METODOLOGÍA DE OBTENCIÓN DE LOS PRECIOS DE REFERENCIA - RES. DNCP N° 1890/2020 DEL 07/05/2020.

CD N° 69/2021 – SERVICIO DE SOPORTE DE ALINEACIÓN A ESTANDAR CSP SWIFT - ID N° 394941

										Área técnica responsable: Departamento de Ciberseguridad (DCS)										
LOTES	ÍTEM	DESCRIPCIÓN				CONTRATACIÓN ANTERIOR				FUENTES DE REFERENCIA			PROMEDIO	PRESENTE LLAMADO				VARIACIÓN ENTRE LA ADJUDICACIÓN ANTERIOR Y EL PRECIO REFERENCIAL CONSIDERADO	DIFERENCIAS A SER CONSIDERADAS ENTRE EL PRECIO REFERENCIAL Y POTENCIALES OFERTAS	
						Duración del contrato/ tipo	Precio Unitario	Cantidad Adjudicada	Total	1	2	3		Duración del contrato/ tipo	Procedimiento/ Método	Cantidad	Precio referencial considerado	Prec. Ref./Ult. Contrato.	15 % por encima del precio referencial	25% por debajo del precio referencial
N/A		TIPO DE CONTRATACIÓN	NUEVA	AMPLIACIÓN	RENOVACIÓN					Presupuesto 2021 Empresa: Enrst & Young	Presupuesto 2021 Empresa: Deloitte	Presupuesto 2021 Empresa: Parasur								
			X																	
	1	Implementación del CSP de Swift				N/A	N/A	N/A	N/A	55.000.000	65.000.000	56.000.000	58.666.667	Duración del contrato: Hasta el cumplimiento total de las obligaciones contractuales/ Tipo: Contrato Cerrado.	Precio más bajo entre las fuentes de referencia	1	**55.000.000**	N/A	63.250.000	41.250.000
	2	Auditoría del CSP de Swift				N/A	N/A	N/A	N/A	37.400.000	45.000.000	40.000.000	40.800.000			1	**37.400.000**	N/A	43.010.000	28.050.000
														TOTALES			**92.400.000**		**106.260.000**	**69.300.000**

Dictamen UOC: con base en los datos proporcionados por el área técnica incluidos en la presente planilla, los documentos respaldatorios adjuntos y el método indicado por la misma, esta Unidad Operativa de Contratación señala que las metodología utilizada a fin de determinar los precios referenciales ha sido: la del precio más bajo entre todas las fuentes obtenidas.

Los precios referenciales han sido obtenidos de acuerdo a las siguientes fuentes: Presupuesto 2021 presentado por la firma Enrst & Young, Presupuesto 2021 presentado por la firma Deloitte y el Presupuesto 2021 presentado por la firma Parasur. Cabe aclarar que, por la particularidad y especialidad de los servicios solicitados solo se han podido obtener 3 (tres) precios de potenciales oferentes por correo electrónico, no siendo posible la combinación con otras fuentes como ser: precios ofrecidos por empresas al público en general, a través de portal público de internet, publicaciones periodísticas, revistas, páginas web, catálogos, u otros documentos, respecto de bienes, servicios u obras similares o idénticos a lo solicitado, y tampoco se cuenta con precios de una contratación anterior con el mismo objeto, ya sea de esta convocante, como de otros organismos, entidades o municipalidades. Por lo que, se obtiene el precio conforme a lo establecido en el Anexo de la Resolución DNCP N° 1890/2020 que establece lo siguiente: *"Excepcionalmente, si por la complejidad, especialidad o particularidad de la contratación no resultare posible alcanzar la cantidad de 3 (tres) fuentes requeridas para la obtención de los precios, la convocante podrá adoptar el mecanismo que considere apropiado para obtener los Precios de Referencia, en cuyo caso tal situación deberá ser suficientemente fundada en el Dictamen firmado por el Encargado de la UOC en el que se detalle la metodología utilizada para la obtención de los Precios de Referencia."*

MARIA EMILIA ACHA PALACIOS

Firmado digitalmente por MARIA EMILIA ACHA PALACIOS
Fecha: 2021.08.02 19:24:16 -04'00'

MARCELO GALVAN AVALOS
2021.08.04 12:08:13 -04'00'

Ariel Emilio Caceres Ramirez

De: Cristhian Ozorio <cristhian.ozorio@py.ey.com>
Enviado el: viernes, 30 de abril de 2021 18:15
Para: Ariel Emilio Caceres Ramirez
CC: Seguridad de la Información; Javier Vergara; Luis Ayala; Mateo Franco
Asunto: RE: Consulta y solicitud de presupuesto servicios CSP Swift
Datos adjuntos: Asistencia SWIFT_2021_BCP_EY.pdf

Categorías: Documentación de proveedores

Buenas tardes Ariel
Espero te encuentres bien.
Adjunto al correo el alcance de los servicios requeridos y la cotización referencial de cada uno.
Cualquier duda a las órdenes.
Gracias desde ya por tenernos en cuenta.

Regards,

Find us on: Facebook | LinkedIn | Twitter | YouTube

Cristhian Ozorio | ISO 27001 LA | ISO 20000 LI | Senior Manager | Business Consulting - IT & Cybersecurity

Ernst & Young Paraguay - Auditores y Asesores de Negocios
Mcal. López 3794 esq. Cruz del Chaco, Edificio Citicenter - 6° Piso, Asunción, Departamento Central 1808, Paraguay
Office: +595-21-664308 | Fax: +595-21-608 985 | cristhian.ozorio@py.ey.com
Cell: +595-976-301749
Website: http://www.ey.com
Elegidos en el 2021, por quinto año consecutivo, como uno de los mejores lugares para trabajar en Paraguay según Great Place to Work®

From: Ariel Emilio Caceres Ramirez <acaceres@bcp.gov.py>
Sent: Monday, April 26, 2021 1:00 PM
To: Cristhian Ozorio <cristhian.ozorio@py.ey.com>
Cc: Seguridad de la Información <dsi@bcp.gov.py>
Subject: Consulta y solicitud de presupuesto servicios CSP Swift
Importance: High

Estimado Cristhian,

Antes que nada, espero que te encuentres bien. El motivo de mi correo es para consultarte si actualmente están ofreciendo los siguientes servicios relacionados con Swift:

1. **Consultoría CSP (*Customer Security Program)*:** El servicio debería contemplar mínimamente la evaluación y diagnóstico del estado de implementación de los controles del CSP, recomendaciones de mejoras o controles que deben ser aplicados y el acompañamiento continuo en todas las fases del servicio.
2. **Auditoría CSP:** El servicio debe determinar el grado de implementación de los controles del CSP de Swift y emitir un informe resultante que sirva como evidencia del estado de la implementación del programa, y sea reconocido por Swift.

Si es que este es el caso, te agradeceríamos si nos pudieran indicar los detalles de los servicios ofrecidos y también nos puedan brindar un presupuesto estimado de ambos.

Consideraciones adicionales:

- Tanto la empresa como los profesionales que llevarán a cabo los trabajos, deben contar con experiencia comprobada en la realización de estos servicios.

- La duración para ambos servicios debe ser de 12 meses.
- No se debe cotizar por horas de servicio, sino por servicio (Ítem 1 “Consultoría CSP” e Ítem 2 “Auditoría CSP”).
- Las sesiones de acompañamiento, tanto para el ítem 1 como para el ítem 2, podrán ser llevadas a cabo de forma virtual como presencial.

Quedamos atentos ante cualquier duda o consulta adicional.
Muchas gracias.

ARIEL EMILIO
CÁCERES RAMIREZ
Dpto. de Ciberseguridad
BANCO CENTRAL DEL PARAGUAY
Federación Rusa y Augusto Roa Bastos
4to. Piso Asunción, Paraguay
E-mail: acaceres@bcp.gov.py
dsi@bcp.gov.py

Cualquier comentario, queja, reclamo o sugerencia acerca de nuestros servicios o productos, por favor envíelo a: info@bcp.gov.py

Aviso Legal: Este correo electrónico puede contener información de carácter reservado y/o confidencial perteneciente al Banco Central del Paraguay (BCP) o a terceros, y se encuentra protegida de acuerdo a lo prescripto por la Ley N° 489/95 “Orgánica del Banco Central del Paraguay” y la Ley N° 861/96 “General de Bancos, Financieras y Otras Entidades de Créditos”. Sea usted el destinatario o no del presente correo (o responsable de la entrega del mensaje a la persona indicada), no podrá utilizar, copiar, reproducir o distribuir el mensaje de manera total o parcial, sin autorización previa. Los criterios, opiniones, conclusiones y otras informaciones expresadas en el presente correo electrónico, no podrán ser considerados como información oficial del BCP, salvo expresa autorización del Directorio del BCP o Dependencia autorizada por el mismo. Se han tomado todas las precauciones razonables a fin de garantizar la ausencia de cualquier tipo de software malicioso en este correo electrónico. El BCP no se hace responsable de cualquier pérdida o daño causado por el uso de correo electrónico o archivos adjuntos. No obstante se recomienda el análisis pertinente del correo, que incluya los procedimientos inherentes a la verificación de software malicioso antes de su uso. Si ha recibido este mensaje por error, notifique al BCP por correo electrónico o a la línea telefónica 595 21 608 011/60 y elimínelo inmediatamente.

Disclaimer: This email may contain proprietary and/or confidential information belonging to the Central Bank of Paraguay (CBP) or third parties, and is protected by Law 489/95 "Charter of the Central Bank of Paraguay" and Law 861/96 "General Banking, Financial and Other Credit Institutions". Whether you are the intended recipient of this mail or not (or responsible for delivering the message to the right recipient), you are not allowed to use, copy, reproduce or distribute the message in whole or in part, without prior authorization. The views, opinions, conclusions and other information expressed in this email may not be considered as official information from CBP, unless prior written authorization of the CBP’s Board of Directors or Unit duly authorized by it. All reasonable precautions have been taken to ensure the absence of any malicious software in this email. The CBP is not liable for any loss or damage caused by the use of e-mail or attachments. However, the relevant analysis of the mail, including the pertinent malicious software detection methods before use, is highly recommended. If you have received this message by mistake, please notify CBP by email or telephone: 595-21-608011/60 and delete it immediately.”

The information contained in this communication is intended solely for the use of the individual or entity to whom it is addressed and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this information is strictly prohibited and may be unlawful. If you have received this communication in error, please notify us immediately by responding

to this email and then delete it from your system. EY is neither liable for the proper and complete transmission of the information contained in this communication nor for any delay in its receipt.

BANCO CENTRAL DEL PARAGUAY

Análisis de Seguridad CSP de SWIFT

Propuesta de Servicios Profesionales

30 de abril de 2021

Asunción, Paraguay

Building a better working world

Confidencialidad

- Este material es propiedad de Ernst & Young, para ser utilizado únicamente por **BANCO CENTRAL DEL PARAGUAY** con el fin exclusivo de evaluar nuestro enfoque para la prestación de Servicios Profesionales

- Este material no podrá ser utilizado con otros propósitos, por **BANCO CENTRAL DEL PARAGUAY** ni por terceros, salvo autorización expresa de Ernst & Young

- Igualmente, queda totalmente prohibida su reproducción parcial o total por cualquier método, físico, óptico o magnético sin el consentimiento escrito de la compañía

Contenido

Sección		Página
1	Introducción y Objetivos	4
2	Nuestro Enfoque	6
3	Entregables del Proyecto	16
4	Plazos	18
5	Equipo de trabajo	20
6	Honorarios	24

Introducción y Objetivos

Nuestro entendimiento de sus necesidades

El área de Seguridad de la Entidad, requiere un amplio nivel de cobertura con respecto a sus funciones y responsabilidades, para la custodia de los activos informáticos de la Entidad relativos al sistema de mensajería financiera SWIFT, a fin de protegerlos razonablemente y asegurar un adecuado cumplimiento a las normas de seguridad requeridas por SWIFT.

En el mencionado contexto, el **BANCO CENTRAL DEL PARAGUAY** ha solicitado la asistencia de EY con la finalidad de ejecutar una evaluación sobre los controles de seguridad implementados actualmente, que afectan a los activos relativos a SWIFT y concluir acerca del nivel de adecuación de dicho modelo con los requerimientos del ente regulador.

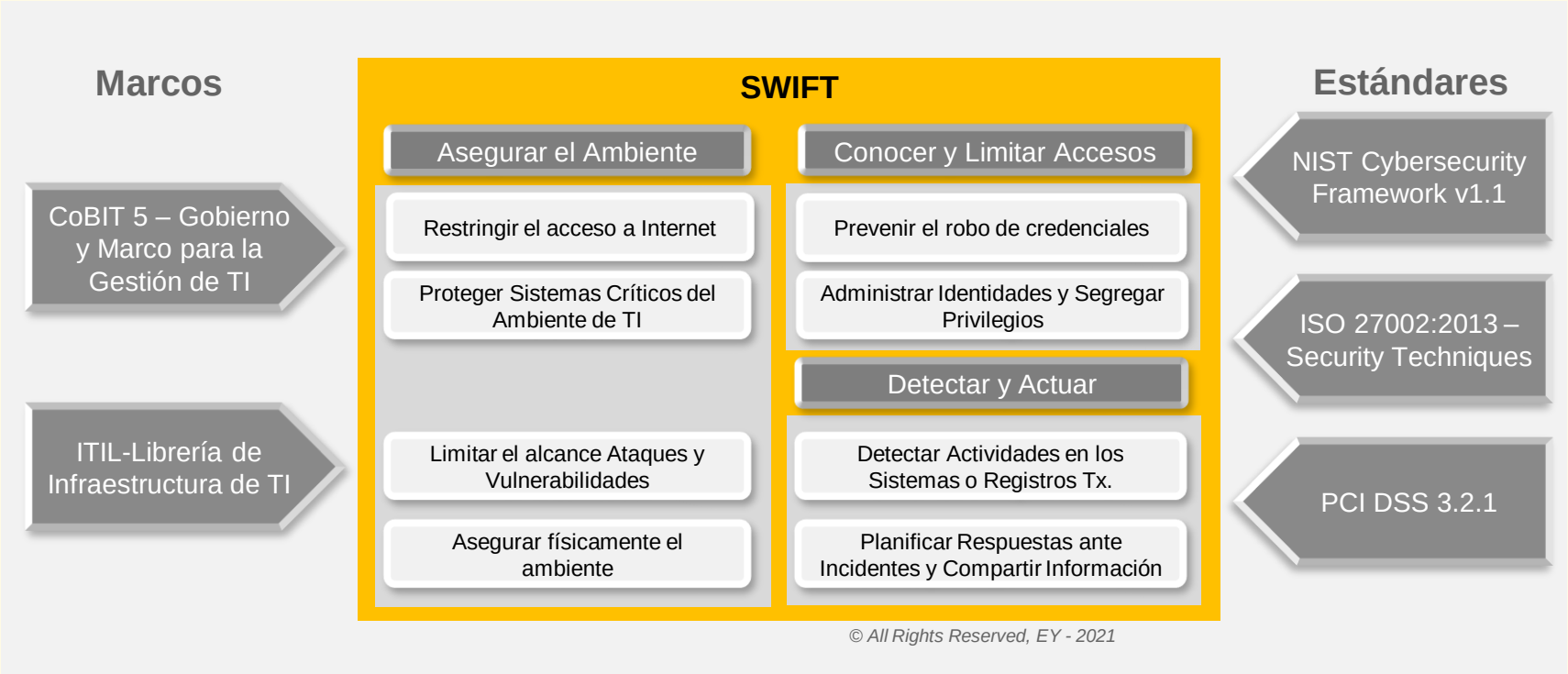
EY propone, a través de la presente Propuesta, un alcance técnico que combina la experiencia de sus profesionales en la ejecución de proyectos de Evaluación de Gestión Seguridad de la Información, respecto a las mejores prácticas de mercado.

EY proporcionará un equipo de trabajo multidisciplinario, aplicará las mejores practicas recomendadas por el ente regulador y una amplia experiencia con el fin de asegurar el éxito de este proyecto. Nuestro equipo propuesto incluiría personal que ha trabajado extensamente en los compromisos de asesoramiento de Gestión de Gobierno de TI y SI, Auditoria Interna Informática, revisiones de Procesos de Tecnología y Seguridad de la Información.

Metodología y Enfoque

Metodología y Enfoque

Aprovecharemos nuestra vasta base de conocimientos y recursos internos de EY, además utilizaremos como guía principal el Marco de Referencia de Controles de Seguridad para Clientes publicado por SWIFT v2021, el cual se encuentra alineado a los marcos y estándares líderes como ISO 27002, NIST Cybersecurity 1.1 y PCI DSS 3.2.1 como se muestra a continuación.



1. Consultoría CSP

Nuestro enfoque de trabajo (Consultoría CSP)

Etapas	1 Planificar	2 Identificar	3 Diagnosticar	4 Reportar y Acompañar
	Comunicación Continua & Coordinación			
Actividades Principales	1.1 Planificación del Proyecto ▸ Realizar la planificación del proyecto. ▸ Alinear la metodología de diagnóstico con las expectativas y necesidades de la Entidad. ▸ Identificar a los interesados claves del sector de Seguridad Informática, así como de las áreas de negocio.	2.1 Evaluación del Modelo Actual ▸ Comprender los objetivos de Seguridad informática relativos a la Integridad, Confidencialidad y Disponibilidad del sistema SWIFT. ▸ Realizar entrevistas con los interesados claves. ▸ Recopilar y evaluar información sobre los sub-procesos de Seguridad Informática que afectan al sistema SWIFT.	3.1 GAP Análisis ▸ Revisar los principales controles de seguridad Informática implementados y controles claves identificados, que aplican a la Arquitectura de la Entidad. ▸ Mapear los procesos aplicables en base al Marco de Referencia de SWIFT que define los controles de Seguridad y determinar las brechas existentes.	4.1 Reporte y Planes de Acción ▸ Generar el reporte de diagnóstico, recomendaciones e iniciativas. ▸ Generar Road Map de Implementación. ▸ Validar el reporte de diagnóstico con la contraparte interna del proyecto. ▸ Concluir y entregar el reporte final. ▸ Realizar seguimiento sobre los hallazgos reportados.*
Entregables	▸ Planificación del Proyecto	▸ Informe de Diagnóstico y resultados del Gap Análisis. ▸ Road Map o Plan de Implementación.		
Fuentes	▸ Relevamientos con Interesados Clave	▸ Relevamientos ▸ Políticas y Procedimientos de la Entidad	▸ SWIFT Customer Security Controls Framework v2021	▸ Bases de Conocimiento EY ▸ Herramientas de EY Global Security.

Nota: *se realizarán seguimientos mensuales de hasta 8 hs, para validar las remediaciones implementadas por la Entidad.*

Nuestro enfoque de trabajo (Consultoría CSP)

Etapas y Actividades

Para la ejecución del proyecto proponemos una metodología basada en las siguientes etapas y actividades:

Planificar → Identificar → Diagnosticar → Reportar

Planificar

Esta etapa tendrá las siguientes tareas:

- Definir la planificación del proyecto.
- Alinear la metodología de diagnóstico con las expectativas y necesidades de la Entidad.
- Identificar a los interesados claves del sector de Seguridad de la Información y Tecnologías de la Información, así como otras áreas clave de negocio.
- Confirmar el Equipo de Trabajo de EY y el Equipo de Trabajo de la Entidad.

Entregables y Plazos

- Planificación del Proyecto

- Plazo de ejecución: se prevé una duración aproximada de 16 horas.
- Dedicación de tiempo: 1 (un) profesional asignado para llevar a cabo esta tarea.

Identificar

Esta etapa tendrá como finalidad ejecutar las actividades propias del proyecto conforme los alcances previstos.

- Comprender los objetivos de Seguridad de la Información relativos a la Integridad, Confidencialidad y Disponibilidad del sistema SWIFT.
- Realizar entrevistas con los interesados claves
- Recopilar y evaluar información sobre los sub-procesos de Seguridad de la Información que afectan al sistema SWIFT.

Entregables y Plazos

- Informe de Diagnóstico y resultados del Gap Análisis.
- Road Map o Plan de Implementación.

- Plazo de Ejecución: se prevé una duración aproximada de 40 horas.
- Dedicación de Tiempo: 2 (dos) profesionales asignado para llevar a cabo esta tarea

Nuestro enfoque de trabajo (Consultoría CSP)

Etapas y Actividades

Para la ejecución del proyecto proponemos una metodología basada en las siguientes etapas y actividades.

Planificar → Identificar → Diagnosticar → Reportar

Diagnosticar

Esta etapa tendrá como finalidad ejecutar las actividades propias del proyecto conforme los alcances previstos.

- Revisar los principales controles de seguridad informática implementados y controles claves identificados, que aplican a la Arquitectura implementada por la Entidad.
- Mapear los procesos aplicables en base al Marco de Referencia de SWIFT v2021 que define los controles de Seguridad y determinar las brechas existentes.

Entregables y Plazos

- Informe de Diagnóstico y resultados del Gap Análisis.
- Road Map o Plan de Implementación.

- Plazo de Ejecución: se prevé una duración aproximada de 80 horas.
- Dedicación de Tiempo: 2 (dos) profesionales asignado para llevar a cabo esta tarea

Reportar y Acompañar

Esta etapa tendrá como finalidad realizar la reunión de conclusión y cierre. Las siguientes tareas serán ejecutadas en este componente de proyecto:

- Generar el reporte de diagnóstico e iniciativas.
- Generar Road Map de Implementación.
- Validar el reporte de diagnóstico con la contraparte interna del proyecto.
- Concluir y entregar el reporte final.
- Realizar seguimiento sobre los hallazgos reportados*.

*se realizarán seguimientos mensuales de hasta 8 hs, para validar las remediaciones implementadas por la Entidad

Entregables y Plazos

- Informe de Diagnóstico y resultados del Gap Análisis.
- Road Map o Plan de Implementación.

- Plazo de Ejecución: se prevé una duración aproximada de 32 horas.
- Dedicación de Tiempo: 2 (dos) profesionales asignado para llevar a cabo esta tarea

2. Auditoría CSP

Nuestro enfoque de trabajo (Auditoría CSP)

Etapas	1 Planificar	2 Identificar	3 Diagnosticar	4 Reportar
	Comunicación Continua & Coordinación			
Actividades Principales	1.1 Planificación del Proyecto ▸ Realizar la planificación del proyecto. ▸ Alinear la metodología de diagnóstico con las expectativas y necesidades de la Entidad. ▸ Identificar a los interesados claves del sector de Seguridad Informática, así como de las áreas de negocio.	2.1 Evaluación del Modelo Actual ▸ Comprender los objetivos de Seguridad informática relativos a la Integridad, Confidencialidad y Disponibilidad del sistema SWIFT. ▸ Realizar entrevistas con los interesados claves. ▸ Recopilar y evaluar información sobre los sub-procesos de Seguridad Informática que afectan al sistema SWIFT.	3.1 Auditoría ▸ Revisar los principales controles de seguridad Informática implementados y controles claves identificados, que aplican a la Arquitectura de la Entidad. ▸ Mapear los procesos aplicables en base al Marco de Referencia de SWIFT que define los controles de Seguridad y determinar las brechas existentes.	4.1 Reporte de Auditoria ▸ Generar el reporte de Auditoria. ▸ Validar el reporte de diagnóstico con la contraparte interna del proyecto. ▸ Concluir y entregar el reporte final.
Entregables	▸ Planificación del Proyecto	▸ Informe de Diagnóstico y resultados (Auditoria).		
Fuentes	▸ Relevamientos con Interesados Clave	▸ Relevamientos ▸ Políticas y Procedimientos de la Entidad	▸ SWIFT Customer Security Controls Framework v2021	▸ Bases de Conocimiento EY ▸ Herramientas de EY Global Security.

Nuestro enfoque de trabajo (Auditoría CSP)

Etapas y Actividades

Para la ejecución del proyecto proponemos una metodología basada en las siguientes etapas y actividades:

Planificar → Identificar → Diagnosticar → Reportar

Planificar

Esta etapa tendrá las siguientes tareas:

- Definir la planificación del proyecto.
- Alinear la metodología de diagnóstico con las expectativas y necesidades de la Entidad.
- Identificar a los interesados claves del sector de Seguridad de la Información y Tecnologías de la Información, así como otras áreas clave de negocio.
- Confirmar el Equipo de Trabajo de EY y el Equipo de Trabajo de la Entidad.

Entregables y Plazos

- Planificación del Proyecto

- Plazo de ejecución: se prevé una duración aproximada de 16 horas.
- Dedicación de tiempo: 1 (un) profesional asignado para llevar a cabo esta tarea.

Identificar

Esta etapa tendrá como finalidad ejecutar las actividades propias del proyecto conforme los alcances previstos.

- Comprender los objetivos de Seguridad de la Información relativos a la Integridad, Confidencialidad y Disponibilidad del sistema SWIFT.
- Realizar entrevistas con los interesados claves
- Recopilar y evaluar información sobre los sub-procesos de Seguridad de la Información que afectan al sistema SWIFT.

Entregables y Plazos

- Informe de Auditoria.

- Plazo de Ejecución: se prevé una duración aproximada de 40 horas.
- Dedicación de Tiempo: 2 (dos) profesionales asignado para llevar a cabo esta tarea

Nuestro enfoque de trabajo (Auditoría CSP)

Etapas y Actividades

Para la ejecución del proyecto proponemos una metodología basada en las siguientes etapas y actividades.

Planificar → Identificar → Diagnosticar → Reportar

Diagnosticar

Esta etapa tendrá como finalidad ejecutar las actividades propias del proyecto conforme los alcances previstos.

- Revisar los principales controles de seguridad informática implementados y controles claves identificados, que aplican a la Arquitectura implementada por la Entidad.
- Mapear los procesos aplicables en base al Marco de Referencia de SWIFT v2021 que define los controles de Seguridad y determinar las brechas existentes.

Entregables y Plazos

- Informe de Auditoria.

- Plazo de Ejecución: se prevé una duración aproximada de 60 horas.
- Dedicación de Tiempo: 2 (dos) profesionales asignado para llevar a cabo esta tarea

Reportar

Esta etapa tendrá como finalidad realizar la reunión de conclusión y cierre. Las siguientes tareas serán ejecutadas en este componente de proyecto:

- Generar informe de Auditoría.
- Validar el reporte de diagnóstico con la contraparte interna del proyecto.
- Concluir y entregar el reporte final.

Entregables y Plazos

- Informe de Auditoría.

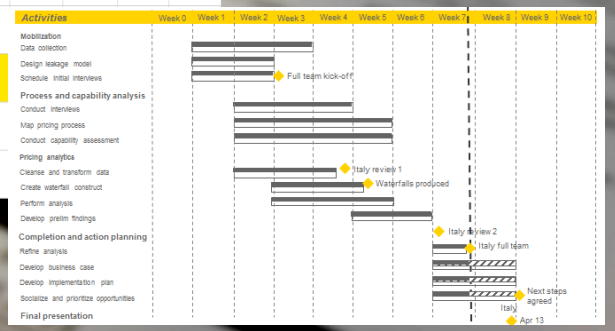
- Plazo de Ejecución: se prevé una duración aproximada de 32 horas.
- Dedicación de Tiempo: 2 (dos) profesionales asignado para llevar a cabo esta tarea

Entregables del Proyecto

Entregables

Plan detallado del proyecto

S.No.	Actividad	S1	S2	S3	S4	S5	S6	S7	S8
1	Planificación								
2	Evaluación								
3	Reportes								
4	Diseño								
5	Seguimiento								

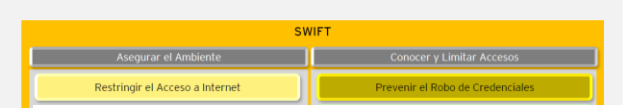


Informe de Diagnostico y Gap Análisis

Resumen Ejecutivo
Nivel de Madurez Actual

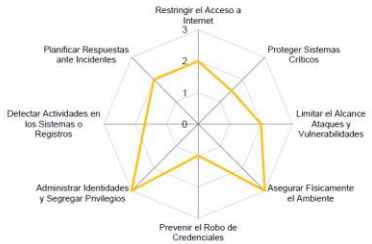
De acuerdo con los procedimientos de evaluación desarrollados, la siguiente gráfica indica el nivel de madurez que tiene el Marco de Referencia de Controles de Seguridad para Clientes publicado por SWIFT, actualmente implementado en Banco Atlas.

SWIFT CUSTOMER SECURITY CONTROLS FRAMEWORK 1.0



Resumen Ejecutivo
Nivel de Madurez Actual

El resultado de evaluar cada Principio con los Controles del Framework SWIFT, nos suministró un entendimiento inicial del estado actual de adecuación del Banco a dicho modelo de SWIFT, concluyendo que el mismo se encuentra en el nivel Adaptarse.

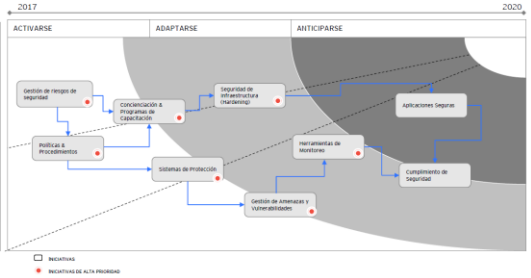


Las organizaciones que se encuentran en estado entre ***Activarse*** y ***Adaptarse***, están en el proceso de implementar fundamentos adicionales de seguridad lógica, sin desarrollar esfuerzos adicionales.

Hoja de ruta propuesta

Road Map de Recomendaciones
Mapa de Iniciativas

La priorización de iniciativas esta dada bajo el marco de trabajo aplicado para establecer la ruta hacia el nivel de maduración deseado de la Norma SWIFT.
La ejecución de las iniciativas de seguridad planteadas en el Road Map, están diseñadas para lograr mejoras consistentes en el modelo de seguridad lógica que rige actualmente en la Entidad.



Plazos

Plazos del proyecto

De acuerdo al alcance solicitado, hemos mapeado las actividades principales que serán ejecutadas, los tiempos estimados, propuestos para el desarrollo de los trabajos son los siguientes:

Componentes	Meses											
	1	2	3	4	5	6	7	8	9	10	11	12
GAP ANALISIS CSP SWIFT												
Planificar												
Identificar												
Diagnosticar												
Reportar y acompañar												
AUDITORÍA ANALISIS CSP SWIFT												
Planificar												
Identificar												
Diagnosticar												
Reportar												

Nota: este plan refleja el horizonte de tiempo del proyecto, no el total de horas que deben ser utilizadas durante la ejecución de las distintas tareas y actividades previstas. Estos plazos están sujetos al grado de acompañamiento de la contraparte de la Entidad para dar soporte y aprobar los documentos generados.

Equipo de Trabajo

Equipo de trabajo

Nuestro Equipo cuenta con el conocimiento y las credenciales apropiadas para éste Proyecto

Luis Ayala
Socio

Tel.: +595 (21) 664 308
Email: luis.ayala@py.ey.com

Rol en el Proyecto

- Socio a cargo del Proyecto

Experiencia

Socio de la división de Consulting Services de Ernst & Young Paraguay, miembro de Ernst & Young Global. Cuenta con más de 16 años de experiencia en asesoramiento de negocios, incluyendo proyectos de optimización de procesos y rediseño organizacional de empresas, y consultorías organizacionales. Lideró proyectos relacionados con evaluación y reingeniería de procesos así como la revisión de implementación de plataformas ERP (JDE y SAP). Su formación incluye:

- Licenciado en Ciencias Contables, Universidad Católica (1997).
- Licenciado en Administración de Empresas, Universidad Católica (1998).
- Máster en Administración de Empresas (MBA), Universidad Americana (2002).
- ISO 27001 Lead Auditor - Certificado
- Certificación de Auditor de Sistemas de Información – ISACA
- COBIT Foundation 4.1 - Certificado
- COBIT 5.0 Foundation - Certificado

Cristhian Ozorio
Senior Manager

Tel.: +595 (21) 664 308
Email: cristhian.ozorio@py.ey.com

Rol en el Proyecto

- Senior Manager Consulting

Experiencia

Cristhian Ozorio se ha incorporado a E&Y, miembro de Ernst & Young Global en Agosto de 2008 después de trabajar los anteriores 7 años como Networking Administrador en una empresa de telefonía móvil. Desde el 2014 se desempeña como Senior Manager de la Firma Ernst & Young Paraguay Auditores y Asesores de Negocios, en el área de Consulting Services. Su formación incluye:

- Licenciado en Análisis de Sistemas
- Especialista en Tecnología de la Información y Comunicación, Universidad Nacional de Asunción
- Máster en Tecnología de la Información y
- Comunicación (Fase Presentación de Tesis)
- ISO 27001:2013 Lead Auditor. Certificado
- COBIT 5 Foundation - Certificado
- ITIL Foundation 2011
- CCNA1 – Fundamentos de Redes.
- CCNA 2 – Protocolos y Conceptos de Ruteo.
- CCNA 3 – Switcheo y Wireless LAN
- CCNA 4 – Accediendo la WAN

Mateo Franco
Manager Cybersecurity

Tel.: +595 (21) 664 308
Email: mateo.franco@py.ey.com

Rol en el Proyecto

- Manager Cybersecurity

Experiencia

Actualmente gerente de Consultoría y cuenta con más de 12 años de experiencia en seguridad informática y ciberseguridad en entidades financieras, gobierno, comerciales, telecomunicaciones y de servicios.

Lideró proyectos de reingeniería de sistemas, cambios de plataformas informáticas, aseguramiento de redes, implementación y publicación de plataformas web y móviles. Identificación de vulnerabilidades sobre infraestructuras internas, externas, aplicaciones web y móviles, algunos de estos proyectos fueron desarrollados en Colombia, Brasil, Bolivia y Paraguay.

- Finalizó la carrera Ingeniería Informática - Universidad Columbia del Paraguay - 2015
- Certified Ethical Hacker – (CEH #ECC61666777133 ECCouncil – 2015)
- ORACLE 1 – Fundamentos SQL - (Centro Tecnológico UCSA - 2010)
- ORACLE 2 – Workshop Administrador I - (Centro Tecnológico UCSA - 2011)
- ORACLE 3 – Workshop Administrador II - (Centro Tecnológico UCSA – 2013
- EY Cybersecurity – Bronze – 2020

Equipo de trabajo

Nuestro Equipo cuenta con el conocimiento y las credenciales apropiadas para éste Proyecto

Micaela Marsal
Senior

Tel.: +595 (21) 664 308
Email: micaela.marsal@py.ey.com

Rol en el Proyecto

- Senior Experimentado

Experiencia

Micaela Marsal se ha incorporado a E&Y, miembro de Ernst & Young Global en Febrero de 2015 después de trabajar durante los últimos 2 años como Auditor y Consultora de TI en una Firma de Auditoria. Antes, se desempeñó como Oficial de Seguridad de una Entidad Financiera. Desde el 2015 se desempeña como Consultor Senior de la Firma Ernst & Young Paraguay Auditores y Asesores de Negocios, en el área de Consulting Services. Su formación incluye:

- Licenciada en Análisis de Sistemas (UCA)
- Especialista en Tecnología de la Información y Comunicación (UNA)
- Máster en Tecnología de la Información y Comunicación con énfasis en Seguridad de la Información. (UNA)
- ISO 27001:2013 Lead Auditor – Certificado
- ISO 27001:2013 Lead Implementer – Certificado
- ISO 20000: Lead Implementer. Certificado
- COBIT 5 Foundation – Certificado
- ITIL Fundation – Certificado
- EY Cybersecurity – Bronze – 2020

Ariel Frutos
Senior

Tel.: +595 (21) 664 308
Email: ariel.frutos@py.ey.com

Rol en el Proyecto

- Senior Experimentado

Experiencia

Ariel Frutos se ha incorporado a E&Y, miembro de Ernst & Young Global en Junio de 2010. Desde el 2014 se desempeña como Senior de la Firma Ernst & Young Paraguay Auditores y Asesores de Negocios, en el área de Consulting Services. Su formación incluye:

- Cursando el último año de la carrera de Licenciatura en Análisis de Sistemas (UNA)
- Certified Ethical Hacker – (CEH #ECC50114056436 ECCouncil – 2015)
- Cursos de administración y seguridad de plataformas Windows 2003, 2000, 2008, XP, Vista.
- CCNA1 – Fundamentos de Redes.
- CCNA 2 – Protocolos y Conceptos de Ruteo.
- CCNA 3 – Switcheo y Wireless LAN
- CCNA 4 – Accediendo la WAN

Marco Aponte
Senior

Tel.: +595 (21) 664 308
Email: marco.aponte@py.ey.com

Rol en el Proyecto

- Senior Experimentado

Experiencia

Marco Aponte se ha incorporado a E&Y, miembro de Ernst & Young Global en Octubre de 2015 después de trabajar durante el último año y medio como soporte técnico en E-Services S.R.L. Desde el 2018 se desempeña como Consultor Senior de la Firma Ernst & Young Paraguay Auditores y Asesores de Negocios, en el área de Consulting Services. Su formación incluye:

- Ingeniero de Informática (UNA) (2018)
- Certified Ethical Hacker v8 EC-Council (CEH # ECC47685436537)

Honorarios

Honorarios del proyecto

Basados en el alcance del trabajo documentado en la presente propuesta, la dedicación de nuestro equipo de trabajo y la duración presupuestada, nuestros honorarios profesionales fueron determinados conforme al siguiente esquema:

COMPONENTE	Gs (IVA incluido)
1, GAP Análisis de Seguridad CSP de SWIFT	55.000.000
2, Auditoría de Seguridad CSP de SWIFT	37.400.000

Proponemos facturar nuestros honorarios de la siguiente manera: 50% al inicio de los trabajos y el 50% posterior a la entrega Reporte de Diagnóstico, Iniciativas y Plan de Implementación. La condición de pago de dichas facturas es dentro de los treinta días de la fecha de emisión de las mismas.

Los honorarios mencionados anteriormente representan nuestra mejor estimación considerando los tópicos definidos por Ustedes y nuestra experiencia en trabajos similares, nuestros actuales costos de operación y la cooperación que estimamos recibir del personal de la Compañía que intervenga en el trabajo.

Dichos honorarios no incluyen gastos de traslado, hotel y/o alojamiento en caso de ser requerido realizar viajes al interior del país. Si se produjeran circunstancias especiales no contempladas en esta estimación o modificaciones en las condiciones económico-financieras vigentes a la fecha de esta propuesta que afecten nuestros costos de operación, esperamos poder acordar con ustedes el eventual impacto en nuestros honorarios.

EY | Assurance | Tax | Transactions | Consulting

Acerca EY

EY es líder global en servicios de Consultoría, Auditoría, Impuestos, Transacciones y Mercados de Crecimiento Estratégico.

EY se refiere a la organización mundial de firmas miembro de EY Global Limited, cada una de las cuales es una persona jurídica independiente. EY Global Limited, sociedad del Reino Unido limitada por garantía, no presta servicios a clientes.

Este material ha sido preparado únicamente con fines informativos generales y no tiene la intención de emitir una opinión profesional sobre temas relacionados a contabilidad, impuestos u otro tipo de asesoramiento.

Por favor consulte a sus asesores para recomendaciones específicas.

Para obtener más información, visite nuestra página www.ey.com.

© 2021 Ernst & Young Paraguay
Todos los derechos reservados.
ED None.

Ariel Emilio Caceres Ramirez

De: Aranda, Mariel <maaranda@deloitte.com>
Enviado el: lunes, 24 de mayo de 2021 12:26
Para: Ariel Emilio Caceres Ramirez
CC: Seguridad de la Información
Asunto: RE:Consulta y solicitud de presupuesto servicios CSP Swift

Buenas tardes Ariel,

Adjunto cotización referencial para el servicio que han consultado:

1. Ítem 1 "Consultoría CSP": G. 65.000.000 (Guaraníes sesenta y cinco millones).-
2. Ítem 2 "Auditoría CSP": G. 45.000.000 (Guaraníes cuarenta y cinco millones).-

Ambas cotizaciones incluyen el IVA.
Gracias,
Saludos,

--
Mariel Aranda
T: +595 (21) 237 5000 | C: +595 (983) 336 817
Deloitte.

From: Ariel Emilio Caceres Ramirez <acaceres@bcp.gov.py>
Sent: jueves, 6 de mayo de 2021 13:46
To: Aranda, Mariel <maaranda@deloitte.com>
Cc: Seguridad de la Información <dsi@bcp.gov.py>
Subject: [EXT] Consulta y solicitud de presupuesto servicios CSP Swift
Importance: High

Estimada Mariel,

Antes que nada, espero que te encuentres bien. El motivo de mi correo es para consultarte si actualmente están ofreciendo los siguientes servicios relacionados con Swift:

1. **Consultoría CSP (*Customer Security Program)*:** El servicio debería contemplar mínimamente la evaluación y diagnóstico del estado de implementación de los controles del CSP, recomendaciones de mejoras o controles que deben ser aplicados y el acompañamiento continuo en todas las fases del servicio.
2. **Auditoría CSP:** El servicio debe determinar el grado de implementación de los controles del CSP de Swift y emitir un informe resultante que sirva como evidencia del estado de la implementación del programa, y sea reconocido por Swift.

Te agradeceríamos si nos brindar un presupuesto estimado de los mismos.

<u>Consideraciones adicionales:</u>

- Tanto la empresa como los profesionales que llevarán a cabo los trabajos, deben contar con experiencia comprobada en la realización de estos servicios. Los profesionales pueden ser parte de la filial local de vuestra firma, como de cualquier otra filial de otros países, siempre y cuando la comunicación sea en español.
- La duración para ambos servicios debe ser de 12 meses.
- No se debe cotizar por horas de servicio, sino por servicio (Ítem 1 "Consultoría CSP" e Ítem 2 "Auditoría CSP").

- Las sesiones de acompañamiento, tanto para el ítem 1 como para el ítem 2, podrán ser llevadas a cabo de forma virtual y eventualmente de manera presencial.

Quedamos atentos ante cualquier duda o consulta adicional.
Muchas gracias.

ARIEL EMILIO
CÁCERES RAMIREZ
Dpto. de Ciberseguridad
BANCO CENTRAL DEL PARAGUAY
Federación Rusa y Augusto Roa Bastos
4to. Piso Asunción, Paraguay
E-mail: acaceres@bcp.gov.py
dsi@bcp.gov.py

Cualquier comentario, queja, reclamo o sugerencia acerca de nuestros servicios o productos, por favor envíelo a: info@bcp.gov.py

Aviso Legal: Este correo electrónico puede contener información de carácter reservado y/o confidencial perteneciente al Banco Central del Paraguay (BCP) o a terceros, y se encuentra protegida de acuerdo a lo prescripto por la Ley N° 489/95 "Orgánica del Banco Central del Paraguay" y la Ley N° 861/96 "General de Bancos, Financieras y Otras Entidades de Créditos". Sea usted el destinatario o no del presente correo (o responsable de la entrega del mensaje a la persona indicada), no podrá utilizar, copiar, reproducir o distribuir el mensaje de manera total o parcial, sin autorización previa. Los criterios, opiniones, conclusiones y otras informaciones expresadas en el presente correo electrónico, no podrán ser considerados como información oficial del BCP, salvo expresa autorización del Directorio del BCP o Dependencia autorizada por el mismo. Se han tomado todas las precauciones razonables a fin de garantizar la ausencia de cualquier tipo de software malicioso en este correo electrónico. El BCP no se hace responsable de cualquier pérdida o daño causado por el uso de correo electrónico o archivos adjuntos. No obstante se recomienda el análisis pertinente del correo, que incluya los procedimientos inherentes a la verificación de software malicioso antes de su uso. Si ha recibido este mensaje por error, notifique al BCP por correo electrónico o a la línea telefónica 595 21 608 011/60 y elimínelo inmediatamente.

Disclaimer: This email may contain proprietary and/or confidential information belonging to the Central Bank of Paraguay (CBP) or third parties, and is protected by Law 489/95 "Charter of the Central Bank of Paraguay" and Law 861/96 "General Banking, Financial and Other Credit Institutions". Whether you are the intended recipient of this mail or not (or responsible for delivering the message to the right recipient), you are not allowed to use, copy, reproduce or distribute the message in whole or in part, without prior authorization. The views, opinions, conclusions and other information expressed in this email may not be considered as official information from CBP, unless prior written authorization of the CBP's Board of Directors or Unit duly authorized by it. All reasonable precautions have been taken to ensure the absence of any malicious software in this email. The CBP is not liable for any loss or damage caused by the use of e-mail or attachments. However, the relevant analysis of the mail, including the pertinent malicious software detection methods before use, is highly recommended. If you have received this message by mistake, please notify CBP by email or telephone: 595-21-608011/60 and delete it immediately."

Deloitte refers to a Deloitte member firm, one of its related entities, or Deloitte Touche Tohmatsu Limited ("DTTL"). Each Deloitte member firm is a separate legal entity and a member of DTTL. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

[Mensaje procesado por lista blanca]

Ariel Emilio Caceres Ramirez

De: Adriana <adriana@parasursa.com.py>
Enviado el: martes, 25 de mayo de 2021 14:52
Para: Ariel Emilio Caceres Ramirez
CC: Fabrizio; Seguridad de la Información
Asunto: RE: Presentación Servicios SWIFT CSP
Datos adjuntos: Att. Banco Central del Paraguay - Presupuesto Parasur S.A..pdf

Buenas tardes Lic. Ariel,

Tengo el agrado de presentarles nuestro presupuesto estimado.

Quedo atenta a cualquier consulta.

Muchas gracias,

Saludos cordiales,

Adriana Armoa
CISO
adriana@parasursa.com.py
Fijo: +595 293 072
Movil: +595 981 366318
Avda. Ñu Guazu y Cabo Esteban Ríos

De: Ariel Emilio Caceres Ramirez <acaceres@bcp.gov.py>
Enviado el: lunes, 10 de mayo de 2021 13:15
Para: Adriana <adriana@parasursa.com.py>
CC: Fabrizio <fabrizio@parasursa.com.py>; Seguridad de la Información <dsi@bcp.gov.py>
Asunto: RE: Presentación Servicios SWIFT CSP

Buenas tardes, Adriana:
Antes que nada, muchas gracias por contactar y por el documento remitido.
Con relación al CSP, nosotros actualmente estamos requiriendo dos servicios, que serían los siguientes:

1. **Consultoría CSP (*Customer Security Program)*:** El servicio debería contemplar mínimamente la evaluación y diagnóstico del estado de implementación de los controles del CSP, recomendaciones de mejoras o controles que deben ser aplicados y el acompañamiento continuo en todas las fases del servicio.
2. **Auditoría CSP:** El servicio debe determinar el grado de implementación de los controles del CSP de Swift y emitir un informe resultante que sirva como evidencia del estado de la implementación del programa, y sea reconocido por Swift.

En este sentido, quisiéramos solicitarles si nos pudieran remitir un presupuesto estimado, teniendo en cuenta además las siguientes consideraciones:

- Tanto la empresa como los profesionales que llevarán a cabo los trabajos, deben contar con experiencia comprobada en la realización de estos servicios. Los profesionales pueden ser parte de la filial local de

vuestra firma, como de cualquier otra filial de otros países, siempre y cuando la comunicación sea en español.

- La duración para ambos servicios debe ser de 12 meses.
- No se debe cotizar por horas de servicio, sino por servicio (Ítem 1 “Consultoría CSP” e Ítem 2 “Auditoría CSP”).
- Las sesiones de acompañamiento, tanto para el ítem 1 como para el ítem 2, podrán ser llevadas a cabo de forma virtual y eventualmente de manera presencial.

Muchas gracias.

ARIEL EMILIO
CÁCERES RAMIREZ
Dpto. de Ciberseguridad
BANCO CENTRAL DEL PARAGUAY
Federación Rusa y Augusto Roa Bastos
4to. Piso Asunción, Paraguay
E-mail: acaceres@bcp.gov.py
dsi@bcp.gov.py

Cualquier comentario, queja, reclamo o sugerencia acerca de nuestros servicios o productos, por favor envíelo a: info@bcp.gov.py

---

De: Adriana <adriana@parasursa.com.py>
Enviado el: lunes, 10 de mayo de 2021 12:12
Para: Seguridad de la Información <dsi@bcp.gov.py>
CC: Fabrizio <fabrizio@parasursa.com.py>
Asunto: Presentación Servicios SWIFT CSP

Buenas tardes Señores,

Tengo el agrado de presentarles nuestros servicios de Consultoría SWIFT Customer Security Programme (CSP), esperando que pueda ser de utilidad para ustedes.

Quedo atenta ante cualquier duda o consulta.

Muchas gracias,

Saludos cordiales,

Adriana Armoa
CISO
adriana@parasursa.com.py
Fijo: +595 293 072
Movil: +595 981 366318
Avda. Ñu Guazu y Cabo Esteban Ríos

Aviso Legal: Este correo electrónico puede contener información de carácter reservado y/o confidencial perteneciente al Banco Central del Paraguay (BCP) o a terceros, y se encuentra protegida de acuerdo a lo prescripto por la Ley N° 489/95

“Orgánica del Banco Central del Paraguay” y la Ley N° 861/96 “General de Bancos, Financieras y Otras Entidades de Créditos”. Sea usted el destinatario o no del presente correo (o responsable de la entrega del mensaje a la persona indicada), no podrá utilizar, copiar, reproducir o distribuir el mensaje de manera total o parcial, sin autorización previa. Los criterios, opiniones, conclusiones y otras informaciones expresadas en el presente correo electrónico, no podrán ser considerados como información oficial del BCP, salvo expresa autorización del Directorio del BCP o Dependencia autorizada por el mismo. Se han tomado todas las precauciones razonables a fin de garantizar la ausencia de cualquier tipo de software malicioso en este correo electrónico. El BCP no se hace responsable de cualquier pérdida o daño causado por el uso de correo electrónico o archivos adjuntos. No obstante se recomienda el análisis pertinente del correo, que incluya los procedimientos inherentes a la verificación de software malicioso antes de su uso. Si ha recibido este mensaje por error, notifique al BCP por correo electrónico o a la línea telefónica 595 21 608 011/60 y elimínelo inmediatamente.

Disclaimer: This email may contain proprietary and/or confidential information belonging to the Central Bank of Paraguay (CBP) or third parties, and is protected by Law 489/95 "Charter of the Central Bank of Paraguay" and Law 861/96 "General Banking, Financial and Other Credit Institutions". Whether you are the intended recipient of this mail or not (or responsible for delivering the message to the right recipient), you are not allowed to use, copy, reproduce or distribute the message in whole or in part, without prior authorization. The views, opinions, conclusions and other information expressed in this email may not be considered as official information from CBP, unless prior written authorization of the CBP’s Board of Directors or Unit duly authorized by it. All reasonable precautions have been taken to ensure the absence of any malicious software in this email. The CBP is not liable for any loss or damage caused by the use of e-mail or attachments. However, the relevant analysis of the mail, including the pertinent malicious software detection methods before use, is highly recommended. If you have received this message by mistake, please notify CBP by email or telephone: 595-21-608011/60 and delete it immediately.”

Propuesta Comercial Banco Central del Paraguay

parasur
Tecnología a tu medida

LSQA CERTIFICADO CERTIFICATE ISO 9001:2015 REG: 2436/01
IQNet CERTIFIED MANAGEMENT SYSTEM
qualityaustria SYSTEM CERTIFIED

parasur
Tecnología a tu medida

Cotización

Consultoría y Auditoría CSP(Customer Security Program) SWIFT		
	Ítem 1 Consultoría CSP*:* El servicio debería contemplar mínimamente la evaluación y diagnóstico del estado de implementación de los controles del CSP, recomendaciones de mejoras o controles que deben ser aplicados y el acompañamiento continuo en todas las fases del servicio.	**PYG 56.000.000**
	Ítem 2 Auditoría CSP: El servicio debe determinar el grado de implementación de los controles del CSP de Swift y emitir un informe resultante que sirva como evidencia del estado de la implementación del programa, y sea reconocido por Swift.	**PYG 40.000.000**

parasur
Tecnología a tu medida

Gracias!