DIRECCION GENERAL DE IMPUESTOS

25 de mayo de 2023

PRESENTACIÓN DE OFERTA

Señores
Dirección General de Impuestos Internos (DGII)

Nosotros, los suscritos, declaramos que:

a) Hemos examinado y no tenemos reservas a la Ficha Técnica para el procedimiento de excepción de referencia, incluyendo la(s) siguiente(s) adenda(s) realizadas a la misma:

_____
_____
_____

b) De conformidad con la Ficha Técnica y según el plan de entrega especificado en el Programa de Suministros/ Cronograma de Ejecución, nos comprometemos a suministrar los siguientes bienes y servicios conexos, o ejecutar los siguientes servicios:

Item	Nro de parte	Descripción	Cantidad
1	Iso Tools	Renovación Soporte Anual 2 años Seguridad de la Información + Continuidad del Negocio	1

c) Nuestra oferta se mantendrá vigente por un período de (……) días, contado a partir de la fecha límite fijada para la presentación de ofertas, de conformidad con la Ficha Técnica de este Procedimiento de Excepción. Esta oferta nos obliga y podrá ser aceptada en cualquier momento hasta antes del término de dicho período.

d) Si nuestra oferta es aceptada, nos comprometemos a obtener una garantía de fiel cumplimiento del Contrato, de conformidad con la Ficha Técnica del Procedimiento de Excepción, por el importe del **CUATRO POR CIENTO (4%)** del monto total de la adjudicación, para asegurar el fiel cumplimiento del Contrato.

e) Para este Procedimiento de Excepción no somos partícipes en calidad de Oferentes en más de una Oferta, excepto en el caso de ofertas alternativas, de conformidad con la Ficha Técnica del presente Procedimiento de Excepción.

f) Nuestra firma, sus afiliadas o subsidiarias, incluyendo cualquier subcontratista o proveedor de cualquier parte del Contrato, no han sido declarados inelegibles por el Comprador para presentar ofertas.

g) Entendemos que esta Oferta, junto con su aceptación por escrito que se encuentra incluida en la notificación de adjudicación, constituirán una obligación contractual, hasta la preparación y ejecución del Contrato formal.

h) Entendemos que el Comprador no está obligado a aceptar la Oferta evaluada como la más baja ni ninguna otra de las Ofertas que reciba.

i) Hemos leído y entendido el Código de Ética por el cual se rige la Dirección General de Impuestos Internos.

Link: https://dgii.gov.do/transparencia/comprasContrataciones/Documents/Codigo-de-Etica-Mayo-2021.pdf?csf=1&e=h2YBkQ

Emilio Predy Perez Moquete en calidad de **Gerente de País**, debidamente autorizado para actuar en nombre y representación de **INFOSEC LATIN AMERICA INC (Sistemas Aplicativos SISAP nombre comercial).**

Firma _____

Sello

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

SNCC.F.033

Impuestos Internos

No. EXPEDIENTE

DGII-CCC-PEPU-2023-0012

DIRECCIÓN GENERAL DE IMPUESTOS INTERNOS

24 de mayo de 2023

OFERTA ECONÓMICA

NOMBRE DEL OFERENTE:

Ítem No.	Descripción del Bien, Servicio u Obra	Unidad de medida[1]	Cantidad[2]	Precio Unitario	ITBIS	Precio Unitario Final
1	Renovación Soporte Anual 2 años Seguridad de la Información + Continuidad del Negocio		1	$1,908,109.64	Exento	$1,908,109.64

VALOR TOTAL DE LA OFERTA: $1,908,109.64 **RD$**

Valor total de la oferta en letras: Un millón novecientos ocho mil ciento nueve con 64/100 Pesos Dominicanos

Emilio Predy Perez Moquete en calidad de Gerente de País, debidamente autorizado para actuar en nombre y representación de INFOSEC LATIN AMERICA, INC (SISAP- Sistemas Aplicativos nombre comercial).

Firma _____

24/05/2023

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

[1] Si aplica.
[2] Si aplica.

DISTRIBUCIÓN Y COPIAS
Original 1 - Expediente de Compras
Copia 1 – Agregar Destino

/UR.02.2011

Clasificación: Confidencial Externo

Dirección General CONTRATACIONES PÚBLICAS Transparencia para el progreso

Santo Domingo, 24 de mayo de 2023

INFOSEC LATIN AMERICA, INC
(SISTEMAS APLICATIVOS - SISAP)
RNC: 130-97411-1
Torre empresarial NOVO-CENTRO, Av. Lope de Vega No. 29, piso 7, oficina 703, Santo Domingo, República Dominicana.
Teléfono: 809-683-6538

Sres.
Comité de Compras y Contrataciones
Dirección General de Impuestos Internos (DGII)

Portafolio de servicios y soluciones

Somos Sistemas Aplicativos, (SISAP), una empresa fundada en 1985.

Nuestra casa matriz está en la ciudad de Guatemala en el país Guatemala. Tenemos presencia y oficinas en Panamá, Costa Rica, El Salvador, Nicaragua, Honduras, Colombia, Estados Unidos, México y República Dominicana. Nuestra razón social en República Dominicana es **INFOSEC LATIN AMERICA INC** con número de RNC **130974111.**

Con más de 33 años de experiencia, integramos el mejor conocimiento disponible con opciones de las tecnologías líderes en su campo, en soluciones adecuadas para resolver sus necesidades de **Seguridad de la Información, Gestión del Riesgo Tecnológico y Continuidad del Negocio,** donde hemos apoyado a clientes en toda la región de Centroamérica y República Dominicana.

Durante este tiempo hemos incursionado en muchas áreas de Tecnología de la Información, liderando el mercado a través de Innovación, Calidad y Servicio al Cliente. Diseñamos las soluciones a la medida del problema y prevemos futuras amenazas. Nuestras soluciones están destinadas a conseguir sistemas de información seguros y confiables. Tomamos en cuenta las circunstancias no informáticas imprevisibles o inevitables y que pueda afectar a su información, nos concentramos que su negocio siga caminando.

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

UBICACIONES

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

INFOSEC Latinamerica Inc.
Information Security

SISAP
Sistemas Aplicativos

¿Por qué SISAP?

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

33+ años de experiencia

Presencia en **7** países

100+ ingenieros en la región

Somos **PCI-QSA**

1000+ Certificaciones técnicas y comerciales

Soporte **24/7**

Security Service Provider **SWIFT**

190+ Colaboradores

Capacitación constante

95+ marcas aliadas

Control de **CALIDAD** constante

Laboratorio **FORENSE**

Alianzas estratégicas

Aunque SISAP tiene alianzas estratégicas con muchos players que son líderes mundiales en el campo de la seguridad, cabe destacar dos (2) alianzas estratégicas importantes que son las que se mencionan a continuación:

IBM

- Atendida por 24 de nuestros profesionales en seguridad para temas de soporte de nivel 2 y 3 desde hace más de 10 años

VERIZON

- Atendida por nuestros profesionales para hacer la entrega de programas de seguridad a diversos clientes alrededor del mundo desde 1998 como True Secure

¿Por qué son importantes estas alianzas estratégicas?

Las dos compañías más grandes y referentes a nivel mundial por ser pioneros a nivel de tecnología y seguridad de la información, han escogido de entre muchos -después de rigurosas evaluaciones- a SISAP como su aliado para entregar servicios relacionados a temas de soporte de nivel 2 y 3 a clientes internacionales y, además, la entrega de servicios para evaluar y establecer estrategias de seguridad de la información en organizaciones de renombre.

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

Ofrecemos servicios de consultoría tales como:

- Evaluación y acompañamiento en el cumplimiento estándares específicos como:
  - Acompañamiento y Auditoria PCI-DSS (Ente autorizado)
  - SWIFT (Ente autorizado)
  - Otras normativas específicas de cada país relacionadas a seguridad, gobierno electrónico y/o de T.I. como ente autorizado

- Evaluación de los controles de seguridad implementados (Ethical Hacking):
  - Análisis de vulnerabilidades
  - Pruebas de penetración (Pen Test)
  - Phishing

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

- Servicios expertos de consultoría:
  - Evaluación y creación de estrategias de seguridad de la información
  - Evaluación y asesoría en el cumplimiento de estándares y marcos de referencia de:
    - Seguridad (ISO 27001, 27002, 27005)
    - Continuidad (ISO 22301)
    - Gobierno tecnológico (CoBiT, ITIL, FiTSM)

- Evaluación y acompañamiento en el cumplimiento estándares específicos como:
  - PCI-DSS (Ente autorizado)
  - SWIFT (Ente autorizado)
  - Otras normativas específicas de cada país relacionadas a seguridad, gobierno electrónico y/o de T.I. como ente autorizado

- Evaluación del riesgo
  - En forma cualitativa a través de controles esenciales de seguridad
  - En forma cualitativa a través de los procesos de negocio de la organización y un catálogo de amenazas
  - En forma cuantitativa a través de un modelo de cálculo del riesgo, probabilidad de ocurrencia, impacto en el negocio, tendencias y predicciones

- Programas de seguridad de la información certificables
  - Verizon Security Management Program

- Programa anual de revisión de controles de seguridad físicos, lógicos
- Asesoría por parte de expertos en el cumplimiento de controles
- Acceso a obtener una certificación por parte de Verizon como consecuencia de haber implementado todas las prácticas de seguridad esenciales y que han sido evaluadas en cuanto a su efectividad y cumplimiento

➢ Servicios de análisis forense

➢ Proveedor de servicios gestionados de seguridad (MSS)

  - SOC
  - Colección y correlación de eventos
  - Monitoreo 24x7
  - Reporte y seguimiento a alertas
  - Reportes periódicos

Ofrecemos soluciones para las siguientes verticales de seguridad, donde es importante resaltar que brindamos los servicios de implementación, soporte 24x7, capacitación para los administradores y operadores, y además si es fuese necesario servicio de monitoreo y administración gracias a nuestro Security Operation Center (SOC):

- Creación de Métricas y tableros: ISO Tools.
- Gestión de vulnerabilidades: Qualys, Rapid7, Tenable, Beyond Trust.
- Endpoint Protection: Kaspersky, McAfee, Trend Micro, Symantec, Sophos
- FIM: Tripwire, Qualys, Beyond Trust.
- MDM/EMM: BlackBerry, Airwatch.
- DLP/DRM: Symantec, Forepoint, McAfee, Imperva, Titus
- Criptografía: Vormetric, Microfocus
- Protección de base de datos: Imperva, McAfee
- WAF: Imperva, Whitehat, Veracode
- NAC: Cisco, ForeScout
- Autenticación Robusta: HID, RSA, Gemalto
- Administración de Usuarios Privilegiados: Beyond Trust, CyberArk
- Control de navegación: Cisco, Symantec, Forcepoint, McAfee, Palo Alto
- Email Security: Cisco, Proofpoint, McAfee
- IAM: RSA, Microfocus,
- WIFI: Purple, Cisco Meraki
- Protección Perimetral: Palo Alto, Cisco, Watchguard, Sophos, Forcepoint, Barracuda.
- IPS: Cisco, Trend Micro, McAfee, Palo Alto
- Filtrado de reputación: Risk Analytics
- Optimización de Ancho de Banda: Symantec, Exinda

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

- Seguridad DNS: Infoblox
- Enlace dedicados: Ufinet
- Balanceadores de carga: A10, Brocade
- DDOS: Arbor, Imperva, Radware
- Optimización de firewall: Firemoon, Algosec
- Pruebas de volumen: Redwolf, Ixia
- Backup: Veritas, Barracuda, Arcserve, Veeam
- Investigación Forense: Passware, Symantec, Cellebrite, Guidance, EnCase…
- Monitoreo de Usuarios: Veriato
- Peritaje: EnCase, Cellebrite, Digital Intelligence
- Recuperación de Información: Kroll Ontrack
- SIEM: McAfee on premise y como as a Service, RSA, Alien Vault, LogRhythm
- Visibilidad: RSA, Exinda, Symantec
- Detección de Malware Avanzado: FireEye, Cisco, Palo Alto, Encase Endpoint Security, Trend Micro, Sophos
- Anti- Fraude: Easy Solutions
- Threat Intelligence & Security Analytics: Anomali, BluVector, Rank
- Respuesta a Incidentes: Guidance, Encase Endpoint Security, Symantec
- Elaboración de planes de respuesta a incidentes: servicio de SISAP en conjuto con Verizon

Ofrecemos Capacitaciones de:

- Terranova para concientizar a los usuarios de la organización
- Somos representantes de ISC2 para impartir sus training
- COBIT® 5 Foundation
- ITIL fundamentos 2011
- ITIL niveles Intermedio y Experto
- Implementador Líder ISO 27001:2013 Certificado
- Auditor ISO 27001:2013 Certificado
- Implementador ISO 22301 Certificado BCP
- Auditor ISO 22301 Certificado BCP
- ISO 27005 IT Risk Managment
- Implementador ISO 20000 Certificado
- Auditor ISO 20000 Certificado
- ISO 31000 Riesgo Integral
- Curso taller teóricopráctico BIA -Business Impact Analysis-
- Information Security RiskManagement
- Principios y prácticas para la gestión de Proyectos

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

- Estándares y buenas prácticas en Administración de proyectos con enfoque PMI
- PMP BOOTCAMP Seminario de preparación para la certificación Certified Information System Auditor –CISA
- Curso PCI
- Entrenamiento Redes Inalámbricas
- OWASP TOP 10 y OWASP TOP 10 Controles Proactivos
- Curso Taller de Desarrollo Seguro
- SKILLBRIDGE
- KNOWBE4

Sin otro particular, nos despedimos de ustedes, no sin antes informarles que estamos a su disposición para cualquier consulta.

Atentamente,

Emilio Perez

Representante Legal

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

España, 24 de mayo de 2023

Estimados Sres de la Dirección General de Impuestos Internos,

La presente carta es para informar que la siguiente empresa está autorizada para comercializar ISOTools en República Dominicana y es único representante de ISOTools para la línea de soluciones de Seguridad de la Información y Continuidad del Negocio, como Aliado Estratégico Preference.

Esta Alianza finaliza el 31 de Diciembre de 2025 si alguna de las partes manifiesta ésta intención, en caso contrario, se prorroga por períodos de 12 meses automáticamente.

Nombre	RNC	Mail
SISAP Infosec Latinamerica	130974111	Emilio.Perez@sisap.com

Esta compañía se encarga de la venta, implementación, capacitación y puesta en marcha de la herramienta en las entidades públicas y privadas del mencionado país.

Siendo ISOTools, la solución informática para los sistemas de Gestión ISO y los modelos de excelencia (ISOTools – www.isotools.org), desarrollada y de propiedad exclusiva de COINNOVA (Proyectos y Consultoría de Innovación Tecnológica, S.L.).

Atentamente,

Marco Sevillano

Dirección ISOTools

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

Santo Domingo, 24 de mayo de 2023

INFOSEC LATIN AMERICA, INC
(SISTEMAS APLICATIVOS - SISAP)
RNC: 130-97411-1
Torre empresarial NOVO-CENTRO, Av. Lope de Vega No. 29, piso 7, oficina 703, Santo Domingo, República Dominicana.
Teléfono: 809-683-6538

Sres.
Comité de Compras y Contrataciones
Dirección General de Impuestos Internos (DGII)

Carta constancia de aceptación de los términos de pago, requerimientos, tiempo de entrega, penalidad y garantía según lo establecido en el presente formato.

Por medio de la presente queremos extenderles nuestra aceptación de los términos de pago, requerimientos, tiempo de entrega, penalidad y garantía según lo establecido en el pliego de **DGII-CCC-PEPU-2023-0012: "Renovación de soporte de módulo de Seguridad de la Información y Continuidad de Negocios. Plataforma ISOTOOLS, soporte anual dos (2) años".**

Sin otro particular, nos despedimos de ustedes, no sin antes informarles que estamos a su disposición para cualquier consulta.

Atentamente,

Emilio Perez

Representante Legal

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

CERTIFICADO

OCA Instituto de Certificación, S.L.U.

Certifica el sistema de gestión de la seguridad de la información
de la organización

PROYECTOS Y CONSULTORÍA DE INNOVACIÓN TECNOLÓGICAS, S.L. (ISOTOOLS EXCELLENCE)

Pol. Ind. Tecnocordoba - C/ Villnius, 6 11 H6. 14014 Córdoba

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

conforme con la norma:

UNE-ISO/IEC 27001:2014

aplicable a:

Los sistemas de información que dan soporte al diseño, desarrollo y mantenimiento de aplicaciones informáticas. Alojamiento de aplicaciones informáticas.

SOA versión del 07/04/2020

Certificado nº: 34/5700/17/0404

Fecha certificación inicial: 02/05/2017
Fecha certificación ciclo actual: 02/05/2020
Fecha de caducidad: 02/05/2023
Fecha auditoría renovación: 03 y 17/04/2020
Fecha de emisión de certificado: 02/05/2020

Este certificado sustituye al certificado con fecha de emisión: 02/05/2017

INTERNATIONAL ACCREDITATION FORUM
ENAC CERTIFICACIÓN Nº 8/C-SG057

David Lao
Director General
OCA INSTITUTO DE CERTIFICACIÓN S.L.U.

ISOTools

SISAP
Sistemas Aplicativos

SOFTWARE DE GESTIÓN PARA LA EXCELENCIA EMPRESARIAL

Propuesta técnica para DGII

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

Resumen ejecutivo

Objeto

El objeto de la propuesta es renovar la plataforma ISOTools para la gestión y automatización de los sistemas de gestión de Seguridad de la Información y de Continuidad del Negocio.

Alcance

El alcance de la propuesta es renovar el soporte de la plataforma ISOTools para los módulos de Seguridad de la Información y de Continuidad del Negocio para 25 usuarios.

- Periodo: Del 01-JUL-2023 al 30-JUN-2025

Modalidad a contratar

Modalidad On Premise. Plan de Soporte Corporate.

Módulos y Add-Ons a incluir

- Soporte Seguridad de la Información
- Continuidad del Negocio

Nº de usuarios a contratar

25 usuarios que dispone DGII

Plazos aproximados de ejecución

24 meses

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

Algunos clientes internacionales que ya han confiado en ISOTools

Colpensiones
AXA COLPATRIA reinventando los seguros
terpel
falabella
enel
CEMEX
ENAP
NUEVOPUDAHUEL
Coca-Cola
Televisa
VEOLIA
PEPSICO
ECOLAB
ANDREANI
LUZ DEL SUR
Parker
SGS
ARKEMA INNOVATIVE CHEMISTRY
entel
LAP LIMA AIRPORT PARTNERS
Talma SERVICIOS AEROPORTUARIOS
celepsa
NEPTUNIA
TPP Terminales Portuarios Peruanos

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

Clasificación: Confidencial Externo

SLA de acceso y uso

1. Introducción y Objetivos
2. Servicio y Atención al cliente
3. Disponibilidad de Acceso y Uso
4. Priorización de Incidencias y Peticiones de Servicio
5. Cargas de Trabajo
6. Informes de Servicio
7. Comunicaciones
8. Penalizaciones
9. Exclusiones

ELABORADO POR	REVISADO Y APROBADO POR	HISTÓRICO DE CAMBIOS			
Marta Cobos	Gema Ariza	NOMBRE	VERSIÓN	FECHA	HCO CAMBIOS
		SLA acceso y uso	4	20/06/2013	Separar de catálogo de servicios. Revisar servicio de acceso y uso.
		SLA acceso y uso	5	14/02/2014	Revisión y modificación de contenidos.
Ana Montero		SLA acceso y uso	6	25/10/2014	Revisión estructura y actualización de contenidos.
Marta Cobos		SLA acceso y uso	7	01/01/2018	Revisión y modificación de contenidos.
Marta Cobos		SLA acceso y uso	8	25/04/2018	Inclusión de soporte internacional.

SLA de acceso y uso

1. Introducción y Objetivos

SLA del Servicio se define como los servicios de acceso a la herramienta ISOTools y el uso de funcionalidades y módulos según la oferta contratada.

Estos servicios se prestan de la siguiente manera:

- Acceso y uso de ISOTools a través de https://siu.isotools.org (o cualquier subdominio de isotools.org) o mediante servidores compartidos en modalidad clúster con back-up en https://siu.isotools.eu y en https://siu.isotools.es para acceso alternativo en modo lectura.

2. Servicio y Atención al Cliente

Horarios

El horario del servicio de acceso y uso de ISOTools es de 7x24 los 365 días del año. Para dichos servicios, el horario de atención al cliente es:

ESPAÑA (CASA MATRIZ)	CHILE	COLOMBIA	MÉXICO	PERÚ	INTERNACIONAL
Lunes a Viernes 08:00 a 19:00	Lunes a Viernes 08:30 a 18:30	Lunes a Viernes 08:00 a 18:00	Lunes a Viernes 09:00 a 18:00	Lunes a Viernes 08:00 a 18:30	Lunes a Viernes 08:00 a 18:30 GTM-5

* No habrá atención al cliente en festivos nacionales e internacionales.

Periodo de validez del SLA

La validez del presente acuerdo de nivel de servicio estará definida dentro de la relación comercial entre el cliente y la empresa dejando de ser aplicable en el momento en el que esa relación sea interrumpida por alguna de las causas recogidas en el acuerdo de licencia de usuario final.

Este acuerdo se revisará con el cliente en los periodos de renovación del contrato (normalmente de manera anual) o cuando el cliente lo solicite expresamente y lo revise con el departamento comercial.

3. Disponibilidad de Acceso y Uso

Disponibilidad de acceso a la plataforma

El cálculo de la disponibilidad se realizará mediante la siguiente fórmula:

Disp = 100 x (T - Tc) / T

Dónde:

- *Disp = % de disponibilidad del servicio (disponibilidad de conectividad y acceso)
- **T = Tiempo total anual
- ***Tc = Tiempo transcurrido desde la caída del servicio hasta la restitución de la conectividad al servicio, excluyéndose mantenimientos programados

Este tipo de incidencias se categorizan como incidencias de prioridad Muy Alta.

El valor de disponibilidad del servicio será como mínimo del 99,5% anual, siendo el periodo máximo sin servicio de 12 horas naturales continuado. Ante interrupciones del servicio superiores a este tiempo, la empresa pondrá en marcha el plan de continuidad y disponibilidad del servicio.

Disponibilidad de uso de la plataforma

Las incidencias registradas por el usuario o cliente en relación a la degradación de los servicios de uso de ISOTools cuentan con un acuerdo de nivel de servicio orientado al tiempo de respuesta de dichas incidencias, según su priorización por parte del operador, desde el momento que son registradas, pasando por su categorización y su necesidad de escalamiento hasta el inicio de su análisis para la resolución por parte del especialista a quien haya sido asignado. Igualmente existe un compromiso de respuesta ante las peticiones de servicio registradas.

Para garantizar la detección de incidentes y errores del sistema antes de que impacten en los procesos del cliente la empresa realiza mantenimiento preventivo de ISOTools mediante pruebas periódicas y controles.

Esta es la categorización de las incidencias de uso y peticiones de servicio y su nivel de respuesta en función del Plan de Soporte contratado:

	PLAN BASIC	PLAN PROFESSIONAL	PLAN CORPORATE	
PRIORIDAD	HORAS RESPUESTA A INCIDENCIAS Y PETICIONES DE SERVICIO			CUMPLIMIENTO
Muy alta	16	12	8	99%
Alta	24	16	12	95%
Media	32	24	16	90%
Baja	40	32	24	85%

Dónde:

- **Prioridad** = establecida por el operador
- **Tiempo de respuesta** = horas hábiles (de 09:00 a 17:00) desde el registro de la incidencia hasta el inicio de las tareas de resolución.
- **% de cumplimiento** = compromiso de cumplimiento del tiempo de respuesta establecido respecto del total de incidencias, según la tipología.

4. Priorización de Incidencias y Peticiones de Servicio

A. Incidencia

Definimos Incidencia como cualquier incidente que cause una interrupción en el servicio de **acceso y uso** de la plataforma ISOTools. Son las que se generan cuando falla alguna opción específica dentro de la aplicación que imposibilita realizar alguna operación (**por ejemplo: acceder a la aplicación, completar una encuesta, subir un documento, finalizar un flujo o parametrizar un campo de un reporte**).

B. Petición de servicio

Definimos **Petición de Servicio** como las solicitudes que los usuarios pueden plantear para mejorar el servicio, no cuando éste falla. Peticiones de servicio son:

- solicitudes de información o consejo,
- peticiones de cambios estándar (el usuario olvida su contraseña y solicita una nueva, cambio de logo,...)
- y peticiones de acceso a servicios (aumento del número de usuarios, acceso a nuevas aplicaciones...)

C. Mejora

Definimos **Mejora** como el requerimiento de cualquier optimización del servicio de acceso y uso de ISOTools como la inclusión de opciones que consideran de mejor aplicabilidad para su centro, por ejemplo: requerir columnas adicionales, poseer más filtros de los estándares, tener accesos directos diferentes. Son en definitiva cambios en la configuración normal del servicio o desarrollos nuevos.

El acuerdo de nivel de servicio se establece únicamente para las **Incidencias** y las **Peticiones de Servicio**.

ISOTools atiende las incidencias y las peticiones de según la PRIORIDAD que establecen nuestros operadores, que se calcula en función del Impacto y la Urgencia, para lo que se sigue la siguiente tabla:

Definición de impacto

El impacto es establecido por el operador N1 en la clasificación del ticket en base a estos criterios:

IMPACTO	AFECTA A	INCIDENCIA	PETICIÓN SERVICIO
MUY ALTO	Todo el sistema / todos los usuarios.	El sistema se encuentra fuera de servicio. **Por ejemplo:** caída del sistema o imposibilidad de ingresar con su usuario.	**Por ejemplo:** pérdida de clave.
ALTO	Toda una aplicación / un grupo de usuarios.	El sistema funciona, pero es imposible el acceso o uso a una o varias de las aplicaciones y a todas sus funcionalidades. **Por ejemplo:** no acceso a la aplicación de NC o existe lentitud extrema para todos los usuarios que imposibilita el trabajo.	**Por ejemplo:** dar de alta una aplicación, dar de alta usuarios.
MEDIO	Una funcionalidad concreta de ejecución de una aplicación.	Existe una afectación moderada del sistema. Inestabilidad con interrupciones periódicas del servicio o pérdida menor de funcionalidad. **Por ejemplo:** Dar de alta una NC, crear un documento o imprimir un reporte. También se incluye lentitud moderada del sistema.	**Por ejemplo:** consulta sobre la operación de una aplicación.
BAJO	Una función de configuración de una aplicación.	Afectación pequeña del sistema. El cliente es completamente capaz de operar con el sistema, pero hay alguna incidencia vinculada a la configuración, la cual se puede postponer. **Por ejemplo:** crear un campo personalizado en NC.	**Por ejemplo:** consulta o duda sobre una operación de parametrización.

Definición de urgencia

La urgencia es establecida por el operador N1 en base a lo especificado por el cliente / usuario en el ticket:

URGENCIA	DESCRIPCIÓN
!! MUY ALTA	El cliente ha comunicado y se encuentra dentro de fechas establecidas de reuniones / eventos con un impacto externo a la organización: Auditorías Externas, reuniones con clientes / proveedores o bien actividades programadas específicamente para el día o día posterior que sucede la incidencia o se requiere del servicio (p.e. estamos realizando unas inspecciones en el día de hoy)
! ALTA	El cliente ha comunicado y se encuentra dentro de fechas establecidas de reuniones / eventos de impacto interno (Auditoría Interna, Presentación de Resultados, Capacitaciones) o bien para actividades con fechas programadas (p.e vamos a realizar unas inspecciones la próxima semana).
– NORMAL	El cliente no ha comunicado ningún tipo de fechas de reuniones establecidas o actividades programadas.

Nivel de Prioridad en función de Urgencia e Impacto

Cálculo de la prioridad del ticket (incidencia / petición de servicio).		URGENCIA		
		NORMAL	! ALTA	!! MUY ALTA
IMPACTO	MUY ALTO	Alta	Muy Alta	Muy Alta
	ALTO	Media	Alta	Muy Alta
	MEDIO	Baja	Media	Alta
	BAJO	Baja	Baja	Baja

Los tiempos de respuesta quedan establecidos en función de:

- La categorización del ticket en Incidencia / Petición de Servicio por el operador N1.
- La PRIORIDAD dada por el operador N1 de la incidencia / petición de servicio en base a IMPACTO y URGENCIA.
- El Plan de Soporte contratado por el cliente.

Se considera que la Incidencia / Petición de Servicio se ha respondido cuando:

- El operador N1 ha categorizado el ticket.
- El operador N1 ha priorizado el ticket.
- Se revisa el ticket, se analiza su causa y se comienza a resolver, bien por N1, N2 o N3 dando una respuesta al cliente.

5. Cargas de trabajo

Disponibilidad de recursos para garantizar el servicio de uso de ISOTools

El servicio de atención al cliente de ISOTools trabaja con un Help Desk mediante el cual se gestionan todas las incidencias y peticiones del servicio tal y como se describen en el catálogo de servicios.

Para la prestación del servicio ISOTools dispone de los recursos humanos por cliente necesarios para atender las incidencias y demás notificaciones que puedan generarse en el desarrollo de su proyecto.

Las cargas de trabajo asumibles por el personal de soporte técnico varía en función del tipo de incidencia y/o notificación, y de la solución técnica a aportar.

Los recursos humanos disponibles para atender estas cargas de trabajo, se distribuyen en 3 tipologías:

- Técnico N1 de primera atención.
- Técnicos N2 de segundo nivel, con mayores conocimientos de los proyectos.
- Técnicos N3 que son técnicos programadores y de sistemas.

Anualmente realizamos un informe de capacidad en el que tenemos en consideración el número de recursos humanos para prestar un servicio de calidad y establecemos previsiones futuras de crecimiento y las necesidades que debemos abordar de manera preventiva

6. Informes de servicio

Con periodicidad anual, se elaborará un informe de servicio que se hará llegar al cliente mediante alguno de los medios de contacto indicados por el cliente. En este informe se comunicarán al cliente los principales resultados y el nivel de cumplimiento de los acuerdos establecidos para la prestación de servicio durante el período considerado.

7. Comunicaciones

Ante interrupciones del servicio prolongadas

La empresa cuenta con un Plan de Contingencias cuyo objetivo principal es el de garantizar la pronta recuperación de los servicios de acceso a ISOTools frente a diferentes escenarios de catástrofe.

Dicho plan será activado según la evaluación de la situación realizada por el comité de crisis. En caso de activación esta situación será comunicada a los clientes mediante medios disponibles dependiendo de la naturaleza de la catástrofe (mensaje plataforma, emails, teléfono, etc).

Mantenimiento programado

Se avisará mediante mensaje llamativo en la plataforma, sólo disponible a los administradores, desde 48 horas antes Siempre se intentará programarlo los sábados en horario nocturno en casa matriz para minimizar impacto en cliente.

Mantenimiento de urgencia

Se avisará mediante una pantalla al acceder a la plataforma, con un mensaje especificando el tipo de mantenimiento que se está realizando e indicando la duración aproximada del mismo.

8. Penalizaciones

Proceso de reclamación

Para facilitar la notificación de reclamaciones por parte del cliente debido a su disconformidad en la prestación de los servicios de acceso y uso de ISOTools o en la gestión de la relación con las diversas áreas de la empresa (comercial, administración, dirección técnica, etc.) se pone a su disposición un mecanismo para el registro y seguimiento de dichas reclamaciones en la página principal de acceso a HelpDesk. Este mecanismo es el mismo mediante el cual se registra incidencias o peticiones de servicio y que se detalla en el procedimiento de gestión de las relaciones del negocio.

Penalizaciones

Para el acuerdo de nivel de servicio de acceso a ISOTools se tomará en cuenta la cuota anual del cliente y se realizará el cálculo proporcional a las horas de disponibilidad esperadas (dentro del acuerdo) respecto de las interrupciones que excedan el nivel de servicio acordado.

1. Penalización por no disponibilidad del servicio acumulado anual

- DS = Disponibilidad del servicio = 24 x 365 = 8.760 horas
- Compromiso de disponibilidad acordado = 99,5% = 8.716,2 horas
- Penalización por incumplimiento = CA x TD / DS
  - CA = Cuota anual
  - TD= Tiempo de no disponibilidad que exceda del acuerdo DS

2. Penalización por no disponibilidad del servicio superior al máximo consecutivo (12 horas)

- DS= Disponibilidad del servicio = 24 x 365 = 8.760 horas
- Compromiso de no indisponibilidad acordado consecutivo = 12 horas
- **Penalización por incumplimiento = CA x TI / DS**
  - CA = Cuota anual
  - TI = Tiempo de indisponibilidad consecutivo excedido de 12 horas

Para el **acuerdo de nivel de servicio de uso** de ISOTools se tomará en cuenta un porcentaje de la cuota anual del cliente y se realizará el cálculo proporcional al tiempo de respuesta esperado sobre **incidencias blockers de uso respecto** del tiempo que exceda el nivel de servicio acordado.

Esta penalización solo será aplicable si el porcentaje de cumplimiento es inferior al 99% de las incidencias totales anuales por cliente.

Tiempo de respuesta a incidencia blocker de uso = 8 horas (tiempo máximo).

Penalización por incumplimiento = 0,1% CA x TRE / TR

- CA = Cuota anual
- TRE = Σ de tiempo de respuesta a incidencia grave excedido
- TR = Tiempo de respuesta a incidencias graves acordado

Todas las penalizaciones serán abonadas mediante descuentos sobre la cuota anual al siguiente periodo.

9. Exclusiones (Cuándo no aplica este SLA)

El acuerdo de nivel de servicio no es de aplicación en caso de que el cliente no pueda acceder o usar la herramienta ISOTools debido a:

- Mantenimiento programado que se avisará mediante mensaje llamativo en la plataforma, sólo disponible a los administradores, desde 48 horas antes. Siempre se intentará programarlo los sábados en horario nocturno en sede central.
- Circunstancias ajenas al control de ISOTools, incluyendo, sin limitación, las motivadas por causas de fuerza mayor. Se consideran fuera del control de ISOTools, entre otros, los siguientes elementos o recursos:
  - Errores de configuración y/o parametrización de ISOTools por parte del cliente.
  - El sistema informático del usuario/s, versiones obsoletas.
  - Software de navegación o de conexión y accesorios del usuario, versiones obsoletas (por ejemplo en Internet Explorer se soportará la versión actual en el mercado hasta -2 versiones).
  - Software malicioso, nocivo o perjudicial en el equipo del usuario.
  - La infraestructura de transporte de datos o telecomunicaciones (incluida la propagación de DNS y configuraciones de cortafuegos) que no dependa de ISOTools o sus suministradores.

- Incumplimiento de una o más bases de prestación de servicio (ALUF) e impago de las cuotas del servicio contratado, razones por las cuales ISOTools se reserva el derecho a desactivar, suspender o desconectar el servicio contratado por el cliente mediando aviso previo, o no, según la urgencia y gravedad.
- Se excluye de este acuerdo de nivel de servicio plazos o compromisos de respuesta a cualquier sugerencia o petición de cambio sobre el servicio de acceso y uso de ISOTools modo SaaS reservándonos el derecho de aplicar, o no dichas sugerencias tras realizar su evaluación pertinente.

Planes de Soporte

Cuando contrata una solución de ISOTools, es recomendable hacerlo bajo un plan de soporte.

A continuación se detallan las características de los diferentes planes de soporte, el cual irá atado al alcance contratado y al perfil de su compañía.

¿Qué disfruta contratando el plan de soporte?

- Actualizaciones permanentes mientras esté en soporte.
- Los servicios que incluya su plan de soporte.
- Las funcionalidades añadidas que incluya su plan de soporte.

PLAN	¿QUÉ CUBRE?	¿PARA QUIÉN ES?
BASIC	Soporte técnico para incidencias y actualización continua de las aplicaciones.	Organizaciones que utilizan ISOTools para procesos de baja criticidad, involucrando a pocas personas y en sistemas de gestión sencillos.
PROFESSIONAL	Soporte remoto personalizado. Transferencia de conocimiento sobre el uso operacional de las aplicaciones.	Organizaciones que utilizan ISOTools para sistemas de gestión más complejos, y que involucran a varias áreas de la organización. Poseen necesidades de integración e interactuación externa.
CORPORATE	Soporte remoto prioritario, con compromisos de respuesta y capacidad para negociar tiempos de resolución a incidencias. Capacidad de integración e interactuación externa. Horas de personalización y asesoramiento.	Organizaciones con un sistema de gestión complejo que involucra a toda la organización en procesos de máxima criticidad que requieren alta disponibilidad, confiabilidad y eficacia operacional. Requieren, además, de personalización (mantenimiento adaptativo).

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

Características / Servicios incluidos	B BASIC	P PROFESSIONAL	C CORPORATE
CARACTERÍSTICAS PRINCIPALES			
Qué normas y modelos permite	QMS	Todas (no BI)	Todas
Gestión Multisede	NO	Máximo 5	Ilimitado
CARACTERÍSTICAS DEL PLAN DE SOPORTE			
Acceso de usuarios externos	✗	✗	✓
Posibilidad de Integración con Office 365	✗	✗	✓
WIP con posibilidad de diseño	✗	✓	✓
Geolocalización	✗	✓	✓
Capacidad de gestionar flujos avanzados	Ninguno por defecto	✓ Análisis contexto ✓ PPII ✓ Capacitación ✓ Revisión dirección ✓ Planes de Mejora ✓ Proveedores ✓ Producto No Conforme ✓ Emergencias ambientales ✓ Inspecciones ✓ Incidentes	Todos
Nº de Workflows Gestor Documental	1 por defecto	3	ilimitado
Editor Avanzado Gestor Documental	✗	✓	✓
Personalización de avisos en flujos	✗	✗	✓
Integración con otras soluciones	✗	Web Services	Web Services
Integración con AD	✗	✗	✓

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.

Características / Servicios incluidos	B BASIC	P PROFESSIONAL	C CORPORATE
SERVICIOS DEL PLAN DE SOPORTE			
Actualizaciones de software	✔	✔	✔
Permite Modificaciones al software	✕	✕	Previo estudio y cotización
Métodos de Contacto para soporte	HelpDesk	HelpDesk	Chat, Tlf, HelpDesk
Asistencia técnica a través de control remoto	✕	✕	✔
Contactos autorizados de soporte	1	1	3
Support Account Manager	✕	✕	✔
Tiempo máximo respuesta incidencias Blocker	16 horas	12 horas	8 horas
Análisis de nuevos requisitos y necesidades	✕	✔	✔

Características y Servicios de los Planes de Soporte

- **Actualizaciones del Software:** Tendrás derecho de acceso a las actualizaciones de ISOTools Excellence y a las nuevas versiones, que contemplan todas nuestras innovaciones en requisitos funcionales, tecnológicos y ergonómicos.

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R. D.

- **Modificaciones al software:** Es el mantenimiento adaptativo. Optando por el plan Corporate Premium podrás solicitar desarrollos adaptados a tus requerimientos. Estas acciones las estudiamos y decidimos si son viables o no (van en contra del propio funcionamiento de la plataforma) y las ejecutamos siempre bajo presupuesto.
- **Vías de Contacto para soporte:** Todos los clientes de ISOTools Excellence, de acuerdo con su plan de soporte, cuentan con unos métodos de contacto establecidos para que puedan resolver sus dudas y cualquier incidencia que pueda presentarse en la herramienta. Estos métodos son: help desk, teléfono y chat.
- **Asistencia técnica a través de control remoto:** Es el soporte que te prestamos como si estuviésemos contigo sentados en tu oficina. Realizamos una intervención directa a través de control remoto sobre tú sistema para resolver incidencias o consultas.
- **Contactos autorizados de soporte:** Es el número máximo de personas que podrás designar en tu empresa y que podrán entrar en contacto con el nuestro centro de soporte. De esta forma os podemos proporcionar continuidad y construiremos el conocimiento técnico y de negocio entre ambas partes para mejorar el servicio.
- **Support Account Manager:** ¿Siempre quieres ser atendido por un mismo consultor que te conozca a ti y tu proyecto?. ISOTools Excellence te designa un support account manager que centralizará la atención del cliente
- **Tiempo Máximo de Respuesta Incidencias Blocker:** El tiempo máximo de respuesta indica el tiempo en el que nos comprometemos a responder a tus solicitudes de soporte. Este tiempo se verá afectado por la prioridad de la solicitud.
- **Análisis de nuevos requisitos y necesidades del cliente:** Anualmente, un consultor experto realizará una auditoría inductiva, valorada en una sesión de trabajo, del uso de ISOTools Excellence en tu organización proponiéndote mejoras en base su evaluación.

INFOSEC LATIN AMERICA, INC.
RNC: 130974111
Santo Domingo, R.D.