS, INCLUYENDO AL MENOS LA LICENCIA PARA ALTA DISPONIBILIDAD
- ✓ CON EL FIN DE ASEGURAR LA CALIDAD ESPECIALIZADA Y EL POSICIONAMIENTO TECNOLÓGICO DE LA SOLUCIÓN OFERTADA, EL FABRICANTE APARECE EN EL CUADRANTE DE "LÍDERES" DURANTE LOS ÚLTIMOS 7 AÑOS DEL REPORTE DE "GARTNER MAGIC QUADRANT FOR ENTERPRISE NETWORK FIREWALLS", ASÍ COMO EN EL ÚLTIMO PUBLICADO.
- ✓ LA CONSOLA DE ADMINISTRACIÓN DEL FIREWALL,PROPORCIONA UNA VISIÓN CLARA DEL CUMPLIMIENTO DE MÚLTIPLES REGULACIONES NECESARIAS PARA LAS OPERACIONES DE LA CONVOCANTE (ISO 27001 E ISO 27002) A TRAVÉS DEL MONITOREO DE LAS POLÍTICAS DE SEGURIDAD EN UNA SOLA VISTA.
- ✓ EL GATEWAY SOPORTA REDUNDANCIA A ENLACES, SIN LA NECESIDAD DE UNA LICENCIA ADICIONAL O SOFTWARE / HARDWARE DE TERCEROS.
- ✓ CON LA FINALIDAD DE INCREMENTAR EL PERFORMANCE, LOS APPLIANCE (OUT OF THE BOX), PARA LAS PLATAFORMAS MULTINÚCLEO, SOPORTA LA MULTI REPLICACIÓN DEL KERNEL DEL FIREWALL Y PERMITIR QUE SEAN EJECUTADOS EN OTROS NÚCLEOS.
- ✓ BRINDA UN MÉTODO PARA BLOQUEO SOBRE MENSAJERÍA INSTANTÁNEA DE AL MENOS LAS SIGUIENTES OPCIONES: VIDEO, VOZ, APLICACIONES COMPARTIDAS, TRANSFERENCIA DE ARCHIVOS Y ASISTENCIA REMOTA.

VPN

- ✓ SON SOPORTADAS TANTO UNA CA INTERNA COMO UNA CA EXTERNA PROVISTA POR UN TERCERO.
- ✓ SON SOPORTADOS 3DES Y AES-256 PARA LAS FASES I Y II DE IKE
- ✓ CON EL FIN DE SOPORTAR UN MÁXIMO NIVEL DE CIFRADO SE SOPORTA LOS SIGUIENTES GRUPOS DIFFIE-HELLMAN: GRUPO 1 (768 BIT), GRUPO 2 (1024 BIT), GRUPO 5 (1536 BIT), GRUPO 14 (2048 BIT), GRUPO 19 (256-ECP) Y GRUPO 20 (384-ECP).
- ✓ CON EL FIN DE ASEGURAR LA MÁXIMA INTEGRIDAD DE DATOS SE SOPORTA LOS ESQUEMAS: MD5, SHA1, SHA384 Y AES-XCBC
- ✓ INCLUYE SOPORTE A LAS TOPOLOGÍAS VPNS SITE-TO-SITE: FULL MESHED (TODOS A TODOS), STAR (OFICINAS REMOTAS A SITIO CENTRAL) Y HUB AND SPOKE (SITIO REMOTO A TRAVÉS DEL SITIO CENTRAL HACIA OTRO SITIO REMOTO)
- ✓ SOPORTE A VPNS CLIENT-TO-SITE BASADAS EN IPSEC.
- ✓ TIENE LA POSIBILIDAD DE REALIZAR VPNS SSL SIN CLIENTE PARA ACCESO REMOTO, SIN NECESIDAD DE INSTALAR UN CLIENTE.

FINANCIADO CON RECURSOS FASP 2015

ACTA DE ENTREGA-RECEPCIÓN
"ADQUISICIÓN DE UN SERVIDOR DE CÓMPUTO DE SEGURIDAD FIREWALL"

ACTA No. SAIG-164/2015

- ✓ CON EL FIN DE EVITAR LA CONEXIÓN MEDIANTE VPN DE DISPOSITIVOS NO CONFIABLES, LA SOLUCIÓN PUEDE CONFIGURADA PARA DETECTAR Y EVITAR LA CONEXIÓN DE TERMINALES MÓVILES CUANDO ESTOS SEAN VULNERADOS MEDIANTE JAILBROKEN (IOS) Y ROOTING (ANDROID).
- ✓ INCLUYE UN MÉTODO SIMPLE Y CENTRAL, DE CREAR TÚNELES PERMANENTES ENTRE GATEWAYS DEL MISMO FABRICANTE.
- ✓ SOPORTA VPNS TIPO "DOMAIN BASED" Y "ROUTE BASED", USANDO AL MENOS BGP Y OSPF
- ✓ INCLUYE UN MECANISMO PARA MITIGAR EL IMPACTO A ATAQUES DE DENEGACIÓN DE SERVICIO DOS A IKE, HACIENDO DIFERENCIA ENTRE CONEXIONES CONOCIDAS Y DESCONOCIDAS.
- ✓ PUEDE ESTABLECER VPNS CON GATEWAYS CON DIRECCIONES IP DINÁMICAS PÚBLICAS.
- ✓ SOPORTE A COMPRESIÓN IP PARA VPNS CLIENT-TO-SITE Y SITE-TO-SITE.
- ✓ ES POSIBLE CREAR UNA ÚNICA ASOCIACIÓN DE SEGURIDAD (SA) POR PAR DE REDES O SUBREDES.
- ✓ LA SOLUCIÓN CUENTA CON UN MECANISMO QUE PERMITA SELECCIONAR QUÉ ENLACE UTILIZAR PARA TRÁFICO DE VPN ENTRANTE Y SALIENTE, ADEMÁS DE ESCOGER LA MEJOR RUTA PARA DICHO TRÁFICO.
- ✓ LA SOLUCIÓN TIENE LA POSIBILIDAD DE ESTABLECER VPN'S SITIO A SITIO CON IP DINÁMICAS.

IPS

- ✓ EL IPS CONTIENE GRUPO DE PROTECCIONES QUE IDENTIFICAN CUANDO EL TRÁFICO NO CUMPLE CON LOS ESTÁNDARES DEL PROTOCOLO.
- ✓ EL IPS INCLUYE GEO-PROTECCIONES
- ✓ EL IPS CONTIENE GRUPO DE PROTECCIONES QUE IDENTIFICA EL TRÁFICO QUE INTENTA EXPLOTAR UNA VULNERABILIDAD ESPECÍFICA.
- ✓ LOS MÓDULOS DE IPS INTEGRADO Y DE FIREWALL, ESTAN INTEGRADOS OFRECIENDO DE ESTA MANERA, PROTECCIÓN MULTICAPA.
- ✓ HABILIDAD PARA EXCLUIR ESPECÍFICAMENTE DIRECCIONES IP DEL ANÁLISIS DEL IPS.

UTILIZADO CON RECURSOS FASP 2015