INSTITUTO FEDERAL DE TELECOMUNICACIONES
COORDINACION GENERAL DE ORGANIZACIÓN Y TECNOLOGIAS DE LA INFORMACION
DIRECCION DE SEGURIDAD DE SISTEMAS INFORMÁTICOS

INVESTIGACIÓN DE MERCADO

Nombre del proveedor	Número de identificación del bien, arrendamiento o servicio	Proporciona las condiciones solicitadas de calidad y oportunidad	Cantidad que puede surtir	Origen del bien	Contar con personal certificado	Considerar el alcance de la especificación técnica	Entregables del proyecto	Precio Unitario	PRECIO UNITARIO ESTIMADO * (MONEDA NACIONAL)
Fortalitia S.A. de C.V.	33301	SI	1	NACIONAL	Cumple	Cumple	Cumple	$44'022,013.92 M.N.	$44'022,013.92
Scitum S.A. de C.V.		SI	1	NACIONAL	Cumple	Cumple	Cumple	$40'583,628.46 M.N.	$40'583,628.45
Alelkon Partners S.A. de C.V.		SI	1	NACIONAL	Cumple	Cumple	Cumple	$46'388,432.65 M.N.	$46'388,432.65

* Monto expresado en pesos Mexicanos, incluye IVA. Monto correspondiente a 36 meses.

Fecha 07 de Julio de 2014

No. de requisición 85

Procedimiento Licitación Pública

No. de Partida	CUCOP	DESCRIPCION
1	33300001	Servicios de Informática

FUENTES CONSULTADAS:

Se consultó el Sistema Compranet, no encontrándose contrataciones para los mismos servicios.

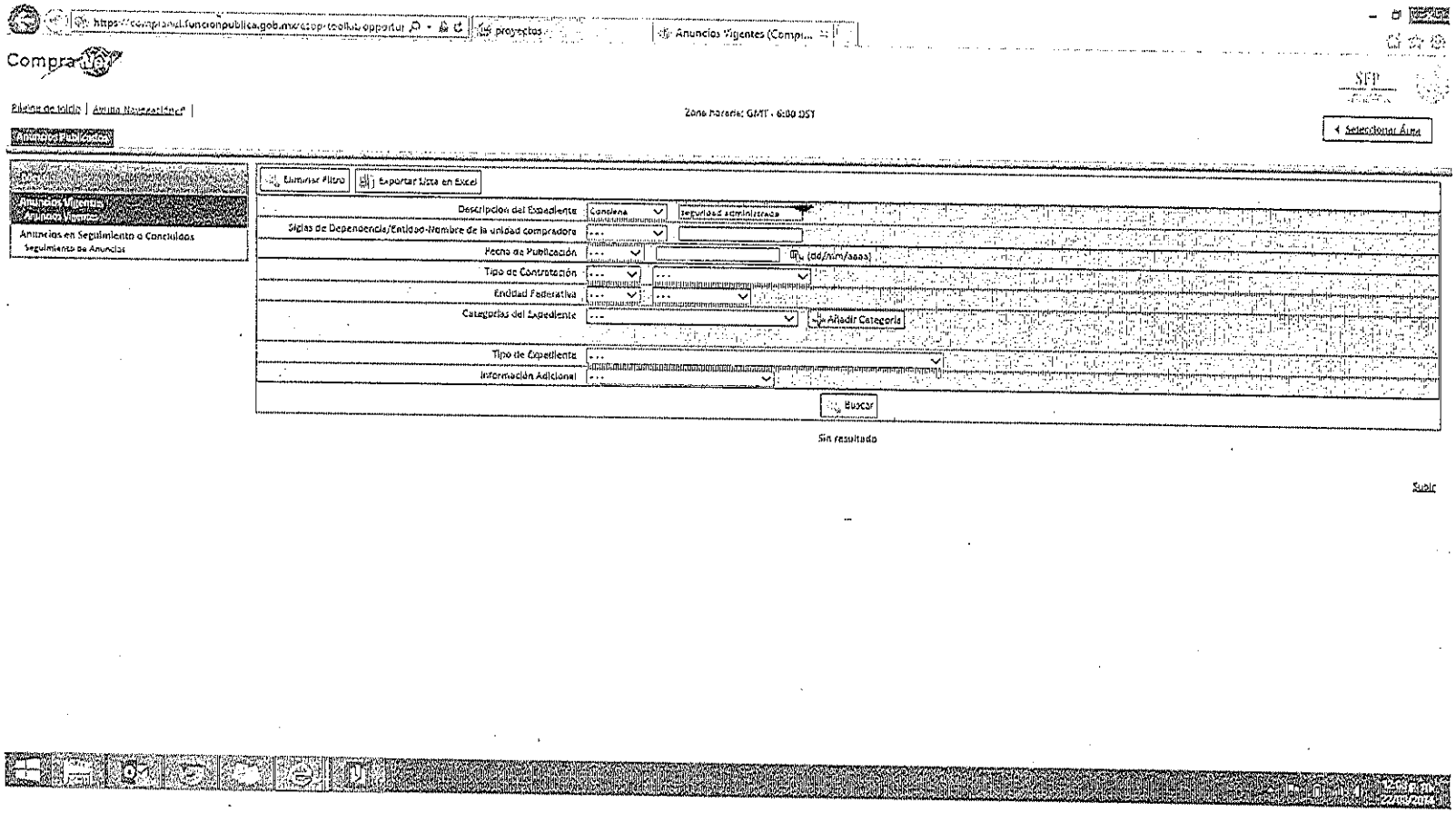
Elaboró

Ney Galicia Arteaga
Director de Seguridad de Sistemas Informáticos.

Autorizó

Hugh Harleston López Espino
Coordinador General de Organización y Tecnologías de la Información

Consulta Compranet



FECHA: 23 de junio de 2014.

ASUNTO: PETICIÓN DE OFERTAS

Muy estimado Alexandro Nieto Plett
Domicilio: Av. Insurgentes Sur 3500, piso 2; colonia Peña Pobre; Delegación Tlalpan; código postal: 14060; México, Distrito Federal. Teléfonos de contacto: (55) 9150 7400 ext. 1510..

El Instituto Federal de Telecomunicaciones (IFT), como órgano autónomo del Gobierno Federal, requiere para sus actividades de suministro, arrendamiento y/o prestación de servicios, mismas que se encuentran reguladas por las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones y por los Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, obtener información para contratar bajo las mejores condiciones disponibles para el Estado.

En este sentido y en términos de lo previsto en el artículo 2, fracción V de las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, su representada ha sido identificada por este ente público, como un posible prestador de servicio y/o proveedor.

Por lo antes mencionado y con el objeto de conocer: a).- la existencia de bienes, arrendamientos o servicios a requerir en las condiciones que se indican; b).- posibles proveedores a nivel nacional o internacional, y c).- el precio estimado de lo requerido, nos permitimos solicitar su valioso apoyo a efecto de proporcionarnos una cotización de los bienes y/o servicios y/o arrendamientos descritos en el documento anexo.

Dicha cotización se requiere que la remita en documento de la empresa, debidamente firmada por persona facultada, a la siguiente dirección: Av. Insurgentes Sur, 1143, Col. Noche Buena, Delegación Benito Juárez, C.P. 03720, D.F. y que sea dirigida a nombre del Lic. Ney Galicia Arrocena, Director de Seguridad de Sistemas Informáticos.

Mucho agradeceré que en su respuesta se incluya: Lugar y fecha de cotización y vigencia de la misma.

Para el caso de dudas, comentarios y/o aclaraciones, remitirlas al correo: ney.galicia@ift.org.mx

La fecha límite para presentar la cotización indicada es el: **03 de julio de 2014.**

Favor de enviar acuse de recibo de esta solicitud al correo electrónico: ney.galicia@ift.org.mx

NOTA: Vencido el plazo de recepción de cotizaciones, el Instituto Federal de Telecomunicaciones con fundamento en lo previsto en el artículo 24 de las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, definirá el procedimiento a seguir para la contratación, el cual puede ser: LICITACIÓN PÚBLICA, INVITACIÓN A CUANDO MENOS TRES PERSONAS y/o ADJUDICACIÓN DIRECTA, mismo que se informará a las personas que presentaron su cotización.

Este documento no genera obligación alguna para el Instituto Federal de Telecomunicaciones.

A t e n t a m e n t e

Lic. Ney Galicia Arrocena,
Director de Seguridad de Sistemas Informáticos

Para efectos de control interno, en el caso de no recibir respuesta o manifestar un inconveniente o imposibilidad, se procederá a hacer la anotación respectiva en nuestros registros, circunstancias que deberán ser consideradas al momento de definir el tipo de procedimiento de contratación) FO-CON-04

PARA FORMULAR SU COTIZACIÓN, SE DEBERA CONSIDERAR LOS SIGUIENTES ASPECTOS:

Datos que en su caso, se deben proporcionar para que el destinatario de la solicitud conteste:

1. Los datos de los bienes, arrendamientos o servicios a cotizar (mismos que se especifican en el anexo de esta solicitud de cotización).
2. Condiciones de entrega:
   - Los trabajos requeridos deberán iniciarse al día siguiente de que el IFT apruebe la propuesta del proveedor seleccionado y formalice la contratación.
   - El lugar de entrega de los servicios será en las oficinas del Instituto Federal de Telecomunicaciones sitas en Av. Insurgentes Sur, 1143, Col. Noche Buena, Delegación Benito Juárez, C.P. 03720, D.F.
3. Considerar en su cotización que el pago es a los 20 días naturales posteriores a la entrega de la factura, previa entrega de los bienes o prestación de los servicios a satisfacción del IFT.
4. Señalar en su caso, el porcentaje del anticipo: NO APLICA.
5. El porcentaje de garantía de cumplimiento será del 10 % del monto total aprobado del proyecto.
6. Penas convencionales por atraso en la entrega de bienes y/o servicios será establecido en el anexo técnico del proceso de adjudicación correspondiente.

   El archivo adjunto de especificaciones técnicas se hace consistir en 26 fojas
7. En su caso, los métodos de prueba que empleará el ente público para determinar el cumplimiento de las especificaciones solicitadas. NO APLICA.
   - Normas que deben de cumplirse
   - Registros Sanitarios o Permisos Especiales, en su caso.
8. Origen de los bienes (nacional o país de importación): NO APLICA.
9. En caso de bienes de importación la moneda en que cotiza: NO APLICA.
10. En caso de que el proceso de fabricación de los bienes requeridos sea superior a 60 días, señale el tiempo que correspondería a su producción. NO APLICA.
11. En su caso, especificar si el costo incluye:
    - Instalación.
    - Capacitación.
    - Puesta en marcha.
12. Otras garantías que se debe considerar, indicar el o los tipos de garantía, o de responsabilidad civil señalando su vigencia.

Recibido 23-Junio-14
Alexandra Medina

SCITUM, S.A. DE C.V.
Av. Insurgentes Sur 33500 Piso 2
Col. Peña Pobre, Tlalpan
14060 México, D.F.
Tel. 9150 7400 fax 9150 7478
www.scitum.com.mx

México, D.F., a 19 de septiembre del 2014

ATENCION:

Ing Ney Galicia

Cliente: Instituto Federal de Telecomunicaciones
Proyecto: Servicios de Seguridosd Administrada
Contacto Consultor: NA
Contacto Comercial:

En respuesta a su amable solicitud, nos permitimos poner a su consideración nuestra oferta económica esperando cumplir con sus requerimientos.

PROPUESTA ECONÓMICA A 36 MESES

No. Parte	Descripción	Cantidad	Precio Unitario	Importe Total MXP
SVC	Servicio Administrado de Seguridad en Redes Sociales	1	$ 696,391.67	$ 696,391.67
SVC	Servicio Admnistrado de Pruebas de Seguridad	1	$ 1,240,833.03	$ 1,240,833.03
SVC	Gestion de Infraestructura Actual	1	$ 4,862,695.83	$ 4,862,695.83
SVC	Servicio Administrado de Filtrado WEB	1	$ 4,030,471.03	$ 4,030,471.03
SVC	Servicio Administrado de Filtrado MAIL	1	$ 2,001,852.77	$ 2,001,852.77
SVC	Servicio Administrado de Amtimalware RED	1	$ 2,986,368.85	$ 2,986,368.85
SVC	Servicio Administrado de Amtimalware Correo	1	$ 2,953,165.34	$ 2,953,165.34
SVC	Servicio Administrado de Seguridad para Aplicaciones WEB, Bases de Datos, Archivos Compartidos y Sharepoint	1	$ 10,534,270.54	$ 10,534,270.54
SVC	Servicio Administrado de Correlación de eventos y administración de Bitácoras	1	$ 5,679,837.55	$ 5,679,837.55
				$34,985,886.60

Condiciones Comerciales:
Los precios están expresados en moneda nacional (pesos mexicanos) y no incluyen I.V. A
Esta cotización tiene una vigencia de 30 días a partir de la fecha de la cotización
Tiempo de entrega de infraestructura: 6 Semanas
No se admiten cancelaciones ya ingresado su pedido.
No incluye viáticos para el servicio de soporte técnico en sitio
Forma de pago:
SERVICIOS DE SEGURIDAD PERIMETRAL: 36 pagos (1 por mes) de $971,830.12 pesos mas IVA.
El pago se deberá realizar mediante transferencia bancaria con un plazo de 20 días naturales a partir de que se ingrese la factura.

Alexandro Nieto
Gerente de Cuenta
Sector Servicios

FECHA: 23 de junio de 2014.

ASUNTO: PETICIÓN DE OFERTAS

Muy estimado Pascual Perez del Real
Domicilio: Av. Pacifico 182 interior 1; colonia El rosedal; código postal 04330, México, D.F..

El Instituto Federal de Telecomunicaciones (IFT), como órgano autónomo del Gobierno Federal, requiere para sus actividades de suministro, arrendamiento y/o prestación de servicios, mismas que se encuentran reguladas por las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones y por los Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, obtener información para contratar bajo las mejores condiciones disponibles para el Estado.

En este sentido y en términos de lo previsto en el artículo 2, fracción V de las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, su representada ha sido identificada por este ente público, como un posible prestador de servicio y/o proveedor.

Por lo antes mencionado y con el objeto de conocer: a).- la existencia de bienes, arrendamientos o servicios a requerir en las condiciones que se indican; b).- posibles proveedores a nivel nacional o internacional, y c).- el precio estimado de lo requerido, nos permitimos solicitar su valioso apoyo a efecto de proporcionarnos una cotización de los bienes y/o servicios y/o arrendamientos descritos en el documento anexo.

Dicha cotización se requiere que la remita en documento de la empresa, debidamente firmada por persona facultada, a la siguiente dirección: Av. Insurgentes Sur, 1143, Col. Noche Buena, Delegación Benito Juárez, C.P. 03720, D.F. y que sea dirigida a nombre del Lic. Ney Galicia Arrocena, Director de Seguridad de Sistemas Informáticos.

Mucho agradeceré que en su respuesta se incluya: Lugar y fecha de cotización y vigencia de la misma.

Para el caso de dudas, comentarios y/o aclaraciones, remitirlas al correo: ney.galicia@ift.org.mx

La fecha límite para presentar la cotización indicada es el: **03 de julio de 2014.**

Favor de enviar acuse de recibo de esta solicitud al correo electrónico: ney.galicia@ift.org.mx

NOTA: Vencido el plazo de recepción de cotizaciones, el Instituto Federal de Telecomunicaciones con fundamento en lo previsto en el artículo 24 de las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, definirá el procedimiento a seguir para la contratación, el cual puede ser: LICITACIÓN PÚBLICA, INVITACIÓN A CUANDO MENOS TRES PERSONAS y/o ADJUDICACIÓN DIRECTA, mismo que se informará a las personas que presentaron su cotización.

Este documento no genera obligación alguna para el Instituto Federal de Telecomunicaciones.

A t e n t a m e n t e.

Lic. Ney Galicia Arrocena,
Director de Seguridad de Sistemas Informáticos

Para efectos de control interno, en el caso de no recibir respuesta o manifestar un inconveniente o imposibilidad, se procederá a hacer la anotación respectiva en nuestros registros, circunstancias que deberán ser consideradas al momento de definir el tipo de procedimiento de contratación) FO-CON-04

PARA FORMULAR SU COTIZACIÓN, SE DEBERA CONSIDERAR LOS SIGUIENTES ASPECTOS:

Datos que en su caso, se deben proporcionar para que el destinatario de la solicitud conteste:

1. Los datos de los bienes, arrendamientos o servicios a cotizar (mismos que se especifican en el anexo de esta solicitud de cotización).
2. Condiciones de entrega:
   - Los trabajos requeridos deberán iniciarse al día siguiente de que el IFT apruebe la propuesta del proveedor seleccionado y formalice la contratación.
   - El lugar de entrega de los servicios será en las oficinas del Instituto Federal de Telecomunicaciones sitas en Av. Insurgentes Sur, 1143, Col. Noche Buena, Delegación Benito Juárez, C.P. 03720, D.F.
3. Considerar en su cotización que el pago es a los 20 días naturales posteriores a la entrega de la factura, previa entrega de los bienes o prestación de los servicios a satisfacción del IFT.
4. Señalar en su caso, el porcentaje del anticipo: NO APLICA.
5. El porcentaje de garantía de cumplimiento será del 10 % del monto total aprobado del proyecto.
6. Penas convencionales por atraso en la entrega de bienes y/o servicios será establecido en el anexo técnico del proceso de adjudicación correspondiente.

   El archivo adjunto de especificaciones técnicas se hace consistir en 26 fojas
7. En su caso, los métodos de prueba que empleará el ente público para determinar el cumplimiento de las especificaciones solicitadas. NO APLICA.
   - Normas que deben de cumplirse
   - Registros Sanitarios o Permisos Especiales, en su caso.
8. Origen de los bienes (nacional o país de importación): NO APLICA.
9. En caso de bienes de importación la moneda en que cotiza: NO APLICA.
10. En caso de que el proceso de fabricación de los bienes requeridos sea superior a 60 días, señale el tiempo que correspondería a su producción. NO APLICA.
11. En su caso, especificar si el costo incluye:
    - Instalación.
    - Capacitación.
    - Puesta en marcha.
12. Otras garantías que se debe considerar, indicar el o los tipos de garantía, o de responsabilidad civil señalando su vigencia.

Recibido
Paschal Perez
23-06-2014

Aleikon

MEXICO D.F. A 19 DE SEPTIEMBRE DEL 2014

ATENCIÓN
ING. NEY GALICIA ARROCENA
INSTITUTO FEDERAL DE TELECOMUNICACIONES.
DIRECCIÓN DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN.

Referente a la solicitud de cotización realizada para los solicitados, anexamos nuestra propuesta económica.

Concepto	Precio
SERVICIOS DE SEGURIDAD ADMINISTRADA POR 36 MESES	$39,990,028.15
SUB-TOTAL	$39,990,028.15
IVA	$6,398,404.50
TOTAL	$46,388,432.654

Términos Comerciales

Precios expresados en pesos mexicanos
Forma de pago: 30 días naturales posteriores a la entrega de la factura, previa entrega de los bienes o prestación de los servicios a satisfacción del IFT.
No se aceptan cancelaciones

Condiciones de entrega

- Los trabajos requeridos deberán iniciarse al día siguiente de que el IFT apruebe la presente propuesta.
- El lugar de entrega de los servicios será en las oficinas del Instituto Federal de Telecomunicaciones sitas en Av. Insurgentes Sur, 1143, Col. Noche Buena, Delegación Benito Juárez, C.P. 03720, D.F.

Rascual Perez del Real
Gerencia Comercial

FECHA: 23 de junio de 2014.

ASUNTO: PETICIÓN DE OFERTAS

Muy estimado Arturo Duke Naves, Technical Account Manager
Domicilio: Asturias 30A – 103; colonia Insurgentes Mixcoac, México, D.F.; código postal 03920.

El Instituto Federal de Telecomunicaciones (IFT), como órgano autónomo del Gobierno Federal, requiere para sus actividades de suministro, arrendamiento y/o prestación de servicios, mismas que se encuentran reguladas por las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones y por los Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, obtener información para contratar bajo las mejores condiciones disponibles para el Estado.

En este sentido y en términos de lo previsto en el artículo 2, fracción V de las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, su representada ha sido identificada por este ente público, como un posible prestador de servicio y/o proveedor.

Por lo antes mencionado y con el objeto de conocer: a).- la existencia de bienes, arrendamientos o servicios a requerir en las condiciones que se indican; b).- posibles proveedores a nivel nacional o internacional, y c).- el precio estimado de lo requerido, nos permitimos solicitar su valioso apoyo a efecto de proporcionarnos una cotización de los bienes y/o servicios y/o arrendamientos descritos en el documento anexo.

Dicha cotización se requiere que la remita en documento de la empresa, debidamente firmada por persona facultada, a la siguiente dirección: Av. Insurgentes Sur, 1143, Col. Noche Buena, Delegación Benito Juárez, C.P. 03720, D.F. y que sea dirigida a nombre del Lic. Ney Galicia Arrocena, Director de Seguridad de Sistemas Informáticos.

Mucho agradeceré que en su respuesta se incluya: Lugar y fecha de cotización y vigencia de la misma.

Para el caso de dudas, comentarios y/o aclaraciones, remitirlas al correo: ney.galicia@ift.org.mx

La fecha límite para presentar la cotización indicada es el: **03 de julio de 2014.**

Favor de enviar acuse de recibo de esta solicitud al correo electrónico: ney.galicia@ift.org.mx

NOTA: Vencido el plazo de recepción de cotizaciones, el Instituto Federal de Telecomunicaciones con fundamento en lo previsto en el artículo 24 de las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, definirá el procedimiento a seguir para la contratación, el cual puede ser: LICITACIÓN PÚBLICA, INVITACIÓN A CUANDO MENOS TRES PERSONAS y/o ADJUDICACIÓN DIRECTA, mismo que se informará a las personas que presentaron su cotización.

Este documento no genera obligación alguna para el Instituto Federal de Telecomunicaciones.

A t e n t a m e n t e.

Lic. Ney Galicia Arrocena,
Director de Seguridad de Sistemas Informáticos

Para efectos de control interno, en el caso de no recibir respuesta o manifestar un inconveniente o imposibilidad, se procederá a hacer la anotación respectiva en nuestros registros, circunstancias que deberán ser consideradas al momento de definir el tipo de procedimiento de contratación) FO-CON-04

PARA FORMULAR SU COTIZACIÓN, SE DEBERA CONSIDERAR LOS SIGUIENTES ASPECTOS:

Datos que en su caso, se deben proporcionar para que el destinatario de la solicitud conteste:

1. Los datos de los bienes, arrendamientos o servicios a cotizar (mismos que se especifican en el anexo de esta solicitud de cotización).
2. Condiciones de entrega:
   - Los trabajos requeridos deberán iniciarse al día siguiente de que el IFT apruebe la propuesta del proveedor seleccionado y formalice la contratación.
   - El lugar de entrega de los servicios será en las oficinas del Instituto Federal de Telecomunicaciones sitas en Av. Insurgentes Sur, 1143, Col. Noche Buena, Delegación Benito Juárez, C.P. 03720, D.F.
3. Considerar en su cotización que el pago es a los 20 días naturales posteriores a la entrega de la factura, previa entrega de los bienes o prestación de los servicios a satisfacción del IFT.
4. Señalar en su caso, el porcentaje del anticipo: NO APLICA.
5. El porcentaje de garantía de cumplimiento será del 10 % del monto total aprobado del proyecto.
6. Penas convencionales por atraso en la entrega de bienes y/o servicios será establecido en el anexo técnico del proceso de adjudicación correspondiente.

   El archivo adjunto de especificaciones técnicas se hace consistir en 26 fojas
7. En su caso, los métodos de prueba que empleará el ente público para determinar el cumplimiento de las especificaciones solicitadas. NO APLICA..
   - Normas que deben de cumplirse
   - Registros Sanitarios o Permisos Especiales, en su caso.
8. Origen de los bienes (nacional o país de importación): NO APLICA.
9. En caso de bienes de importación la moneda en que cotiza: NO APLICA.
10. En caso de que el proceso de fabricación de los bienes requeridos sea superior a 60 días, señale el tiempo que correspondería a su producción. NO APLICA.
11. En su caso, especificar si el costo incluye:
    - Instalación.
    - Capacitación.
    - Puesta en marcha.
12. Otras garantías que se debe considerar, indicar el o los tipos de garantía, o de responsabilidad civil señalando su vigencia.

Recibido el 23-06-2014

Para efectos de control interno, en el caso de no recibir respuesta o manifestar un inconveniente o imposibilidad, se procederá a hacer la anotación respectiva en nuestros registros, circunstancias que deberán ser consideradas al momento de definir el tipo de procedimiento de contratación) FO-CON-04

FORTALITIA

ift INSTITUTO FEDERAL DE TELECOMUNICACIONES

RESPUESTA A ESTUDIO DE MERCADO

SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD DE LA INFORMACIÓN

ATENCIÓN
Ney Galicia Arrocena
Director de Área
Seguridad de la Información

19 de Septiembre del 2014.

COTIZACIÓN

NOMBRE DEL EMPRESA: Fortalitia, S.A. de C.V.		
R.F.C.:		
DOMICILIO: Asturias 30A – 103, Col Insurgentes Mixcoac, México D.F. C.P 03920.		
NO: DE TELÉFONO: (55) 3329 1010		
SERVICIO: SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD DE LA INFORMACIÓN		
COLUMNAS	A	B
SERVICIO	PRECIO MENSUAL S/IVA M.N. (SERVICIO)	PRECIO POR LA VIGENCIA DEL SERVICIO 36 MESES S/IVA M.N. (SERVICIO)
SERVICIO INTEGRAL ADMINISTRADO DE SEGURIDAD DE LA INFORMACIÓN • Administración de Infraestructura Actual • Servicio Administrado de monitoreo de internet para prevención de ataques • Servicio Administrado de Pruebas de Seguridad (AV/PT) • Servicio Administrado de Filtrado WEB • Servicio Administrado de Filtrado para correo electrónico • Servicio Administrado de Amtimalware RED • Servicio Administrado de Amtimalware Correo	$1,054,167.00	$37,950,012.00

• Servicio Administrado de Seguridad Bases de Datos • Servicio Administrado de Seguridad File Server • Servicio Administrado de Seguridad Share Point • Servicio Administrado de Correlación de eventos		
	SUBTOTAL	$37,950,012.00
	+ 16% IVA.	$607,2001.92
	TOTAL	$44,022,013.92
CUARENTA Y CUATRO MILLONES VEINTI DOS MIL Y TRECE PESOS 92/100 M.N.		
VIGENCIA: ESTA PROPUESTA TIENE UNA VIGENCIA DE 60 DÍAS NATURALES.		

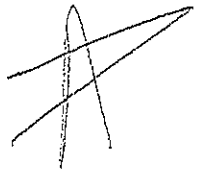
PREMISAS DE LA COTIZACIÓN

1. Esta cotización fue hecha con base en la solicitud de estudio de mercado realizada por el IFT

2. Para la elaboración, se han considerado tanto lo solicitado por el IFT como la experiencia que como empresa tenemos en la entrega de estos servicios.

3. Esta cotización se entrega al IFT como una referencia para su estudio de mercado, y en ningún caso obliga a FORTALITIA a entregar servicio alguno al IFT. Su contenido es CONFIDENCIAL y sólo para los propósitos que nos fue requerida.

CONTACTO CON FORTALITIA. S.A DE C.V.



Arturo Duke Naves
Technical Account Manager
Dir. (55) 3329-1010
Cel. [redacted]
aduke@fortalitia.com.mx

ELIMINADO 1 RENGLÓN, ARTÍCULO 18 FRACCIÓN II DE LA LEY FEDERAL DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA GUBERNAMENTAL.

INSTITUTO FEDERAL DE TELECOMUNICACIONES

México D.F. a 16 de junio de 2014.

ANEXO TÉCNICO

De conformidad con lo dispuesto en el artículo 24, quinto párrafo, de las Normas en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, la Coordinación General de Organización y Tecnologías de Información del Instituto Federal de Telecomunicaciones, a través de la Dirección de Seguridad de Sistemas Informáticos, emite el presente Anexo Técnico para establecer los requisitos, especificaciones y condiciones para el procedimiento de contratación de los **"Servicios de Seguridad administrada para el IFT".**

Objeto de la contratación: Contar con servicios especializados en el aseguramiento de la red de comunicaciones, servidores de cómputo central, aplicaciones de cómputo utilizadas para soportar procesos de áreas sustantivas e información electrónica contenida en las bases de datos del Instituto, todo esto a través de la implementación, configuración, operación y soporte de soluciones de seguridad específicas que complementarán los dispositivos de seguridad con los que ya cuenta el Instituto. Los servicios de seguridad administrada permitirán proteger a las redes de datos e infraestructura de Tecnologías de la Información de ataques o explotación de vulnerabilidades que puedan afectar la disponibilidad, integridad y confidencialidad de la información del Instituto.

Especificaciones, cantidades y condiciones de "Los Servicios"

SERVICIOS	ESPECIFICACIONES	CANTIDAD
Servicios de Seguridad administrada para el IFT.	Las especificaciones se encuentran descritas en la sección denominada "Especificaciones Técnicas de los Servicios de Seguridad administrada para el IFT", que forma parte integral del presente ANEXO TÉCNICO.	1

Fecha y Lugar para la prestación de "Los Servicios":

Fecha:	A partir de la notificación del fallo y hasta 36 meses posteriores a la misma.
Lugar:	Insurgentes Sur 1143, Piso 2, Col. Noche Buena, Del. Benito Juárez, México, D.F. C.P. 03720, México, D.F.
Horario:	Las 24 horas del día durante los 7 días de la semana durante la vigencia del contrato, de acuerdo con los requerimientos del Administrador del contrato por parte del IFT.

Área encargada de la administración del contrato y verificación de "Los Servicios":

El área de Tecnologías de la Información y Comunicaciones del Instituto Federal de Telecomunicaciones, a través de la Dirección de Seguridad de Sistemas Informáticos, será el área responsable de la supervisión del proyecto y administración del contrato, quien tendrá en todo tiempo el derecho de verificar cualquier asunto relacionado con la prestación de los servicios, la cual está ubicada en Insurgentes Sur 1143, Segundo Piso, Col. Noche Buena, Delegación Benito Juárez, C.P. 03720, México, D.F.

Responsabilidad de "El Proveedor":

"El Proveedor" será el único responsable por la prestación en tiempo y forma de "Los Servicios" ajustándose a las especificaciones, cantidades y condiciones requeridas por el presente Anexo Técnico, y en su caso a las indicaciones que al respecto reciba del Área responsable de la administración del contrato y verificación de "Los Servicios".

Precios de "Los Servicios":

La cotización deberá indicar el costo unitario de los servicios, el monto total por la prestación de los mismos, desglosando el Impuesto al Valor Agregado, la oferta será a precios fijos e incondicionados en moneda nacional.

Forma de pago:

La forma de pago se hará en treinta y seis exhibiciones, de acuerdo al calendario establecido en la sección de Especificaciones Técnicas, apartado "Forma de pago", dentro de los veinte días naturales posteriores a la aceptación formal de la factura correspondiente al periodo de que se trate, a través de transferencia electrónica a la cuenta bancaria que sea proporcionada por el Proveedor Adjudicado, de conformidad con lo establecido en el artículo 53 de las Normas en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, de conformidad con los siguientes datos:

Titular;
RFC;
Institución Bancaria;
Plaza;
Sucursal; y,
Número de cuenta CLABE.

Para el pago de "Los Servicios", "El Proveedor" presentará ante la Dirección de Seguridad de Servicios Informáticos de la Coordinación General de Organización y Tecnologías de la Información del Instituto Federal de Telecomunicaciones, las facturas y los entregables que acrediten la prestación de "Los Servicios", para que ésta a su vez, los revise y firme a entera satisfacción de conformidad con lo establecido en el Contrato respectivo y a las Especificaciones Técnicas del proyecto, dando por recibida la factura para su pago dentro de los 20 (veinte) días naturales siguientes a la recepción de "Los Servicios".

Si las facturas o los documentos presentan algún error, la Dirección de Seguridad de Sistemas Informáticos de la Coordinación General de Organización y Tecnologías de la Información, en un plazo no mayor a 3 (tres) días hábiles, indicará por escrito a "El Proveedor" las deficiencias que deberá corregir. El periodo que transcurra a partir del citado escrito y hasta que "El Proveedor" presenta las correcciones, no se computará para efectos del plazo previsto en el artículo 53 de las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones.

En caso de que "El Proveedor" no presente en el tiempo señalado la documentación requerida para el trámite de pago, la fecha de pago se correrá el mismo número de días que dure el retraso.

Pena Convencional y/o Deducciones:

Pena Convencional	Deducciones
Medio punto porcentual (0.5%) sobre el monto de los servicios no entregados oportunamente por causas imputables al proveedor, por cada día natural de atraso en la prestación del servicio especificado en el anexo técnico del contrato, de conformidad con lo dispuesto por el Artículo 55 de las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, la penalización máxima a aplicar es del 10% del valor de los servicios entregados con atraso. La suma de las penas convencionales no deberá exceder del importe de la garantía de cumplimiento del contrato, en el entendido de que si el contrato es rescindido no procederá el cobro de dichas penas ni la contabilización de las mismas al hacer efectiva la garantía de cumplimiento.	Las deducciones serán equivalentes al 0.5% (cero punto cinco por ciento) en función de "Los Servicios" prestados de manera deficiente, las cuales se harán efectivas sobre la factura que se presente para su pago hasta por un 10 % (diez por ciento); en caso de que se supere dicho monto, se podrá cancelar o rescindir administrativamente el contrato correspondiente en términos de los Artículos 56 y 57 de las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones y 86 de los Lineamientos en materia de adquisiciones, arrendamientos y Servicios del Instituto Federal de Telecomunicaciones.

Garantía de Cumplimiento:

El Proveedor Adjudicado para garantizar el cumplimiento de sus obligaciones, de conformidad con el artículo 92 de los Lineamientos en Materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones, podrá otorgar las garantías en alguna de las formas siguientes: depósito de dinero constituido a través de certificado o billete de depósito expedido por institución de crédito autorizada; fianza otorgada por institución autorizada; depósito de dinero constituido ante la Tesorería del Instituto; carta de crédito irrevocable, expedida por institución de crédito autorizada; cheque certificado o de caja expedido a favor del Instituto, y cualquier otra que, en su caso, autorice la Coordinación General de Administración.

Para este proyecto se solicita preferentemente, que el Proveedor Adjudicado otorgue fianza expedida por institución autorizada para ello, a favor del Instituto Federal de Telecomunicaciones, por un importe equivalente al 10% (diez por ciento) del monto total del contrato correspondiente, sin considerar el Impuesto al Valor Agregado. Lo anterior, de conformidad con lo establecido en el artículo 50 fracción II y 51 de las Normas en materia de Adquisiciones, Arrendamientos y Servicios del Instituto Federal de Telecomunicaciones.

Dicha garantía será indivisible y deberá presentarse en la Dirección de Recursos Materiales y Servicios Generales de la Coordinación General de Administración del Instituto Federal de Telecomunicaciones sita en Avenida Insurgentes Sur Número 838, Quinto Piso, Colonia del Valle, Delegación Benito Juárez, Código Postal 03100, México, Distrito Federal, dentro de los 10 días naturales posteriores a la firma del contrato correspondiente.

INSTITUTO FEDERAL DE
TELECOMUNICACIONES

ESPECIFICACIONES TÉCNICAS
Servicios de seguridad administrada para el IFT

Tabla de contenido

1. Glosario

1.1 Glosario

Término/ Acrónimo	Descripción
IFT o Instituto	Instituto Federal de Telecomunicaciones
CGOTI	Coordinación General de Organización y Tecnologías de la Información
TI	Tecnologías de la información
OAP	Oficina de Administración de Proyectos de TI de la CGOTI.
PAP	Plan de Administración del Proyecto
ANS	Acuerdo de nivel de servicio
Componentes Habilitadores	Dispositivos necesarios para la prestación de los servicios de seguridad administrados considerados en el proyecto.
7 x 24	Las 24 horas del día durante los 7 días de la semana.
SOC	Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés, Security Operations Center)
Bitácoras	Registro de eventos generados por los componentes de la infraestructura de cómputo o comunicaciones.
WAFEC	Web Access Firewall Evaluation Criteria
SQL	Lenguaje para consulta de datos estructurados (Structured Query Language)
SOW	Documento formal en el que se definen las actividades de trabajo con respecto a una tarea específica (SOW, por sus siglas en Inglés).
ITIL	Information Tecnology Infrastructure Library

2. Introducción

2.1 Situación Actual

Uno de los retos de la CGOTI es proteger y asegurar la información electrónica, bajo el resguardo del Instituto Federal de Telecomunicaciones, de posibles ataques informáticos internos y/o externos. Los retos detectados son:

- Proteger las redes de datos e infraestructura crítica de TI de ataques o explotación de vulnerabilidades que puedan afectar la disponibilidad, integridad y confidencialidad de la información del IFT.
- Contar con las herramientas necesarias para mitigar los riesgos detectados en la infraestructura y activos del IFT.
- Responder de forma proactiva ante posibles ataques dirigidos a los activos de información del IFT.
- Identificar las brechas de seguridad a través de la correlación y resguardo de bitácoras que permitan la trazabilidad de los eventos de seguridad.

2.2 Propósito

Este proyecto permitirá contar con servicios especializados en el aseguramiento de la red de comunicaciones, la infraestructura de cómputo, aplicaciones e información contenida en bases de datos y servidores de archivos del Instituto, todo esto a través de la implementación, puesta a punto, operación y soporte de soluciones de seguridad específicas detalladas en este documento, y que complementarán las soluciones de seguridad con las que ya cuenta el Instituto.

Objetivos

- Contar con servicios de seguridad administrada que permitan al IFT minimizar los riesgos de intrusión y/o robo de información de su red de datos e infraestructura de TI, con procesos alineados a las mejores prácticas de seguridad y bajo un modelo de operación de mejora continua.
- Implementar servicios de seguridad administrada a la medida, acordes a la cantidad de usuarios, bases de datos, número de aplicaciones, bajo un modelo de operación 7 x 24 (7 días a la semana durante las 24 horas del día), que permita la disminución de los riesgos potenciales de seguridad informática de fuentes internas y/o externas.
- Homologar la operación y administración entre los controles de seguridad con que ya cuenta el Instituto y los controles de seguridad que serán implementados como parte de este proyecto, de tal forma que permitan la mitigación de ataques a la infraestructura crítica de TI del IFT.
- Contar con el soporte técnico de 1er, 2do y 3er nivel de las soluciones tecnológicas de seguridad y las herramientas requeridas para la operación de los servicios durante los 36 meses de vigencia del contrato.

2.3 Beneficios esperados

Este proyecto incrementará la seguridad perimetral del Instituto a través del aseguramiento de la red de comunicaciones, la infraestructura de cómputo, aplicaciones e información contenida en bases de datos y servidores de archivos. Asimismo permitirá responder de forma proactiva ante posibles ataques informáticos dirigidos a los activos de información del Instituto.

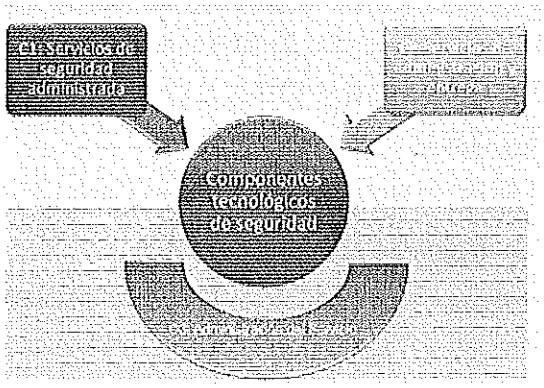
Durante la vigencia del contrato, se contará con una operación bajo un esquema 7 x 24 (7 días a la semana durante las 24 horas del día) de servicios de monitoreo y administración de los equipos de seguridad perimetral, que permitirán al Instituto obtener reportes de desempeño, incidencias, eventos y tiempos de resolución de acuerdo a los objetivos y los niveles de servicio requeridos; contar con análisis detallados de carácter técnico y planes de remediación para resolver problemas o vulnerabilidades identificadas en la infraestructura de Tecnologías de la Información, disponer de servicios de análisis de la actividad de los sistemas para prevenir la ejecución de acciones maliciosas o que afecten la confidencialidad, integridad o disponibilidad de los servicios de Tecnologías de Información y Comunicaciones y contar con recomendaciones de mejora a las políticas, configuraciones y reglas de operación de los servicios de Tecnologías de la Información; todo ello con apego a estándares aceptados en

materia de seguridad de la información y administración de servicios de Tecnologías de la Información.

3. Alcance

3.1 Componentes de la Solución

La solución debe contemplar los componentes que se muestran gráficamente en la siguiente figura:



3.1.1 Descripción breve y funcional del diagrama

1. Servicios de seguridad administrada

   Los servicios de seguridad administrada se refieren a los servicios de gestión, monitoreo y soporte de la infraestructura de seguridad que proveerá protección directa a la red y sistemas del Instituto. A través de estos servicios, el IFT busca detectar vulnerabilidades de forma oportuna y contrarrestar las amenazas informáticas provenientes de Internet o de la red interna que puedan afectar la disponibilidad, confidencialidad y/o integridad de la información en servidores y servicios críticos del Instituto.

   Para ello, el Proveedor Adjudicado deberá instalar, configurar, afinar, administrar y operar las herramientas de seguridad requeridas y proveer los recursos técnicos y humanos especializados para cubrir las necesidades de protección de la red, infraestructura de TI y sistemas de información del Instituto durante la vigencia del contrato.

   El licenciamiento y los equipos requeridos que formarán parte del servicio, estarán a cargo del Proveedor Adjudicado y el IFT no adquirirá ninguno de los mismos.

2. Servicios de administración y entrega

   El Proveedor Adjudicado deberá contar con un Centro de Operación de Seguridad (SOC) que proporcione las herramientas de software y hardware necesarias para realizar actividades de entrega, seguimiento y operación de los Servicios Administrados que conforman el Componente 1: Servicios de Seguridad Administrada.

3. Administración del servicio

El proveedor deberá proporcionar los recursos técnicos y humanos especializados para realizar las actividades involucradas en el proyecto; así como para la elaboración de la documentación soporte de la ejecución de las actividades y seguimiento general del proyecto.

El Proveedor Adjudicado deberá presentar una propuesta de trabajo previa a la ejecución de cualquier actividad y deberá contar con la aprobación del supervisor del proyecto y del Administrador del contrato por parte de la CGOTI para su ejecución. La programación de las actividades deberá ser acordada de manera conjunta entre el personal asignado por el Proveedor Adjudicado y el supervisor del proyecto y Administrador del contrato por parte de la CGOTI.

3.2 Especificación de los Componentes

A continuación se presenta el detalle de los productos y servicios requeridos para cada uno de los Componentes:

3.2.1 Componente 1: Servicio de Seguridad Administrada

Los servicios de seguridad administrada tienen por objeto brindar el monitoreo, soporte y gestión de toda la infraestructura de seguridad perimetral del Instituto Federal de Telecomunicaciones, implementando nuevos servicios e incorporando los dispositivos de seguridad que actualmente ya se encuentra instalados y operando en el Instituto. De tal forma que el Proveedor Adjudicado provea un servicio integral de seguridad que permita detectar y contrarrestar las amenazas informáticas provenientes de Internet o de la red interna que puedan afectar la disponibilidad, confidencialidad y/o integridad de la información del Instituto.

Para ello, el Proveedor Adjudicado deberá instalar, configurar, ajustar, administrar y operar el software, hardware y dispositivos de comunicación que se requieran; así como proveer los recursos técnicos y humanos especializados para cubrir estas necesidades.

3.2.1.1 Nuevos servicios

El Componente de Servicios de Seguridad Administrada estará integrado por al menos los siguientes nuevos servicios de seguridad para la red del IFT:

- Gestión de infraestructura y monitoreo de eventos de los componentes de seguridad perimetral del IFT.
- Servicios de correlación de eventos y administración de bitácoras.
- Servicios de análisis de vulnerabilidades y pruebas de penetración.
- Servicios de control de Acceso Firewall
- Servicios de protección de aplicaciones Web, servidores de archivos y bases de datos.
- Servicios de protección de amenazas de nueva generación para tráfico de correo electrónico.
- Servicios de Monitoreo Proactivo de Seguridad en Internet
- Servicio de Enrutamiento de Enlace de internet

Para esto, el Proveedor Adjudicado deberá considerar en su propuesta los componentes tecnológicos que se utilizarán para la prestación de los servicios de seguridad administrada durante la vigencia del contrato, a los que en adelante se les denominará Componentes Habilitadores y serán al menos:

- Solución tecnológica para administración de bitácoras y correlación de eventos.
- Solución tecnológica para análisis de vulnerabilidades.
- Solución tecnológica de control de acceso firewall
- Solución tecnológica para protección de aplicaciones, servidores de archivos y bases de datos.
- Solución tecnológica para protección y filtrado de contenido de páginas WEB
- Solución tecnológica para ruteo de enlace a internet

El IFT ofrecerá el espacio en su centro de datos para la instalación de los gabinetes, alimentación eléctrica ininterrumpida y condiciones adecuadas de ambiente para la instalación de las herramientas necesarias para la prestación del servicio por parte del Proveedor Adjudicado. Por su parte, el Proveedor Adjudicado deberá considerar como parte del equipamiento el suministro y tendido de cada uno de los cables que la solución requiera, debiendo dejar cada uno de los Dispositivos Habilitadores de servicio debidamente montado y los cables de red debidamente colocados (etiquetados y peinados). El Proveedor Adjudicado debe considerar en su propuesta de solución, los elementos tecnológicos auxiliares para habilitar dichas soluciones, tales como:

- Infraestructura para montaje del equipo (rack, PDUs, cables certificados entre dispositivos, accesorios, etc.) que sea compatible con las características del centro de cómputo del IFT.

Todo el equipo provisto y colocado en sitio por el Proveedor Adjudicado para este proyecto, deberá:

- Ser nuevo, de última generación y dedicado sólo a la solución diseñada para el Instituto.
- Cuando la solución lo permita, ser equipo de propósito específico (appliance) para cada servicio que así lo requiera.
- Cumplir con un ciclo de vida básico de al menos 12 meses posteriores a la fecha de término del proyecto, es decir, no estar en condiciones de fin de vida (EoL) o fin de soporte (EoS) por parte del fabricante, durante al menos la vigencia del contrato.

El Proveedor Adjudicado deberá instalar, configurar, afinar, administrar y operar el software, hardware y dispositivos de comunicación que su solución requiera.

En caso de que las instalaciones del centro de datos del IFT sufran modificaciones durante la vigencia del contrato (como parte de mejoras a las instalaciones, requerimientos internos o incluso atendiendo observaciones de auditorías), será responsabilidad del proveedor adjudicado proporcionar los recursos necesarios para reubicar,

configurar, reinstalar y ajustar los Componentes Habilitadores que lo necesiten. El Proveedor Adjudicado deberá considerar al menos 2 modificaciones durante la vigencia del contrato.

3.2.1.2 Administración y monitoreo de la infraestructura de seguridad perimetral existente

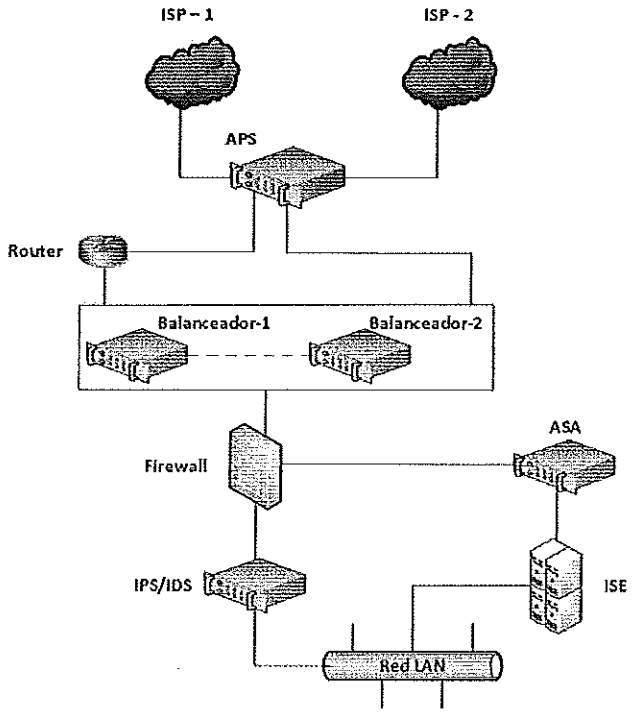
El Proveedor Adjudicado deberá considerar, como parte del proyecto, la administración y monitoreo de los dispositivos de seguridad perimetral que actualmente se encuentran instalados en el IFT, sean arrendados o propiedad del Instituto. El Proveedor Adjudicado deberá incorporar estos dispositivos al servicio denominado "Gestión de infraestructura y monitoreo de eventos de los componentes de seguridad perimetral del IFT", distinguiendo:

- Dispositivos de control de ataques de denegación de servicios.
- Dispositivos balanceadores de carga.
- Dispositivos de control de acceso (Firewall).
- Dispositivos de prevención y detección de intrusos (IPS/IDS).
- Dispositivos de control de acceso a la red LAN, WLAN y VPN.
- Dispositivos de protección contra amenazas de nueva generación.
- Dispositivos de seguridad para servidores virtuales.

Es importante que el Proveedor Adjudicado tome en cuenta que algunos de estos equipos deberán migrarse, o bien instalarse y configurarse desde cero. En la tabla que se muestra a continuación, se listan las cantidades y modelos de los equipos, y se da la descripción de uso de cada uno y si deberá o no ser considerado para migración de localidad.

Dispositivo	Marca	Modelo / Versión	Cantidad	Descripción de función	Migración de localidad
APS	Arbor	PRA-APS-2104	1	Protección de ataques de DDoS	No
Balanceador de carga	F5	LTM2000	2	Balanceo de enlaces de Internet	No
IPS	SourceFire	3D7120	1	Sistema de protección de intrusos	No
Defense Center	SourceFire	Defense Center 750	1	Consola de administración de IPS	No
Firewall / VPN	Cisco	ASA 5525-X	1	Establece conexiones VPN y hace el filtrado de contenido Web de los clientes que se conectan remotamente	Si
ISE	Cisco	Cisco ISE Software versión 1.2	2	Autentica y autoriza el acceso de usuarios y dispositivos a la red, ya sea por medios cableados o inalámbricos.	No
Deep Security	Trend Micro	Versión 8.0	152	Plataforma integral de seguridad para servidores físicos / virtuales (152 licencias)	No
Deep Discovery	Trend Micro	NA	1	Seguridad avanzada de red	No

A continuación se muestra un diagrama general de cómo están instalados actualmente dichos equipos e infraestructura:



3.2.1.3 Servicios de transferencia de conocimientos

El Proveedor Adjudicado deberá considerar dentro de su propuesta la transferencia de conocimientos de todas las soluciones tecnológicas de seguridad (incluidas las que son propiedad o ya están arrendadas por el IFT) considerando el número de asistentes por solución tecnológica que se presenta en la siguiente tabla:

Solución tecnológica	No. de asistentes	Temas a considerar
Administración de bitácoras y correlación de eventos.	4	1. Vista general de la solución a. Arquitectura b. Componentes 2. Ciclo de vida de eventos 3. Manejo de la consola de eventos 4. Manejo de filtros de eventos en la consola 5. Manejo de tableros de control y monitores de eventos 6. Generación de reportes 7. Explicación del esquema de eventos 8. Manejo de listas y reglas 9. Manejo de consultas de eventos

Análisis de vulnerabilidades.	4	1. Vista General de la solución 2. Motor de escaneo 3. Base de conocimientos 4. Mapeo y descubrimiento de red 5. Administración de activos 6. Escaneo de vulnerabilidades 7. Reporteo 8. Gestión de usuarios y seguridad 9. Políticas de remediación
Control de acceso firewall	4	1. Administración 2. Monitoreo 3. Generación de reportes
Protección de aplicaciones, servidores de archivos y bases de datos.	5	1. Descubrimiento y clasificación de bases de datos 2. Políticas de auditoría 3. Gestión de la información de auditoría 4. Reporteo 5. Archivado y notificaciones 6. Inventario de vulnerabilidades y mitigación de riesgos 7. Perfilado de base de datos 8. Políticas de Seguridad Avanzadas 9. Mejora y ajuste de la herramienta y su configuración 10. Gestión de privilegios de usuarios
Protección de correo electrónico	4	1. Administración 2. Monitoreo 3. Generación de reportes
Protección y filtrado de contenido de páginas WEB	4	1. Administración 2. Monitoreo 3. Generación de reportes
Control de ataques de denegación de servicios (APS)	4	1. Explicación de ataques DDoS 2. Monitoreo de ataques 3. Mitigación de ataques 4. Niveles de protección 5. Protección de grupos 6. Protección de servicios 7. Opciones de despliegue 8. Mejores prácticas 9. Diagnóstico y resolución de problemas 10. Tareas de administración
Balanceador de carga de enlaces de Internet (F5)	4	1. Administración 2. Monitoreo 3. Generación de reportes
Prevención y detección de intrusos (IPS)	4	1. Configuración y gestión del equipo 2. Opciones de despliegue 3. Configuración de políticas

		4. Análisis de eventos 5. Reportes
Control de acceso a la red LAN, WLAN y VPN (ISE)	4	1. Administración 2. Monitoreo 3. Generación de reportes
Protección contra amenazas de nueva generación (Deep Discovery)	4	1. Administración 2. Monitoreo 3. Generación de reportes
Protección para servidores virtuales. (Deep Security)	4	4. Administración 5. Monitoreo 4. Generación de reportes

La transferencia de conocimientos de los componentes de administración de bitácoras y correlación de eventos, análisis de vulnerabilidades, protección de aplicaciones, servidores de archivos y bases de datos, control de ataques de denegación de servicios y balanceador de carga de enlaces de Internet deberán ser impartidos directamente por el fabricante.

3.2.1.4 Condiciones de los Servicios de Seguridad Administrada

- Las soluciones se deberán considerar para dar soporte a al menos 1200 usuarios internos del Instituto. El Proveedor Adjudicado deberá considerar como parte del servicio propuesto el crecimiento que pueda darse a lo largo de la vigencia del proyecto en usuarios o equipos conectados a la infraestructura del IFT en al menos un 10% anual.
- El Proveedor Adjudicado deberá proporcionar el equipamiento necesario, la instalación y configuración para la puesta en marcha del servicio; así como la afinación, depuración y el mantenimiento del mismo durante la vigencia del contrato, en el entendido de que todos los equipos y licenciamientos requeridos formarán parte del servicio ofrecido por parte del Proveedor Adjudicado y que el IFT no adquirirá ninguno de los mismos.
- El Proveedor Adjudicado deberá considerar dentro de su propuesta técnica un esquema de monitoreo, soporte técnico y administración de seguridad perimetral 7 x 24 (7 días a la semana durante las 24 del día) para todos los componentes tecnológicos durante la vigencia del contrato.
- El soporte técnico se llevará a cabo de manera remota siempre y cuando se cumplan los niveles de servicio establecidos. En caso necesario, el Proveedor Adjudicado colocará especialistas en sitio para atender requerimientos específicos relacionados con amenazas a la seguridad del IFT bajo el mismo nivel de servicio.
- Es responsabilidad del Proveedor Adjudicado solucionar todos los incidentes de seguridad que involucren los servicios contratados, deberá documentar las actividades realizadas en la solución y en los casos en que el IFT lo requiera, realizar el análisis forense del mismo.

- El IFT podrá realizar un monitoreo de disponibilidad con sus propias herramientas con el fin de validar la información proporcionada por el Proveedor Adjudicado en los reportes mensuales, por lo que el Proveedor Adjudicado deberá aceptar la instalación de los agentes necesarios en la infraestructura inmersa en el servicio, si fuese necesario.
- Los Componentes Habilitadores serán administrables de forma remota por el Proveedor Adjudicado y radicarán físicamente en las instalaciones del IFT. En caso necesario, el Proveedor Adjudicado asignará en sitio a personal de su plantilla para la atención de incidentes o mantenimiento necesario del equipo involucrado en el proyecto, previo acuerdo con el IFT respecto de los horarios y alcance de los servicios.
- El acceso remoto a los equipos será a través de canales seguros. El Proveedor Adjudicado deberá proporcionar un enlace dedicado de al menos 4Mb entre el Centro de Datos Principal del IFT y el SOC del Proveedor Adjudicado, asegurando que los tiempos de respuesta del monitoreo remoto y configuración de los equipos sean adecuados para proporcionar eficientemente el servicio durante la vigencia del contrato.
- El Proveedor Adjudicado a través del SOC deberá realizar respaldos a las configuraciones y políticas de todos los dispositivos administrados al menos 1 vez cada 24 horas e inmediatamente después de cada cambio programado. Estos respaldos deberán ser almacenados en dispositivos que cuenten con mecanismos de control de acceso seguro y sólo serán accesibles a personal autorizado por el IFT, en caso necesario se deberán entregar dichos respaldos a el IFT a través de los mecanismos que de común acuerdo se establezcan para el efecto. Las políticas de retención deberán considerar la conservación de los respaldos por 90 días para cada respaldo.
- De forma trimestral, se deberá entregar una copia (en un medio externo) de las bitácoras de eventos del servicio de correlación de eventos, el cual debe contener los eventos generados por los servicios requeridos en este documento. En caso necesario el IFT podrá solicitar la entrega de las bitácoras con una frecuencia diferente o en atención a algún incidente de seguridad específico.

El Proveedor Adjudicado integrará como parte de la solución, un portal Web de información (Portal de Servicio al IFT) que deberá contar con las siguientes características mínimas:

- El portal deberá permitir al IFT al menos: Consultar los reportes generados de forma periódica de cada uno de los servicios que integran el servicio de seguridad administrada, consultar reportes históricos generados durante la vigencia del contrato, consultar reportes bajo demanda de servicios específicos (cuando así le sea solicitado al Proveedor Adjudicado), dar de alta tickets de soporte/requerimientos en el sistema, consultar el estado de los tickets de servicio y validar su culminación o cumplimiento por parte del Proveedor Adjudicado.
- Ser adaptado para uso exclusivo del IFT,
- Proporcionar acceso a través de conexiones seguras,

- Permitir la definición de privilegios de los usuarios con acceso a la herramienta por parte del IFT, considerando al menos los perfiles de operador (sólo lectura) y supervisor (privilegios de lectura, generación de reportes y configuración de consultas de acuerdo a requerimientos particulares del Instituto).
- Proporcionar como mínimo 5 cuentas de usuario para el IFT.

El Proveedor Adjudicado deberá considerar los siguientes requerimientos referentes al Portal de Servicio al IFT:

- Entregar manuales de usuario,
- Proporcionar capacitación para su uso para al menos 10 usuarios que serán designados por el IFT.
- Considerar el soporte técnico necesario para el uso de la herramienta por parte del IFT y la corrección de errores que se identifiquen a lo largo del proyecto.
- Considerar en el alcance el diseño y aplicación de mejoras solicitadas por el IFT a los reportes disponibles a través del portal, relacionados con los servicios prestados por el Proveedor adjudicado.
- De forma trimestral se revisará, de manera conjunta entre el IFT y el Proveedor Adjudicado, la necesidad de implementar acciones de capacitación sobre el uso y alcance del Portal de Servicio al IFT derivadas de cambios de versión, nuevos requerimientos o cambios en el personal dedicado al proyecto por parte del IFT.

3.2.1.5 Productos

El Instituto establecerá de manera conjunta con el proveedor los reportes necesarios para dar seguimiento a la operación de los servicios, al menos deberán considerarse los siguientes:

Entregable	Descripción	Requerimientos
E.3.2.1.1 Reporte mensual de capacidades.	Reporte con la información sobre comportamiento de los parámetros principales de operación de cada uno de los Componentes Habilitadores.	Debe contener al menos: R.3.2.1.1.1 Identificación del Componente Habilitador R.3.2.1.1.2 Datos de ocupación de disco, memoria, procesador, desempeño y rangos de operación establecidos. R.3.2.1.1.3 Identificación de fallas o incidentes relacionados con el Componente Habilitador de que se trate. R.3.2.1.1.4 Acciones correctivas ejecutadas y resultado de las mismas.
E.3.2.1.2 Reporte mensual de incidentes.	Reporte que enumere los tipos, de incidentes detectados y las acciones realizadas para atenderlos.	El reporte debe contener al menos: R.3.2.1.2.1 Listado y tipos de incidentes detectados en el periodo. R.3.2.1.2.2 Fecha, hora y duración del incidente. R.3.2.1.2.3 Impacto, acciones tomadas y resultado de las mismas.
E.3.2.1.3 Reporte mensual de eventos identificados en el servicio de correlación de eventos.	Reporte que enumere los eventos de seguridad identificados por los servicios de correlación y análisis de bitácoras.	El reporte debe contener al menos: R.3.2.1.3.1 Listado y tipos de eventos detectados en el periodo. R.3.2.1.3.2 Fecha, hora, tipo y duración del evento. R.3.2.1.3.3 Impacto, acciones tomadas y resultado de las mismas.

E.3.2.1.4 Copia de bitácoras. (Trimestral)	Respaldo de las bitácoras generadas por los servicios de administración de filtrado de contenido, detección/prevención de Intrusos, control de acceso firewall, protección contra amenazas de nueva generación y protección de aplicaciones Web, servidores de archivos y bases de datos.	El reporte debe contener al menos: R.3.2.1.4.1 Identificación de la bitácora de que se trata. R.3.2.1.4.2 Periodo de respaldo. R.3.2.1.4.3 Resumen de incidentes de seguridad identificados en el periodo y documentados en las bitácoras. R.3.2.1.4.5 Mecanismos de seguridad que aseguren su integridad y no repudio.
E.3.2.1.5 Reporte ejecutivo de análisis de vulnerabilidades y pruebas de penetración. (Por ciclo de pruebas)	Documento con la información resultante del análisis, formulado en lenguaje claro y dirigido a la alta gerencia.	Este documento deberá contener, al menos: R.3.2.1.5.1 Identificación de las pruebas realizadas y el ambiente utilizado R.3.2.1.5.2 Identificación de los resultados obtenidos R.3.2.1.5.3 Recomendaciones de mejora de acuerdo a la infraestructura de los activos objetivo.
E.3.2.1.6 Reporte técnico de análisis de vulnerabilidades y pruebas de penetración. (Por ciclo de pruebas)	Documento con la información detallada del análisis, formulado en lenguaje claro y orientado a las áreas técnicas del IFT.	Este documento deberá contener, al menos: R.3.2.1.6.1 Descripción detallada de los activos de información analizados. R.3.2.1.6.2 Identificación detallada de vulnerabilidades detectadas, efectos de su explotación, causa raíz y recomendaciones de solución. R.3.2.1.6.3 Dictamen del resultado de las pruebas de penetración realizadas R.3.2.1.6.4 Listado de herramientas utilizadas para realizar el análisis
E.3.2.1.7 Reporte de incidentes por nivel de protección (aplicación Web, base de datos, servidor de archivos) Mensual	Documento con la información detallada del análisis de los incidentes que se presenten en el periodo para cada nivel protegido por el servicio.	Este documento deberá contener, al menos: R.3.2.1.7.1 Descripción detallada de los incidentes identificados. R.3.2.1.7.2 Listado de vulnerabilidades detectadas, efectos de su explotación, causa raíz y recomendaciones de solución.
E.3.2.1.8 Reporte de incidentes por código malicioso. Mensual	Documento con la identificación de incidentes ocasionados por malware en general.	Este documento deberá contener, al menos: R.3.2.1.8.1 Incidentes ocasionados por malware en general identificado en el Instituto. R.3.2.1.8.2 Identificación de equipos más atacados, fuentes de malware y acciones de remediación ejecutadas.
E.3.2.1.9 Reporte de incidentes relacionados al servicio de protección de correo electrónico. Mensual	Documento con la identificación de incidentes ocasionados por spam y/o malware en general en correo electrónico.	Este documento deberá contener, al menos: R.3.2.1.9.1 Incidentes ocasionados por spam y/o malware en general sobre correo electrónico identificado en el Instituto.
E.3.2.1.10 Reporte de actividades relacionados con el servicio de filtrado de contenido Web. Mensual	Documento con la identificación de acceso a sitios autorizados y no autorizados.	Este documento deberá contener, al menos: R.3.2.1.10.1 Actividades relacionadas con accesos no autorizados por el servicio de filtrado de URL's. R.3.2.1.10.2 Actividades relacionadas con accesos autorizados y no autorizados por categoría R.3.2.1.10.3 Actividades relacionadas con accesos por consumo de ancho de banda R.3.2.1.10.4 Actividades relacionadas con accesos autorizados y no autorizados por protocolo. R.3.2.1.10.5 Actividades relacionadas con accesos por riesgo.

E.3.2.1.11 Reporte de actividades relacionados con el servicio de monitoreo proactivo de seguridad en Internet. Mensual	Documento con la identificación de incidentes ocasionados por grupos hacktivistas nacionales y extranjeros que puedan representar una amenaza al IFT y que estén dedicados a perpetrar o difundir campañas de ataque informáticos en contra del IFT.	R.3.2.1.11.1 Actividades relacionadas con identificación de amenazas detectadas en las redes sociales. R.3.2.1.11.2 Actividades relacionadas con identificación de incidentes detectados en los canales de IRC R.3.2.1.11.3 Actividades relacionadas con identificación de incidentes detectados en foros, blogs y comunidades. R.3.2.1.11.4 Actividades relacionadas con identificación de incidentes detectados en foros, blogs y comunidades. R.3.2.1.11.5 Actividades relacionadas con identificación de incidentes detectados fuentes abiertas de noticias tanto nacionales o extranjeras.
E.3.2.1.12 Reporte de actividades relacionadas con el servicio de control de acceso Firewall. Mensual	Documento con la identificación de actividades relacionadas con el tráfico permitido y bloqueado del Firewall.	R.3.2.1.12.1 Actividades relacionadas con el tráfico de internet origen – destino R.3.2.1.12.2 Actividades relacionadas con el tráfico por política origen – destino R.3.2.1.12.3 Actividades relacionadas con el tráfico bloqueado en cada regla e interface R.3.2.1.12.4 Actividades relacionadas con el tráfico bloqueado por puerto TCP/UDP R.3.2.1.12.5 Actividades relacionadas con los usuarios y servicios que generen más tráfico hacia internet R.3.2.1.12.6 Actividades con los usuarios y servicios que generen más tráfico hacia servidores DMZ R.3.2.1.12.7 Actividades relacionadas con los Servidores que generen más tráfico origen – destino.
E.3.2.1.13 Reporte de actividades relacionadas con el dispositivo de control de ataques de denegación de servicio. Mensual	Documento con la identificación de actividades relacionadas con el sistema de protección de disponibilidad.	R.3.2.1.13.1 Actividades relacionadas con el total de tráfico R.3.2.1.13.2 Actividades relacionadas con el tráfico permitido y bloqueado R.3.2.1.13.4 Actividades relacionadas con el host bloqueados R.3.2.1.13.5 Actividades relacionadas con el tráfico por servicio bloqueado R.3.2.1.13.6 Actividades relacionadas con ataque contra aplicaciones R.3.2.1.13.7 Actividades relacionadas con ataques por categoría R.3.2.1.13.8 Actividades relacionadas con el IP que más tráfico generan R.3.2.1.13.9 Actividades relacionadas con protección basada en ubicación de IP
E.3.2.1.14 Reporte de actividades relacionadas con los dispositivos de balanceo de carga. Mensual	Documento con la identificación de actividades relacionadas con el sistema de balanceo de enlaces de internet.	R.3.2.1.14.1 Actividades relacionadas con disponibilidad de cada enlace R.3.2.1.14.2 Actividades relacionadas con accesos Fallidos R.3.2.1.14.3 Actividades relacionadas con enlace más utilizado R.3.2.1.14.4 Actividades relacionadas con usuarios con mayor acceso R.3.2.1.14.5 Actividades relacionadas con estado y disponibilidad de las conexiones
E.3.2.1.15 Reporte de actividades relacionadas con los dispositivos de prevención y detección de intrusos. Mensual	Documento con la identificación de incidentes en base a firmas, políticas y anomalías del tráfico de red.	R.3.2.1.15.1 Actividades relacionadas con ataques a segmentos de red R.3.2.1.15.2 Actividades relacionadas con ataques a Aplicaciones R.3.2.1.15.3 Actividades relacionadas con ataques a URL's R.3.2.1.15.4 Actividades relacionadas con ataques a usuarios o

		servidores R.3.2.1.15.5 Actividades relacionadas con ataques bloqueados R.3.2.1.15.6 Actividades relacionadas con ataques Falso - positivo R.3.2.1.15.7 Actividades relacionadas con Trafico de IP R.3.2.1.15.8 Actividades relacionadas con ataques de códigos maliciosos.

3.2.1.6 Servicio de gestión de infraestructura y monitoreo de eventos de los componentes de seguridad perimetral del IFT.

S.1.1 - [Servicio de gestión de infraestructura y monitoreo de eventos de seguridad de los componentes de seguridad perimetral del IFT.]	
Característica	**Descripción**
Propósito	El Proveedor Adjudicado tomará la administración de los equipos de seguridad perimetral provistos por el IFT como parte del proyecto. El Proveedor Adjudicado deberá realizar un monitoreo 7 x 24 (las 24 horas del día, los 7 días de la semana, durante la vigencia del contrato) a la infraestructura de seguridad involucrada en los servicios de seguridad administrada. El Proveedor Adjudicado deberá instalar el software y hardware necesario, así como administrar los recursos humanos que integre al proyecto con el fin de dar cumplimiento a los niveles de servicio definidos.
Tipo de servicio	Requerimiento.
Área geográfica y/o Lógica de cobertura	Oficinas del IFT consideradas en el alcance del proyecto.
Vigencia	Durante la vigencia del contrato.
Horario del servicio	[7 x 24] (7 días a la semana durante las 24 del día)
Prioridad	Crítica
Periodicidad de revisión del ANS	Mensual
Indicador de Desempeño	Nivel de disponibilidad mensual (porcentaje) Total de minutos del mes (43,200) = 30 días * 24 horas * 60 min. Disponibilidad mínima aceptada (42,984) = 43,200 * 0.995 Indisponibilidad tolerada (216 minutos por mes) = 43,200 * 0.005 Indisponibilidad registrada = Minutos en que la solución está fuera de servicio durante el mes desde la hora en que se registra la caída del servicio hasta su recuperación a nivel operativo. Disponibilidad total mensual = [Disponibilidad mínima aceptada + (Indisponibilidad tolerada – indisponibilidad registrada)]/ Total de minutos del mes
Nivel de Servicio mínimo esperado	99.5 % mensual
Penalización	Conforme a lo establecido en el apartado 5.- Penalizaciones
Requerimientos Adicionales	El Proveedor Adjudicado es responsable de realizar el monitoreo de las capacidades de los Componentes Habilitadores (Memoria, Disco, procesador, etc.), con el fin de prever incidentes que comprometan los niveles de servicio pactados. El Proveedor Adjudicado deberá proporcionar un reporte mensual del monitoreo de capacidades de los dispositivos administrados que se describen en el numeral 3.2.1.2 Administración y monitoreo de la infraestructura de seguridad perimetral existente.

3.2.1.7 Servicio de correlación de eventos y administración de bitácoras

S.1.2 - [Servicio de correlación de eventos y administración de bitácoras.]	
Característica	**Descripción**
Propósito	Concentrar, analizar y explotar las bitácoras de los dispositivos del IFT con la finalidad de conocer exactamente qué pasa en distintos puntos de la red de forma centralizada y eliminar falsos positivos.
Tipo de servicio	Requerimiento.
Área geográfica y/o Lógica de cobertura	Oficinas del IFT consideradas en el alcance del proyecto.
Vigencia	Durante la vigencia del contrato.
Horario del servicio	[7 x 24] (7 días a la semana durante las 24 del día)
Prioridad	Crítica
Periodicidad de revisión del ANS(bitácora)	Mensual
Indicador de Desempeño	Nivel de disponibilidad mensual (porcentaje) Total de minutos del mes (43,200) = 30 días * 24 horas * 60 min. Disponibilidad mínima aceptada (42,984) = 43,200 * 0.995 Indisponibilidad tolerada (216 minutos por mes) = 43,200 * 0.005 Indisponibilidad registrada = Minutos en que la solución está fuera de servicio durante el mes desde la hora en que se registra la caída del servicio hasta su recuperación a nivel operativo. Disponibilidad total mensual = [Disponibilidad mínima aceptada + (Indisponibilidad tolerada – indisponibilidad registrada)]/ Total de minutos del mes
Nivel de Servicio mínimo esperado	99.5 % mensual
Penalización	Conforme a lo establecido en el apartado 5.- Penalizaciones
Requerimientos Adicionales	Establecer los mecanismos necesarios para salvaguardar evidencia que pueda ser utilizada de manera explícita, que no deje dudas sobre las conclusiones alcanzadas y que no esconda, sobrescriba o borre datos importantes para el análisis forense que se encuentren almacenados en las bitácoras de los Dispositivos Habilitadores.

El IFT requiere una solución para llevar a cabo la administración, correlación y análisis de eventos de seguridad que permita la administración de eventos e información necesaria para el monitoreo, análisis, administración y generación de reportes identificando en tiempo real las amenazas, dotando de procesos, herramientas y flujos de trabajo para la contención oportuna de ataques, identificación de incidentes y riesgos potenciales para la infraestructura y los servicios tecnológicos de IFT.

Dicha solución deberá realizar la administración de toda la información de seguridad generada por todos los dispositivos de la infraestructura de red de distintos fabricantes y proveedores, mediante una aplicación inteligente que recopile, analice y correlacione los datos de todos los eventos de seguridad que se presenten dentro la red de IFT, utilizando las bitácoras que generan los equipos. La solución deberá consolidar automáticamente, administrar y escalar amenazas en tiempo real (con la mayor proximidad al ciclo de un posible ataque). Dicha información deberá ser manejada y almacenada hasta 90 días en línea. Se deberá incluir el almacenamiento fuera de línea de toda la información colectada y generada por la solución de correlación, debido a que podrá ser solicitada y/o consultada por el Instituto en cualquier momento durante la vigencia del contrato.

La tecnología deberá incluir y operar al menos con las siguientes características:

- La solución tecnológica de correlación de eventos y administración de bitácoras deberá ser una solución líder en el mercado (que se encuentre dentro del cuadrante de líderes de Gartner más reciente para soluciones tipo SIEM) que proporcione al SOC alertas de seguridad de eventos en tiempo real, monitoreo y desglose de la funcionalidad forense, la plataforma de correlación deberá brindar a los administradores una visión clara de la información relevante. La solución de correlación debe tener la capacidad suficiente para recolectar los logs de cada uno de los dispositivos definidos dentro del alcance de este documento.
- La solución tecnológica de correlación de eventos y administración de bitácoras deberá ser una solución de propósito específico (appliance).
- El sistema deberá colectar, agregar, y filtrar bitácoras crudas de las fuentes que el IFT determine.
- Correlacionar los eventos para las plataformas del IFT, alertar en tiempo real cuando una amenaza ocurra y priorizar los eventos con base en su criticidad.
- Después de éste filtrado inicial, la arquitectura deberá ser capaz de:
    - Analizar las bitácoras en tiempo real y conservarlos para un análisis posterior.
    - Almacenar localmente todas las bitácoras crudas Se requiere que el servicio de monitoreo de bitácoras del Proveedor Adjudicado tenga una cobertura de 24x7 durante la vigencia del contrato.
- El almacenamiento de bitácoras deberá hacerse en las instalaciones del IFT y deberá contar con un mecanismo para generar reportes en forma local.
- Se requiere que a través de la consola de administración se permita a los responsables asignar reportes de bitácoras a usuarios específicos, quienes pueden revisarlos y conservarlos para una investigación futura, permitiendo al IFT dar seguimiento al flujo de trabajo y crear una ruta para propósitos de análisis de cumplimiento.
- Durante los primeros 90 días del proyecto, los consultores del Proveedor Adjudicado deberán trabajar en conjunto con el personal del IFT para asegurar que la tecnología para el monitoreo de bitácoras sea configurada de forma adecuada, así como también ayudar a:
    - Identificar los dispositivos y aplicaciones críticos.
    - Comprender los tipos y métodos de captura de bitácoras
    - Definir los tipos de eventos a ser reportados
    - Implementar las reglas de filtrado de bitácoras para capturarlos y reportarlos.
- La tecnología utilizada deberá actualizarse en tiempo real conforme aparecen las amenazas para poder rápidamente reportar y responder a cualquier amenaza de seguridad de la información.

El servicio deberá soportar todas las plataformas que tiene el IFT, incluyendo sistemas operativos, dispositivos de red, bases de datos, entre otros.

La tecnología debe ser flexible y deberá permitir el diseño rápido de soluciones que acepten la entrada de bitácoras de aplicaciones hechas en casa y otras fuentes de bitácoras no estándares. La solución deberá ser lo suficientemente robusta para eliminar, en lo posible, el desarrollo e ingeniería para soportar nuevos bitácoras.

La solución provista para este servicio debe considerar al menos las plataformas de comunicaciones, cómputo y almacenamiento disponibles en las instalaciones del IFT.

El Proveedor Adjudicado deberá integrar a su propuesta la capacidad de análisis forense cuando se presenten incidentes de seguridad, para ello deberá integrar los recursos de almacenamiento, protección y administración de las bitácoras de los Dispositivos Habilitadores.

El Proveedor Adjudicado deberá considerar el procedimiento de administración de las bitácoras, el cual deberá definir la identificación de las bitácoras que se activarán para cada dispositivo, el tamaño máximo de cada bitácora, los eventos que se deberán incluir para cada dispositivo y la forma en que se realizará la transferencia a un almacenamiento debidamente catalogado, que permita en el futuro su consulta sin mayores esfuerzos por parte del IFT (formato abierto). El servicio de administración de bitácoras deberá mantenerse transparente al usuario; es decir, quién está siendo monitoreado a través de este medio, no debe conocer de su existencia, ni mucho menos conocer su ubicación ni tener acceso a las bitácoras. El almacenamiento en donde se concentre la información de las bitácoras deberá contar con mecanismos de cifrado que resguarden su integridad.

La solución de administración de bitácoras debe de considerar una retención de datos de hasta 90 días en línea y 365 días en histórico. Al cabo de los 365 días se entregará un respaldo a el IFT en formato legible para sus equipos (formato abierto) considerando mecanismos de seguridad que aseguren su integridad y confiabilidad.

3.2.1.8 Análisis de vulnerabilidades y pruebas de penetración

S.1.3- [Servicio de análisis de vulnerabilidades y pruebas de penetración.]	
Característica	**Descripción**
Propósito	Determinar el nivel de riesgo que presenta la infraestructura del Instituto frente a las distintas amenazas a las que puede enfrentarse de acuerdo a su ubicación, uso, sensibilidad, entre otros factores relevantes.
Tipo de servicio	Requerimiento.
Área geográfica y/o Lógica de cobertura	Oficinas del IFT consideradas en el alcance del proyecto. Dispositivos de red y aplicaciones definidas para este servicio.
Vigencia	Durante la vigencia del contrato.
Horario del servicio	[7 x 24] (7 días a la semana durante las 24 del día)
Prioridad	Crítica
Periodicidad de revisión del ANS	Conforme se programen las pruebas de aplicaciones

S.1.3- [Servicio de análisis de vulnerabilidades y pruebas de penetración.]	
Característica	**Descripción**
Requerimientos Adicionales	El Proveedor Adjudicado deberá generar el reporte de las vulnerabilidades identificadas como críticas en el momento en que las descubra, este reporte debe incluir: Descripción de la vulnerabilidad detectada, Recomendaciones de solución inmediata, Identificación de causa raíz, Recomendaciones de solución de la causa raíz, Identificación de recursos requeridos para solucionar la vulnerabilidad.

a) Análisis de Vulnerabilidades

Como parte del servicio, el Proveedor Adjudicado deberá integrar herramientas para análisis de vulnerabilidades Web (a través de URL's de aplicaciones internas y/o externas) y análisis de vulnerabilidades de infraestructura (a través de las IP´s de los dispositivos) que permitan:

- Evaluar la existencia de vulnerabilidades en la infraestructura de red y/o seguridad del IFT.
- Determinar el impacto y la probabilidad de ataque de una vulnerabilidad en el contexto de la infraestructura de red y/o seguridad del IFT, así como para proponer posibles soluciones.
- Obtener reportes estadísticos de activos más atacados, patrones más frecuentes de ataque (fuentes, horarios, tipos, etc.), tipos de ataque más realizados, activos más vulnerables, activos con más impacto probable, entre otros.

El objeto de estos servicios es identificar las vulnerabilidades a las que están expuestos los servicios, puertos de dispositivos de comunicaciones, servidores, estaciones de trabajo y otros dispositivos IP, así como de las aplicaciones que forman parte de los activos críticos del IFT y que pueden ser comprometidos ante ataques.

La CGOTI en conjunto con el Proveedor Adjudicado, definirán los servicios de negocio, aplicaciones y activos de información críticos para que estos sean analizados trimestralmente.

Se deberá ejecutar un proceso trimestral incremental de análisis de vulnerabilidades sobre las aplicaciones, infraestructura existente y nuevos desarrollos, se deberán de considerar hasta 25 IP's y 5 URL's nuevas mensualmente, la información del análisis se deberá incluir en la correlación. Las IP's y URL's serán proporcionadas por el IFT.

El IFT definirá los tiempos para la ejecución de los escaneos, el tipo de pruebas, así como los responsables por parte del IFT.

Los análisis de vulnerabilidades que ejecute el Proveedor Adjudicado en forma trimestral deberán cubrir por lo menos los siguientes rubros:

- Identificar los servicios, incluyendo la versión de los sistemas operativos analizados.

- Identificación de vulnerabilidades conocidas, lista que deberá ser actualizada semestralmente acorde con organizaciones como OWASP (Open Web Application Security Project) y CVE (Common Vulnerability and Exposures).
- Inyección Sql o Html
- Cross-Site Scripting XSS,
- Autenticación débil o manejo de sesiones
- Cross-Site Request Forgery (CSRF)
- Protección insuficiente en la transmisión de datos
- Identificación de configuraciones por defecto.
- Los reportes y evidencia de hallazgos deben ser resguardados.
- Identificación de malas configuraciones respecto a la política de seguridad del IFT.

El Proveedor Adjudicado deberá generar un reporte donde se listen las vulnerabilidades y malas configuraciones detectadas en los sistemas. Este reporte deberá contener una propuesta de solución técnica a las vulnerabilidades detectadas, así como recomendaciones que contengan los rubros de gente, procesos y procedimientos, dicho reporte deberá ser presentado al supervisor del proyecto y Administrador del contrato por parte de la CGOTI.

El Proveedor Adjudicado deberá entregar, por dispositivo o aplicación analizada, una lista que incluya los servicios detectados así como las versiones de los mismos. El Proveedor Adjudicado deberá entregar como evidencia, en formato digital, las bitácoras generadas por de las herramientas usadas durante el estudio.

El Proveedor Adjudicado deberá presentar y explicar a detalle el informe de vulnerabilidades críticas y las acciones que recomienda para su mitigación

Para la realización de este servicio el Proveedor Adjudicado deberá instalar los dispositivos y herramientas necesarias para la prestación del servicio, deberá mantenerlas actualizadas y encargarse de la administración y soporte que estas necesiten.

La remediación de las vulnerabilidades está fuera del alcance de este servicio.

Los reportes de análisis de vulnerabilidades que el Proveedor Adjudicado proporcionará, deberán identificar y notificar de nuevas vulnerabilidades o recurrentes vulnerabilidades que puedan impactar a los sistemas o aplicaciones del IFT. Por este motivo, el Proveedor Adjudicado deberá generar las recomendaciones a seguir para la mitigación de los huecos de seguridad encontrados.

El Proveedor Adjudicado deberá apoyarse en alguna metodología reconocida por la industria (como puede ser OWASP) para la realización de los estudios de análisis de vulnerabilidades. Para ello deberá entregar, en su propuesta, un documento con el resumen de dicha metodología.

El Proveedor Adjudicado deberá usar el Common Vulnerability Scoring System (CVSS) para la clasificación de los hallazgos.

El IFT proveerá al Proveedor Adjudicado de las direcciones IP necesarias para la instalación del o los dispositivos que habilitaran este servicio y se asegurará de que tengan visibilidad suficiente para realizar el análisis de vulnerabilidades.

Para proveer el servicio, el Proveedor Adjudicado deberá utilizar una solución tecnológica (no opensource) con las siguientes características:

- Basado en un dispositivo de uso específico.
- La solución debe ser capaz de evaluar al menos los siguientes sistemas operativos:
    - Microsoft Windows.
        - Windows Server 2012
        - Windows Server 2008
        - Windows Server 2003 (SP1, R2, SP2)
        - Windows XP
        - Windows 7
        - Windows 8
    - Linux
        - Red Hat® Enterprise Linux ES (versión 3 y 4)
        - Suse Linux Enterprise (versión 9)
        - Suse Linux Enterprise (versión 11)
- La solución debe ser capaz de evaluar las siguientes bases de datos sin necesidad de tener credenciales para autenticarse:
    - Oracle
    - SQL Server
    - MySQL
- La solución debe ser capaz de evaluar los sistemas operativos de los siguientes dispositivos:
    - Ruteadores
    - Switches
    - Hubs
    - Firewalls
- La actualización de vulnerabilidades y otros aspectos del mantenimiento (como parches y actualizaciones) deberá ser de forma automatizada desde el sitio Web del fabricante del producto.
- La solución que se implemente para análisis de vulnerabilidades debe tener al menos las siguientes características:
    - Deberá permitir crear mapas o topologías de la red.
    - Deberá permitir escanear las vulnerabilidades en la red.

- Deberá permitir escanear aplicaciones Web.
- Deberá tener la opción de implementar políticas de seguridad e identificar aquellos equipos que no cumplan con las mismas.
- Deberá permitir asignar diferentes cronogramas para la automatización de cada mapeo y escaneo.
- Los reportes de topologías y escaneo podrán ser guardados en distintos formatos, considerando al menos los archivos de formato portable PDF, archivos de formato abierto XML, CVS o HTML.
- Deberá enviar correos electrónicos de alerta, al personal designado por el Instituto, con un resumen del número de nuevas vulnerabilidades detectadas.
- Deberá de tener una precisión de menos de 3.4 errores por millón de escaneo (un error siendo un falso positivo, falso negativo, o negación de servicio).
- Deberá poder clasificar las vulnerabilidades y riesgos en varios niveles de criticidad, considerando al menos los niveles bajo, medio, alto y crítico.
- Deberá poder clasificar por grupos en función de las propiedades de las vulnerabilidades o riesgos a fin de poder asignar las tareas de remediación.
- Deberá poder administrar múltiples usuarios para la remediación de las vulnerabilidades y riesgos.
- Deberá permitir el seguimiento de las tareas de remediación mediante un sistema de tickets independiente del de la mesa de servicio.
- El sistema de tickets deberá generar tickets y asignarlos a usuarios en forma automática, con base en reglas de negocio.
- Deberá permitir asignar usuarios y claves para cada equipo a escanear, resguardando las credenciales de forma cifrada y asegurando que no puedan ser recuperadas por el administrador de la herramienta.
- Deberá mantenerse actualizado en forma automática con las últimas vulnerabilidades de los diversos sistemas operativos y sus versiones.
- El sistema no deberá requerir la instalación de agentes de ningún tipo, ni requerir equipo dedicado, Web servers locales en la red, bases de datos, etc.
- Deberá contar con un módulo de reportes que permita la creación de filtros por: vulnerabilidad, equipo, aplicación, puerto, severidad, protocolo, fecha y periodo.
- El módulo de reportes deberá contar con la capacidad de creación de reportes en distintos formatos, considerando al menos los archivos de formato portable PDF, archivos de formato abierto XML, CVS o HTML.

b) Pruebas de Penetración

Las pruebas de penetración serán trimestrales y tendrán un máximo de 5 objetivos.

El Proveedor Adjudicado deberá considerar los siguientes tipos de pruebas de penetración (internas/externas) para este servicio:

- Evaluación de Caja Negra de Aplicaciones (código abierto).
- Test de Intrusión (Hackeo Ético), utilizando herramientas comerciales. El uso de herramientas de software libre deberá ser únicamente de forma complementaria a los reportes obtenidos por la herramienta comercial.
- Petición de ejecución de pruebas de penetración (dependiendo de la prueba, puede o no incluir la lista de dispositivos a analizar por parte del IFT (pruebas de caja negra).
- Generación de documentos de trabajo (SOW) y cronogramas de trabajo por parte del Proveedor Adjudicado para las pruebas de penetración, donde se definan los tiempos de ejecución, el tipo de pruebas, así como los responsables por parte del Proveedor Adjudicado y el IFT.
- Aquellas pruebas que, por su naturaleza puedan afectar la estabilidad de los sistemas del IFT tendrán que ser analizadas y autorizadas por el supervisor del proyecto y Administrador del contrato por parte de la CGOTI.

Por ningún motivo el Proveedor Adjudicado podrá modificar configuraciones en los equipos comprometidos o considerados en las pruebas a fin de obtener mayor penetración en los sistemas, a menos que el supervisor del proyecto y Administrador del contrato por parte de la CGOTI lo autorice.

El Proveedor Adjudicado deberá dejar banderas en los sistemas comprometidos; como pueden ser archivos de texto, podrá crear usuarios en los sistemas que llevarán el nombre definido entre el IFT y el Proveedor Adjudicado.

El IFT tomará como evidencia los resultados de la solución a usar, capturas de pantalla de los sistemas, así como banderas que el Proveedor Adjudicado pueda dejar en los sistemas comprometidos.

El Proveedor Adjudicado deberá determinar la viabilidad de un ataque de aquellas fallas que no puedan ser mitigadas y realizar un informe detallado de acuerdo a los hallazgos de la infraestructura del IFT.

El Proveedor Adjudicado deberá entregar como evidencia, en formato digital, las bitácoras de la solución usada durante el estudio.

Para la prestación de este servicio el Proveedor Adjudicado deberá utilizar una herramienta comercial, la cual mantendrá actualizada durante la vigencia del contrato, el Proveedor Adjudicado deberá entregar en su propuesta técnica carta bajo protesta de decir verdad que cumplirá estas condiciones y anualmente el Proveedor Adjudicado deberá presentar evidencia del fabricante de la herramienta en la que demuestre que tiene contratados sus servicios de soporte y mantenimiento.

El servicio deberá estar basado en el siguiente proceso:

- Descubrimiento
- Enumeración (obtención de nombres de usuarios, información de la red, versiones, servicios)
- Explotación
- Reporteo

En el caso de requerir viajar para la prestación de este servicio el Proveedor Adjudicado deberá considerar los viáticos correspondientes para el traslado de su personal a la ubicación donde el IFT requiera la ejecución del servicio.

Los reportes mensuales de pruebas de penetración que el Proveedor Adjudicado proporcionará, deberán identificar y notificar huecos de seguridad que puedan impactar a los sistemas o aplicaciones del IFT. Por este motivo, el Proveedor Adjudicado deberá generar las recomendaciones a seguir para la mitigación de los huecos de seguridad encontrados.

El Proveedor Adjudicado deberá apoyarse de alguna metodología reconocida por la industria para la realización de pruebas de penetración. Para ello deberá entregar, en su propuesta, un documento con el resumen de dicha metodología.

El Proveedor Adjudicado deberá usar el Common Vulnerability Scoring System (CVSS) para la clasificación de los hallazgos.

En el caso en que las pruebas de penetración se realicen en las localidades físicas del IFT, éste asignará un lugar físico de trabajo para que el Proveedor Adjudicado desarrolle las actividades correspondientes. Para ello se proporcionará:

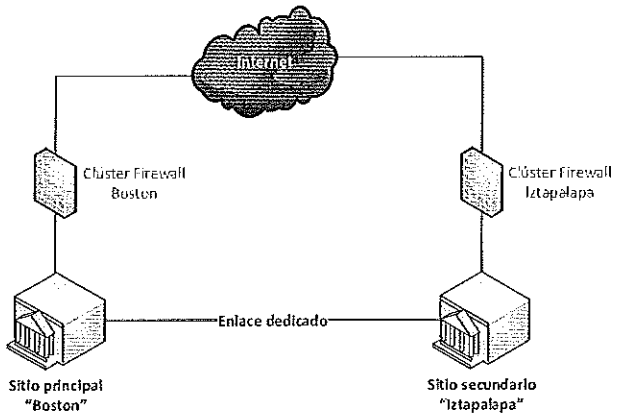
- Dos (2) nodos de red con conectividad a la red interna.
- Dos (2) direcciones IP que tengan visibilidad de los dispositivos a ser auditados.

3.2.1.9 Servicio de control de acceso Firewall

S.1.4- [Servicio de control de acceso Firewall]	
Característica	**Descripción**
Propósito	Contar con una solución en alta disponibilidad que ofrezca protección perimetral a la red del IFT con la finalidad de proteger la infraestructura, las aplicaciones, la información y los servicios de Internet de accesos no autorizados. La zona de seguridad perimetral se considera aquella entre la conexión a Internet y la conexión a la red de datos del IFT e incluye la protección a usuarios internos, dispositivos de red, servidores web y aplicaciones internas que usan los protocolos TCP/IP. Existe un gran número de aplicaciones y servicios web que están disponibles para usuarios externos e internos del Instituto por lo que es imperioso contar con políticas de acceso para cada uno de los servicios que el IFT pone a disposición de la ciudadanía. La solución requerida en este servicio es redundante para minimizar el tiempo de interrupción en el acceso a las aplicaciones del IFT en caso de presentarse una falla en los equipos.
Tipo de servicio	Requerimiento.

S.1.4- [Servicio de control de acceso Firewall]	
Característica	**Descripción**
Área geográfica y/o Lógica de cobertura	Aplicaciones con acceso Web, dispositivos de red, usuarios internos y bases de datos del IFT.
Vigencia	Durante la vigencia del contrato.
Horario del servicio	[7 x 24] (7 días a la semana durante las 24 del día)
Prioridad	Crítica
Periodicidad de revisión del ANS	Mensual
Indicador de Desempeño	Nivel de disponibilidad mensual (porcentaje) Total de minutos del mes (43,200) = 30 días * 24 horas * 60 min. Disponibilidad mínima aceptada (42,984) = 43,200 * 0.999 Indisponibilidad tolerada (216 minutos por mes) = 43,200 * 0.001 Indisponibilidad registrada = Minutos en que la solución está fuera de servicio durante el mes desde la hora en que se registra la caída del servicio hasta su recuperación a nivel operativo. Disponibilidad total mensual = [Disponibilidad mínima aceptada + (Indisponibilidad tolerada – indisponibilidad registrada)]/ Total de minutos del mes
Nivel de Servicio mínimo esperado	99.9 % mensual
Penalización	Conforme a lo establecido en el apartado 5.- Penalizaciones
Requerimientos Adicionales	Se debe considerar la protección de control de acceso firewall para las siguientes localidades del IFT: - Clúster activo - activo de control de acceso Firewall en el edificio denominado "Boston" - Clúster activo – activo de control de acceso Firewall en el edificio denominado "Iztapalapa"

El IFT requiere como parte de este servicio que el Proveedor Adjudicado considere la implementación de dispositivos de control de acceso Firewall en alta disponibilidad en los sitios que se ilustran en el siguiente diagrama:



Los clúster de firewall que serán instalados en el sitio principal "Boston" y en el sitio secundario "Iztapalapa" deberán configurarse bajo un esquema activo – activo y tendrán diferentes características y funcionalidades habilitadas que se describen a continuación:

a) Firewall sitio principal "Boston"

La solución de firewall que se instalará en el sitio principal del IFT denominado "Boston" deberá estar bajo un esquema de alta disponibilidad y cumplir con al menos las siguientes características:

- Ser una solución en hardware (appliance).
- Contar con la consola de administración integrada.
- Operar bajo el concepto de Blades de Software.
- Estar basado en la tecnología Stateful Inspection.
- Contar con autenticación para acceso al dispositivo (a nivel de grupo y a nivel de usuario).
- Contar con capacidad para integrarse a un directorio activo.
- Debe permitir crear controles de acceso a por lo menos 150 aplicaciones/servicios/protocolos predefinidos.
- Debe proteger implementaciones de VoIP, soportando H.323 v2/3/4 (incluido h.225 v.2/3/3 y h.254 v3/5/7), SIP. MGCP y SCCP.
- Debe incluir 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.
- Permitir implementar reglas aplicadas a intervalos de tiempo específicos.
- La comunicación entre los servidores de administración y los gateways, debe ser cifrada y autenticada.
- El firewall debe soportar métodos de autenticación, por usuario, cliente y por sesión.
- Debe ser capaz de autenticar sesiones de cualquier servicio, tales como HTTP, HTTPS.
- Soportar los esquemas de autenticación a través de: tokens (por ejemplo, SecureID), TACACS, RADIUS, certificados digitales y dispositivos biométricos.
- Incluir una base de datos local que permita realizar autenticación, sin depender de un dispositivo externo.
- Incluir la posibilidad de implementar dos reglas de NAT que apliquen para una única conexión.
- Soportar DHCP en modos server y relay.
- Debe incluir la posibilidad de que el Firewall trabaje en modo transparente (bridged mode).
- Debe permitir el controlar el acceso a archivos compartidos de Microsoft usando CIFS, y que el administrador decida que carpetas se pueden acceder y cuáles no.
- Debe soportar alta disponibilidad y balanceo de carga de gateways con sincronización de estados.
- Deberá contar con un throughput de 11 Gbps para firewall.

b) Firewall sitio secundario "Iztapalapa"

La solución de firewall que se instalará en el sitio principal del IFT denominado "Iztapalapa" deberá implementarse bajo un esquema de alta disponibilidad y deberá tener habilitadas las funcionalidades de VPN, filtrado de URL's, protección contra intrusos, modelado de tráfico, antivirus, Antispam, inspección SSL y control de aplicaciones. El dispositivo deberá tener la capacidad suficiente para tener configuradas y operando simultáneamente todas las funcionalidades descritas para al menos 1200 usuarios.

A continuación se describen las características mínimas, más no limitativas, que deberá contener la solución de firewall que será instalada en Iztapalapa:

- Ser una solución en hardware (appliance).
- Basado en tecnología ASIC "Application-Specific Integrated Circuit" y ser capaz de brindar una solución de "Complete Content Protection".

- Capacidad de re-ensamblado de paquetes en contenido para buscar ataques o contenido prohibido, basado en hardware.
- Capacidad de ser configurado en modo Gateway o en modo transparente en la red. En modo transparente, el equipo no requerirá de hacer modificaciones en la red en cuanto a ruteo o direccionamiento IP.
- Sistema operativo pre-endurecido específico para seguridad que sea compatible con el "appliance", no se aceptan soluciones sobre sistemas operativos genéricos tales como GNU/Linux, FreeBSD, SUN Solaris, HP-UX, AIX o Windows.
- Contar con un rendimiento (throughput) de Firewall de al menos 78 Gbps para paquetes de 1518 y 512 bytes, un rendimiento de VPN de al menos 48 Gbps, rendimiento de detección de intrusos de al menos10 Gbps, rendimiento de antivirus en modo proxy de al menos 4.2 Gbps, rendimiento de antivirus en modo Flow de 12 Gbps.
- El equipo debe soportar al menos 11 millones de sesiones concurrentes
- El equipo debe soportar 240,000 nuevas sesiones por segundo.
- El equipo debe de contar desde un inicio con la funcionalidad y licenciamiento de por lo menos 1300 usuarios de VPN SSL y IPSec Client to Gateway.
- El equipo debe soportar la generación de VPN's IPSec Gateway to Gateway
- El equipo debe contar con al menos 10 Interfaces GigaEthernet RJ45, 10 Interfaces GigaEthernet SFP y 8 interfaces 10 GigEthernet SFP+.
- Por granularidad y seguridad, el firewall deberá poder especificar políticas tomando en cuenta puerto físico fuente y destino. Esto es, el puerto físico fuente y el puerto físico destino deberán formar parte de la especificación de la regla de firewall.
- Será posible definir políticas de firewall que sean independientes del puerto de origen y puerto de destino.
- Las reglas del firewall deberán tomar en cuenta dirección IP origen (que puede ser un grupo de direcciones IP), dirección IP destino (que puede ser un grupo de direcciones IP) y servicio (o grupo de servicios) de la comunicación que se está analizando.
- Soporte a reglas de firewall para tráfico de multicast, pudiendo especificar puerto físico fuente, puerto físico destino, direcciones IP fuente, dirección IP destino.
- Las reglas de firewall deberán poder tener limitantes y/o vigencia en base a fechas (incluyendo día, mes y año).
- Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos.
- Debe poder definirse el tiempo de vida de una sesión inactiva de forma independiente por puerto y protocolo (TCP y UDP).
- Capacidad de hacer traslación de direcciones estático, uno a uno, NAT.
- Capacidad de hacer traslación de direcciones dinámico, muchos a uno, PAT.

- Deberá soportar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario).
- La solución deberá tener la capacidad de balancear carga entre servidores.
- En la solución de balanceo de carga entre servidores, debe soportarse persistencia de sesión al menos mediante HTTP Cookie o SSL Session ID.
- En la solución de balanceo de carga de entre servidores deben soportarse mecanismos para detectar la disponibilidad de los servidores, de forma tal de poder evitar enviar tráfico a un servidor no disponible.
- Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs.
- Soporte a ruteo estático, incluyendo pesos y/o distancias y/o prioridades de rutas estáticas.
- Soporte a políticas de ruteo (policy routing). El soporte a políticas de ruteo deberá permitir que ante la presencia de dos enlaces a Internet, se pueda decidir cuál tráfico sale por un enlace y qué tráfico sale por otro enlace.
- Soporte a ruteo dinámico RIP V1, V2, OSPF, BGP y IS-IS.
- La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow.
- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- Soporte para IKEv2 y IKE Configuration Method.
- Debe soportar la configuración de túneles L2TP y PPTP
- Soporte de VPNs con algoritmos de cifrado: AES y 3DES.
- Se debe soportar longitudes de llave para AES de 128, 192 y 256 bits.
- Se debe soportar al menos los grupos de Diffie-Hellman 1, 2, 5 y 14.
- Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256.
- Posibilidad de crear VPN's entre gateways y clientes con IPSec. esto es, VPNs IPSeC site-to-site y VPNs IPSec client-to-site. En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.
- Tanto para IPSec como para L2TP debe soportarse los clientes terminadores de túneles nativos de Windows y MacOS X.
- Capacidad de realizar SSL VPNs.
- Soporte a certificados PKI X.509 para construcción de VPNs SSL.
- Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN.
- Soporte de renovación de contraseñas para LDAP y RADIUS.
- Soporte a asignación de aplicaciones permitidas por grupo de usuarios
- Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet.

- Deberá poder verificar la presencia de antivirus (propio y/o de terceros y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL.
- La VPN SSL integrada deberá soportar a través de algún plug-in ActiveX y/o Java, la capacidad de meter dentro del túnel SSL tráfico que no sea HTTP/HTTPS
- Deberá soportar la redirección de página HTTP a los usuarios que se registren en la VPN SSL, una vez que se hayan autenticado exitosamente
- Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo al grupo de pertenencia de dichos usuarios.
- Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall.
- Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión.
- Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general.
- Capacidad de poder definir ancho de banda garantizado en Kbps por segundo.
- Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en Kbps por segundo
- Capacidad de para definir prioridad de tráfico, en al menos tres niveles de importancia.
- Capacidad de integrarse con Servidores de Autenticación RADIUS.
- Capacidad nativa de integrarse con directorios LDAP.
- Capacidad incluida, al integrarse con Microsoft Windows Active Directory, de autenticar transparentemente usuarios sin preguntarles username o password. Esto es, aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On".
- Capacidad de autenticar usuarios para cualquier aplicación que se ejecute bajo los protocolos TCP/UDP/ICMP. Debe de mostrar solicitud de autenticación (Prompt) al menos para Web (HTTP), FTP y Telnet.
- Soporte a certificados PKI X.509 para construcción de VPNs cliente a sitio (client-to-site).
- La solución soportará políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo al grupo de pertenencia de los usuarios.
- Deben poder definirse usuarios y grupos en un repositorio local del dispositivo.
- Para los administradores locales debe poder definirse la política de contraseñas que especificará como mínimo:
    - Longitud mínima permitida.
    - Restricciones de tipo de caracteres: numéricos, alfanuméricos, etc.
    - Expiración de contraseña.

  - Capacidad de limitarse la posibilidad de que dos usuarios o administradores tengan sesiones simultáneas desde distintas direcciones IP.
- La detección de intrusos debe poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de línea, el equipo recibirá el tráfico a inspeccionar desde un Switch con un puerto configurado en SPAN o MIRROR.
- La detección de intrusos podrá implementarse en línea y fuera de línea en forma simultánea para distintos segmentos.
- Capacidad de actualización automática de firmas IPS mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).
- La detección de intrusos deberá de estar orientado para la protección de redes.
- La detección de intrusos deberá estar integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la prevención de intrusos. La interfaz de administración de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad "appliance", sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso.
- La detección de intrusos deberá identificar y solventar ataques por Anomalía (Anomaly detection) además de firmas (signature based / misuse detection).
- Basado en análisis de firmas en el flujo de datos en la red, y deberá permitir configurar firmas nuevas para cualquier protocolo.
- Tecnología de detección tipo Stateful basada en Firmas (signatures).
- Actualización automática de firmas para el detector de intrusos.
- El Detector de Intrusos deberá mitigar los efectos de los ataques de negación de servicios.
- Mecanismos de detección de ataques:
  - Reconocimiento de patrones y Análisis de protocolos.
  - Detección de anomalías.
  - Detección de ataques de RPC (Remote procedure call).
  - Protección contra ataques de Windows o NetBios.
  - Protección contra ataques de SMTP (Simple Message Transfer Protocol) IMAP (Internet Message Access Protocol, Sendmail o POP (Post Office Protocol)
  - Protección contra ataques DNS (Domain Name System)
  - Protección contra ataques a FTP, SSH , Telnet y Rlogin
  - Protección contra ataques de ICMP (Internet Control Message Protocol)."
- Métodos de notificación:
  - Alarmas mostradas en la consola de administración del "appliance".

- Alertas vía correo electrónico.

- Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado.
- La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto."
- Debe ofrecerse la posibilidad de guardar información sobre el paquete de red que detonó la detección del ataque así como al menos los 5 paquetes sucesivos. Estos paquetes deben poder ser visualizados por una herramienta que soporte el formato PCAP.
- Lo solución de control de aplicaciones debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo.
- La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico.
- La solución de control de aplicaciones debe tener un listado de al menos 3,000 aplicaciones ya definidas por el fabricante y actualizarse periódicamente.
- Para aplicaciones identificadas y desconocidas deben poder definirse al menos las siguientes opciones: Permitir, Bloquear, Registrar en logs.
- Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping.
- La solución de Firewall debe soportar la capacidad de inspeccionar tráfico que esté siendo encriptado mediante TLS al menos para los siguientes protocolos: HTTPS, IMAPS, SMTPS, POP3S.
- La inspección deberá realizarse mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle).
- La inspección de contenido encriptado no debe requerir ningún cambio de configuración en las aplicaciones o sistema operativo del usuario.
- Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado.
- Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer Antivirus en tiempo real en al menos los siguientes protocolos aplicativos: HTTP, SMTP, IMAP, POP3, FTP.
- La función de antivirus deberá poder configurarse en modo Proxy, así como en modo de Flujo. En el primer caso, los archivos serán totalmente reconstruidos por el motor antes de hacer la inspección. En el segundo caso, la inspección de antivirus se hará por cada paquete de forma independiente.

- Función de antivirus en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
- La configuración de Antivirus en tiempo real sobre los protocolos HTTP, SMTP, IMAP, POP3 y FTP deberá estar completamente integrada a la administración del dispositivo "appliance", que permita la aplicación de esta protección por política de control de acceso.
- El antivirus deberá soportar múltiples bases de datos de virus de forma tal de que el administrador defina cuál es conveniente utilizar para su implementación evaluando desempeño y seguridad.
- El "appliance" deberá de manera opcional poder inspeccionar por todos los virus conocidos (Zoo List).
- La función de antivirus integrada deberá tener la capacidad de poner en cuarentena archivos encontrados infectados que estén circulando a través de los protocolos HTTP, FTP, IMAP, POP3, SMTP.
- La función de antivirus integrada tendrá la capacidad de poner en cuarentena a los clientes cuando se haya detectado que los mismos envían archivos infectados con virus.
- La función deberá incluir capacidades de detección y detención de tráfico SPYWARE, ADWARE y otros tipos de MALWARE/GRAYWARE que pudieran circular por la red.
- La función de antivirus deberá poder hacer inspección y cuarentena de archivos transferidos por mensajería instantánea (Instant Messaging).
- La función de antivirus deberá ser capaz de filtrar archivos por extensión.
- La función de antivirus deberá ser capaz de filtrar archivos por tipo de archivo (ejecutables por ejemplo) sin importar la extensión que tenga el archivo.
- Capacidad de actualización automática de firmas de antivirus mediante tecnología de tipo "Push" (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo "pull" (Consultar los centros de actualización por versiones nuevas).
- La capacidad antispam incluida deberá ser capaz de detectar palabras dentro del cuerpo del mensaje de correo, y en base a la presencia/ausencia de combinaciones de palabras, decidir rechazar el mensaje.
- La capacidad antispam incluida deberá permitir especificar listas blancas (confiables, a los cuales siempre se les deberá pasar) y listas negras (no confiables, a los cuales siempre les deberá bloquear). Las listas blancas y listas negras podrán ser por dirección IP o por dirección de correo electrónico (e-mail address).
- La capacidad antispam deberá poder consultar una base de datos donde se revise por lo menos dirección IP del emisor del mensaje, URLs contenidos dentro del mensaje y "checksum" del mensaje, como mecanismos para detección de SPAM.
- En el caso de análisis de SMTP, los mensajes encontrados como SPAM podrán ser etiquetados o rechazados (descartados). En el caso de etiquetamiento del mensaje, debe tenerse la flexibilidad para etiquetarse en el motivo (subject) del mensaje o a través un encabezado MIME en el mensaje.

- El firewall deberá contar con la facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías
- Filtrado de contenido basado en categorías en tiempo real, integrado a la plataforma de seguridad "appliance". Sin necesidad de instalar un servidor o "appliance" o dispositivo externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido.
- Configurable directamente desde la interfaz de administración del dispositivo "appliance". Con capacidad para permitir esta protección por política de control de acceso.
- Deberá permitir diferentes perfiles de utilización de la web (permisos diferentes para categorías) dependiendo de fuente de la conexión o grupo de usuario al que pertenezca la conexión siendo establecida.
- Los mensajes entregados al usuario por parte del URL Filter (por ejemplo, en caso de que un usuario intente navegar a un sitio correspondiente a una categoría no permitida) deberán ser personalizables.
- Capacidad de filtrado de scripts en páginas web (JAVA/Active X).
- La solución de filtrado de contenido debe soportar el forzamiento de "Safe Search" o "Búsqueda Segura" independientemente de la configuración en el browser del usuario. Esta funcionalidad no permitirá que los buscadores retornen resultados considerados como controversiales. Esta funcionalidad se soportará al menos para Navegadores tales como Google, Yahoo! y Bing.
- Será posible definir cuotas de tiempo para la navegación. Dichas cuotas deben poder asignarse por cada categoría y por grupos.
- Será posible exceptuar la inspección de HTTPS por categoría.
- Sera posible configurar el equipo para que automáticamente redirija el tráfico de www.youtube.com a http://www.youtube.com/education para que se acceda únicamente a contenido categorizado por el portal como contenido educativo.
- Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS).
- La interfaz gráfica de usuario (GUI) vía Web deberá estar en español y en inglés, configurable por el usuario.
- Interfaz basada en línea de comando (CLI) para administración de la solución.
- Comunicación cifrada y autenticada con username y password, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH o TELNET).
- Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden Administrar y realizar cambios de configuración.
- El equipo ofrecerá la flexibilidad para especificar que los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, TELNET, HTTP o HTTPS.

- El equipo deberá administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional.
- Soporte de SNMP versión 2 y Soporte de SNMP versión 3.
- Soporte de SYSLOG para poder enviar bitácoras a servidores de SYSLOG remotos.
- Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall.
- Monitoreo de comportamiento del "appliance" mediante SNMP, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.
- Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión.
- La interfaz gráfica de usuario (GUI) deberá de contar con la funcionalidad de autentificarse con un TOKEN (Autentificación de segundo factor) sin necesidad de integrar un equipo adicional o solución de otro fabricante.
- La solución deberá de incluir la funcionalidad de reporteo y análisis de bitácoras la cual podrá estar incluida en el mismo appliance o en un equipo externo siempre y cuando sea del mismo fabricante y esto no limite las funcionalidades solicitadas.
- La solución de reporteo y bitácoras del Firewall deberá cumplir con las siguientes funcionalidades:
    - Sistema de Almacenamiento de bitácoras y Reportes.
    - Integrar dispositivos para que reporten actividad o bitácoras, estableciendo comunicaciones de tipo seguras con dichos dispositivos.
    - Asignar cuotas de espacio en disco por dispositivo, de modo que un solo dispositivo no consuma la totalidad del disco de la solución.
    - Contar con espacio suficiente en disco para el almacenamiento de bitácoras y reportes generados durante la vigencia del contrato.
    - Generar reportes personalizados de acuerdo a las necesidades del Instituto.
    - Genera reportes de: Utilización de la red (ancho de banda o conexiones), usuarios, direcciones IP y/o servicios con mayor consumo de recursos.
    - Genera reportes de los ataques detectados/detenidos con mayor frecuencia en la red, por fuente y/o por destino.
    - Genera reportes de las páginas y/o categorías de URL visitadas con mayor frecuencia, por fuente y/o por destino.
    - Generar la incidencia de virus detectados/removidos a nivel red por fuente y/o por destino.
    - Generar un reportes de las actividades administrativas (ingresos de administradores, cambios de configuración) realizadas.

- Personalizar los criterios bajo los cuales será obtenido el reporte, tales como origen, destinos, servicios, fechas y/o día de la semana.
- Especificar el período de tiempo específico para el cual el reporte va a ser obtenido, por períodos relativos (hoy, ayer, esta semana, semana pasada, este mes, mes pasado) o bien por períodos absolutos (de la fecha día/mes/año a la fecha día/mes/año).
- Generación de reportes calendarizados y en formatos portables tales como PDF y DOC.

- En el caso que la funcionalidad de reporteo y logs se proponga en un appliance externo, esta funcionalidad (reporteo y logs) no deberá de ser considerada en HA.

3.2.1.10 Servicio de protección de aplicaciones Web, servidores de archivos y bases de datos.

S.1.5- [Servicio de protección de aplicaciones Web (WAF), servidores de archivos y bases de datos.]	
Característica	**Descripción**
Propósito	Contar con una solución que ofrezca protección a nivel capa 7, que garantice la seguridad de aplicaciones Web y bases de datos del IFT, mediante la automatización de la seguridad Web, considerando una implementación flexible y transparente. Asegurar las bases de datos mediante el bloqueo de amenazas, inspeccionando peticiones e impidiendo que el tráfico malicioso alcance la aplicación destino garantizando la disponibilidad, confiabilidad e integridad de los servicios sustantivos.
Tipo de servicio	Requerimiento.
Área geográfica y/o Lógica de cobertura	Aplicaciones con acceso Web y bases de datos del IFT.
Vigencia	Durante la vigencia del contrato.
Horario del servicio	[7 x 24] (7 días a la semana durante las 24 del día)
Prioridad	Crítica
Periodicidad de revisión del ANS	Mensual
Indicador de Desempeño	Nivel de disponibilidad mensual (porcentaje) Total de minutos del mes (43,200) = 30 días * 24 horas * 60 min. Disponibilidad mínima aceptada (42,984) = 43,200 * 0.999 Indisponibilidad tolerada (216 minutos por mes) = 43,200 * 0.001 Indisponibilidad registrada = Minutos en que la solución está fuera de servicio durante el mes desde la hora en que se registra la caída del servicio hasta su recuperación a nivel operativo. Disponibilidad total mensual = [Disponibilidad mínima aceptada + (Indisponibilidad tolerada – indisponibilidad registrada)]/ Total de minutos del mes
Nivel de Servicio mínimo esperado	99.9 % mensual
Penalización	Conforme a lo establecido en el apartado 5.- Penalizaciones
Requerimientos Adicionales	Se debe considerar la protección contra, al menos: Reescritura de comandos entre sitios; Falsificación de solicitud entre sitios; Inyección de código SQL; Seguridad XML; Desbordamiento de buffer; Robo de datos;

Dado que un porcentaje importante de ataques exitosos a través de Internet explotan las vulnerabilidades de las aplicaciones, se requiere contar con el servicio de aseguramiento de las aplicaciones Web del IFT, como mínimo se deberá evitar la divulgación involuntaria o intencional de información confidencial o reservada y contribuir al cumplimiento con las reglas de seguridad de la información aplicables por el IFT.

La solución propuesta para este servicio deberá tener la capacidad para adaptar las políticas de seguridad para cualquier aplicación, incluidas aquellas que usan JavaScript del lado del cliente; contar con un motor de aprendizaje que determine de forma automática el comportamiento de una aplicación y genere recomendaciones legibles para el administrador del proyecto que refuercen las políticas de seguridad y permitan un comportamiento aceptable de la aplicación.

La instalación inicial deberá contar con una base de firmas existentes para analizar ataques conocidos.

La solución propuesta deberá proteger los servidores Web sin disminuir el rendimiento ni los tiempos de respuesta de las aplicaciones, se debe considerar el bloqueo de ataques conocidos y de día cero a nivel de aplicación, de manera adicional debe considerar la protección mediante la exploración de firmas actualizadas de forma automática.

La tecnología para la seguridad de aplicaciones Web, servidores de archivos y bases de datos deberá incluir y operar al menos con las siguientes características:

a) Protección para aplicaciones WEB

El modelo positivo de seguridad deberá definir lo que está permitido y bloquear todo lo demás. Deberá incluir direcciones URL, directorios, cookies, campos, parámetros (identificando además el formato y tipo de estos), métodos HTTP.

Para facilitar la configuración del modelo positivo de seguridad, el dispositivo deberá aprender automáticamente la estructura y los elementos de la aplicación de manera constante y sin intervención humana.

La solución deberá contar con un modo aprendizaje para rastrear cambios continuos en las aplicaciones Web, deberá reconocer cambios en la aplicación y simultáneamente protegerlas. Deberá contar con las siguientes características.

- Deberá aprender los valores aceptables para los campos de ingreso de datos con base en el registro de la actividad.
- Los valores aprendidos podrán ser utilizados como la configuración inicial sobre la que se revisarán los datos ingresados en el modelo positivo de seguridad.
- El modo aprendizaje, deberá aprender la estructura y elementos de la aplicación (directorios, url's, parámetros, cookies) y el comportamiento esperado del usuario (longitud del valor esperado, caracteres aceptados, si el parámetro es de sólo lectura o editable por el usuario) y esta información deberá estar disponible para automatizar la configuración del modelo positivo de seguridad.

La configuración aprendida deberá ser accesible y modificable para el administrador del dispositivo.

La solución deberá correlacionar múltiples eventos de seguridad para distinguir tráfico deseado del tráfico inadecuado.

La solución deberá permitir la modificación de reglas de seguridad. Los administradores deberán poder definir reglas para el modelo de seguridad positivo o negativo y deberán crear reglas de correlación con múltiples criterios.

Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación Web. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:

- Estado de autenticación de la sesión Web.
- Por el URL de autenticación y el resultado del intento de autenticación.
- Por URL, a través del prefijo, ruta o host.
- Por la existencia o contenido de cualquier Header HTTP.
- Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier customización por expresiones regulares), ya sea en el HTTP Request o el Response por parte del servidor Web.
- Tipo de archivo siendo transmitido en cualquier sentido.
- Host o dominio accedido.
- Métodos HTTP usados.
- Número de ocurrencias en intervalos de tiempo definidos.
- La existencia o contenido de cualquier Parámetro Web.
- Por el protocolo usado, HTTP o HTTPS.
- IPs de origen y destino.
- Por la existencia o contenido de Cookies o el identificador de Sesión.
- Response Code y Headers en el Response HTTP por parte del servidor Web.
- Hora del Dia.
- Por usuario firmado en el aplicativo Web.
- User-Agent.
- Referer-URL.
- Tiempo de respuesta o tamaño de la respuesta HTTP.

La solución deberá contar con el modo de instalación proxy transparente,

Deberá cubrir todas las vulnerabilidades expresadas en el OWASP Top Ten 2013 más reciente al momento de la adjudicación del proyecto y actualizarse durante la vigencia del contrato.

La solución deberá cumplir con todos los criterios de evaluación del WAFEC definidos por el Web Application Security Consortium.

La solución deberá soportar la integración con seguridad para base de datos del mismo fabricante, para ofrecer seguridad de extremo a extremo; desde internet hasta la base de datos sin ningún cambio en la aplicación Web. La seguridad integrada de la base de datos deberá proteger contra ataques conocidos a las bases de datos, deberá también tener capacidad de monitorear y controlar la actividad de la base de datos

La solución deberá proporcionar el bloqueo de direcciones IP, sesiones TCP o usuarios de la aplicación Web.

La solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones Web SSL y HTTPS.

- La solución deberá tener la capacidad de recibir y utilizar los certificados y pares de llaves público/privadas para los servidores Web protegidos.
- La solución deberá desencriptar el tráfico SSL, de las aplicaciones Web, entre el cliente y el servidor y re-encriptarlo antes de su reenvío.
- En los modos puente (bridge) o sniffer, la solución deberá poder desencriptar el tráfico SSL para inspección, sin terminar o cambiar la conexión HTTPS.
- La solución deberá tener la capacidad de proteger aplicaciones Web que incluyan el contenido de servicios Web (xml). La protección XML deberá contar con mecanismos automatizados de aprendizaje, similares a los de la protección de aplicaciones Web.

La solución deberá contar con funcionalidades que permitan:

- Rastrear e identificar las fuentes de los ataques originadas desde proxies anónimos, direcciones ip maliciosas, botnets y sitios de phishing.
- Actualizar las fuentes de ataque para identificar y bloquear el tráfico malicioso.
- Ajustar dinámicamente las políticas de seguridad con base en la identificación de las fuentes de ataque o de las fuentes que denoten actividad sospechosa.
- Bloquear solicitudes de acceso basado en la reputación de la fuente del tráfico, como direcciones IP conocidas por su comportamiento malicioso por Botnet, DDoS, Phishing o redes de Anonimización (TOR y Proxies Anónimos).
- Bloquear solicitudes de acceso basado en el país de origen de la conexión.
- Realice un análisis automático de distribución de alertas en relación al país de origen, con opción a representar la información a través de un mapa mundial.
- Detallar y analizar los eventos de seguridad ocurridos, orígenes y método del ataque, dirección IP y localización geográfica del ataque.

La solución deberá:

- Inspeccionar y monitorear todos los datos http y la aplicación, incluyendo, los encabezados http, campos de formularios, y el cuerpo http.
- Inspeccionar las peticiones y respuestas http.

- Tener la habilidad de decodificar datos a su mínima expresión a partir de diferentes sistemas de encoding Web y validarla.
- Validar todos los tipos de datos ingresados, incluyento URLs, formularios, cookies, cadenas de queries, campos y parámetros ocultos, métodos http, elementos XML y acciones SOAP.

b) Protección para servidores de Archivos

La solución deberá auditar, en tiempo real, todos los accesos a archivos ya sea a través de la red o dispositivos NAS. Dicha auditoría deberá de almacenarse localmente en la solución y alternativamente poder ser enviada por Syslog a otro dispositivo.

La solución deberá proporcionar mecanismos de control de acceso y prevención en tiempo real para todos los accesos a archivos ya sea a través de la red o dispositivos NAS.

La solución debe de poder auditar actividad local realizada por administradores directamente sobre los archivos dentro de los servidores de archivos.

La solución deberá tener la capacidad de integrarse con sistemas de Directorio Activo y analizar tanto la propiedad (ownership) como los privilegios de acceso (lectura, escritura, borrado) para cada archivo en todos los recursos compartidos de archivos de red y dispositivos NAS. Esto con el fin de identificar privilegios excesivos y privilegios en desuso.

La solución deberá de poder revocar permisos a usuarios y archivos específicos dentro de servidores de archivos y Directorio Activo.

La solución deberá de identificar archivos compartidos que se encuentran en desuso y que ocupan espacio innecesariamente.

Capacidad de integrar los resultados de clasificación de datos y archivos producidos por herramientas de terceros.

Capacidad de alertar cuando los privilegios de acceso a los archivos sean cambiados, otorgados o eliminados.

La información que capturará la herramienta como parte de su auditoría deberá ser al menos: usuario que realiza la acción, tipo de operación, ruta completa al archivo, nombre del archivo, dirección IP de origen y opcionalmente cualquier dato contenido dentro del sistema de Directorio como puede ser Departamento o unidad organizacional a la que pertenece el usuario, nombre completo, nombre del equipo, rol o grupo del usuario.

En base a la actividad y patrones de acceso a los archivos, la herramienta deberá de identificar a quién pertenece y/o está a cargo de la información.

Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad del sistema de archivos en red. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:

- Ubicación de archivo por share, directorio, nombre de archivo.
- Clasificación del tipo de dato contenido en el archivo.
- Código de error en caso de fallar la operación.
- IP's de origen y destino.
- Por la extensión del archivo.
- Operación sobre el archivo (Close, Read, Create, Delete, Modify, Copy, Rename, Permission/Owner change).
- Hora del día.
- Ocurrencias en una fecha específica o lapso de tiempo.
- Por usuario firmado en el aplicativo Web.
- Si es un otorgamiento de permisos a un determinado usuario/grupo/departamento.
- Por el departamento o grupo o tipo o dominio del usuario.

c) Protección para bases de datos

La solución deberá contar con tecnología de auto-aprendizaje con mínima intervención humana, el proceso deberá ser constante y deberá aprender estructura de bases de datos, incluyendo esquemas, objetos, tablas, sistemas, aplicaciones, campos, directorios, así como el comportamiento de cada usuario; todo esto para el establecimiento de una línea base de monitoreo y seguridad. El modo aprendizaje podrá ser activado y desactivado manualmente para extender el tiempo de reconocimiento de los patrones de conducta.

La solución deberá proporcionar protección por medio de bloqueos y alertas contra violaciones de seguridad por ataques conocidos, actividad sospechosa o cualquier actividad específica a definir.

La solución deberá generar reportes y tendencias en tiempo real, así como permitir la modificación de los mismos.

La solución deberá contar con facilidades o herramientas analíticas para la conducción de análisis forense cuando sea reportado algún incidente.

La solución no deberá requerir el instalar agentes de software en los servidores a monitorear, pero deberá tener la opción en caso de ser necesario.

La solución deberá funcionar independiente a la activación de la auditoría nativa de la base de datos.

La solución deberá ser transparente para la base de datos y/o las aplicaciones que accedan a ella, es decir, no requerirá que se realicen cambios en la programación, configuración u operación (triggers, stored procedures, etc.) de ninguna de ellas.

El repositorio para el registro de la actividad en el appliance, no deberá ser accesible por ningún otro mecanismo que no sea la interacción mediante la GUI (interfaz gráfica) proporcionada por el fabricante o por medios administrativos debidamente asegurados.

La solución deberá ser capaz de descubrir servidores de bases de datos y realizar análisis de vulnerabilidades sobre el software de manejo de la base de datos, el protocolo de comunicación, y configuración de seguridad, sin importar el sistema operativo sobre el que se encuentren instaladas.

La solución deberá realizar una evaluación exhaustiva de los riesgos de la infraestructura objetivo a diferentes niveles/capas de la infraestructura de base de datos incluyendo:

- Cuestiones de configuración de la base de datos tales como nivel de parcheo, configuración de las cuentas de usuario, evaluación de la fortaleza de las contraseñas, vigencia de contraseñas.
- Cuestiones de configuración de la plataforma, incluyendo configuración del sistema operativo de los servidores que soportan el software de base de datos.

La solución deberá de poder realizar descubrimientos automatizados en la red para identificar nuevas bases de datos siendo habilitadas, ya sea a nivel de servidor o puertos habilitados en servidores conocidos.

La solución deberá tener la capacidad de analizar y clasificar los tipos de dato dentro de las Bases de Datos de acuerdo a las políticas de negocio. Las definiciones de tipo de dato deberán poder crearse de manera flexible y granular.

La solución deberá proveer un servicio de protección del software de base de datos mediante la aplicación de parches virtuales que impidan atacar las vulnerabilidades encontradas en dicho software, independientemente de la liberación de la corrección o actualización del fabricante.

La solución deberá tener la capacidad de mapear los privilegios de acceso y transaccionales (instrucciones DML, DDL de DB) para cada objeto/tabla dentro de los manejadores de DB. Esto con el fin de identificar privilegios excesivos, de sobra o en desuso.

La solución deberá apoyar en los esfuerzos de análisis de vulnerabilidades, configuración de seguridad, comportamiento/performance de aplicativos y control de cambios.

La solución deberá monitorear toda la actividad de las bases de datos, y deberá almacenar los comandos SQL tal cual fueron escritos por el usuario o aplicación, incluyendo comandos DDL, DML y DCL.

La solución deberá monitorear e interactuar con la actividad de la base de datos sin importar el punto de entrada, ya sean conexiones directas, servidores de aplicaciones, acceso directo a la base de datos, ligas, stored procedures, entre otros.

La solución deberá hacer análisis y auditoría sobre todo el tráfico en tiempo real, sin importar el volumen de tráfico, sin necesidad de crear un archivo log primero para su análisis posterior.

La solución deberá tener capacidad de monitorear el tráfico encriptado hacia las Bases de Datos.

La solución deberá proveer detalles sobre alertas ya sean falsos positivos o negativos y deberá tener la facilidad de cambiar una política desde la alerta.

La solución deberá manejar reglas y políticas tan amplias o granulares como se requieran y deberán poder ser construidas automáticamente o manualmente y deberán poder ser actualizadas, igualmente, de forma manual o automática.

Las políticas granulares para control de acceso o generación de alertas deberán de contar con los siguientes criterios para la validación de la actividad en la aplicación de Base de Datos. Los criterios deberán de poder usarse en cualquier número y cualquier combinación:

- Número de registros a regresar por la consulta (SQL Query).
- Número de registros afectados.
- Tipo de datos accesado (financiero, recursos humanos, inventarios, o cualquier definición personalizada).
- Acceso a datos marcados como sensibles.
- Base de Datos, Schema, Instancia, Tabla y Columna accesada.
- Estado de autenticación de la sesión.
- Usuario y/o Grupo de Usuarios de Base de Datos conectado.
- Usuario conectado en la capa aplicativa, a diferencia del usuario conectado a la DB.
- Por búsqueda en diccionarios de datos (tarjetas de crédito, datos privados, o cualquier personalización por expresiones regulares).
- Logins, Logouts, Queries.
- IP's de origen y destino.
- Nombre de Host origen, Usuario firmado en el Host origen.
- Aplicación usada para la conexión a la base de datos.
- Tiempo de respuesta/procesamiento del query.
- Errores en el manejador de SQL.
- Número de ocurrencias en intervalos de tiempo definidos.
- Por operaciones básicas (Select, Insert, Update, Delete).
- Por operaciones privilegiadas (Create, Alter, Drop, Grant, Revoke, Truncate, Export).
- Por Stored Procedure o Function utilizada.
- Hora del día.

La solución deberá identificar individualmente a los usuarios finales que realicen actividades mediante aplicaciones, aún si utilizan mecanismos comunes de comunicación entre la aplicación y la base de datos, ésta actividad no deberá implicar la modificación de la aplicación y/o de la base de datos.

La solución debe posibilitar los análisis en tiempo real e histórico bajo demanda, es decir, sin necesidad de pasar por un proceso batch previo.

La solución deberá asociar y correlacionar eventos que individualmente podrían no constituir un riesgo pero que en conjunto son indicativos de una potencial violación de seguridad.

La solución deberá proteger contra ataques SQL y no-SQL (como buffer overflow)

La solución deberá correlacionar actividad en base de datos con actividad de aplicaciones Web para entender detalladamente como los usuarios están accesando datos privilegiados sin necesidad de alterar la aplicación Web.

La solución deberá contar con un mecanismo de actualización de la inteligencia interna de seguridad, que incluye las pruebas de las evaluaciones de vulnerabilidad, las firmas contra ataques, la granularidad de las políticas de seguridad y defensas contra comportamientos considerados de emergencia para potenciales violaciones de la información que incluyan, enunciativa mas no limitativamente:

- Altos volúmenes de acceso a datos sensibles más allá de lo habitual.
- Acceso a datos inusual para cierta hora del día.
- Acceso a datos desde una ubicación (física) desconocida.
- Acceso a datos utilizando aplicaciones/herramientas no autorizadas.

La solución debe manejar una auditoría sobre sí misma, manteniendo un control de cambios sobre las políticas autorizadas y configuraciones realizadas.

La solución debe tener facilidades de archivado de la información histórica y de auditoría, con flexibilidad de opciones de protocolo o medio (como SAN o por medio de FTP, HTTP, NFS, SCP)

La solución deberá tener la capacidad de exportar datos y eventos, tales como alertas, eventos de sistema y base de datos, información de seguridad/administración, entre otras, hacia otras herramientas de administración por medio de protocolos SNMP y Syslog.

La solución deberá analizar los eventos generados desde diferentes bases de datos. El análisis deberá contemplar los siguientes criterios:

- Deberá mostrar el número de eventos ocurridos, el número de usuarios sospechosos y/o los sistemas comprometidos.
- Deberá contar con un sistema de correlación basado en la dirección de los ataques. Deberá determinar si los ataques provienen desde dentro de la organización hacia afuera de la misma o viceversa.
- Deberá realizar una correlación automática y en tiempo real de eventos, vulnerabilidades y bases de datos.
- Deberá ejecutar una correlación que permita identificar usuarios de aplicación asociados con consultas –y determinadas actividades– en bases de datos específicas sin necesidad de alterar aplicaciones o instalar API's.
- Deberá correlacionar eventos como número de errores inusuales de sentencias de SQL ó al momento de hacer login a las bases de datos.

La solución debe permitir el manejo de alarmas y notificaciones –en tiempo real– para los eventos de correlación mencionados anteriormente.

La solución debe tener la capacidad de monitorear aplicaciones Web en la misma solución, ofreciendo una visibilidad, seguridad y control desde el usuario Web hasta la base de datos.

La solución deberá contar con un servicio de investigación sobre vulnerabilidades y amenazas informáticas y tener la posibilidad de documentar el descubrimiento de las mismas.

La solución deberá soportar y aplicar simultáneamente un modelo de seguridad positivo y negativo. El modelo negativo de seguridad define explícitamente las firmas de ataques conocidos, por lo que deberá además cumplir con las siguientes especificaciones:

- Deberá bloquear las transacciones que tengan contenido que coincida con firmas de ataque conocidos.
- Deberá incluir una lista pre configurada y detallada de las firmas de ataque.
- Deberá permitir la modificación o adición de firmas por el administrador.
- Deberá permitir la actualización automática de la base de datos de firmas, asegurando una completa protección contra las amenazas de aplicación más recientes.
- Deberá detectar ataques conocidos en múltiples niveles, incluyendo, la red, sistemas operativos, software del servidor Web y ataques a nivel de aplicación.

d) Plataforma

Los diferentes componentes de seguridad de los aplicativos Web, bases de datos y sistemas de archivos distribuidos en red deberán de administrarse a través de una consola centralizada.

Los equipos que realicen el monitoreo deben de tener la capacidad de ejecutar simultáneamente los componentes de seguridad de los aplicativos Web, bases de datos y sistemas de archivos distribuidos en red dentro de la misma solución.

La consola centralizada deberá de ser el único punto de contacto, administración, control, análisis y reporteo para las diferentes soluciones e infraestructura de seguridad en aplicaciones Web, bases de datos y sistemas de archivo de red.

La solución deberá soportar ser desplegada o implementada en línea y deberá permitir:

- En el modo monitoreo el administrador podrá visualizar alertas, ataques, errores de servidor y otra actividad no autorizada.
- En el modo de cumplimiento de políticas, la solución deberá bloquear ataques proactivamente.
- Respecto de algún ataque o alguna otra actividad no autorizada, la solución deberá ser capaz de tomar las acciones adecuadas, tales como: terminar las solicitudes y respuestas, bloquear la sesión TCP, bloquear el usuario de la aplicación, o bloquear la dirección IP.
- Respecto de ataques particularmente destructivos, la solución deberá ser capaz de bloquear la dirección IP por un periodo de tiempo configurable.

- En modo analizador de paquetes o sniffer, la solución deberá ser capaz de enviar un paquete TCP RST a ambos extremos de la conexión. Alternativamente, si así se configura, la solución podrá reportar el comportamiento anómalo pero no tomar acción alguna.

El proveedor adjudicado deberá de considerar que la solución deberá soportar el análisis de los aplicativos web, bases de datos y servidores de archivos como sigue:

- 6 servidores de aplicación web.
- 12 servidores de base de datos.
- 1 servidor de SharePoint.
- 1 servidor de archivos.

La solución deberá ser desplegada dentro de ambientes virtuales VMWare (appliance virtual) en servidores físicos en caso de ser necesario.

3.2.1.11 Servicios de protección para correo electrónico.

S.1.6 - [Servicio de protección para correo electrónico.]	
Característica	**Descripción**
Propósito	Proporcionar un servicio de filtrado de correo electrónico, evitando el correo no deseado (spam) y previniendo descargas de archivos maliciosos y/o infectados en tráfico válido de mensajería.
Tipo de servicio	Requerimiento.
Área geográfica y/o Lógica de cobertura	Red de datos del Instituto y Correo electrónico institucional.
Vigencia	Durante la vigencia del contrato.
Horario del servicio	[7 x 24] (7 días a la semana durante las 24 del día)
Prioridad	Crítica
Periodicidad de revisión del ANS	Mensual
Indicador de Desempeño	Nivel de disponibilidad mensual (porcentaje) Total de minutos del mes (43,200) = 30 días * 24 horas * 60 min. Disponibilidad mínima aceptada (42,984) = 43,200 * 0.995 Indisponibilidad tolerada (216 minutos por mes) = 43,200 * 0.005 Indisponibilidad registrada = Minutos en que la solución está fuera de servicio durante el mes desde la hora en que se registra la caída del servicio hasta su recuperación a nivel operativo. Disponibilidad total mensual = [Disponibilidad mínima aceptada + (Indisponibilidad tolerada – indisponibilidad registrada)]/ Total de minutos del mes
Nivel de Servicio mínimo esperado	99.5 % mensual
Penalización	Conforme a lo establecido en el apartado 5.- Penalizaciones

Solución de detección y protección de amenazas de nueva generación para tráfico de correo electrónico que se deberá colocar en el flujo de entrada de la solución de correo del Instituto con las características y funcionalidades que se detallan a continuación:

- Capacidad para soportar al menos 1200 buzones de correo electrónico.
- Deberá soportar la redirección de correo electrónico hospedado en la nube (Gmail).

- Debe soportar la plataforma de Microsoft Exchange server 2010 o posterior.
- La solución deberá proteger contra ataques spear-phising en correos electrónicos.
- Solución basada en la nube sin necesidad de instalar algún tipo de dispositivo (hardware) o software.
- La herramienta solicitada deberá poder interactuar con la solución de detección antimalware basado en Web para detener ataques combinados a través de múltiples vectores de amenazas.
- Deberá poder analizar correos electrónicos en busca de amenazas como son exploits día cero, ataques escondidos en archivos comprimidos ZIP/RAR/TNEF y ligas (URL) maliciosas.
- La herramienta deberá proveer análisis para todo tipo de archivos adjuntos: EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 entre otros.
- La solución en modo protección deberá poner en cuarentena los correos maliciosos con opción a notificar a los usuarios.
- Contar con un motor de detección no basado en firmas para poder detener ataques avanzados explotando vulnerabilidades no conocidas en el sistema operativo, navegador y aplicativos así como código malicioso embebido en archivos y contenido multimedia.
- Contar con un portal para visualizar en tiempo real las alertas y generar reportes.
- La solución deberá proporcionar información forense que pueda ser usada para proteger la red local. Como mínimo deberá contener la siguiente información:
    - Fecha y hora del ataque
    - Remitente
    - Correo destino
    - Hash MD5 o SHA-1 de los binarios maliciosos
    - Tipo de archivo malicioso detectado
    - Captura de tráfico en formato PCAP, en caso de generar tráfico de red
    - Entrega de pieza de código malicioso en archivo comprimido
    - Deberá poder entregar los encabezados del correo en formato plano (raw) para poder analizar toda la información real de los mismos.
    - Capacidades nocivas de la amenaza: capacidades de robo de información, comportamiento malicioso, cambios al sistema operativo
- La herramienta debe ser capaz de ejecutar todo el código sospechoso, URL's y diversos tipos de archivos en un entorno virtual propietario de inspección dentro del mismo dispositivo
- La solución deberá poder revisar correo cifrado mediante el protocolo TLS.
- En el entorno virtual de análisis, el malware deberá ser inspeccionado y examinado en diversas máquinas virtuales correspondientes a varios sistemas operativos, aplicaciones, navegadores y complemento de navegadores.

3.2.1.12 Servicio de filtrado de contenido Web.

S.1.7 - [Servicio de filtrado de contenido Web.]	
Característica	**Descripción**
Propósito	Proporcionar un servicio de filtrado de contenido Web, evitando que se haga mal uso de los recursos de acceso a Internet del Instituto y previniendo descargas de archivos maliciosos y/o infectados en tráfico válido http/https.
Tipo de servicio	Requerimiento.
Área geográfica y/o Lógica de cobertura	Red de datos del Instituto.
Vigencia	Durante la vigencia del contrato.
Horario del servicio	[7 x 24] (7 días a la semana durante las 24 del día)
Prioridad	Crítica
Periodicidad de revisión del ANS	Mensual
Indicador de Desempeño	Nivel de disponibilidad mensual (porcentaje) Total de minutos del mes (43,200) = 30 días * 24 horas * 60 min. Disponibilidad mínima aceptada (42,984) = 43,200 * 0.995 Indisponibilidad tolerada (216 minutos por mes) = 43,200 * 0.005 Indisponibilidad registrada = Minutos en que la solución está fuera de servicio durante el mes desde la hora en que se registra la caída del servicio hasta su recuperación a nivel operativo. Disponibilidad total mensual = [Disponibilidad mínima aceptada + (Indisponibilidad tolerada – indisponibilidad registrada)]/ Total de minutos del mes
Nivel de Servicio mínimo esperado	99.5 % mensual
Penalización	Conforme a lo establecido en el apartado 5.- Penalizaciones

El Proveedor Adjudicado deberá ofrecer una solución de propósito específico para el control sobre el tráfico de Internet, que cumpla con al menos las siguientes características:

- Soportar el filtrado de hasta 2000 usuarios concurrentes.
- Permitir el control de al menos 85 categorías de sitios Web y al menos 15 categorías de sitios Web 2.0
- Deberá permitir la personalización de mensajes hacia los usuarios, para notificar cuando no tengan autorización de acceder a un sitio determinado.
- Permitir el bloqueo de sitios de spyware
- Almacenamiento en caché de contenido y optimización del tráfico
- Gestión de ancho de banda
- Autenticación fuerte de usuarios
- Inspección profunda de contenido
- Inspección y validación de tráfico SSL
- Deberá contar con un sistema operativo propietario
- Deberá poder integrarse a un sistema de gestión centralizado.
- Deberá permitir establecer horarios de acceso o restricción a determinados sitios o categorías.

- Deberá permitir contar con un Dashboard en tiempo real a través del cual se puedan identificar los eventos de seguridad, el estatus actual y las tendencias.
- La solución deberá contar con una consola de reporteo que permita el control de acceso basado en roles.
- La solución deberá poder dar reportes, al menos:
  - Spyware
  - Uso de Video
  - Uso de aplicaciones Web
  - Perfiles de tráfico
  - Autenticación de usuarios
  - Categorías de filtrado

3.2.1.13 Servicio de monitoreo proactivo de seguridad en Internet.

S.1.8 - [Servicio de monitoreo proactivo de seguridad en Internet]			
Fase	Nombre	Descripción	Periodicidad
Inicial	E.3.2.1.16 Documento SOW	Documento que describe el alcance de los servicios, así como las fuentes de información que formarán parte del mismo.	Único al inicio del proyecto
Operación	E.3.2.1.17 Documento de alerta temprana.	Documento que contiene la información necesaria para que el Proveedor Adjudicado tome las medidas necesarias para minimizar el impacto de la amenaza detectada y debe contener al menos las siguientes secciones: • Descripción de la amenaza • Fuente de donde se obtuvo la información. • Descripción si es una amenaza confirmada o solo un indicio. • Descripción del actor de la amenaza. • Descripción de acciones que debe realizar el Proveedor Adjudicado para minimizar el impacto de la amenaza.	Por cada amenaza detectada, no mayor a 24 horas de la detección o publicación.

Servicio activo y proactivo que deberá usar técnicas de OSINT (Open Source Intelligence por sus siglas en Inglés) para poder identificar amenazas o indicios de amenazas que permitan al Instituto en conjunto con el Proveedor Adjudicado tomar decisiones proactivas para la protección de los servicios del Instituto.

El servicio deberá ser ofrecido desde el centro de operaciones del Proveedor Adjudicado en un horario de 7 x 24 x 365 (7 días a la semana durante las 24 del día, los 365 días de cada año) y debe contemplar al menos las siguientes actividades:

- Monitoreo y seguimiento de cuentas de redes sociales relacionada a grupos hacktivistas nacionales y extranjeros que puedan representar una amenaza para el Instituto. El Instituto acordará con el Proveedor Adjudicado la lista de cuentas a monitorear y su relevancia para el Instituto. Las redes sociales que al menos deberán monitorearse por parte del Proveedor Adjudicado son:
  - Twitter
  - Facebook

- Google+
- Instagram

- Monitoreo de canales de IRC dedicados donde se perpetren y difundan campañas de ataques informáticos.
- Monitoreo de foros y comunidades donde se perpetren y difundan campañas de ataques informáticos. Estos foros deben incluir aquellos que vivan en el ecosistemas de la red Onion/Tor.
- Monitoreo de fuentes abiertas de noticias tanto nacionales o extranjeras donde se pudieran general indicios de amenazas.

Cuando el monitoreo obtenga información relevante se tiene que iniciar una investigación que responda a las siguientes preguntas.

1. ¿Es una amenaza confirmada o solo un indicio?
2. ¿Quién es el actor de la amenaza?
3. ¿Cuáles son las fechas de ataque?
4. ¿Cuál es la infraestructura o activos que se podrían ver afectados por el ataque?

Esta información deberá verse reflejada en el entregable E.3.2.1.17 Documento de alerta temprana que deberá entregarse al Instituto por parte del Proveedor Adjudicado.

La naturaleza del servicio es detectar de manera proactiva algún ataque, sin embargo si durante el monitoreo se detecta que un ataque ya sucedió y tuvo un impacto en la organización también deberá emitirse el mismo informe.

3.2.1.14 Servicio de enrutamiento de enlace de Internet

S.1.9 - [Servicio de enrutamiento de enlace de Internet]	
Característica	**Descripción**
Propósito	Proporcionar un servicio para el enrutamiento del enlace de Internet que recibe el enlace que entrega la CFE al IFT.
Tipo de servicio	Requerimiento.
Área geográfica y/o Lógica de cobertura	Red de datos del Instituto.
Vigencia	Durante la vigencia del contrato.
Horario del servicio	[7 x 24] (7 días a la semana durante las 24 del día)
Prioridad	Crítica
Periodicidad de revisión del ANS	Mensual
Indicador de Desempeño	Nivel de disponibilidad mensual (porcentaje) Total de minutos del mes (43,200) = 30 días * 24 horas * 60 min. Disponibilidad mínima aceptada (42,984) = 43,200 * 0.999 Indisponibilidad tolerada (216 minutos por mes) = 43,200 * 0.001 Indisponibilidad registrada = Minutos en que la solución está fuera de servicio durante el mes desde la hora en que se registra la caída del servicio hasta su recuperación a nivel operativo. Disponibilidad total mensual = [Disponibilidad mínima aceptada + (Indisponibilidad tolerada – indisponibilidad registrada)]/ Total de minutos del mes
Nivel de Servicio mínimo esperado	99.9 % mensual

S.1.9 - [Servicio de enrutamiento de enlace de Internet]	
Característica	**Descripción**
Penalización	Conforme a lo establecido en el apartado 5.- Penalizaciones

El proveedor adjudicado deberá proveer un servicio de Enrutamiento del Enlace de Internet, para lo cual deberá implementar un equipo con hasta dos slots de servicios de ruteo con las siguientes características:

- Desempeño de al menos 75 Mbps.
- Un ruteador con arquitectura modular
- Soporte a al menos 3 interfaces Giga Ethernet de Cobre
- Al menos uno de los puertos deberá soportar conectividad basada en SFP en vez de RJ-45
- Que cuente al menos con 256MB de Flash
- Soporte al menos 1 slot de servicio.
- Deberá soportar un máximo de memora externa de 8 GB
- Deberá soportar 512MB en DRAM
- Deberá contar con procesador multicore de alto desempeño
- Deberá soportar los siguientes protocolos: IPv4, IPv6, Static Routes, Open Shortest Path First (OSPF), Enhanced IGRP (EIGRP), Border Gateway Protocol (BGP), BGP Router Reflector, Intermediate System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol (IGMPv3) Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM), Distance Vector Multicast Routing Protocol (DVMRP), IPSec, Generic Routing Encapsulation (GRE), Bi-Directional Forwarding Detection (BVD), IPv4-to-IPv6 Multicast, MPLS, L2TPv3, 802.1ag, 802.3ah, L2 and L3 VPN.
- Deberá contar con la capacidad de integración de servicios de voz, datos, video, movilidad, y servicios de datos.

3.2.2 Componente 2: Servicio de administración y entrega

El Proveedor Adjudicado deberá contar con un Centro de Operación de Seguridad que proporcione las herramientas de software o hardware necesarias para realizar actividades de entrega, seguimiento y operación de los Servicios Administrados que conforman el Componente 1: Servicios de Seguridad Administrada.

3.2.2.1 Centro de Operaciones de Seguridad (SOC)

El Proveedor Adjudicado deberá proporcionar el servicio de administración y monitoreo de eventos de seguridad desde su Centro de Operaciones de Seguridad que deberá estar formalmente establecido conforme a estándares y mejores prácticas a fin de garantizar los acuerdos de nivel de definidos en el proyecto.

El SOC será el responsable de responder ante amenazas en lo que respecta a la solución de seguridad integrada para el IFT, por lo que debe cumplir, como mínimo, con las siguientes especificaciones:

- Contar con por lo menos, 10 años de experiencia en la operación de un SOC a la fecha de inicio de los servicios objeto de este proyecto.

- Estar instalado en territorio mexicano y en las instalaciones del Proveedor Adjudicado.
- Contar con un SOC redundante, que en caso de que se presente algún evento donde le impidiera continuar con la operación, este le permita dar continuidad al servicio. De igual forma, este deberá encontrarse en territorio mexicano y a una distancia mínima de 50 km del SOC principal.
- El monitoreo, soporte técnico y administración de la seguridad perimetral deberá considerar un nivel de servicio de 7 x 24 (7 días a la semana durante las 24 del día). El soporte técnico se llevará a cabo de manera remota siempre y cuando se cumplan los niveles de servicio establecidos. En caso necesario, el Proveedor Adjudicado colocará especialistas en sitio para atender requerimientos específicos relacionados con amenazas a la seguridad del IFT bajo el mismo nivel de servicio.
- El SOC deberá contar con la certificación ISO/IEC 27001:2005 con una antigüedad de al menos 3 años para sus procesos de Administración de cambios y Administración de incidentes de seguridad. El monitoreo deberá vigilar:
    - La disponibilidad de la infraestructura administrada propiedad del Proveedor Adjudicado.
    - La disponibilidad de la infraestructura administrada propiedad del IFT.
    - Los parámetros de operación de los activos involucrados para que se mantengan bajo condiciones normales. Como mínimo deberá considerar la utilización de los recursos de red, CPU, memoria, disco, desempeño, entre otros.
    - Las bitácoras de los diferentes Componentes Habilitadores y de la infraestructura administrada para proveer los servicios.
- El SOC deberá de tener las alianzas y/o fuentes de información de inteligencia de seguridad para tener acceso a la información relativa a nuevas y viejas amenazas, el comportamiento de las amenazas y su remediación; estás funcionalidades deberán estar inmersas en el mecanismo de identificación y detección de amenazas y deberá mostrar las principales amenazas en el Portal de Servicio a el IFT.
- Para la prestación de los servicios del SOC se deberán utilizar mecanismos de seguridad para garantizar la confidencialidad de la información del IFT con los siguientes requerimientos:
    - La comunicación entre los dispositivos y el SOC deberá transmitirse cifrada. El Proveedor Adjudicado deberá manifestar el tipo de cifrado que utiliza. Como mínimo deberá considerarse IPSEC y/o SSL, en todo momento el Proveedor Adjudicado deberá aplicar las acciones correctivas necesarias para atender vulnerabilidades relacionadas con el servicio en cualquiera de sus componentes, sean físicos o lógicos.

- Todas las acciones que realicen los operadores deberán de quedar registradas en un subsistema de auditoría, al cual tendrá acceso el IFT con privilegios de "sólo lectura" y el Proveedor Adjudicado deberá asegurar la protección de los registros.
- El Proveedor Adjudicado deberá realizar el análisis de vulnerabilidades al menos cada 90 días, al equipamiento administrado y a los servidores considerados en el alcance de los servicios de seguridad administrada y las alertas deberán ser notificadas al IFT. En caso necesario, el IFT podrá solicitar la ejecución de estos análisis con una frecuencia distinta.

Procesos mínimos con los que debe operar el SOC.

El SOC deberá contar con procesos documentados y operando, y deberán ser al menos:

- Proceso de atención a clientes.
- Proceso de aprovisionamiento inicial.
- Proceso de afinación continúa de los servicios prestados por el SOC.
- Proceso de control de cambios.
- Proceso de respuesta a incidentes.
- Proceso para notificación de incidentes de seguridad.
- Proceso de incidentes mayores.

3.2.2.2 Centro de Monitoreo del SOC

El Proveedor Adjudicado deberá contar con un centro de monitoreo independiente con las siguientes características mínimas:

- El centro de monitoreo deberá ser exclusivo para el SOC.
- Deberá alojar únicamente al personal del SOC.
- Acceso mediante controles de biométricos o automatizados.
- Consolas de monitoreo para visualizar los eventos.
- Herramientas de monitoreo en tiempo real.
- Sistema de Administración de solicitudes de servicio comercial (No Sofware Libre, ni Open Source) (tickets) ITILv3 Compliance. El Proveedor Adjudicado deberá integrar en su propuesta la información que demuestre la existencia y operación de una metodología de operación del SOC, para lo cual deberá incorporar la documentación que describa la estructura operativa de la organización del SOC evidenciado que cuenta como mínimo con las siguientes funciones:

- Operaciones, deberá contar con personal de operación para cubrir el nivel de servicio 7 x 24 (7 días a la semana durante las 24 del día).
- Pruebas, deberá contar con personal encargado de atención a pruebas de penetración o análisis de vulnerabilidades y fortalecimiento (hardening) de soluciones o plataformas.
- Administración de incidentes.
- Soporte técnico

3.2.2.3 Centro de Datos del SOC

El Proveedor Adjudicado deberá alojar las soluciones de su Centro de Operaciones de Seguridad en un centro de datos independiente a las instalaciones del SOC, que cuente con al menos las siguientes características:

- Video vigilancia continua 7 x 24 (7 días a la semana durante las 24 del día).
- Sistema de control de acceso físico de al menos doble factor.
- Sistema de energía ininterrumpida (UPS).
- Redundancia en el aprovisionamiento de energía.
- Cableado estructurado con certificación nivel 6 o superior.
- Aire acondicionado de alta precisión.
- Sistema de detección y supresión de fuego.
- Infraestructura de comunicaciones y seguridad interna para los enlaces de comunicaciones.
- Infraestructura de servidores que soportan la operación del SOC.
- Personal de seguridad corporativa privada o pública en esquema de 7 x24 (7 días a la semana durante las 24 del día).
- Certificación en alguno de los estándares de diseño y funcionamiento de Centros de Cómputo, al menos ICREA nivel 4 o TIER III.

3.2.2.4 Productos

Entregable	Descripción	Requerimientos
E.3.2.2.1 Metodología del SOC	Documento que describa la metodología bajo la que trabaja el Centro de Operación de Seguridad del Proveedor Adjudicado, a través de la cual operarán los servicios de seguridad para el IFT.	R.3.2.2.1.1 El documento debe ser claro y mostrar la relación entre los procesos solicitados: • Proceso de atención a clientes. • Proceso de aprovisionamiento inicial. • Proceso de afinación continúa de los servicios prestados por el SOC. • Proceso de control de cambios. • Proceso de respuesta a incidentes. • Proceso para notificación de incidentes de seguridad.

Entregable	Descripción	Requerimientos
		• Proceso de incidentes mayores.
E.3.2.2.2 Matriz de Escalamiento de Problemas e Incidentes	Documento que describe las condiciones y responsables de los diferentes servicios contratados, así como los niveles y tiempos de escalamiento.	E.3.2.2.2.1 Este documento se debe actualizar cada que haya cambios en la organización, ya sea por parte del proveedor, o bien por parte del IFT. El documento deberá contener información tanto del Proveedor Adjudicado, como del IFT, al menos: • Rol de la persona, o puesto en la organización, según aplique • Nombre • Correo Electrónico • Teléfono Móvil • Nivel de escalamiento
E.3.2.2.3 Memorias Técnicas	Memorias Técnicas de las soluciones implementadas.	E.3.2.2.3.1 Las memorias técnicas de las soluciones implementadas deberán contener al menos: • Inventario de dispositivos instalados • Descripción general del servicio o dispositivo • Diagrama Físico y lógico de la implementación • Descripción técnica de la implementación • Políticas configuradas • Capacidades del dispositivo • Funcionalidades habilitadas en el dispositivo • Funcionalidades que podrían habilitarse con una licencia o costo adicional. Se deberán actualizar cada que haya un cambio en la configuración de los componentes.

3.2.3 Componente 3: Administración del servicio

El propósito de este componente es asegurar que el proyecto termine en tiempo, bajo el presupuesto acordado y cumpliendo con todos sus requerimientos.

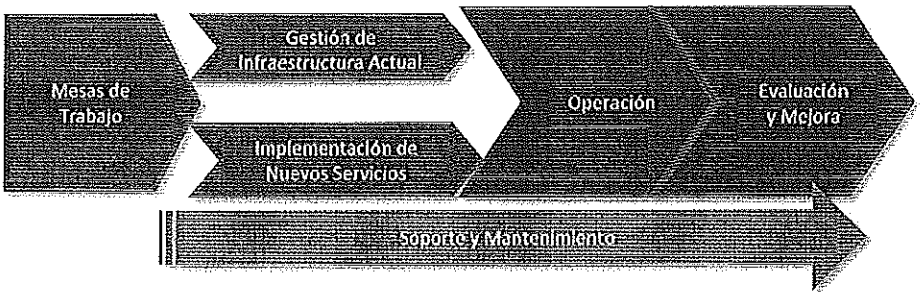
3.2.3.1 Productos

Entregable	Descripción	Requerimientos
E.3.2.3.1 Presentación de la Junta de inicio del proyecto	Presentación de objetivos, metas y recursos del proyecto.	R. E.3.2.3.1.1 Evidencia de asistencia a la presentación de todos los involucrados en el proyecto.

Entregable	Descripción	Requerimientos
E.3.2.3.2 Plan de Administración del Proyecto	Es el Plan que describe el modo en que el proyecto será ejecutado, monitoreado y controlado. Integra y consolida todos los planes y líneas base de los procesos de planificación.	El Documento que deberá incluir al menos: R.3.2.3.2.1 Enunciado del Alcance del Proyecto • Estructura de Desglose del Trabajo EDT • Diccionario de la EDT R.3.2.3.2.2 Plan de Gestión del Cronograma/ Línea base del cronograma • Cronograma del proyecto • Calendarios del Proyecto R.3.2.3.2.3 Plan de Gestión de la Calidad • Métricas del Proyecto • Límites de Control R.3.2.3.2.4 Plan de Gestión de los Recursos Humanos • Roles y responsabilidades (Rol, Autoridad, Responsabilidad y competencia) • Organigrama del Proyecto R.3.2.3.2.5 Plan de Gestión de las Comunicaciones • Información que será comunicada, incluidos el formato, contenido y nivel de detalle • Plazo y frecuencia para la distribución de la información • Persona responsable de distribuir la información R.3.2.3.2.6 Plan de Gestión de Riesgos • Registro de riesgos (lista de riesgos identificados, priorizados y respuestas potenciales)
E.3.2.3.3 Reportes de Avance	Informe periódico para el monitoreo y seguimiento del avance del proyecto.	R.3.2.3.3.1 Presentar de acuerdo a la periodicidad y medio establecido en el mecanismo de comunicación.
E.3.2.3.4 Plan de Transición	Estrategia para la transferencia tecnológica y de conocimiento hacia el IFT (capacitaciones, manuales)	R. 3.2.3.1.4.1 Firma de conformidad por parte de los principales usuarios del producto y/o servicio.
E.3.2.3.5 Presentación de Cierre	Presentación ejecutiva de los resultados.	R. 3.2.3.1.5.1 Incluir objetivos alcanzados, entregables, riesgos mitigados, problemas pendientes, metas cumplidas, beneficios obtenidos y lecciones aprendidas.
E.3.2.3.6 Acta de Cierre	Formaliza la entrega satisfactoria de los productos y/o servicios.	R. 3.2.3.1.6.1 Describir los productos y servicios entregados de acuerdo a la estructura definida en el PAP.

3.3 Estrategia de Proyecto

El licitante debe considerar la siguiente estrategia para el desarrollo del proyecto:



Mesas de Trabajo. Al inicio del proyecto, el proveedor llevará a cabo mesas de trabajo con el personal del IFT durante las cuales deberá:

- Afinar el diseño para la implementación de los nuevos servicios.
- Obtener la información necesaria para incorporar la infraestructura actual de seguridad con que ya cuenta el Instituto a los servicios considerados en el proyecto, con la finalidad de asegurar que las acciones de implementación, migración u operación de la misma (según sea el caso), tengan el menor impacto posible para el Instituto y se ajusten a los tiempos de implementación del proyecto.
- Detallar el plan de trabajo de la gestión de infraestructura actual y de la implementación de nuevos servicios.

Gestión de infraestructura actual. Durante la etapa de gestión de la infraestructura actual, el licitante ganador deberá llevar a cabo las actividades necesarias para que la infraestructura actual opere con base en los servicios para los que fue adquirida, sin que esto suponga un impacto para la operación del Instituto, ni un demérito de los Niveles de Servicio con que actualmente opera dicha infraestructura.

Implementación de Nuevos Servicios. En la etapa de implementación de nuevos servicios, el licitante ganador deberá llevar a cabo todas las tareas de implementación que sean necesarias, acorde con el plan de trabajo que haya sido afinado en mesas de trabajo. Asimismo, el licitante deberá considerar que esta etapa terminará una vez que el Instituto dé su visto bueno a la implementación de las soluciones, que deberá estar basado en un listado de verificación que haya sido acordado en mesas de trabajo, con la finalidad de no dejar nada a interpretación de ninguna de las dos partes.

Operación. La etapa de operación de los servicios iniciará una vez que se haya aceptado el diseño, instrumentado e implementado la solución propuesta para cada uno de los servicios solicitados por el Instituto.

Evaluación y Mejora. En esta etapa el Proveedor Adjudicado llevará a cabo tareas de evaluación de la operación y ajustes a la misma con base, tanto en valoraciones propias, como recomendaciones del Instituto con base en los resultados de la operación, la medición y apego a los Niveles de Servicio establecidos en este documento.

3.4 Elementos dentro del Alcance

Elementos que pueden impactar la ejecución del proyecto, por lo que deben ser considerados en la propuesta del Proveedor Adjudicado.

La configuración y atención de requerimientos para la operación de equipos y herramientas de software y hardware utilizadas por el Proveedor Adjudicado para el proyecto serán realizadas por su propio personal y deberán ser acordes con las condiciones que establezca el supervisor del proyecto y Administrador del contrato por parte de la CGOTI. .

La configuración de los equipos y herramientas de software propiedad del Proveedor Adjudicado, deberá ser realizada por personal de su plantilla con acompañamiento de personal del IFT y sin afectar los servicios del Instituto. Cualquier actividad del Proveedor Adjudicado deberá ser autorizada previamente por el el supervisor del proyecto y Administrador del contrato por parte de la CGOTI.

El Proveedor Adjudicado deberá contar y dedicar al proyecto especialistas certificados en temas relacionados con seguridad de información y administración de proyectos, como mínimo deberá contar con personal certificado en PMP, CISSP, CISM, CISA, CEH y GIAC conforme se detallan en el capítulo 6. Requisitos de especialidad.

3.4.1 Organización

Área / Unidad	Afectada / Involucrada	Observación / Comentario
CGOTI	Involucrada	Participa en la administración del proyecto y en la implementación de controles técnicos de acuerdo a la norma de referencia y a las guías de implementación aplicables.
Otras áreas del IFT	Involucradas	Utilizan servicios proporcionados por CGOTI

3.4.2 Procesos relacionados

Proceso	Impacto
Administración de Servicios informáticos	Provee servicios de TIC a todas las áreas del Instituto.

3.4.3 Aplicaciones relacionadas

Nombre Aplicaciones	Descripción
Bases de Datos	Repositorios de datos que contienen la información del IFT de forma estructurada e indexada para facilitar el acceso a esta.
Aplicaciones con acceso a través de Internet	Sistemas de información que pueden ser accedidos por los usuarios internos y/o externos desde Internet.

3.4.4 Marcos de Referencia y Mejores Prácticas

Durante la realización de la solución, se deben utilizar los siguientes marcos de referencia y/o metodologías:

Ámbito	Modelo/Metodología/Lineamientos
Proyectos	Project Management Body of Knowledge (PMBoK®) Guide The Standard for Portfolio Management ©
Servicios y Proveedores	ITIL®
Seguridad	ISO 27001©

3.5 Premisas

Para la realización y diseño de la solución tecnológica se deben considerar las siguientes premisas:

3.5.1 Patrocinio

La Alta Dirección de la Coordinación General de Organización y Tecnologías de Información proporciona el apoyo permanente y adecuado, para garantizar que los recursos necesarios (presupuesto, personal, tiempo) están disponibles y hay colaboración suficiente de la organización para lograr los objetivos de acuerdo al Cronograma del servicio.

3.5.2 Disponibilidad de Recursos en el IFT

Existe disponibilidad de los interesados para las actividades de definición, análisis, seguimiento y validación de los productos y servicios.

3.5.3 Acceso a la Información

El IFT provee el apoyo para acceder a información y entrevistas necesarias para el desarrollo de los servicios y productos.

3.5.4 Relaciones y/o Dependencias con otros Proyectos

Durante la realización de los servicios se deben considerar las dependencias que tengan impacto en la realización del proyecto, actualmente se tienen identificadas las siguientes:

Proyecto	Tipo de Dependencia	Descripción de la Dependencia	Criticidad
1 "Comunicaciones"	Servicio	Se encuentra en ejecución la actualización de equipo de comunicaciones del Instituto. Los procesos de análisis deberán realizarse sobre la nueva infraestructura.	Alta
2 "Servidores"	Servicio	Los servidores con los que cuenta el Instituto dan soporte a los ambientes de producción, pruebas y desarrollo del Instituto por lo que los trabajos de este proyecto no deben afectar la disponibilidad de los mismos.	Alta

3.6 Restricciones

Para la realización y diseño de la solución tecnológica se consideran las siguientes restricciones:

3.6.1 Temporalidad

Este proyecto tiene una duración estimada de 36 meses contados a partir de la notificación del fallo correspondiente. A continuación se presenta una estimación de la programación en la que se incorporaran los servicios solicitados, sin embargo, la incorporación de los servicios está sujeta a la planeación estratégica de la Coordinación General de Organización y Tecnologías de la Información:

Servicio solicitado	2014			2015											
	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12	Mes 13	Mes 14	Mes 15
S.1.1 - Servicio de gestión de infraestructura y monitoreo de eventos de seguridad de los componentes de seguridad perimetral del IFT.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
S.1.2 - Servicio de correlación de eventos y administración de bitácoras.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
S.1.3 - Servicio de análisis de vulnerabilidades y pruebas de penetración.	x			x			x			x			x		
S.1.4 - Servicio de control de acceso Firewall.		x	x	x	x	x	x	x	x	x	x	x	x	x	x
S.1.5 - Servicio de protección de aplicaciones web (WAF), servidores de archivos y bases de datos.								x	x	x	x	x	x	x	x
S.1.6 - Servicio de protección para correo electrónico.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
S.1.7 - Servicio de filtrado de contenido Web.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
S.1.8 - Servicio de monitoreo proactivo de seguridad en Internet.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
S.1.9 - Servicio de enrutamiento de enlace de Internet.	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Servicio solicitado	2016											
	Mes 16	Mes 17	Mes 18	Mes 19	Mes 20	Mes 21	Mes 22	Mes 23	Mes 24	Mes 25	Mes 26	Mes 27
S.1.1 - Servicio de gestión de infraestructura y monitoreo de eventos de seguridad de los componentes de seguridad perimetral del IFT.	x	x	x	x	x	x	x	x	x	x	x	x
S.1.2 - Servicio de correlación de eventos y administración de bitácoras.	x	x	x	x	x	x	x	x	x	x	x	x
S.1.3 - Servicio de análisis de vulnerabilidades y pruebas de penetración.	x			x			x			x		
S.1.4 - Servicio de control de acceso Firewall.	x	x	x	x	x	x	x	x	x	x	x	x
S.1.5 - Servicio de protección de aplicaciones web (WAF), servidores de archivos y bases de datos.	x	x	x	x	x	x	x	x	x	x	x	x
S.1.6 - Servicio de protección para correo electrónico.	x	x	x	x	x	x	x	x	x	x	x	x
S.1.7 - Servicio de filtrado de contenido Web.	x	x	x	x	x	x	x	x	x	x	x	x
S.1.8 - Servicio de monitoreo proactivo de seguridad en Internet.	x	x	x	x	x	x	x	x	x	x	x	x
S.1.9 - Servicio de enrutamiento de enlace de Internet.	x	x	x	x	x	x	x	x	x	x	x	x

Servicio solicitado	2017								
	Mes 28	Mes 29	Mes 30	Mes 31	Mes 32	Mes 33	Mes 34	Mes 35	Mes 36
S.1.1 - Servicio de gestión de infraestructura y monitoreo de eventos de seguridad de los componentes de seguridad perimetral del IFT.	x	x	x	x	x	x	x	x	x
S.1.2 - Servicio de correlación de eventos y administración de bitácoras.	x	x	x	x	x	x	x	x	x
S.1.3 - Servicio de análisis de vulnerabilidades y pruebas de penetración.	x			x			x		
S.1.4 - Servicio de control de acceso Firewall.	x	x	x	x	x	x	x	x	x
S.1.5 - Servicio de protección de aplicaciones web (WAF), servidores de archivos y bases de datos.	x	x	x	x	x	x	x	x	x
S.1.6 - Servicio de protección para correo electrónico.	x	x	x	x	x	x	x	x	x
S.1.7 - Servicio de filtrado de contenido Web.	x	x	x	x	x	x	x	x	x
S.1.8 - Servicio de monitoreo proactivo de seguridad en Internet.	x	x	x	x	x	x	x	x	x
S.1.9 - Servicio de enrutamiento de enlace de Internet.	x	x	x	x	x	x	x	x	x

3.6.2 Plan de Trabajo por entregables.

Durante la vigencia del contrato el Proveedor Adjudicado deberá considerar la generación de entregables que deberán ser facilitados al administrador del proyecto de acuerdo al calendario estimado que a continuación se presenta.

	2014			2015											
Entregable	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12	Mes 13	Mes 14	Mes 15
E.3.2.1.1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.2	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.3			x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.4			x			x			x			x			x
E.3.2.1.5	x			x			x			x			x		
E.3.2.1.6	x			x			x			x			x		
E.3.2.1.7								x	x	x	x	x	x	x	x
E.3.2.1.8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.9	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.11	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.12		x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.13	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.14	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.15	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.16		x													
E.3.2.1.17	Por evento														
E.3.2.2.1	x														
E.3.2.2.2	x														
E.3.2.2.3	x	x			x			x							
E.3.2.3.1	x														
E.3.2.3.2	x														
E.3.2.3.3	x	x	x			x			x			x			x
E.3.2.3.4															
E.3.2.3.5															
E.3.2.3.6															

	2016												2017								
Entregable	Mes 16	Mes 17	Mes 18	Mes 19	Mes 20	Mes 21	Mes 22	Mes 23	Mes 24	Mes 25	Mes 26	Mes 27	Mes 28	Mes 29	Mes 30	Mes 31	Mes 32	Mes 33	Mes 34	Mes 35	Mes 36
E.3.2.1.1	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.2	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.3	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.4			x			x			x			x			x			x			x
E.3.2.1.5	x			x			x			x			x			x			x		
E.3.2.1.6	x			x			x			x			x			x			x		
E.3.2.1.7	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.9	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.10	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.11	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.12	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.13	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.14	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x
E.3.2.1.15	x																				
E.3.2.1.16																					
E.3.2.1.17	Por evento																				
E.3.2.2.1																					
E.3.2.2.2																					
E.3.2.2.3																					
E.3.2.3.1																					
E.3.2.3.2																					
E.3.2.3.3			x			x			x			x			x			x			x
E.3.2.3.4																		x			
E.3.2.3.5																					x
E.3.2.3.6																					x

3.6.3 Forma de Pago

Se realizarán 36 pagos mensuales (a mes vencido) al Proveedor Adjudicado por los servicios prestados durante el periodo una vez que se hayan aprobado, por parte del supervisor del proyecto y administrador del contrato de la CGOTI, los entregables descritos en el numeral "3.2 Especificación de Componentes" correspondientes al periodo de que se trate de acuerdo con el Artículo 53 de las Normas en materia de adquisiciones, arrendamientos y servicios del Instituto Federal de Telecomunicaciones.

3.6.4 Recursos provistos por el IFT para la prestación del servicio

Por la naturaleza del proyecto no se requiere que el Proveedor Adjudicado coloque de forma permanente recursos en sitio, durante la implementación de los servicios, el IFT proporcionará:

Recurso	Cantidad
Espacio de trabajo	[2]
Acceso telefónico (extensión interna)	[1]
Nodos para Internet	[2]
Conexiones eléctricas	[4]

4. Lineamientos para el Proveedor Adjudicado

Esta sección establece los lineamientos que debe seguir el Proveedor Adjudicado durante la realización de las actividades y la vigencia del contrato. Para facilitar su referencia, los lineamientos se han clasificado en lineamientos generales que aplican durante toda la vigencia del contrato y lineamientos específicos para las etapas de planeación, ejecución y cierre.

Nombre de la Etapa	Criterios de Término
Planeación	• Se ha firmado el contrato con el Proveedor Adjudicado. • Se cuenta con el Plan de Administración del Proyecto. • Se cuenta con el Cronograma del Servicio. • Se ha efectuado la junta de Inicio del proyecto.
Ejecución	• Todos los entregables descritos con las evidencias correspondientes, se han revisado y aprobado por parte del supervisor del proyecto y administrador del contrato de la CGOTI.
Cierre	• Se ha firmado el "Acta de Cierre" del servicio por parte del supervisor del proyecto y administrador del contrato de la CGOTI y por el Administrador del Servicio del Proveedor Adjudicado. • Se han entregado los productos y servicios. • Se han liberado los recursos del proyecto.

4.1 Lineamientos para la Planeación

4.1.1 Inicio de Actividades

El Proveedor Adjudicado debe iniciar las actividades del servicio a partir del primer día hábil después de la fecha de notificación del fallo para la adjudicación del contrato.

El Proveedor Adjudicado, de manera conjunta con el supervisor del proyecto y administrador del contrato de la CGOTI, deberá realizar una revisión minuciosa de la situación actual del IFT y definir el plan de trabajo para implementar los servicios contratados en un periodo de 90 días a partir de la firma del contrato garantizando la continuidad de la operación del IFT.

El Proveedor Adjudicado en conjunto el supervisor del proyecto y administrador del contrato de la CGOTI realizarán un inventario de las aplicaciones y servicios, asociando a cada uno sus necesidades de tráfico (protocolo, puertos TCP/UDP, direcciones IP), el cual será la base para la definición de configuraciones de los diferentes dispositivos que conforman el servicio.

Con el fin de establecer los diversos procedimientos para la administración del servicio, el Proveedor Adjudicado deberá ajustar las entradas y salidas de cuando menos los siguientes procedimientos de acuerdo a los requerimientos del IFT, debiendo quedar perfectamente documentados y firmados el Proveedor

Adjudicado y el supervisor del proyecto y administrador del contrato de la CGOTI antes de iniciar con la operación del servicio:

1. Levantamiento y cierre de solicitudes de servicio (tickets).
2. Administración de cambios.
3. Administración de configuraciones.
4. Administración de vulnerabilidades.
5. Administración de incidentes.
6. Administración de problemas.
7. Notificación de alertas y actividades sospechosas.

El Proveedor Adjudicado deberá revisar la configuración de los equipos del IFT y proponer las acciones para un adecuado funcionamiento de la seguridad, estos cambios deberán ser avalados por el IFT antes de su aplicación, en caso de que las recomendaciones del Proveedor Adjudicado afecten la prestación de los servicios del IFT deberán proponerse alternativas de solución adecuadas a la operación del IFT.

El Proveedor Adjudicado deberá revisar la configuración de los políticas definidas en la herramienta del servicio de filtrado de contenido Web y proponer las modificaciones para incrementar el nivel de seguridad del servicio, estos cambios deberán ser avalados por el personal técnico del IFT.

El Proveedor Adjudicado, en coordinación con el IFT, definirá las bitácoras de los servidores, bases de datos y aplicaciones que se deberán centralizar para la activación de alertas y servicios de correlación de eventos y administración de bitácoras.

El Proveedor Adjudicado deberá realizar una propuesta de trabajo que incluya:

1. Rediseño de la arquitectura de red y seguridad perimetral.
2. El plan de migración, instalación, sugerencias y mejoras para cada servicio.
3. Prioridades de ejecución y actividades.
4. Programación del primer análisis de vulnerabilidades.
5. Programación de la primera prueba de penetración.
6. El Proveedor Adjudicado tendrá a partir de la firma del contrato 90 días naturales para la instalación de los equipos y habilitación de servicios.

4.1.2 Administrador del Servicio

El Proveedor Adjudicado debe nombrar a un Administrador de Servicio como único punto de contacto para las cuestiones de control y evaluación del servicio. Se debe proporcionar el número de teléfono de su oficina, número de teléfono móvil y su dirección de correo electrónico. El Proveedor Adjudicado se compromete a notificar por escrito, al menos con 5 días de anticipación, en el domicilio del Instituto cualquier cambio en el punto de contacto.

El Administrador del Servicio no deberá tener funciones en la operación del servicio y tendrá como mínimo las siguientes responsabilidades:

- Coordinar todas las acciones relacionadas al "Componente 3 Administración del Servicio"
- Planear y gestionar los cambios con el SOC y el IFT.
- Revisar de forma periódica los servicios prestados con la finalidad de asegurar la satisfacción del Instituto con la prestación de los mismos.
- Administrar la memoria técnica del proyecto.
- Contacto único para el seguimiento a los tickets levantados, atendidos y del cumplimiento de los niveles de servicios mensuales.
- Entrega de reportes y factura mensual.

4.1.3 Administrador técnico de la cuenta

Dada la complejidad del proyecto se requiere que, además del Administrador del Servicio, se asigne también un administrador técnico de la cuenta quien actuará como punto de contacto para el seguimiento de solicitudes de soporte y atención de aspectos técnicos relacionados con el proyecto.

4.2 Lineamientos para la Ejecución

4.2.1 Apego al Plan de Administración del Proyecto

El Proveedor Adjudicado debe realizar las actividades del servicio con apego al Plan de Administración del Proyecto definido en la etapa de Planeación.

4.2.2 Apego al Cronograma del Servicio

El Proveedor Adjudicado debe realizar las actividades del proyecto con apego al Cronograma del Servicio aprobado. Cualquier tipo de omisión, retraso o cambio en las actividades del servicio que afecten los hitos de entrega de productos puede tener un fuerte impacto en cuanto a los tiempos asignados originalmente, por lo que debe considerarse una estrategia de resolución de esta afectación. Esta estrategia de resolución debe someterse a la evaluación de la CGOTI para su aceptación y autorización de acuerdo al mecanismo establecido para la administración de cambios.

4.2.3 Entrega de Productos

Todos los productos del proyecto deben cumplir con los lineamientos descritos en el PAS antes de la firma de Actas de aceptación de entregables. Los productos aprobados por parte del IFT deben ser entregados en formato digital antes de firmarse el acta de cierre correspondiente.

Los entregables deben ser digitalizados y resguardados en el repositorio del proyecto en el sitio de la OAP, salvo los casos en que el espacio requerido para su almacenamiento sea mayor al permitido en el repositorio. En caso de auditoría o revisión de cualquier organismo fiscalizador, el Responsable del Proyecto está obligado a presentar las evidencias requeridas así como a responsabilizarse por el contenido y calidad de las mismas.

4.2.4 Control de cambios y atención de incidentes

Para el control de cambios, el Proveedor Adjudicado deberá acordar de manera conjunta con el supervisor del proyecto y administrador del contrato de la CGOTI el procedimiento a seguir, con el fin de garantizar los niveles de servicio acordados. Cada cambio deberá estar formalizado, estableciendo ambas partes los términos y condiciones del cambio. Los cambios a la infraestructura de seguridad administrada deberán realizarse en estricto apego del proceso de "Administración de Cambios" aceptado por ambas partes y deberán ser coordinados entre el Proveedor Adjudicado y el supervisor del proyecto y administrador del contrato de la CGOTI.

El Proveedor Adjudicado deberá considerar, como parte de su servicio, la aplicación de cambios ilimitados a la configuración de la infraestructura provista.

El Proveedor Adjudicado deberá contar con una línea 01-800 o número telefónico específico para comunicación con el SOC, registro de incidentes, cambios, requerimientos, entre otras necesidades del propio proyecto. El Proveedor Adjudicado deberá contar con una herramienta de mesa de servicio y administración de incidentes, accesible a través de Web para la consulta y levantamiento de requerimientos e incidentes con acceso seguro utilizando al menos autenticación de dos factores, por lo que deberá incluir en su propuesta:

- Documento que contenga nombre, fabricante, descripción general de la herramienta y alcance de su implantación en el SOC.
- Evidencia de que la herramienta cumple con el algún nivel de ITIL Compliance, puede ser a través de folletería oficial del fabricante distinguiendo claramente esta característica.

La herramienta debe permitir:

- Registrar incidentes identificados por el IFT o por personal del Proveedor Adjudicado asignado al servicio.

- Clasificar la información de acuerdo a criterios específicos definidos de manera conjunta entre el IFT y el Proveedor Adjudicado.
- Contar con un módulo de Administración de incidentes de seguridad.
- Contar con un módulo de Administración de niveles de servicio.
- Permitir la integración de una base de conocimientos y de resolución de problemas (troubleshooting) relacionada con el soporte técnico de dispositivos de seguridad integrados a la solución. Esta base será consultable por el IFT y se entregará al final del servicio en un formato legible para los equipos del Instituto (formato abierto).

Se deberá proporcionar al IFT, al menos 2 cuentas de acceso para cada consola de administración de los servicios, estas cuentas deben ser personalizadas, auditables y tendrán privilegios de "sólo lectura" para la supervisión de la configuración de los Componentes Habilitadores. Así mismo se deberá proporcionar al menos 1 cuenta de acceso para cada consola de administración de los servicios, esta cuenta debe ser personalizada, auditable y tendrá privilegios de "administración", dicha cuenta será resguardada por el IFT y será responsabilidad del Instituto el uso que se dé a esta cuenta.

4.3 Lineamientos para el Cierre

El servicio es considerado como terminado a satisfacción cuando todos los componentes, entregables y servicios descritos en el numeral "3 Alcance" sean revisados y aprobados formalmente mediante la firma del Acta de Cierre y actas administrativas correspondiente, así como la conformidad del Proveedor Adjudicado de que hasta en tanto ello no se cumpla, estos no se tendrán por recibidos o aceptados.

Antes de firmar el Acta de Cierre y las actas administrativas correspondientes, el IFT debe garantizar:

- Que el Proveedor reciba por parte del IFT la acreditación de que no ha quedado pendiente ningún entregable, salvo lo que resulte por concepto de garantías.

5. Penalizaciones

Conforme a lo establecido en la sección "**Pena Convencional y/o Deducciones**" de este Anexo Técnico.

6. Requisitos de especialidad

6.1.1 Recursos Humanos

El Proveedor Adjudicado deberá comprobar en la presentación de su oferta técnica que cuenta con experiencia en el ramo, tanto en el manejo de infraestructura de seguridad como en el manejo de prácticas y procesos basados en estándares internacionales, por lo que su personal deberá contar con las certificaciones vigentes correspondientes, las cuales deberán incorporarse en la propuesta del Proveedor (copia simple) conforme a lo establecido en el punto 6.1.2.

Los recursos humanos deberán formar parte de la plantilla del personal del Proveedor Adjudicado y será el

personal asignado a la administración y operación del servicio contratado. El Proveedor Adjudicado deberá comprobar mediante el alta del IMSS al menos 90 días de antigüedad para cada uno de los recursos destinados a este proyecto. En caso de que se presenten movimientos del personal, el proveedor deberá sustituir al mismo con otro recurso de iguales características, notificando previamente al IFT.

El equipo técnico asignado a la operación y administración del SOC deberá contar con certificaciones relacionadas a las marcas propuestas por el Proveedor Adjudicado, quien deberá entregar en su propuesta técnica el currículo y copia de las certificaciones del personal asignado a la operación del monitoreo y soporte del servicio del IFT, esperando contar como mínimo las siguientes certificados por cada tecnología propuesta (Firewalls, IDS/IPS, protección de aplicaciones, servidores de archivos y bases de datos, correlación de eventos, protección contra amenazas de nueva generación, filtrado de correo y herramienta de análisis de vulnerabilidades).

6.1.2 Evidencia de Cumplimiento

Para acreditar un recurso, el Proveedor Adjudicado debe comprobar que el recurso asignado al rol correspondiente en la ejecución de los servicios cuenta con las certificaciones solicitadas:

Cantidad	Rol	Evidencia de Cumplimiento
2	Especialista certificado en auditoría de sistemas.	Comprobable mediante certificado de: • CISA (Certified Information Systems Auditor), • CRISK Certified in Risk and Information Systems Control, y • ISO 27001 LA Auditor Líder.
3	Especialista certificado en seguridad de sistemas.	Comprobable mediante certificado de: • CISSP (Certified Information Systems Security Professional).
1	Especialista en hackeo ético de sistemas.	Comprobable mediante certificados de: • CEH (Certified Ethical Hacker), • CISSP (Certified Information Systems Security Professional), • GIAC Certified Incident Handler (GCIH), y • GWAPT Giac web application penetration tester.
1	Especialista en administración de seguridad de la información.	Comprobable mediante certificado de: • CISM (Certified Information Security Manager), • CISSP (Certified Information Systems Security Professional), • ITIL Expert, • CRISK Certified in Risk and Information Systems Control.
2	Especialista en administración de incidentes de seguridad	Comprobable mediante certificado de: • GIAC Incident Handler.
1	Administrador del Servicio (Líder de Proyecto)	Comprobable mediante certificado de: • PMP (Project Management Professional) emitido por el PMI, • CISSP (Certified Information Systems Security Professional), y • CRISK Certified in Risk and Information Systems Control.

6.1.3 Especialización Tecnológica

El proveedor deberá demostrar a través de una carta del fabricante dirigida al Instituto Federal de Telecomunicaciones, con una antigüedad no mayor de 30 días naturales previo a la fecha de convocatoria de la presente licitación, que la infraestructura propuesta para habilitar los servicios requeridos en el presente anexo cuentan con el respaldo del fabricante

El proveedor deberá demostrar, a través de una Carta del Fabricante en donde afirme confirme que cuenta con el mayor nivel de certificación de Partner (Socio de Negocio) para cada una de las tecnologías a ser implementadas por el proveedor y que cuentan con apoyo técnico del mismo en caso de ser requerido.

7. Criterio de evaluación

Para la adjudicación del presente contrato, la CGOTI considera el criterio de evaluación de puntos y porcentajes como la mejor opción para calificar las propuestas de los interesados.

8. Firmas

Responsable del Proyecto y Contenido

Ney Galicia Arrocena
Director de Seguridad de Sistemas Informáticos

Revisión y Vo. Bo.

Guillermo Saavedra Suárez
Director General Adjunto de Tecnologías de Información y Comunicaciones

Autorizó

Hugh Harleston López Espino
Coordinador General de Organización Y Tecnologías de la Información