Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

INF-0214/22

INFORME SOLICITUD DE AUTORIZACIÓN

INSTITUTO NACIONAL DE FORMACIÓN TÉCNICO PROFESIONAL

INFOTEP

INFOTEP-CCC-LPN-2022-0002

OCTUBRE 14, 2022.-

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Informe

Luego de un cordial saludo, sirva la presente para exponer consideraciones de la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC), respecto al proceso de compra para la **adquisición de equipos informáticos,** el cual se nos ha presentado como secretaría técnica del gabinete de transformación digital, a fin de evaluar.

Observaciones:

- Se adjunta carta de solicitud
- Se adjunta justificación de compra
- Se adjunta pliego de condiciones

A groso modo se solicita:

Lotes	Item	Descripción	Cant
Lote I- Renovaciones	**1**	**FortiGate 300D Serial: FGT3HD3917803315/** FGT3HD3915800916 Trade-Up 300F (3 años), Incluye configuracion e instalacion (Oficina Nacional) Licencia 360 Protection Bundle.. Debe incluir las siguientes tecnologías de protección, detección, prevención y soporte: Control de aplicaciones NGFW, Servicio de prevención de intrusiones (IPS), Antivirus, Seguridad de botnet, Reputación de IP / dominio, Servicios de seguridad móvil, Filtrado web, Antispam, FortiSandbox Cloud, Servicios de protección contra ataques de virus (VOS), Desarmado y reconstrucción de contenido (CDR), Clasificación de seguridad, Servicio de Seguridad Industrial, FortiGate Analytics & Management,	2

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Overlay Orchestration, Automation y Monitoring. Soporte FortiCare. 3 años	
	2	Renovación Suscripción por 3 años Cisco Webex: Webex Room, Reuniones avanzadas de espacios, Suite de Webex Meetings, Mensajería avanzada, Control Hub Paquete Pro y Soporte Equipos Telepresencia Cisco Webex: 4 Cisco Webex Room Kit, 1 Cisco Webex Room Kit Pro Precision 60, 4 Cisco Webex Board 70S (incluir A-MST-WX Cisco Webex Video Integration for Microsoft Teams (SVS-FLEX-SUPT-BAS Basic Support for Flex Plan, A-MST-WX-CVI-ROOMS Cisco Webex Video Int for MS Teams CVI per Active Endpoint)	1
	3	**Enterprise Agreement: 36 Meses** **ISE-SEC-SUB Cisco Identity Service Engine Subscription** 1 ISE-E-LIC Cisco Identity Service Engine Essentials Subscription 1500 ISE-A-LIC Cisco Identity Service Engine Advantage Subscription 1000 ISE-P-LIC Cisco Identity Service Engine Premier Subscription 1300 SVS-ISE-SUP-E Enhanced Support for Identity Service Engine Subscription 1 **L-AC-APX-LIC= Cisco AnyConnect Apex Term License, Total Authorized Users** 1300 L-AC-APX-3Y-S5 Cisco AnyConnect Apex License, 3YR, 1000-2499 Users 1300 **L-LC-TI-FC1K= Cisco Secure Network Analytics Threat Intelligence -FC1K Lic** 1	1

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		L-LC-TI-FC1K-3Y Cisco Secure Network Analytics Threat Intelligence 3Y FC1K	1	
		L-ST-FR-LIC= Cisco Secure Network Analytics Flow Rate License	2550	
		L-ST-FR-3Y-S3 Cisco Secure Network Analytics Flow Rate 3Y, 2,500-4,999	2550	
		UMB-SEC-SUB Cisco Umbrella Security Subscription	1	
		SVS-UMB-SUP-E Enhanced Support for Umbrella	1	
		UMB-SIG-ESS-K9 Cisco Umbrella Secure Internet Gateway Essentials	1100	
		AMP4E-SEC-SUB Cisco Secure Endpoint XaaS Subscription	1	
		AMP4E-ADV-CL-LIC Cisco Secure Endpoint Advantage Tier Subscription	1100	
		TG-AMPADV-K9 Cisco Secure Malware Analytics Cloud for Endpoint Advantage	3	
		SVS-AMPE-SUP-E Cisco AMP for Endpoints Enhanced SW Service	1	
		CSEMAIL-SEC-SUB Cisco Secure Email XaaS Subscription	1	
		SVS-EMAILC-SUP-S Solution Support for Cisco Email Security	1	
		CES-ADV-LIC Cisco Secure Email Cloud Advantage, Essential+ GSU+DLP+ENC	100	
		CES-MA-ULTD-LIC Cisco Secure Email Cloud Malware Analytics Unlimited License	1	
	4	**Renovación Infraestructura Cisco DNA** 3 años		1

ogtic
Oficina Gubernamental de Tecnologías de la Información y Comunicación

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Lote I- Renovaciones			
Lote II- Licencias	1	**Licencias Microsoft Office 2021 Standard Educativa**	300
	2	**Licencias Windows 11 Professional**	300
	3	**ManageEngine Desktop Central** edición profesional, licencia perpetua incluye un (1) usuario por defecto y dos (2) adicionales, para un total de tres (3) usuarios, 1500 computadoras, soporte y mantenimiento por 3 años.	1
	4	**Resharper ReSharper C++, 5 usuario por 1 año**	6
	5	**Power BI Pro**	20
	5	**Power BI Premiun por usuario**	5
	6	**Licencia de PHP Storm**	3
Lote II- Licencias			

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Lote III- Computadoras, Laptop y Tabletas	**1**	**Computadora Completa, Small Form Factor Procesador: Intel Core i7-11700 2.5 GHz Base frequency, up to 4.9 GHz o superior Chipset: Intel Q570 Memoria: 16 GB (8 GB x 2) DDR4-3200 no ECC Disco Duro SSD: 256 GB M.2 2280 PCIe Gen 3 NVMe SSD o superior. Video: Tarjeta gráfica integrada Intel UHD Graphics 750, CD-rom interno: 9.5mm Slim DVD-ROM Drive optional. Tarjeta de red: integrada, Audio: integrado. (3) Puertos USB 2.0 Tipo A (posteriores), (1) Puerto USB 3.2 Gen 1 Tipo A (posteriores) con tasa de señalización 5 Gbps, (2) Puertos USB 3.2 Gen 1 Tipo A (frontales) con tasa de señalización 5 Gbps; 1 de carga rápida, (2) Puertos USB 3.2 Gen 2 Tipo A (frontales) con tasa de señalización 10 Gbps, (2) Puertos USB 3.2 Gen 2 Tipo A (posteriores) con tasa de señalización 10 Gbps, (1) Puerto USB 3.2 Gen 2 x2 Tipo C (frontal) con tasa de señalización 20 Gbps, (1) Conector de red RJ-45 (posterior),(2) Conectores DisplayPort 1.4 (posteriores),(1) Conector combinado de micrófono/auriculares (frontal) compatible con CTIA y OMTP (frontal),(1) Salida de línea de audio (posterior)b Dispositivo de entrada: Teclado español, mouse óptico. Sistema Operativo: Windows 10 Pro 64 bits español. Monitor: 19” diagonal, 19.5" HD+ LED LCD Monitor - 16:9 - 20" Class - Twisted nematic (TN) - 1600 x 900 - 200 Nit Typical - 5 ms - 60 Hz Refresh Rate - HDMI - VGA - DisplayPort Equipo nuevo, no reconstruido. Garantía: 3 años de fábrica, no extendida**	289

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	2	**Disco Duro de Estado Solido**, 240G, Sata 3, 2.5, Lectura 500mb/s, Escritura 45 mb/s, SSD Garantia del fabricante.	250
	3	**Discos duros externos USB o Tunderbird (G-drive) 4 Tera**	2
	4	**WorkStation Factor pequeno (SFF) Completa, Intel Core i9 Hexadeca-core (16 Core) i9-12900K 12th Gen 3.20 GHz) 32 GB DDR5 SDRAM RAMIntel(R) Core (TM) i9 Processor Label 512GB PCIe M.2 SSD o superior NVIDIA Quadro T1000 with Max-Q design 4 GB Graphics te de alimentación: Adaptador de CA de 7,4 mm y 180 W (externo), adaptador de CA de 240 W de 7,4 mm (externo) Windows 10 Pro English, French, Spanish Puertos frontales** **2 Type-A SuperSpeed USB 10Gbps signaling rate port (1 charge port supports up to 5V/2.1A), 2 Type-A** **SuperSpeed USB 10Gbps signaling rate port, 1 Type-C SuperSpeed® USB 20Gbps signaling rate port** **(charge supports up to 5V/3A), 1 SD card reader (optional), 1 universal audio jack** **Puertos posteriores** **DisplayPort 1.4 [3], Audio Line out, 1GbE LAN, USB-A 480Mbps ports, USBA 5Gbps** **ports, serial (optional), Flex I/O port (VGA, HDMI 2.0b, DisplayPort 1.4, USB-C® 10Gbps port (Power Delivery 15W, Alt Mode Display Port), Dual USB-A 5Gbps port, 2nd 1GbE LAN, Thunderbolt 3** **with USB4 Type-C® 40Gbps (cabled to PCIe AIC), 1Gbps Fiber LC NIC Monitor USB-C de 27¨ Diagonally Flat IPS with Edge-lit**	12

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		1 HDMI 2.0, 4 USB-A 3.2 Gen 1, 1 USB Type-C™ (Alternative mode DisplayPort™ 1.4, Power Delivery up to 100W), 1 DisplayPort™ 1.4-in, 1 DisplayPort™ 1.4-out Tilt and Height Adjustable, Pivot, Swivel Stand Language selection, On-screen controls, Pivot rotation, Anti-glare, Height adjustablel . Equipo nuevo, no reconstruido. Garantía: 3 años de fábrica, no extendida	
	5	Laptop 14 a 15 pulgada diagonal Procesador Intel® Core™ i7 ultima generación, con gráficos Intel® UHD 620 (frecuencia base de 1,8 GHz, hasta 4,7 o superior Memoria 16 GB, DDR4 sin ECC Disco de estado sólido PCIe NVMe, M.2, clase 35 de 256 GB ó superior 1 puerto USB 3.2 Type C t, 1 puerto USB 3.2 de 1.ª generación, 1 1 puerto USB 2.0, 1 puerto HDMI 1.4ª, 1 puerto RJ-45 Ethernet, 1 puerto de audio, micrófono, Intel Wi-Fi 6 AX201, de banda doble, 2x2, 802.11ax, 160 MHz + Bluetooth universal, lector SD opcional, fuente de alimentación de 65 W, batería de 3 celdas de 45 WHr,1 puerto para adaptador de alimentación Cámara HD de 720º superior con micrófono integrado Garantía por el fabricante 3 años.	111
	6	Mochila para Laptop 14" a 15"	46
	7	Bulto para laptop 14" a 15"	75

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	8	**Laptop 16"** Profesional de 16 pulgadas Pantalla Liquid Retina XDR 16.2” Chip M1 Max Cámara FaceTime HD de 1080p CPU de hasta 10 núcleos, GPU de hasta 32 núcleos Almacenamiento 1TB SSD Memoria 32 GB Sistema de tres micrófonos con calidad de estudio Sistema de sonido de seis bocinas con audio espacial **Incluir adaptador:** Tipo C a Ethernet, HDMI y USB Garantía 1 años por el fabricante.	10
	9	**Tablet** DIMENSIONES Y PESO 285 x 185 x 5,7 milímetros 575 gramos, PANTALLA 12,4" Super AMOLED, 1752 x 2800 pixeles WQXGA+ (266 ppi), 16:10 ratio HDR10+ y 120 Hz tasa de refresco, Altavoces cuádruples con sonido por AKG, Dolby Atmos, RAM 8GB, PROCESADOR Snapdragon 865+, 128 GB de Almacenamiento ampliable con microsdxc, SENSORES de Acelerómetro, Compas, Giroscopio,Sensor de Luz, Lector de huellas,Sensor de efecto Hall, SISTEMA OPERATIVO Android 10 con One UI 2, CONECTIVIDAD Wi-Fi 802.11 a/b/g/n/ac/6, dual-band, Wi-Fi Direct, hotspot, Bluetooth 5.1, GPS, Glonass, Beidou, Galileo, USB-C 3.1, GSM / HSPA / LTE / 5G, CÁMARAS Trasera: 13 MP (f/2.0) y 5 MP (f/2.2). Grabación de vídeo 4K a 30fps, Selfie: 8 MP (f/2.0), BATERÍA Li-Po 10090 mAh con carga rápida a 45W, con carcasa protectora y teclado del mismo frabricante, **Garantia del fabricante mínimo 1 año.**	28

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	10	**Tableta Ultima Generación (2022) 10.9 pulgadas** Capacidad 64 GB, Modelos Wi-Fi + Celular 462 g, Cable de carga USB-C (1 m),Adaptador de corriente USB C de 20 W,Pantalla Liquid Retina,Chip M1 de Apple CPU de 8 núcleos,Procesador gráfico de 8 núcleos,Neural Engine de 16 núcleos,8 GB de RAM,Cámara gran angular de 12 MP y apertura de f/1.8 Cámara FaceTime HD,Zoom digital de hasta 5x,Grabación de video 4K a 24 cps, 25 cps, 30 cps o 60 cps Llamadas de video de FaceTime,Desde el iPad a cualquier dispositivo con FaceTime a través de Wi-Fi o red celular,Bocinas estéreo, Dos micrófonos para llamadas y grabación de audio y video,Sistema Operativo IOS 15 o superior color gris,Magic Keyboard. **Garantía 1 años por el fabricante**	30
Lote IV Solución de Hiperconvergencia y Servidores			
Lote IV Solución de Hiperconvergencia y Servidores	**1**	**Servidor Rack 2U** Gold 5218 Processor, Frequencia 2.3 GHz, 16 Core L3 Cache 22.00 MB 125W, 256 GBDDR4 SmartMemory, 1 Gb 331i Ethernet adapter 4-ports per controller, Discos: 2x SSD 480, 4x HDD 1.2TB, dos fuentes de energia (power supply), **Garantia 3 años por el fabricante.**	8
	2	**Solución de Hiperconvergencia:** **Características Generales:**	1

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Suministrar una solución, compuesta por recursos de cómputo, almacenamiento, gestión centralizada, software de hiperconvergencia de forma integrada homologada y preinstalada de fábrica que aproveche los componentes locales de cada unidad y cree una plataforma de Nube Privada distribuida con capacidad de crecimiento modular ilimitado en el mismo clúster donde todas las funcionalidades estén basadas en el software y no dependan de un componente de hardware específico para su funcionamiento. El software de hiperconvergencia debe poder implementarse sobre diferentes fabricantes de hardware x86. El oferente deberá hacer entrega de la infraestructura mínima para el correcto funcionamiento de la solución ofertada. Esta deberá ser instalada y configurada correctamente por parte del Fabricante o el proponente con ingenieros debidamente certificados por el fabricante. La solución debe incluir de forma nativa una arquitectura que provea a nivel de hardware y software un esquema de alta disponibilidad de tal forma que ante la falla de un nodo, se mantenga operativo el clúster sin afectar el desempeño de las aplicaciones, este esquema no debe incorporar elementos que hagan la función de testigo (witness, quorum o similar). La solución de hiperconvergencia debe estar en capacidad de consolidar diferentes servicios de storage como Servidores de Archivos y almacenamiento de data no estructurada Debe permitir la migración en caliente de Máquinas virtuales en el cluster entre diferentes nodos		

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		La solucion de hiperconvergencia debe de estar basada en configuracion homogenea que garantice la mayor disponibilidad y rendimiento. **Características de Hipervisor:** El hipervisor de la solucion debe estar construida sobre Vmware. El licenciamiento de Vmware debe incluir las licencias de VMware Enterprise Plus + vCenter para todos los procesadores de la Solucion. La administración de la plataforma completa debe ser desde una misma consola de gestión basada en web sin requerir la instalación de una consola o software adicional. Debe ofrecer el servicio nativo para el manejo de imágenes y/o plantillas de máquinas virtuales disponibles para el hipervisor. Debe permitir la adición en caliente de recursos de memoria y capacidad de almacenamiento a una máquina virtual Debe incluir la funcionalidad de ubicación inteligente de nuevas máquinas virtuales utilizando estadísticas de uso de CPU/RAM/almacenamiento del clúster en tiempo real de manera que se garantice a las cargas de trabajo el mejor acceso posible a los recursos. Esta funcionalidad debe venir habilitada por defecto. La solucion debe contar con un portal desde el cual se pueda monitorear la plataforma de hiperconvergencia y los switches que forman parte de la solucion. Debe poder ser actualizado desde la misma consola gestión del sistema hiperconvergente a las últimas versiones sin disrupción del servicio. Debe incluir las herramientas necesarias para ver todas las estadísticas funcionales y operacionales del cluster a nivel de máquina virtual.		

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Debe permitir definir reglas de afinidad y anti-afinidad entre los nodos del cluster Debe permitir entregar y gestionar direccionamiento IP dinámico y estático para máquinas virtuales sin requerir productos adicionales de terceros Debe soportar alta disponibilidad para las máquinas virtuales y ante la caída de un nodo, las máquina virtuales se reinicien de forma automática en otro nodo. Debe soportar la compatibilidad automática entre diferentes modelos y generaciones de CPUs del mismo fabricante sin necesidad de configuraciones manuales para este propósito Debe permitir la creación, clonación, borrado, y protección mediante puntos de restauración automáticos de máquinas virtuales Debe permitir la definición de redes virtuales (SDN) mediante un switch virtual distribuido en todo el cluster con soporte y mapeo de VLANs, link aggregation, y visualización de estadísticas de red sobre los puertos físicos del switch TOR. Debe permitir la migración en caliente de Máquinas virtuales en el cluster entre diferentes nodos **Características de Software:** La solución debe soportar al menos 2 diferentes tipos de hipervisores tales como VMware ESXi, Microsoft Hyper-V. El sistema hiper convergente debe llevar a cabo las tareas de compresión y deduplicación	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		completamente en software. La compresión debe ser en línea (tiempo real). Las funcionalidades de compresión y deduplicación deben estar activas en el cluster todo el tiempo. La solución debe poder ejecutar tareas de compresión y deduplicacion a lo largo de todo el clúster y no limitadas al contenido o tipo de disco. El sistema de hiperconvergencia debe contar con mecanismos de eficiencia de espacio como, Compresión y Deduplicación. La solución de hiperconvergencia debe estar en capacidad de presentar su almacenamiento a servidores externos al cluster por medio de iSCSI. La solución debe permitir agregar nodos solamente de capacidad de almacenamiento sin agregar simultáneamente capacidad de cómputo al clúster. La solución debe permitir agregar nodos solamente de capacidad de cómputo sin agregar simultáneamente capacidad de almacenamiento al clúster y sincosto de licenciamiento HCI adicional. La solución debe permitir agregar discos de diferente tipo (rotacionales y/o estado sólido) con diferente capacidad en cada nodo. La solución debe incluir la funcionalidad de replicación asincrónica nativa de datos (sin requerir la instalación de software adicional) que cumpla con los siguientes requerimientos básicos: - Replica a nivel de máquina virtual de forma granular - Mecanismos de compresión de los datos a ser replicados. - Replicación bidireccional entre dos centros de datos. - Posibilidad de limitar el ancho de banda usado por la replicación desde la interfaz de administración de	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		la solución hiperconvergente. - La solucion de replicacion debe funcionar sin la necesidad de crear snapshots. - La replicacion de las maquinas virtuales debe ser agnostica del repositorio final de replicacion.		
		El sistema hiperconvergente debe soportar nodos con Self-Encrypting Drives (SEDs)		
		El sistema debe contar con un nivel de aseguramiento (hardening) aplicado de fábrica y asimismo contar con un mecanismo nativo para automatizar la remediación de las desviaciones con respecto al hardening que puedan ocurrir durante todo el ciclo de vida de la solución, sin la ejecución de tareas manuales por parte de un administrador. La solución debe incluir la opción de mantener al menos 2 copias de los datos en tiempo real y distribuidas en los distintos nodos del cluster. Esta funcionalidad debe ser automática y sin necesidad de configuración manual alguna. El sistema debe proporcionar de manera nativa, sin herramientas de terceros la capacidad de recuperar las máquinas virtuales, en un lapso de 24 horas. El sistema debe ofrecer la capacidad de mantener consistente la replicación de un grupo de volúmenes y/o máquinas virtuales de tal manera que los snapshot se tomen en el mismo punto en el tiempo. La detención de la réplica de uno de los volúmenes o Máquinas virtuales en el grupo de consistencia debe detener la réplica de todo el grupo.		

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		El sistema debe proveer la capacidad de programar la toma periódica de snapshots a máquinas virtuales, sin depender de funcionalidades heredadas del hipervisor El sistema debe soportar la creación de un disco virtual cuya capacidad es mayor a la capacidad disponible en el nodo en que reside. Todas las tecnologías de Alta Disponibilidad y protección de datos con que cuente la solución deben estar disponibles para un disco virtual con ésta característica. **Caracteristicas de Administracion:** La solución debe entregar el detalle a nivel de disco virtual, como mínimo las siguientes estadísticas: Latencias de escritura y lectura, IOPS de escritura y lectura. Esta información debe estar disponible sin requerir la instalación de ningún componente adicional del mismo fabricante o de terceros. La solución deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del cluster (servicios de storage, firmware de los nodos, versión de BIOS e hipervisor) directamente desde la consola web y de forma no disruptiva, es decir, sin necesidad de reinicio de las máquinas virtuales ni indisponibilidad del servicio. La solución debe proveer un mecanismo para ingresar un nodo en modo de mantenimiento, modo en el que se debe preservar no sólo la disponibilidad de los datos sino asegurar la redundancia configurada para los datos desde el mismo momento en que el nodo queda en modo mantenimiento. Este comportamiento se debe mantener incluso si el clúster sólo tiene 3 nodos.	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		La solución debe proporcionar una herramienta que pueda generar - gráficamente - un mapa de topología de los componentes de infraestructura que conforman la solución HCI.	
		La solución debe incluir una funcionalidad que automática y periódicamente haga una revisión al estado de salud de todos los componentes tanto de hardware como de software del clúster y entregue un reporte detallado para la resolución de problemas	
		La solución debe incorporar una tecnología estándar en la industria para ejecutar chequeos de integridad de los datos, y no debe proveer ninguna opción para que un usuario o administrador deshabilite esta funcionalidad.	
		En la solución no debe haber puntos únicos de falla en la capa de administración de la solución, todos los nodos en el sistema deben tener un módulo de software nativo en el sistema hiperconvergente que permita hacer la administración centralizada de todo el cluster. Esta funcionalidad no debe implicar configuraciones adicionales a la del sistema.	
		La solución debe incluir una funcionalidad que notifique automáticamente al fabricante acerca de condiciones de error de manera proactiva	
		La solución debe incluir una funcionalidad que ejecute tareas de optimización automatizada de recursos, que permita realizar proyecciones de capacidad, tareas de planeación, basadas en tecnologías como machine learning	
		La solución debe incluir una funcionalidad que realice detección de anomalías, basadas en análisis de comportamiento para generar alertas tempranas.	
		La solución debe tener la capacidad de aprender el estado o condición normal de todos los elementos bajo su gestión, a lo largo del tiempo, y alertar cuando las condiciones son anormales.	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		La solución debe incluir una función que permita al grupo de TI crear tareas automatizadas para acciones de remediación o troubleshooting, basadas en alertas a través de un Wizard de Configuración. La solucion ofertada de hiperconvergencia debe ser una solucion hibrida en discos locales en los nodos de la solucion. No debe ser una solucion basada en alamcenamiento externo presentado a los nodos. **Características de Hardware:** Solución debe ser basado en servidores de standalone rackmount de 2U con tres nodos integrados en la siguiente configuración. 2x CPU Intel Xeon I6326 (última generación), 2.9 GHz/16-core por nodo 512 GB de RAM DDR4 (mínimo) por nodo 2x Dual Port 10/25 GbE (NIC). Incluir cables de interconexión con red LAN 30TB Utilizable hibrido en el cluster. Los 30 TB usable deben ser disponibles aun con la salida de un nodo. La solucion debe poder crecer en un solo disco por nodo. Conectividad: 4 puertos por nodos 10/25 GbE mínimo (SFP28). La solucion debe tener la capacidad de virtualizar la capa de RED en varias tarjetas virtuales a la misma velocidad fisica, contener diferentes MAC. La virtualizacion de las NIC debe ocurrir a nivel de hardware sin la intervencion de Sistemas Operativos o Hipervisor.	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		La solucion debe incluir dos (2) Switches de 24 puertos 10/25 GbE SFP28 redundantes para conectividad entre todos los nodos de la solución. **- Requerimientos de implementación:** Instalacion y configuracion en Santo Domingo. Configuración de red. Migración maquinas virtuales (10 VMWare y 5 Hyper V). **- Requerimientos del proveedor:** Los ingenieros que realicen la implementación deben estar certificados de la misma. Carta del fabricante que autorice la venta de esta solución. Actualizaciones, parches y nuevas versiones de software. • El servicio de soporte debe brindar soporte proactivo a través de ingenieros Certificados por el fabricante • Constancia de al menos cinco (5) proyectos implementados y ejecutados por el proveedor localmente. al menos cinco (5) años de experiencia en la marca ofertada. Incluir referencia de los proyectos ejecutados, contactos, copias de las ordenes y cartas de la empresa donde se ejecuto. • El proveedor debe incluir al menos 2 ingeniero certificado por el fabricante de la solución de	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Hiperconvergencia. (Incluir certificado). • Debe incluir entrenamiento del fabricante para 2 personas en la solución ofertada. **Garantia de la solución por el fabricante 3 años 7x24x4h**	
Lote IV Solución de Hiperconvergencia y Servidores			
Lote V- Implesoras, Escanner Lectores de huellas y Lectores Codigo de barra	**1**	**Servicio de mantenimiento anual parque impresoras del INFOTEP** por 2 años Debe cubrir todas las localidades del INFOTEP a nivel nacional,Tiempo de repuesta 5 horas sedes Distrito Nacional 8 a 16 horas laborable localidades remotas.Incluir todos los consumibles tóner, repuestos, piezas, partes y mano de obra,Respaldo en almacén mínimo 60 días de tóner, repuestos, piezas, partes,Software de gestión de la plataforma de impresión administrado por el INFOTEP, que permita la administración y monitoreo de todas las impresoras activas en la red, asignación de código por usuario, manejo de cola, general estadísticas y métricas, reporte automatizado, históricos, tanto por usuario, como por impresoras,Calidad de las impresiones en blanco y negro, full color con una optimización del 100 %,Opción de equipos para eventos especiales,Respaldo o backup de cualquier equipo incluido en el mantenimiento,Cambio de equipo asociado a problema de fabrica,Opción de equipo solicitado a demanda, entrenamiento incluido si tiene característica de uso especiales.Proveer impresoras multifuncionales, o monofuncionales, dependiendo de la necesidad y el volumen de impresión (Carga de Impresión), impresoras (Pequeñas, Medianas, Grandes y de Producción). Mantenimiento preventivo programado mínimo cada tres meses,Mantenimiento correctivo en sitio, programado o por evento.	1

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Las impresoras que pertenecen al parque de la institución, podrán entrar dentro del contracto de mantenimiento a solicitud. Servicio técnico especializado, el equipo técnico debe estar certificado en las marcas de las impresoras a proveer,Proveedor debe retirar los cartuchos, repuestos, piezas, partes utilizada, entregar certificación de la disposición final del producto que se hace bajo lo establecido en la ley 225-20 de manejo de residuos sólidos (recolección, transporte, tratamiento, eliminación, Reciclado) o disposición final dependiendo la condición en la que se encuentre el material,Proveedor debe haber implementado la solución en un mínimo de 6 clientes corporativo,SOLO PAGA LO QUE IMPRIME. No hay elementos condicionantes. No mínimos, ni máximos, ni,Cuotas fijas. Solo paga lo que imprime, se establecerá una fecha de corte, puede ser mensual o trimestral.,El tiempo de implementacion no puede ser mayor a los 3 meses luego de finalizado los termino del contracto PRECIO MAXIMO DE IMPRESIÓN UNIDAD PAG. Tamaño Precio ITBIS incluido PAGINA 8.5 X 11" Blanco y negro precio por pagina RD$1.25 PAGINA 8.5 X 14" Blanco y negro precio por pagina RD$ 1.50 PAGINA 11 X 17" Blanco y negro precio por pagina RD$ 2.35 PAGINA 8.5 X 11" COLOR precio por pagina RD$ 5.0 PAGINA 8.5 X 14" COLOR precio por pagina RD$ 6.35 PAGINA 11 X 17" COLOR precio por pagina RD$ 12.0 Nota: el incumpliendo de cualquiera de los términos	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		establecidos es una razón para rescindir el servicio acordado con el proveedor.	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	2	**Impresora Multifuncional** Impresora de inyección de tinta portátil con pantalla táctil LED HD de 4,3 pulgadas para código de barras QR-Code Fecha de producción Logotipo de bricolaje Dimensiones del paquete 27.8 x 25 x 11.6 cm; 2.09 kilogramos Pilas 1 Litio Ion necesaria(s), incluida(s) Número de modelo del producto BT-HH6105B2 Sistema operativo Linux Tecnología de impresión Inkjet Tipo de media de impresión Tela Tecnología de impresión Inyección de tinta Aparatos compatibles Impresora Pantalla táctil, Memoria interna Pilas / baterías incluidas Sí Tipo de conector USB, **Garantia mínimo 1 años por el fabricante**	1
	3	**Impresora** de etiquetas a color - Imprima etiquetas de productos a todos color bajo demanda, Imprime etiquetas de hasta 4" Ancho x 24" de largo 4800 DPI a todo color con calidad fotográfica impresión de etiquetas, garantia, **Garantia minimo 1 años por el fabricante**	1
	4	**Docking Estación de acoplamiento Pantallas admitidas con entrada Thunderbolt** Para una PC HBR2* 3 pantallas FHD a 60 Hz 3 pantallas QHD a 60 Hz 2 pantallas 4K a 30 Hz Para una PC HBR3 4 pantallas FHD a 60 Hz 4 pantallas QHD a 60 Hz 2 pantallas 4K a 60 Hz Resolución máxima 5K a 60 Hz con sistemas Thunderbolt HBR2/HBR3 8K a 60 Hz con sistemas Thunderbolt HBR3 compatibles con la compresión de flujo de pantalla Interfaces de video Dos DP1.4 de tamaño completo 1 HDMI 1 USB-C MFDP: 1 USB-C Thunderbolt 3™ Puertos USB 3 USB-A 3.1 Gen 1 2 USB-C 3.1 Gen 2 Redes Gigabit Ethernet Tipo de	15

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		ranura de seguridad (el candado de cable se vende por separado) 1 ranura para candado Kensington 1 ranura para candado Noble Wedge Indicadores LED LED de adaptador de alimentación LED de botón de encendido LED de RJ45 Alimentación Adaptador de alimentación de CA de 180 vatios con suministro de alimentación de hasta 130 vatios Suministro de alimentación de hasta 90 vatios para sistemas de otros fabricantes Dimensiones 205 mm x 90 mm x 29 mm 8,07 in x 3,54 in x 1,14 in Peso de la estación de acoplamiento (sin adaptador de alimentación) Característica Especificaciones técnicas Sistemas operativos Microsoft Windows 10 Ubuntu 18.04 Red Hat Enterprise Linux macOS3 Administración de sistemas vPro inalámbrico compatible con laptop o estación de trabajo Interfaz de acoplamiento Thunderbolt 3™ (conector Type-C) Longitud del cable 0,8 m Dirección MAC Dirección MAC de paso **Garantía fabricante mínimo 1 año**	
	5	**Lector Código de Barras** 1D 2D inalámbrico para factura, boletas, tickets y etiquetas. De mano con base, interfaz USB inalámbrico, Escanea códigos de barras desde las pantallas de dispositivos móviles, color negro, cable usb. Compatibilidad OS: Windows, Mac OS, Linux, Android Interfaz: cable USB -OTG Interfaz: cable USB -OTG, **Garantia fabricante**	2

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	6	**Laser Jet Enterprise Blanco y Negro serie MFP M400** Impresora Multifuncional Escáner, Copiadora Velocidad 22 PPM Resolución 1200X1200, bandeja 1 550 hojas Bandeja Multiuso 100 hojas ADF 150 hojas Bandeja Principal Carta, Legal, Declaración Ejecutivo Oficio Sobre, Bandeja Multiuso Carta, Ejecutivo, Espesor papel 60 a 200 gr/m² Reducción y ampliación 25% hasta 400% Resolución de copiado 600X600 DPI, Velocidad 55 PPM Escaneo ADF a doble cara, formato JPG, Tiff, PDF, XPS, Almacenamiento carpeta de red, USB, Correo Electrónico Memoria 1.5 GB, Máximo 2GB Tarjeta de red 100/1000T Disco duro capacidad 16 GB o mas Panel Touch 8.0 Voltaje 110 a 220 VAC Consumo 740 W Soporte Sistema Operativo Windows 10, 11 Professional **Garantía mínimo 1 año fabricante**	24
	7	**Impresora Color LaserJet Pro MFP M479fdw** Velocidad Funciones: Velocidad de impresión de hasta 28 ppm (negro) y 28 ppm (color); Velocidad de escaneado (negro) 29 ppm / Velocidad de escaneo (color)20 ppm Velocidad Procesador: 1200 MHz Volumen mensual de paginas recomendadadas: 750 a 4000 paginas Memoria Standard: 512 MB de NAND flash con 512	10

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		MB de DRAM Conectividad: 1 USB 2.0 de alta velocidad; 1 USB integrado en el lado trasero; red Gigabit Ethernet 10/100/1000BASE-T; Radio Wi-Fi 802.3az(EEE) 802.11b/g/n/2,4/5 GHz Capacidad de hojas: Estandar 300 hojas y máxima 850 hojas Conectividad: USB, Ethernet, Wifi Ciclo mensual (A4): Hasta 50.000 páginas Resolución de impresión: Negro (óptima): 600 x 600 ppp, Tamaños de soportes de impresión admitidos: Bandeja 1, Bandeja 2: A4; A5; A6; B5 (JIS); B6 (JIS); 16K (195 x 270 mm, 184 x 260 mm, 197 x 273 mm); 10 x 15 cm; Oficio (216 x 340 mm); tarjetas postales (un JIS, doble JIS); sobres (DL, C5, B5); Bandeja 3 opcional: A4; A5; A6; B5 (JIS); B6 (JIS); 16K (195 x 270 mm, 184 x 260 mm, 197 x 273 mm); 10 x 15 cm; Oficio (216 x 340 mm); tarjetas postales (un JIS, doble JIS); Unidad dúplex automática: A4; B5; 16K (195 x 270 mm, 184 x 260 mm; 197 x 273 mm); Oficio (216 x 340 mm) Resolución de escaneado: Hardware: Hasta 1200 x 1200 ppp; Óptica: Hasta 1200 x 1200 ppp Impresión automática a doble cara: Automático (por defecto) Panel de Control: Pantalla táctil color de uso intuitivo de 4,3" Capacidad de entrada: Hasta 300 hojas, Capacidad de salida: Hasta 150 hojas Certificado Energy Star: Si **Garantia: un año mínimo**	
	8	**Escáner** Con lector para diseño ScanSnap iX1600 de documentos versátil para Mac o PC, **Garantia minimo 1 año por el fabricante**	1

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	9	**Escanner: ScanJet Enterprise** Flow 7000 s3 Escáner OCR de alimentación de hojas Dimensiones del producto 7.79 x 12.2 x 7.48 pulgadas Peso del producto 8.4 pounds ASIN B01M0TLC7X Item model number ScanJet Enterprise Flow 7000 s3 **Garantia 1 año por el fabricante**	30
	10	**"LECTOR DE HUELLAS BIOMETRICO BIOTRACK, Nota: agregar punto adicionales de ponchados solución existente.** BIOTIME - CONTROL DE ASISTENCIA MULTIMEDIA CON HUELLA DIGITAL: PANTALLA A COLOR DE 3"", SONIDOS CON VOZ, TECLADO DE 16 TECLAS, HUELLA DIGITAL, CLAVE, TARJETA DE PROXIMIDAD, USB HOST Y USB CLIENT, TCP/IP, RS232/RS485, SIRENA INTERNA, 3000 HUELLAS DIGITALES, 100.000 REGISTROS, WEBSERVER, LECTOR DE CRISTAL DE ALTA CALIDAD, CÓDIGO DE TRABAJO. INGLÉS/ESPAÑOL (DISPOSITIVO Y SOFTWARE). INCLUYE SOFTWARE DE ACCESO ILIMITADO Y FUENTE DE PODER **GARANTIA mínima 1 año**	5
	11	**Impresora Mono-Cromática IRAD 527IF** Velocidad Funciones: Velocidad de impresión de hasta 52 ppm (negro); Velocidad de escaneado (negro) 49 ppm / Velocidad Procesador: 175 GHz Dual Core Volumen mensual de páginas recomendadas: 750 a 4000 páginas Memoria Standard: 3 GB RAM Hard disk 250-320 gb Conectividad: USB 3.0 de alta velocidad;Red Gigabit Ethernet 1000BASE-T; Radio Wi-Fi 802.3az(EEE) 802.11b/g/n/2,4/5 GHz	1

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Capacidad de hojas: Estándar 500 hojas y máxima 1000 hojas Conectividad: USB, Ethernet, Wifi Ciclo mensual (A4): Hasta 80.000 páginas Resolución de impresión: Negro (óptima): 600 x 600 dpi, Tamaños de soportes de impresión admitidos: Bandeja 1, Bandeja 2: A4; A5; A6; B5 (JIS); B6 (JIS); 16K (195 x 270 mm, 184 x 260 mm, 197 x 273 mm); 10 x 15 cm; Oficio (216 x 340 mm); tarjetas postales (un JIS, doble JIS); sobres (DL, C5, B5); Bandeja 3 opcional: A4; A5; A6; B5 (JIS); B6 (JIS); 16K (195 x 270 mm, 184 x 260 mm, 197 x 273 mm); 10 x 15 cm; Oficio (216 x 340 mm); tarjetas postales (un JIS, doble JIS); Unidad dúplex automática: A4; B5; 16K (195 x 270 mm, 184 x 260 mm; 197 x 273 mm); Oficio (216 x 340 mm) Resolución de escaneado: Hardware: Hasta 1200 x 1200 ppp; Óptica: Hasta 1200 x 1200 ppp Impresión automática a doble cara: Automático (por defecto) Panel de Control: Pantalla táctil color de uso intuitivo de 4,3" Capacidad de entrada: Hasta 300 hojas, Capacidad de salida: Hasta 450 hojas Certificado Energy Star: Si **Garantía: un año mínimo**	
Lote V- Implesoras, Escanner Lectores de huellas y Lectores Codigo de barra		

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Lote VI-Proyección y Video Conferencia	**1**	**Monitores 21"** Con ajuste de inclinación y panel antirreflejos Backlight Technology: LED Display Type: Widescreen Flat Panel Display Display Screen Coating:Anti-Glare with 3H hardness Audio Output: 1 x Audio line-out Connectivity: 2 HDMI/MHL connector 1 DP connector and 1 mDP connnector, 2 USB 3.0 downstream connector,1 USB 3.0 upstream connector 1Audio line-out port optional **Garantía 3 años por el fabricante.**	6
	2	**Monitor con retroiluminación LED – 32"** Consumo de energía anual 37 kWh, Consumo eléctrico (modo Encendido) 25.1 vatios Concentrador USB 3.2 Gen 1, USB PD 65 vatios Tipo de panel IPS Relación de aspecto 16:9, Resolución nativa: QHD 2560 x 1440 a 60 Hz Paso de pixel: 0.2727 mm, Brillo: 350 cd/m², Relación de contraste: 1000:1, Tiempo de respuesta 8 ms (gris a gris normal); 5 ms (gris a gris rápido), Admisión de color: 1,07 millones de colores, Conectores de entrada: HDMI, DisplayPort, USB-C Ajustes de posición de pantalla: Altura, pivote (rotación), plataforma giratoria, inclinación Recubrimiento de pantalla: Anti-glare 3H hardness Estándares medioambientales TCO Certified Displays 8, Calificado ENERGY STAR **Garantía 3 años por el fabricante**	10

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	3	**MONITOR DE 27"** Diagonally Viewable Size: 70.86 cm, 27.90 Inches Aspect Ratio: Widescreen (16:9) Panel Type, Surface:TN , Anti-Glare Optimal resolution:3840 x 2160 at 60 Hz Contrast Ratio: 1000: 1 (typical), 8 million : 1 (DCR) Brightness: 300 cd/m2 (typical) Response Time:2 ms typical (G to G) Viewing Angle: 160° vertical / 170° horizontal Color Support:Color Gamut1 (typical): 72% of NTSC,1.07 Billion colors Pixel Pitch: 0.16 mm x 0.16 mm Backlight Technology: LED Display Type: Widescreen Flat Panel Display Display Screen Coating:Anti-Glare with 3H hardness Audio Output: 1 x Audio line-out Connectivity: 2 HDMI/MHL connector 1 DP connector and 1 mDP connnector, 2 USB 3.0 downstream connector,1 USB 3.0 upstream connector 1Audio line-out port optional **Garantía 3 años por el fabricante.**	10
	4	**Smart TV Color Negro o Silver 64.5 in.** Pantalla: 64.5 in, VA, Edge LED, 3840 x 2160 pixels. Ángulos de visión (H/V): 178 ° / 178 ° Frecuencia de actualización: 50 Hz / 60 Hz. Interpolación: 120 MR (Motion Rate) Sintonizador de TV: Analog (NTSC/PAL/SECAM), Clear QAM, ATSC. Número de núcleos: 4. Adaptive Sound, Detección de brillo / colorBrightness Detection Apagado automático, Connect Share™ (HDD), Conectividad Móvil, Control Remoto, Control Universal, Navegador Web, Bloqueo de acceso a sitios dañinos 3 HDMI, 2 USB Entrada componente, Entrada compuesta (AV), Ethernet (LAN), Salida de audio	8

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		digital (óptica), Entrada RF (antena / cable), Soporte HDMI A / Soporte para canal de retorno, eARC, HDMI, Quick Switch, Red inalámbrica integrada (WIFI), Bluetooth, Anynet+ (HDMI-CEC). **Garantía 1 año por el fabricante.**	
	5	**Smart TV Color Negro o Silver, Pantalla: 42** in, 3840 x 2160 pixeles. Frecuencia de actualización: 50 Hz / 60 Hz. Motion Enhancement Technology: Si, Sintonizador de TV: Analog (NTSC), Clear QAM, ATSC. Control Remoto, Control Universal, Navegador Web, Bloqueo de acceso a sitios dañinos 3 HDMI mínimo, 2 USB Entrada componente mínimo, Entrada compuesta (AV), Ethernet (LAN), Salida de audio digital (óptica), Entrada RF (antena / cable), Soporte HDMI A / Soporte para canal de retorno (eARC), Red inalámbrica integrada (WIFI), Bluetooth. **Garantía 1 año por el fabricante.**	2
	6	**Pantalla Interactiva Touch** Paneles 4K UHD Tecnología táctil infrarrojos, Multi-Touch 10 a 20 Toques, camara opcional Sistema Operativo Android Integrado, PC Integrado OPS(Computador ultraslim incluido) con especificaciones de: Processors Intel Core i7 (16GB RAM / 256GB SSD) soporta H.265, Soporta pantallas 4K, LAN 10/100/1000 LAN Card (RJ45), Conexión Inalámbrica 802.11a/b/g/n 3T3R MIMO Wi-Fi Conexiones 1x HDMI, 2x USB 2.0, 2x USB 3.0, 1x Micrófono, 1x Auriculares, 1x Internet RJ-45, 2x antenas WiFi ,Dimensiones 180 mm x 119 0mm x 30	3

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		mm, Peso 0,9 Kg Compatible: Windows, Mac, Chrome y Linux, Soporte Movible INCLUIDO Sistema de transmisión de pantalla inalámbrica, Tensión nominal de funcionamiento 100 V ~ 240 V CA, Frecuencia de funcionamiento 50 Hz ~ 60 Hz, Potencia Máx. 450 W. **Garantía mínimo 2 años por el fabricante."** DRN 2 300,000 600,000	
	7	**Smartboards Pizarra Blanca** Tipo de pizarra blanca: Pizarra interactiva Doblado:No Marca:YCZX Número de Modelo:YC650-JX Nombre del producto:Pizarra inteligente interactivo, Soporte Movible INCLUIDO Tamaño:65 pulgadas Resolución:3840*2160 Tipo de pantalla:LCD Aplicación:Reuniones/formación/publicidad I5 o I7, 16 de memoria, HDD SSD 120 GB o Superior, Sistema operativo: PC Integrado OPS(Computador ultraslim incluido) Windows 10/11/ Android 8,0/9,0 Certificado:ISO/CE/FCC/ROHS/CCC Material del marco:De aleación de aluminio La tecnología táctil:Táctil infrarroja Puntos de Contacto:20-punto simultánea contacto" **Garantia minimo 2 años fabricante**	10

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	8	**Cámara Web** Para videollamada Resolución máxima: 1080p/30 fps - 720p/30 fps Cámara mega pixel: 3 Tipo de enfoque: Enfoque automático Tipo de lente: Cristal Funcion de Zoom hasta 1x Micrófono integrado: Estéreo Radio de micrófono: Hasta 1 m Campo visual diagonal (dFoV): 78° Clip universal acoplable a trípode, para monitores, pantallas LCD o laptops permita ajuste atreves de software cable USB-A fijo de 1,5 m Soporte Windows, Mac, Chrome **Garantía mínimo 1 año**	120
	9	**Auriculares Estéreo con Micrófono (Headset)** Tipo De micrófono: Bidireccional Sensibilidad (audífono): 32 ohmios Sensibilidad (audífono): 100 dB +/- 3 dB Sensibilidad (micrófono): -58 dBV/µBar, -38 dBV/Pa +/- 4 dB Respuesta de frecuencia (audífonos): 20 Hz - 20 KHz Respuesta de frecuencia (micrófono): 100 Hz - 16 KHz Tipo USBLongitud del cable: 2,35 m Windows®, macOS o Chrome OS™ y aplicaciones de llamadas populares."	120

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	10	**Cámara Video Conferencia logitech brio** Videoconferencias 4K Ultra HD (hasta 4096 x 2160 píxeles a 30 fps) Videoconferencias Full HD 1080p (hasta 1920 x 1080 píxeles a 30 o 60 fps) Videoconferencias HD 720p (hasta 1280 x 720 píxeles a 30, 60 o 90 fps) Conexión USB Plug and Play Campo visual, Diagonal: 90°, Horizontal: 82,1°, Vertical: 52,2° Zoom digital 5x en Full HD Enfoque automático RightLight 3 con HDR para nitidez de imagen en distintas condiciones de iluminación desde luz escasa a luz solar directa Controles de imagen con la aplicación Camera Settings opcional, para funciones de panorámica, inclinación y zoom Dos micrófonos omnidireccionales integrados con cancelación de eco y ruido Sensor con tecnología infrarroja para Windows (SDK disponible para integración de aplicación) Tapa de obturador externa Varias opciones de montaje, incluidas clip y trípode Admite varios tipos de conexión, incluidos USB 2.0 tipo A y USB 3.0 tipo A y C Funda protectora personalizada **Garantía mínimo 1 año**	18

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	11	**Cámara Video Conferencia Rally pro** Pack Rally Plus "todo en uno" 15 participantes) Cámara Plug&Play PTZ, Ultra HD Altavoz de gran calidad de audio Incluye Rally Hub, 2 Rally Mic Pod y control remoto Posibilidad de ampliar hasta 7 micrófonos (hasta 40 participantes) Sistema de imágenes Ultra-HD para: 4K, 1440p, 1080p, 900p, 720p y SD a 30 fps., 1080p, 720p a 30 fps y 60 fps. Panorámica, inclinación y zoom robotizados y fluidos, Panorámica: ± 90° Inclinación: +50° / -90°, Zoom Full HD 15x., Campo visual de 90°, **Garantia minimo 1 año por el fabricante.**	1
	12	Prosonus Audio Box o Shure BLX, **Garantia minimo 1 año**	6
	13	Sistema de Micrófono Inalámbrico (BLX288/B58-H10), **Garantia minimo 1 año**	6
Lote VI-Proyección y Video Conferencia			

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Lote VII- Equipos de Comunicación	**1**	**Switch Cisco 9500** con 40 Slots SFP+ y capacidad para manejar Conexiones hasta 10G y 2 Uplinks a 40G QSFP+. Algoritmo de cifrado MACSEC de AES 256 a nivel de hardware. Detección de malware en tráfico cifrado y detección de anomalías distribuidas. Soporte de MPLS para segmentación de la red. Programabilidad con soporte de protocolos NETCONF / YANG. Visibilidad y control de aplicaciones para clientes en la red cableada e inalambrica. El switch debe tener embebido RFID Tag para facilitar el inventario de los mismos a través del uso de un lector RFID. 1.6 Tbps switching capacity. 24 puertos SFP+ (1/10/25G). 4 Puertos 40G uplink QSFP+ (40/100G). Transferencia de conocimientos en tareas fundamentales y documentación de proyecto; técnico implementador debe poseer certificación. Proveedor debe ser mínimo: Premier Certified Partner. y Smartnet 8x5XNBD por 3 años. Suscripción Cisco ONE para Switches y Smartnet 8x5XNBD por 3 años la cual debe incluir: ISE, StealthWatch y DNA Center.	1
	2	**Router Cisco: ISR4321 Voice Bundle**, Voice Gateway . Incluye configuraciones e instalacion in situs (conectar con el enlace conectividad virtual, al sip tronking, y los numero SRST transferencia de conocimientos en tareas fundamentales y documentación de proyecto; técnico implementador debe poseer certificación CCNP Collaboration. técnico implementador debe poseer certificación. Proveedor debe ser mínimo: Premier Certified Partner. y Smartnet 8x5XNBD por 3 años.	5

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	3	**SWITCHES DE DISTRIBUCION** (MODELO Cisco C9300-24T)SWITCHES CISCO DE 24 PUERTOS VELOCIDAD DE 1GBps EN CADA INTERFAZ. MODELO: C9300-24T CADA UNO CON UN MODULO C9300-NM-8X. SD-Access: Automatización basada en políticas desde el borde hasta la nube Segmentación y microsegmentación simplificada, con rendimiento y escalabilidad predecibles Automatización a través de Cisco DNA Center Política manejada a través de Cisco Identity Services Engine (ISE) Garantía de red proporcionada a través de Cisco DNA Center Los modelos PoE deben seguir energizando los puertos en caso de un Soft Reset. Los modelos de 24 puertos deben proveer soporte para 190Mpps o más en IPv4 e IPv6. A nivel de Stacking deben de soportar 480Gbps ancho de banda. 48 puertos 10/100/1000 cobre. Módulo de Uplink SFP+ de 8 puertos. 256 Gbps Switching Capacity. Número máximo de Mac Address 32,000. Algoritmo de cifrado MACSEC (802.1AE) AES 256 bits a nivel de hardware. Detección de malware en tráfico cifrado y detección de anomalías distribuidas. Soporte de MPLS para segmentación de la red. Programabilidad con soporte de protocolos NETCONF / YANG. Visibilidad y control de aplicaciones para clientes en la red cableada e inalámbrica. El switch debe tener embebido RFID Tag para facilitar el inventario de los mismos a través del uso de un lector RFID. Soporte de protocolo NBAR2. Suscripción Cisco ONE para Switches ,; técnico implementador debe poseer certificación. Proveedor debe ser mínimo:	5

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Premier Certified Partner. Smartnet 8x5XNBD por 3 años la cual debe incluir: ISE, StealthWatch y DNA Center, Incluye cable de Stack, Configuraciones e Instalación in situs (Santo Domingo), transferencia de conocimientos y documentación de proyecto	
	4	**Switch Cisco Catalyst 9200-48P Series PoE** Flash memory installed size: 4 GB IPv4 routes: 14k Stacking/chassis bandwidth: 288 Gbps - 580 Gbps Switching capacity: 128 Gbps - 400 Gbps MAC address table size: 32k entries Encryption protocols: AES-128/MACsec-128, SSH, TLS, IPsec Capacidades de capa 3 , incluidos OSPF, EIGRP, ISIS, RIP y acceso enrutado. Monitoreo de red avanzado usando NetFlow flexible completo. Acceso definido por software de Cisco (SD-Access): -Implementación y operaciones simplificadas con automatización basada en políticas desde el borde hasta la nube administrada con Cisco Identity Services Engine (ISE). -Garantía de red y tiempo de resolución mejorado a	10

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		través de Cisco DNA Center Los modelos PoE deben seguir energizando los puertos en caso de un Soft Reset. Capacidad de proveer hasta 30 Watts PoE+. Capacidad de soportar hasta 32,000 rutas (IPv4) a nivel de L3. Los modelos de 48 puertos deben proveer soporte para 160Mpps o más en IPv4 e IPv6. A nivel de Stacking deben de soportar 400Gbps ancho de banda. 48 puertos 10/100/1000 cobre. Modulo de Uplink SFP+ de 4 puertos. 160 Gbps Switching Capacity. Numero máximo de Mac Address 32,000. Algoritmo de cifrado MACSEC (802.1AE) AES 256 bits a nivel de hardware. Detección de malware en tráfico cifrado y detección de anomalías distribuidas. Soporte de MPLS para segmentación de la red. Programabilidad con soporte de protocolos NETCONF / YANG y Python. Visibilidad y control de aplicaciones para clientes en la red cableada e inalámbrica. El switch debe tener embebido RFID Tag para facilitar el inventario de los mismos a través del uso de un lector RFID. Soporte de protocolo NBAR2. Suscripción Cisco ONE para Switches y Smartnet 8x5XNBD por 3 años la cual debe incluir: ISE, StealthWatch y DNA Center. Tambien incluye: configuraciones e instalación in situs,, transferencia de conocimientos y documentación de proyecto; técnico implementador debe poseer certificación. Proveedor debe ser mínimo: Premier Certified Partner" DRN 6 200,000 1,200,000, **Smartnet 8x5XNBD por 3 años**	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	5	**Wireless Access Point, compatible con controladora Cisco CATALYST 9800-L**, con soporte del fabricante (end of life) de 5 años (o mas) en hardware y software. Compatibilidad con Cisco DNA. **Garantia de 3 años en piezas y servicios**	50
Lote VII- Equipos de Comunicación			
Lote VIII- UPS	**1**	**UPS: Smart-UPS 10kVA Modular** espandible a 15kVA, con el banco de Batería Interno y pequeñas. 400V, con 2 módulos de Baterías ampl. a 4, puesta en marcha 5X8, bypass de mantenimiento incorporado., capacidad conexion en paralelo Características principales Capacidad eléctrica de salida 8.0 Kilovatios / 10.0kVA Conexiones de salida (1) Hard wire 4-wire (3P + E) (Batería de reserva), (1) Hard wire 5-wire (3P + N + E) (Batería de reserva) (1) Screw terminals (Batería de reserva) Voltaje de salida nominal: 400V 3PH,Voltaje Nominal de Entrada: 400V 3PH, Tipo de Conexión de Entrada: Hard wire 5-wire (3P + N + E), Corriente máxima de entrada: 14.0A Tipo de forma de onda: Onda sinusoidal, Corriente máxima de salida: 16 Distorsión de voltaje de salida: Menos del 5% a plena carga Frecuencia de salida (sincronizada con la red): 47-53 Hz Para 50 Hz nominal Sincronización a la red, 50 Hz +/- 0,1% Para 50 Hz nominal Sin sincronizar Factor de cresta de carga: 3: 1 Frecuencia de entrada: 40 - 70 Hz Detección automática Rango de voltaje de entrada para operaciones principales: 304 - 477V	3

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Otros voltajes de entrada: 380, 415 Factor de potencia de entrada a plena carga: 0,98 Tiempo de recarga típico: 5 horas) Voltaje nominal de la batería: +/- 192 V (batería dividida referenciada a neutral) Duración prevista de la batería (años): 3-5 Voltaje de batería de fin de descarga: +/- 154 V"""" DRN 2 750,000 1,500,000, **Garantia 3 años fabricante,** Incluye instalacion y puesta en marcha en Dirección Regional Cibao Norte	
	2	**UPS DE 20KVA/18KW** Capacidad nominal 20kVA/18 kW ,factor de potencia 0.9 o superior Topología doble conversión, MODALIDAD DE UPGRADE EXTENDIBLE A 30KVA/27KW POR SOFTARE SIN AGREGAR NADA FISICO. Dimensiones del UPS, **Entrada eléctrica** Voltaje nominal de entrada 208V/120V, 220V/127V (+10, -15% o superior) , trifásico configurable Frecuencia de operación 50/60 Hz (45 a 65 Hz) Factor de potencia de entrada 0.99 típico Distorsión de corriente de entrada <5% THD **Salida eléctrica** Voltaje nominal de salida 208/120, 220/120 V ca	4

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		480/227 con transformador de salida 3,831 @ 480V y 600V (con transformador de aislamiento de entrada) Eficiencia 91% tipica **Batería** Tipo de batería 9 Ah, sellada, plomo-ácido, sin mantenimiento,TIEMPO EN BATERIAS 15 minutos minimo a 20kva de carga y 10 minutos minimos a 30kva de carga. Reemplazo de la batería Reemplazable en campo, Cargador Preestablecido es 8A **General** Diagnóstico Autoprueba del sistema completo al arranque, Bypass del UPS Automático en sobrecarga o falla del UPS, Paralelo para redundancia Si, usando tecnología para redundancia y capacidad, Sobrecarga 150% por 5 seg / 125% por 1 min (en línea), 110% por 10 min **Comunicaciones** Pantalla LCD LCD gráfica con luz a de fondo,LED (4) LED para notificación y alarma, **Garantia 3 años fabricante** Incluye instalacion y puesta en marcha en la Dirección Regional, Este, Santo Domingo Este	
Lote VIII- UPS			
IX- Soluciones de Seguridad	**1**	**Gestión y Correlación de Eventos e Incidentes de Seguridad (SIEM)** La solución deberá incluir un sistema de respuesta a incidentes basado orientado a CSIRT (Computer Security Incident Response Teams) permitiendo tener una solución escalable.	1

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

El sistema permite la definición de reglas de correlación de eventos, estableciendo la identificación de incidentes a nivel de red mediante reglas predefinidas para la correlación de eventos en diferentes dispositivos de red, a partir de estas reglas crear nuevas reglas para adaptarlas a las necesidades e identificar de forma automática las alteraciones de la red, aislando proactivamente incidentes o alteraciones de forma rápida y confiable.
El sistema debe incluir reglas de correlación preconfiguradas y parametrizables para ataques/riegos/fallas comunes tales como:
· Ataques de fuerza bruta
· Actividades sospechosas de logins por sistemas WEB
· Actividad multicasting sospechosa
· Ataques de reconocimiento haciendo escaneo de puertos por HTTP o HTTPS, ya sea a partir de eventos o flujos
· Gran cantidad de requerimientos HTTP no estándares
· Cantidad inusual de conexiones a una Base de Datos
· Múltiples logins fallidos desde una misma estación de trabajo.
· Intentos fallidos de login de forma intensa.
· Patrones de gusanos informáticos (Ej: W32.Blaster, SQL, Scanning, etc.)
· Vulnerabilidades conocidas (SSH)
· Cuentas de Windows creadas y eliminadas en menos de X horas (Ej; 24 horas)
· Malware
· Ataques DoS
Las reglas pre-configuradas deberán ser actualizadas por el fabricante y deberán basarse en los ataques, riesgos y fallas más comunes. Los datos de inteligencia de amenazas se pueden integrar en

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	forma de listas de observación, reglas de correlación y consultas de forma que aumenten la tasa de éxito de la detección temprana de fallas.
	La SIEM deberá ser ofertada con licenciamiento, garantías, mantenimiento, actualización y soporte técnico del fabricante por el tiempo que dure el contrato.
	La solución SIEM debe ser instalada directamente por personal del fabricante contratado directamente por el fabricante y de habla hispana
	La solución SIEM deberá soportar la recolección de al menos 12000 eps, en un entorno de arquitectura que permita el crecimiento de la solución de forma modular y conforme el proyecto lo requiera. El soporte de EPS debe ser de tráfico sostenido permitiendo además picos que excedan esas capacidades.
	La solución SIEM deberá ofrecer la capacidad de recolección de hasta 3000 Eventos por Segundo (EPS) y permitir picos de eventos adicionales sin que exista pérdida de eventos. La solución deberá permitir visualizar estadísticos de recolección de EPS, con el objetivo de mantener una correcta línea de funcionalidad.
	La solución SIEM ofertada debe constar en el último “cuadrante de líderes” del Cuadrante Mágico de Gartner en SIEM (Magic Quadrant for Security Information and Event Management). El oferente deberá incluir en su oferta dicho reporte, indicando la posición de la marca en el cuadrante
	La solución SIEM debe contar de forma integrada y sin necesidad de licenciamiento aparte, un módulo para la creación de nuevos recolectores para tecnologías no soportadas por el fabricante de forma nativa.
	La solución SIEM deberá permitir reducir falsos positivos y evaluar de forma dinámica el nivel de

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	riesgo considerando la habilidad de unificar y correlacionar:
	Eventos, información proveniente de herramientas de análisis de vulnerabilidades, y criticidad de los activos o dispositivos.
	La solución SIEM deberá permitir la correlación de eventos entre distintos dispositivos(Cross Device Correlation) al almacenar todos los eventos recolectados en una única tabla dentro de su base de datos, independiente del tipo de dispositivo o aplicativo que la genere, permitiendo así la definición de contenido de correlación entre distintos tipos de dispositivos (Firewalls, IDPs, Sistemas Operativos) sin la necesidad de utilizar estructuras complejas o lenguajes de acceso a datos para la consulta y unión de datos
	La comunicación entre todos los componentes de la solución SIEM debe ser cifrada sin impactar en la performance. Tambien deberá proveer mecanismos para asegurar la integridad de los logs almacenados.
	La solución SIEM deberá ser capaz de ofrecer acceso a los logs almacenados históricos sin la necesidad de hacer una restauración de estos (Restore)
	La solución SIEM deberá soportar la integración de eventos provenientes de Active Directory, DHCP y concentradores VPN para monitorear la asignación de direcciones IP y asociar eventualmente los usuarios.
	La solución SIEM deberá integrarse con las soluciones de gestión de vulnerabilidades que actualmente posee el INFOTEP; también deberá permitir la integración de dispositivos y aplicaciones de diferentes fabricantes, esto con el objetivo de evitar el desarrollo de los conectores.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

La solución SIEM debe proveer la capacidad de integrar fuentes de eventos que no sean soportadas actualmente “fuera de la caja” (tales como aplicaciones o desarrollos hechos en casa) a través de la incorporación de un conjunto de herramientas que permitan definir la lógica para extraer, obtener, normalizar y categorizar los eventos mediante un editor de expresiones regulares
Poder recolectar eventos de fuentes no soportadas deben proporcionar una interfaz que permita al equipo técnico de La compañía realizar las configuraciones necesarias
La solución SIEM deberá tener la posibilidad de detectar actividad anormal en base a comportamiento
Los componentes de la solución SIEM que realizan la recolección de eventos deberán ofrecer la capacidad de ajuste en la hora de los eventos, en el caso de que el dispositivo que genere el evento no cuente con la hora correcta o no tenga configurado un servidor de NTP.
La solución SIEM deberá poder integrarse con más de 1000 distintos tipos de productos y dispositivos en forma nativa sin la necesidad de definir un proceso de colección a la medida
La solución SIEM deberá tener la capacidad de recibir logs en formato crudo (RAW) a través de los siguientes mecanismos:
Syslog (TCP o UDP)
Transferencia remota de archivos con Logs crudos por SCP (Secure Copy), SFTP (Secure FTP)
Archivos de Logs en sistemas de archivos remotos mediante NFS y/o CIFS
OPSEC
La solución SIEM deberá soportar la auditoría de usuarios autorizados en el sistema y registrar su actividad

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

La solución SIEM deberá proporcionar un módulo integrado para la administración de eventos e incidentes de seguridad permitiendo asociar reglas a acciones tales como:
Enviar una notificación al equipo de operadores
Abrir y asignar un caso a un usuario para su investigación
Ejecutar un script
La Solución SIEM deberá permitir una gestión completa de todos sus componentes, empleando una sola consola de administración, incluyendo todas las configuraciones de los dispositivos, configuración de políticas, gestión de eventos, informes, análisis, afinación de la solución, y otras funciones relevantes
La consola de administración centralizada debe proveer la configuración de controles de acceso basado en roles (RBAC) y permitir la configuración de privilegios de acuerdo a los perfiles asignados por el administrador de la solución. Permitiendo la segregación de funciones y acceso a eventos, obedeciendo al principio de mínimo privilegio
La Solución SIEM deberá contar con tableros gráficos de indicadores (dashboards) para el monitoreo de datos y eventos en tiempo real. Un tablero gráfico o dashboard deberá contener y agrupar una o más representaciones gráficas o tabulares de los datos bajo una misma vista permitiendo vistas tipo Top 10 y Top 20.
La Solución SIEM deberá permitir desplegar más de un tablero gráfico (dashboards) de forma concurrente. Su actualización deberá ser en tiempo real sin la intervención del usuario refresco manual. Desde el tablero de indicadores se debe tener la capacidad de visualizar los eventos base (drill down) y el detalle de cada evento.
El sistema deberá permitir recolectar eventos de mínimo las siguientes fuentes y/o formatos:

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

· Syslog, Syslog NG
· SNMP o SNMP TRAPS
· Formatted log files
· ODBC y/o conexión hacia otras bases de datos remotas.
· Windows event logging API
· Plataformas de Seguridad (firewalls, seguridad endpoints, web gateways)
· El sistema debe almacenar los logs en su formato original, firmados, comprimidos y cifrados de forma centralizada. tener capacidad de almacenar al menos 3 años para fines de análisis histórico
· El sistema debe tener la capacidad de almacenar mínimo 3 meses de retención de logs en crudo disponibles en línea.
· El sistema debe ofrecer correlación en tiempo real, permitiendo gestionar las amenazas, rastrear y analizar la progresión de un ataque entre componentes y sistemas y, para el monitoreo de la actividad del usuario, rastrear y analizar la actividad de un usuario en todas las aplicaciones o rastrear y analizar una serie de transacciones relacionadas o eventos de acceso a datos. establecer relaciones entre mensajes o eventos generados por dispositivos, sistemas o aplicaciones, en función de características tales como fuente, destino, protocolo o tipo de evento
· El sistema debe permitir tareas generales como: normalizar, priorizar, recolectar y, evaluar el riesgo y debe permitir el envío de alertas en tiempo real
· El sistema debe permitir la exportación de documentos de auditoría de seguridad, análisis de riesgos y controles de seguridad de aplicación.
El monitoreo debe realizarse con alertas de criticidad, que podrán observarse mediante aplicaciones gráficas, dashboard configurable,

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

estadísticas, cantidad de incidentes, top de alertas, entre otros.
El sistema deberá estar orientado a recolección de registros de eventos para operaciones de seguridad y de cumplimiento de regulaciones y el SIEM deberá contar con dashboards predefinidos para regulaciones tipo
· PCI
· HIPPA
· ISO 27001, 27002
· FISMA
· SOX
· NIST
· SANS
· CIS
Permitir la creación de grupos de Dashboards que ayuden a cumplimientos de regulaciones internas
para proporcionar una interface de administración gráfica (GUI) propia, para el personal operativo, así como una interface de solo lectura diseñada para el personal de monitoreo. Esta interfaz debe ser web y segura (HTTPS)
La solución SIEM deberá incluir una interface administrativa basada en Web segura (HTTPS) para la configuración, monitoreo, análisis y explotación de eventos, así como una interface de administración vía CLI (línea de comandos)
La solución SIEM deberá soportar un mecanismo de autenticación nativo además de soportar mecanismos alternativos como: Microsoft Active Directory, Autenticación de doble factor, LDAP , RADIUS, etc
La solución SIEM deberá soportar autenticación y autorización mediante la definición de roles con privilegios granulares tanto para usuarios como para grupos. Los privilegios deben incluir:
· Agregar/Eliminar equipos

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

· Agregar/Eliminar políticas
· Gestión de Alarmas. Agregar/Eliminar/Editar
· Creación de Reglas custom y variables
· Gestión de Dispositivos
· Gestión de Eventos
· Etc
La solución SIEM deberá ser capaz de enviar alertas vía email, mensajes SMS por protocolo SNMP así como notificaciones directas a usuarios de la misma consola de administración.
El fabricante de la solución deberá contar con servicios profesionales que eventualmente puedan desarrollar Parsers a medida especialmente para la institución
El soporte técnico del fabricante deberá ser en modalidad 7x24 por chat, web y teléfono
El sistema debe permitir la exportación de documentos de auditoría de seguridad, análisis de riesgos y controles de seguridad de aplicación
El sistema debe incluir las funcionalidades de monitoreo, análisis y respuesta de eventos e incidentes de seguridad
La solución SIEM deberá ofrecer la capacidad de generar reportes calendarizados, con la opción de entrega por correo electrónico, publicación dentro de la misma solución, almacenarlo localmente:
· Reportes de Firewalls
· Reportes de Administración de Identidades.
· Reportes de IPS/IDS.
· Reportes de Red
· Reportes de Sistemas Operativos
· Reportes de Accesos
· Reportes de Correlación de Eventos
· Reportes de Vulnerabilidades
· Reportes de Cambios, etc

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

La solución SIEM deberá ofrecer la capacidad de publicar reportes una vez que hayan sido ejecutados para que los reportes puedan ser consultados posteriormente sin necesidad de ejecutarlos nuevamente
La solución SIEM debe contar con una base preinstalada de reportes, y permitir creación de reportes distribuidos en las siguientes categorías:
· Reportes PCI
· Reportes SOX
· Reportes de incidentes de seguridad
· Reportes de alertas de configuración del sistema
· Reportes por cada uno de las soluciones de seguridad integradas
· Reportes de múltiples dispositivos (cross-device)
· Reportes de vulnerabilidades y amenazas
La solución SIEM deberá incluir todos los reportes y no deberá estar limitado en cuanto a términos de licenciamiento
El módulo de reportes deberá permitir generar un reporte, ya sea predeterminado, o bien, copiando y personalizando reportes existentes
Los servicios profesionales de implementación se deben prestar por personal certificados en la solución o en su defecto por el fabricante. La infraestructura tecnológica adquirida debe ser entregada, instalada, configurada, probada y puesta en funcionamiento acorde a los requerimientos del INFOTEP e incluye también capacitación oficial del fabricante para 2 participantes
El proveedor del SIEM debe tener al menos 2 años de experiencia en el mercado de seguridad y proporcionar referencias sobre proyectos exitosos en clientes. Ser capaz de atender todo el alcance de los requisitos del SIEM

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		El ingeniero para la instalación, configuración, pruebas y puesta en funcionamiento de la solución en sitio deberá contar con certificación del manejo de la herramienta SIEM (Security Information and Event Management)	
		Presentar cartas de referencias de proyectos similar e incluye garantia y soporte del fabricante por 3 años	
		El suplidor debe proporcionar evidencia de posición de liderazgo de la solución en el Cuadrante Mágico de Gartner para soluciones de herramienta de clasificación de la información.	
		Debe diseñar y presentar para su aprobación un plan de trabajo, detalle de la metodología a utilizar y cronograma. También debe proporcionar entrenamiento oficial de la solución.	
		Documento de cierre de proyecto que contenga las configuraciones y pasos realizados durante la implementación del producto.	
	2	**HERRAMIENTA PARA CONTROL DE ACCESOS Y GESTION DE IDENTIDADES (IAM)**	1
		Plataformas/dispositivos/sistemas operativos soportados:	
		· Capacidad gestionar el control de acceso y autenticacion adaptiva basado en niveles de riesgo (comportamiento, red de acceso, dispositivo, etc.) de diferentes orígenes o plataformas.	
		· La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de Windows, Linux, entre otros.	
		· La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de MS SQL Server; MySqlServer, Postgres, ORACLE	
		· La solución propuesta deberá ser capaz de administrar cuentas privilegiadas basadas en AD.	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		· La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de dispositivos de red (CISCO, Aruba, Huawei y otros).	
		· La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de aplicaciones (Web y Cliente Servidor).	
		· La solución propuesta deberá ser capaz de administrar cuentas privilegiadas de SaaS/websites/web interfaces.	
		· La solución propuesta deberá ser capaz de soportar cualquier dispositivo de red mediante conexión SSH.	
		· La solución propuesta deberá ser capaz de soportar cualquier repositorio de datos mediante conexión ODBC.	
		· Capacidad de administrar cuentas de diferentes orígenes o plataformas.	
		· La solución propuesta deberá ser capaz de permitir a través de un administrador definir y agregar cuentas privilegiadas	
		· La solución propuesta deberá ser capaz de soportar dispositivos-plataformas "out of the box"	
		· La solución propuesta deberá proporcionar mecanismos para gestionar las cuentas privilegiadas, permitir autenticacion multi-factor por aplicacion y politica	
		· La solución propuesta deberá ser capaz de detectar automáticamente nuevos dispositivos Laptops o PCs Windows, Servicios Windows (Windows Services), Scheduled Tasks, IIS Service Accounts, etc. para su administración en la solución.	
		Administración de la solución	
		· La solución propuesta deberá permitir la gestión completa del ciclo de vida y seguridad simplificada	
		· Autenticación basada en riesgos y prevención proactiva de fraudes en tiempo real, computación	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		que tiene en cuenta el contexto y que recopila, propaga y aprovecha automáticamente la identidad, el dispositivo y el contexto geográfico, tambien gestionar activos no tecnologicos	
		· Si la solución propuesta utiliza una base de datos como back-end, esta base de datos deberá ser autoadministrable, es decir, no se requerirá la participación de un administrador de base de datos DBA para la implementación, respaldo, recuperación o hardening de la base de datos.	
		· La solución propuesta deberá tener la capacidad de aprovisionar usuarios en forma automática a partir de un Active Directory o LDAP, para así contar con un aprovisionamiento automático y transparente de cuentas que reflejen los cambios en dichos directorios.	
		· La solución propuesta deberá gestionar los aprovisionamiento acceso completo basado en roles y facilitar una experiencia mde autoservicio y cumplir con una gestion granular de derechos y la segregacion de funciones.	
		· Permitir rol integrado y aprovisionamiento de usuarios , acceso de autoservicio y gestión del ciclo de vida de roles y vistas completas del acceso de los usuarios con analitica para el cumplimiento, cuadros de mando e informes procesables	
		· La solución propuesta deberá proteger el acceso a aplicaciones institucionales tanto para implementaciones en la nube como on-premises.	
		· Permitir una experiencia segura en cualquier momento y lugar, inicio de sesión único perfecto de cualquier aplicación y desde cualquier dispositivo	
		Arquitectura de la solución	
		· La solución propuesta podrá ser instalada en servidores virtuales	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		· La solución propuesta deberá ser escalable mediante un diseño modular para adaptarse a crecimientos de utilización o de inclusión de más plataformas.	
		Disaster Recovery	
		· La solución propuesta deberá ser capaz de manejar la pérdida de conectividad con el repositorio central de passwords.	
		· La solución propuesta deberá ser capaz de soportar a sistemas replicados en datacenters de Disaster Recovery ubicados en diferentes localidades geográficas.	
		Network architecture support	
		· La solución propuesta deberá ser capaz de soportar una arquitectura de red distribuida donde los diferentes segmentos necesitan ser soportados desde una localidad central.	
		· La solución propuesta deberá contar dentro de su documentación, un diagrama técnico de la arquitectura de la solución incluyendo comunicaciones de red y reglas que permitan la administración de plataformas-servidores remotos conectados a través de un firewall (por ejemplo, servidores en una DMZ, localidades remotas, etc.	
		· La solución propuesta deberá contar dentro de su documentación con una lista de todos los puertos y protocolos utilizados por la solución, así como una descripción del uso de cada uno de estos puertos y protocolos.	
		· La solución propuesta deberá tener la capacidad de integrarse con métodos empresariales de autenticación, por ejemplo, LDAP, Windows SSO, PKI y mecanismos propios de autenticación.	
		· La solución propuesta deberá tener la capacidad de encriptar todos los datos	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		· La solución propuesta deberá tener la capacidad de encriptar la comunicación entre todos los componentes de la solución, incluyendo los componentes que residan en un mismo servidor.	
		· Separación de responsabilidades- La solución propuesta deberá tener la capacidad de permitir que ciertos administradores no puedan visualizar los passwords que son controlados por otros departamentos de la institucion, por ejemplo, que administradores de Windows Server no puedan visualizar los passwords ni accesos a instancias de bases de datos SQL Server.	
		· Plataforma segura - La solución propuesta deberá ser capaz de asegurar el repositorio de passwords (firewall, hardening, control remoto limitado y restringido, etc.)	
		· La solución propuesta deberá ser capaz de contar con un repositorio seguro y a prueba de falsificaciones (tamper-proof) de credenciales privilegiadas, políticas, grabaciones, entitlements, registros de auditorías, etc.	
		Integraciones	
		· La solución propuesta deberá contar con la capacidad de integrarse con sistemas tipo SIEM.	
		· La solución propuesta deberá contar con la capacidad de integrarse con sistemas de tickets tipo service desk.	
		· Identity Management/User Provisioning	
		· Integrarse con aplicaciones nativas, personalizadas y de terceros, servidores de aplicaciones, marcos de persistencia de datos, servidores de directorio, portales y sistemas de gestión de contenido. Tambien la interoperabilidad con estándares de autorización de la industria para conseguir una seguridad mejorada y mayor flexibilidad	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		· La solución propuesta deberá tener la capacidad de hacer búsquedas y controlar el acceso a passwords para nested global groups incluyendo múltiples forests, localidades geográficas, incluyendo búsquedas complejas en LDAP.	
		· La solución propuesta deberá tener la capacidad de integrarse con soluciones de manejo de vulnerabilidades para realizar escaneos automáticos y profundos	
		· La solución propuesta debe tener la capacidad de mapear cuentas privilegiadas y cuentas personales de la institucion con una herramienta stand alone.	
		· La solución propuesta debe tener la capacidad de descubrir e identificar fácilmente cuentas privilegiadas que no se adhieren a la política corporativa de passwords sin haber implementado aún una solución de manejo de cuentas privilegiadas	
		· La solución propuesta deberá tener la capacidad de listar cuentas utilizadas para hacer login a servidores/Workstation en un periodo de tiempo determinado (por ejemplo, en el último trimestre), sin haber implementado aún un sistema de manejo de cuentas privilegiadas.	
		· La solución propuesta deberá tener la capacidad de mostrar en un quick view todas las actividades relativas a una cuenta privilegiada, como el release de un password o sesiones de administración utilizando dicha cuenta.	
		· La solución propuesta deberá tener la capacidad de generar todos los reportes de forma periódica, bajo demanda o en forma programada.	
		· La solución propuesta deberá tener la capacidad de generar reportes detallados y programados con la siguiente información:	
		· Entitlements Reports	
		· Actividad de usuarios	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		· Inventario de cuentas privilegiadas	
		· Inventario de aplicaciones	
		· Reportes de Cumplimiento	
		La solución propuesta deberá tener la capacidad de exportar los reportes a los siguientes formatos	
		· Microsoft Excel	
		· CSV	
		· PDF	
		La solución propuesta deberá tener la capacidad de generar reportes de todos los cambios administrativos en el sistema	
		La solución propuesta deberá tener la capacidad de generar un reporte de todos los accesos al sistema	
		La solución propuesta deberá tener la capacidad de generar un reporte de intentos inválidos de login al sistema	
		La solución propuesta deberá tener la capacidad de generar un reporte de todos los checkouts de passwords y de usuarios que solicitan passwords	
		La solución propuesta deberá tener la capacidad de reportar los cambios automáticos de passwords después del proceso de verificación de los mismos	
		La solución propuesta deberá tener la capacidad de soportar controles duales, la solución debe soportar diferentes configuraciones de aprobaciones cuando por ejemplo un usuario solicite un password. Esto debe incluir notificaciones automáticas vía email.	
		La solución propuesta deberá tener la capacidad de que un usuario pueda solicitar el uso de una cuenta privilegiada para una fecha u hora futura.	
		La solución propuesta deberá tener la capacidad de soportar procesos flexibles de workflows para designar múltiples aprobadores. Por ejemplo, se requieren dos o más aprobaciones antes de que el acceso sea autorizado.	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		La solución propuesta deberá tener la capacidad de generar logs de los procesos de workflow y/o la habilidad de generar reportes o auditarlos.	
		La solución propuesta deberá tener la capacidad de configurar una longitud mínima de contraseña y complejidad para cuentas de super-usuarios de todos los sistemas.	
		La solución propuesta deberá tener la capacidad de fortalecer la política de contraseña cuando las cuentas se cambian manualmente, así como cuando los sistemas cambian la contraseña aleatoriamente	
		La solución propuesta deberá tener la capacidad de enviar correos electrónicos para lo siguiente:	
		* Accesos a Sistemas	
		* Cambios a Sistemas	
		* Uso de Contraseñas	
		* Solicitudes de aprobación de contraseña	
		Monitoreo/Grabación de actividades privilegiada	
		· La solución propuesta deberá tener la capacidad de grabar sesiones privilegiadas en: Windows, Virtual Servers, Linux, Ruteadores y Switches, Bases de Datos, Aplicaciones Web.	
		· La solución propuesta deberá tener la capacidad de extender para soportar cualquier aplicación o dispositivo de conexión para monitorear y habilitar autenticación única privilegiada.	
		· La solución propuesta deberá tener la capacidad de contar con métodos de monitoreo.	
		Arquitectura y Seguridad	
		·Deberá tener la capacidad de no requerir que se instalen agentes en los dispositivos	
		· La solución propuesta deberá tener la capacidad de no requerir cambios en la topología de red con la finalidad de asegurar que todas las sesiones privilegiadas son controladas por la solución.	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		· La solución propuesta deberá tener la capacidad de que las conexiones remotas pueden ejecutarse sin tener que exponer las credenciales privilegiadas aún manteniendo un control de acceso estricto.	
		·Deberá tener la capacidad de soportar auditoría correlacionada y unificada para la administración y actividad de cuentas compartidas y cuentas privilegiadas.	
		· La solución propuesta deberá tener la capacidad de asegurar responsabilidad personal cuando se abre una sesión privilegiada con una cuenta compartida	
		· La solución propuesta deberá tener la capacidad de ayudar a investigar causas raíz y análisis forense.	
		·Deberá tener la capacidad de monitorear, controlar y grabar a Administradores de base de datos y tener la capacidad de no impactar en el rendimiento de la base de datos.	
		· La solución propuesta deberá tener la capacidad de fortalecer la autenticación y flujos de acceso para iniciar una sesión privilegiada en ESX/ hosts de ESXi, administración de herramientas (vCenter), Acropolis, Hypert V, etc	
		·Deberá tener la capacidad de ofrecer análisis inteligente para detectar actividad sospechosa para cuentas privilegiadas.	
		· La solución propuesta deberá tener la capacidad de reportar comportamiento anormal de cuentas privilegiadas - basado en algoritmos de adopción y comportamiento - orientado a soluciones SIEM	
		· La solución propuesta deberá tener la capacidad de generar notificaciones de uso excesivo y uso fuera de horario de cuentas privilegiadas.	
		· La solución propuesta deberá tener la capacidad de detectar si una cuenta privilegiada es usada en una maquina sin una previa solicitud de acceso.	
		Incluye:	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Diseñar y presentar para su aprobación un plan de trabajo, detalle de la metodología a utilizar y cronograma. También debe proporcionar entrenamiento oficial de la solución.	
		El ingeniero para la instalación, configuración, pruebas y puesta en funcionamiento de la solución en sitio deberá contar con certificación oficial del manejo de la herramienta ofrecida	
		Debe realizar la implementación de la solución con las configuraciones, pruebas e implementacion en funcionamiento	
		El proveedor de la herramienta debe tener al menos 3 años de experiencia en el mercado de seguridad y proporcionar referencias sobre proyectos exitosos en clientes.	
		El suplidor debe proporcionar evidencia de posición de liderazgo de la solución en el Cuadrante Mágico de Gartner para soluciones de herramienta de clasificación de la información.	
		Incluye garantia y soporte del fabricante por 3 años	
		Documentación de cierre de proyecto que contenga las configuraciones y pasos realizados durante la implementación del producto	
	3	**HERRAMIENTA PARA CLASIFICACIÓN DE LA INFORMACIÓN**	1
		La solución debe de descubrir e identificar grandes volúmenes de datos, almacenados en las instalaciones, escanear recursos compartidos de red (en las instalaciones y en línea)	
		Ejecutar exploraciones programadas para clasificar automáticamente los archivos en función de varios factores, incluidos las propiedades / atributos del archivo, el contenido y / o los metadatos	
		Cifrar automáticamente los archivos según las reglas de sensibilidad de datos. Esta capa adicional de	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

protección. Se puede agregar en función de los detalles del propio archivo o de su ubicación
Recopilar información del archivo durante los análisis, incluidas las propiedades del archivo, la clasificación (antes y después del análisis), y controles de acceso. Esto le permite ver cuáles son sus datos, dónde están y quién tiene acceso a ellos
Analizar los resultados a través del panel integrado o sus propias herramientas de análisis para minimizar los datos en riesgo. Supervisar las actividades de clasificación y optimizar las políticas de identificación de datos y las soluciones de almacenamiento de datos
La solución debe tener la capacidad de poner en cuarentena los archivos almacenados de forma inadecuada, marcar los archivos para su seguimiento y realizar acciones basadas en los resultados de la exploración. Esto puede incluir la actualización de políticas de seguridad de sus usuarios en el tratamiento de datos sensibles
Mejorar la capacidad de DLP, ERM y otras soluciones de seguridad para aplicar los adecuados controles basados en la clasificación.
Incluye:
Debe diseñar y presentar para su aprobación un plan de trabajo, detalle de la metodología a utilizar y cronograma. También debe proporcionar entrenamiento de curso oficial de la solución.
El ingeniero para la instalación, configuración, pruebas y puesta en funcionamiento de la solución en sitio deberá contar con certificación oficial del manejo de la herramienta ofrecida
Debe realizar la implementación de la solución con las configuraciones y políticas de clasificación de la información del INFOTEP
La empresa debe tener al menos 2 años de experiencia en el mercado de seguridad y

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		proporcionar referencias sobre proyectos exitosos en clientes.	
		El suplidor debe proporcionar evidencia de posición de liderazgo de la solución en el Cuadrante Mágico de Gartner para soluciones de herramienta de clasificación de la información.	
		Incluye garantia y soporte del fabricante por 3 años	
		Documentación de cierre de proyecto que contenga las configuraciones y pasos realizados durante la implementación del producto.	
	4	**WEB APPLICATION FIREWALL (WAF) PARA PROTEGER A LOS SERVIDORES DE APLICACIONES WEB**	1
		OBJETIVOS	
		· Proteger de ataques de inyección SQL	
		· Proteger de scripts entre sitios	
		· Proteger de ataques común aplicaciones web, como la inyección de comandos, el contrabando de solicitudes HTTP, la división de respuestas HTTP y el ataque de inclusión remota de archivos	
		· Detectar errores de configuración de aplicaciones comunes (por ejemplo, Apache, IIS, etc.). · Prevenir contra bots, rastreadores y escáneres.	
		FUNCIONALIDADES DE PLATAFORMA DE WEB APPLICATION FIREWALL (WAF)	
		· 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.	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

· 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.
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

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

· 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
· Por usuario firmado en el aplicativo web
· Tiempo de respuesta o tamaño de la respuesta HTTP
· La solución deberá cubrir todas las vulnerabilidades expresadas en el OWASP, SANS, CWE más reciente.
· La solución deberá cumplir con todos los criterios de evaluación del WAFEC definidos por el Web Application Security Consortium.
· La solución deberá proporcionar el bloqueo de direcciones IP, sesiones TCP o usuarios de la aplicación web.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

· La solución deberá proteger tanto las aplicaciones Web HTTP, como las aplicaciones web SSL y HTTPS.
· Evitar la inyección SQL, XSS, RFI y otros tipos de amenazas a la capa de aplicación gracias a las reglas automatizadas, con lógica de detección avanzada que se ajuste dinámicamente según las características de las solicitudes entrantes
· Proteja las aplicaciones y API contra ataques de denegación de servicio (DoS) mediante la supervisión y el bloqueo de clientes que superen los umbrales de frecuencia de solicitudes. Los infractores se bloqueen automáticamente para proteger los orígenes del sitio.
· Análisis avanzado de seguridad web: acceder a la telemetría de ataques detallada y al análisis de los eventos de seguridad para evaluar qué cambios se necesitan para mejorar las protecciones de seguridad y optimizar las configuraciones en función de las necesidades institucionales específicas.
· 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.
· Controles IP/Geo que nos permitan bloquear o permitir el tráfico que provenga de una IP, subred o área geográfica específicas. Nos permita bloquear solicitudes maliciosas de direcciones IP específicas o del tráfico de The Onion Router (Tor), usado por los hackers para ocultar su identidad.
· Ofrezca un generador de reglas personalizadas para generar de forma rápida y fácil reglas personalizadas que se puedan utilizar para gestionar escenarios únicos no cubiertos por reglas estándar o

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

para reparar rápidamente nuevas vulnerabilidades del sitio web.
· Incluya un certificado SSL o TLS para distribuir nuestro contenido con seguridad, ayude a prevenir el robo de datos y proporcione seguridad HTTPS para los sitios web y nuestros usuarios de forma gratuita.
· Facilite la presentación de informes sobre la seguridad web; supervise y evalúe continuamente la efectividad de las protecciones. Pueda crear informes en tiempo real para supervisar las actividades diarias, investigar ataques por tipo y ver informes sobre API específicas, tráfico DoS y mucho más.
· En los modos puente (bridge) o sniffer, la solución deberá poder desencriptar el tráfico SSL para inspección, sin terminar o cambiar la conexión HTTPS.
· Alertas vía correo electrónico en tiempo real usando filtros estáticos y umbrales que se puedan configurar fácilmente para solo notificar a destinatarios concretos.
· Ofrezca una capa de protección adicional que impida que los atacantes eludan la protección en la nube y dirijan sus ataques a la infraestructura de origen.
· Identifique, categorice y gestiona los bots que acceden a su sitio. Los algoritmos automatizados utilizan la telemetría del comportamiento tanto humano como de los bots para detectar y tratar los bots más sofisticados.
· 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.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

· La solución deberá soportar la conmutación de datos por error o failover.
· La solución deberá soportar las opciones fail-open y fail-closed.
· 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.
· Permitan utilizar aplicaciones SIEM locales y en la nube, como Splunk, QRadar, ArcSight y muchas más
· Proteja los sitios web de amenazas JavaScript, como el robo de información web, el formjacking y los ataques de Magecart, mediante la identificación de recursos vulnerables, la detección de comportamientos sospechosos y el bloqueo de actividades maliciosas.
· 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.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

· 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.
· Mitigación instantánea de ataques DDoS en la capa de red
· Reglas WAF seleccionadas y actualizadas por los investigadores de amenazas para mantenerse al día con las amenazas más recientes
· Modelo de gestión de WAF automatizado para elimina la sobrecarga operativa de la protección de aplicaciones web
· Visibilidad e informes granulares de ataques con paneles de nivel ejecutivo y análisis de seguridad en profundidad
· Gestión de contenido y tráfico, la gestión de enlaces y la protección contra ataques, al mismo tiempo que ayude a escalar las propiedades en línea para satisfacer la demanda máxima.
· Los usuarios se beneficien de los protocolos web modernos, rápidos y eficientes
· 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.
· Garantice la precisión para bloquear con confianza a medida que cambia el panorama de amenazas.
· Creación automática de políticas y propagación de reglas que permitan al equipo de seguridad usar código de terceros sin riesgo.
· Proteja las aplicaciones web y las API, que proteja desde el borde hasta la base de datos, que el tráfico que recibamos sea solo el tráfico que deseamos.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

· Seguridad automatizada compatible con PCI que integre análisis para ir más allá de la cobertura OWASP Top 10 y reduzca los riesgos creados por código de terceros.
· Proteja las aplicaciones activas y heredadas, aplicaciones de terceros, API y microservicios
· Proteja las aplicaciones en la nube, contenedores, máquinas virtuales y más
· Se adapte tan rápido como nuestras aplicaciones mediante la creación de políticas y la propagación de reglas automatizadas.
· Protección local o en la nube, poder implementar el WAF exactamente donde lo necesitemos: dispositivo físico o virtual.
· Poder decidir cómo defender mejor nuestras aplicaciones utilizando perfiles dinámicos e inteligencia de ataques
· Compatible con plataformas:
· SIEM (MicroFocus, Alien Vault, Splunk, LogRhythm, Elastic, QRadar, McAfee, etc)
· API e integraciones (Terraform, Demisto, Github, Servicenow, PageDuty, etc)
· El técnico debe estar certificado por el fabricante de la solución WAF
PRINCIPALES ENTREGABLES
A modo macro se detallan los principales entregables esperados:
El suplidor debe realizar la implementación de la solución con las configuraciones y políticas de protección de las aplicaciones web del INFOTEP
Propuesta de Web Application Firewall (WAF)
Plan de trabajo de Implementación de un Web Application Firewall (WAF)

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		El suplidor debe entregar el equipo Web Application Firewall (WAF) del Instituto Nacional de Formación Técnico Profesional (INFOTEP) en funcionamiento	
		PERFIL PROFESIONAL	
		El proveedor de Web Application Firewall (WAF) debe tener al menos 3 años de experiencia en el mercado de seguridad y proporcionar referencias sobre proyectos exitosos en clientes.	
		El suplidor debe proporcionar evidencia de posición de liderazgo de la solución en el Cuadrante Mágico de Gartner (2019-2022) para soluciones de herramienta Web Application Firewall (WAF)	
		El proveedor debe ser capaz de atender todo el alcance de los requisitos del appliance de seguridad, incluido el rendimiento, velocidad de conexión desde la pequeña oficina hasta el centro de datos en un único dispositivo de hardware.	
		El ingeniero para la instalación, configuración, pruebas y puesta en funcionamiento de la solución en sitio deberá contar con certificación oficial del manejo de la herramienta ofrecida	
		Incluye garantia y soporte del fabricante por 3 años	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

	5	**Solución de detección y respuesta ampliadas XDR 1000-1999** **ADMINISTRACIÓN** Múltiples políticas ,Actualizaciones controladas **REDUCCIÓN DE SUPERFICIE DE ATAQUE** Protección web, Reputación de descargas, Control web / bloqueo de URL basado en categorías, Control de periféricos,Control de aplicaciones,Listas blancas de aplicaciones (bloqueo de servidor) **ANTES DE QUE SE EJECUTE EN EL DISPOSITIVO** Detección de malware con Deep Learning,Escaneado de archivos antimalware,Live Protection,Análisis de comportamiento previo a la ejecución (HIPS),Bloqueo de aplicaciones no deseadas,Sistema de prevención de intrusiones (IPS) **DETENER LA AMENAZA EN EJECUCIÓN** Prevención de pérdidas de datos Análisis de comportamiento en tiempo de ejecución (HIPS) Interfaz de análisis antimalware (AMSI) Detección de tráfico malicioso (MTD) Véase la nota Prevención de exploits Mitigaciones de adversarios activosProtección contra archivos de ransomware Protección del registro de arranque y disco Protección contra Man-in-the-Browser (Navegación segura) Bloqueo de aplicaciones mejorado **DETECTAR** Live Discover (consultas SQL en toda la infraestructura para la búsqueda de amenazas y la higiene de las operaciones de seguridad TI) Biblioteca de consultas SQL (consultas ya escritas totalmente personalizables) Almacenamiento de datos en disco de rápido acceso (hasta 90 días) Fuentes de datos entre productos (p. ej. Firewall, Email) Consultas entre productos Sophos Data Lake (almacenamiento de datos en la	1

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		nube) Consultas programadas **INVESTIGAR** Casos de amenazas (Análisis de causa raíz) Análisis de malware con Deep Learning Información sobre amenazas avanzada de SophosLabs a demanda Exportación de datos forenses **SOLUCIONAR** Eliminación de malware automatizada Seguridad sincronizada con Security Heartbeat Live Response (Acceso remoto al terminal para realizar investigaciones adicionales y tomar medidas) Aislamiento de servidores a demanda "Limpiar y bloquear" en un solo clic **VISIBILIDAD** Protección de cargas de trabajo en la nube (Amazon Web Services, Microsoft Azure, Google Cloud Platform) Control de aplicaciones sincronizado (visibilidad de aplicaciones) Gestión de la posición de seguridad en la nube (supervise y proteja hosts en la nube, funciones sin servidor, buckets de S3 y más) **CONTROL** Caché de actualización y repetidor de mensajes Exclusiones de escaneado automático Monitorización de integridad de archivos **DETECTAR** Live Discover (consultas SQL en toda la infraestructura para la búsqueda de amenazas y la higiene de las operaciones de seguridad TI) Biblioteca de consultas SQL (consultas ya escritas totalmente personalizables) Almacenamiento de datos en disco de rápido acceso (hasta 90 días) Fuentes de datos entre productos (p. ej. Firewall, Email) Consultas entre productos Sophos Data Lake (almacenamiento de datos en la nube)	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Consultas programadas **EXPLOIT PREVENTION** Aplicación de la prevención de ejecución de datos Selección aleatoria del diseño del espacio de direcciones obligatoria ASLR de abajo a arriba Página NULL (Protección de desreferencia NULL) Asignación de pulverización del montón Pulverización dinámica del montón Eje de la pila Ejecución de la pila (MemProt) Mitigaciones de ROP basadas en pilas (Autor de llamada) Mitigaciones de ROP basadas en ramas (Asistidas por hardware) Sobrescritura del controlador de excepciones estructurado (SEHOP) Filtrado de tabla de direcciones de importación (IAF) Carga de bibliotecas Inyección de DLL reflectiva Shellcode Modo Dios de VBScript Wow64 Syscall Vaciado de procesos Secuestro de DLL Omisión de AppLocker Squiblydoo Protección de APC (Double Pulsar / AtomBombing)Aumento de privilegios de procesos Protección shellcode dinámica EFS Guard CTF Guard ApiSetGuard **MITIGACIONES DE ACTIVE ADVERSARY** Protección contra robos de credenciales Mitigación de cuevas de código Protección contra Man-in-the-Browser (Navegación segura) Detección de tráfico malicioso Detección de shell Meterpreter **ANTI-RANSOMWARE** Protección contra archivos de ransomware Detección automática de archivosProtección del registro de arranque y disco **BLOQUEO DE APLICACIONES** Navegadores web (incluido HTA) Complementos de navegadores web Java Aplicaciones multimedia Aplicaciones de Office **PROTECCIÓN CON DEEP LEARNING** Detección de malware con Deep Learning Bloqueo de aplicaciones no deseadas (PUA) con Deep	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Learning Supresión de falsos positivos **RESPONDER INVESTIGAR ELIMINAR** Casos de amenazas (Análisis de causa raíz) Seguridad sincronizada con Security Heartbeat **SERVICIO GESTIONADO** Búsqueda de amenazas a partir de pistas 24/7 Comprobaciones del estado de seguridad Retención de datos Informes de actividades Detección de adversarios Neutralización y remediación de amenazas El proveedor debe tener al menos 2 años de experiencia en el mercado de seguridad y proporcionar referencias sobre proyectos exitosos en clientes. Incluye configuración, implementación y despliegue de la solución El Fabricante debe proporcionar evidencia de posición de liderazgo de la solución en el Cuadrante Mágico de Gartner para soluciones XDR El suplidor debe realizar la implementación de la solución con las configuraciones y políticas de protección INFOTEP **Incluye garantia y soporte del fabricante por 3 años**	
	6	**FortiGuard Enterprise Protection, FortiGate 100F** Licencia 360 Protection Bundle.. Debe incluir las siguientes tecnologías de protección, detección, prevención y soporte: Control de aplicaciones NGFW, Servicio de prevención de intrusiones (IPS), Antivirus, Seguridad de botnet, Reputación de IP / dominio, Servicios de seguridad móvil, Filtrado web, Antispam, FortiSandbox Cloud, Servicios de protección contra ataques de virus (VOS), Desarmado y reconstrucción de contenido (CDR), Clasificación de seguridad, Servicio de Seguridad Industrial, FortiGate Analytics & Management, Overlay Orchestration, Automation y Monitoring. **Soporte FortiCare. 3 años**	2

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

IX- Soluciones de Seguridad			
Lote X-TELEFONIA	1	**TELEFONIA IP, ENTERPRISE AGREEMENT FLEX EDUCATIVO 36 MESES**	1
		CENTRAL TELEFONICA	
		Se solicita la actualizacion de nuestro sistema de Comunicaciones Unificadas, Colaboración y Contact Center Marca Cisco, que actualmente se encuentra en la vesion 11.0	
		Debe soportar e incluir la capacidad de configurar sin necesidad de adquirir componentes adicionales a más de 1,300 usuarios y al menos 5,000 dispositivos finales en la solución propuesta.	
		La solución debe ser entregada On-Premise (Infraestructura local), pero debe permitir el registro de dispositivos en la nube (cloud) que se integren y comuniquen con los elementos On-Premise.	
		La solución debe estar soportada por un sistema operativo reconocido en la industria como robusto y seguro (tal como CentOS, RedHat Linux)	
		Debe ser Virtualizada en VMware y soportar al menos las versiones 6.7 y/o 7.0 del virtualizador ESXi.	
		Se deben incluir los servidores físicos necesarios para alojar la solución propuesta, se debe brindar redundancia y alta disponibilidad física, lógica. Además de redundancia de servidores se debe incluir redundancia eléctrica en los mismos.	
		Los equipos incluidos en la propuesta no deben estar fuera de vida útil por parte del fabricante, ni ser usados o reconstruidos (Refurbished).	
		La central debe estar configurada en HA. Es decir se debe suministrar todo el hardware necesario para lograr redundancia física de los equipos. De igual	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

forma los equipos deben ser redundantes en sus componentes (FAN, Power Supply)
Se debe incluir alta disponibilidad para las aplicaciones.
Requerimientos funcionales
Soportar e incluir funcionalidades de colaboración como son: mensajería instantánea, video llamadas, conferencias, presencia, entre otras.
Soportar e incluir encolamiento de llamadas con capacidad de desplegar diferentes audios durante el tratamiento de la llamada dentro de la misma central telefónica.
Debe incorporar un modulo analitica 100% cloud, que permita monitoriar el sistema y gestionar el manejos de certificados
Soporte nativo para realizar conferencias con PIN y sin PIN, dentro de la misma central telefónica.
Debe soportar IPv6.
La solución propuesta debe incluir la funcionalidad de configurar "extensiones móviles" que permiten a los usuarios utilizar su perfil de teléfono y extensión desde otro dispositivo.
La solución debe permitir a los clientes móviles registrarse a la Central Telefónica, ya sea mediante VPN o vía VPN-less.
Debe incluir configuracion puentes de conferencias de audio
Debe soportar e incluir las música en espera.
Debe soportar la administración y registro de dispositivos de video conferencia y Telepresencia en la central propuesta.
Debe soportar los protocolos como son LDAP para sincronizar los usuarios con un controlador de dominio.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Debe incluir la función de replicación de plan de numeración global para sincronizar el plan de numeración.
Debe contar con herramientas que permita realizar reportaría del estado de la central, los atributos (procesador, memoria, entre otras) de la misma, estadísticas del consumo de sus servicios, entre otros. Estas herramientas deben conectarse al servidor vía HTTPS.
La solución debe permitir agregar los teléfonos manualmente, auto registro o a través de plantillas.
Los usuarios pueden ser creados a través de las siguientes vías: manual y sincronización de LDAP.
Los dispositivos que se registran a la central telefónica deben soportar al menos los siguientes codecs: G.711a/μ-law, G.722, G.729, H265, GSM, iSAC, iLBC, Opus, entre otros.
Debe brindar resúmenes/estadísticas de las llamadas que se hacen a través de la central.
Debe contar con un cliente unificado que soporte e incluya las funcionalidades como sigue:
- Funcionalidad de mensajería instantánea con soporte de conversaciones individuales, en grupo y en salas; con personas dentro y fuera de la organización.
- El usuario debe poder terner acceso a su numero de extension registrado en la PBX para realizar y recibir llamadas.
- La solución presentada debe soportar la funcionalidad de Reuniones Virtuales en tiempo real con Telepresencia y Video conferencia.
- Funcionalidad de poder realizar llamadas de audio y video, de igual forma integración de este dispositivo en llamadas de presencia.
- Funcionalidad de visualización y manejo de los mensajes de voz desde la interfaz de este cliente.
- Funcionalidad de compartir pantalla entre usuarios

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- Funcionalidad de compartir documentos y edicion en linea
- Funcionalidad crear pizarras
- La solución propuesta debe permitir almacenar de manera unificada la información de las reuniones, los archivos de grupos de trabajos, y demás informaciones intercambiadas en el sistema.
- Funcionalidad de acceso remoto, inicio de sesión único en el acceso a todas las cargas de trabajo de colaboración para usuarios móviles y tele trabajadores sin la necesidad de un cliente VPN en el dispositivo.
- Funcionalidad de integración con el calendario O365 y Google
- Debe permitir que los usuarios accedan a sus cuentas de diferentes dispositivos de manera simultánea.
- Funcionalidad de mostrar la presencia del usuario, tales como: en reunión, en llamada, disponible, no disponible, entre otros.
Seguridad
La solución debe proveer un canal de comunicación interno cifrado de última generación y características de alta seguridad para toda la institución.
- La solución debe proveer encriptación en la comunicación "End to End".
- Debe soportar e incluir capacidad de instalar certificados ECDSA al igual que los RSA, tanto en la parte administrativa de la plataforma como de servicios.
- Debe soportar la funcionalidad de Single Sign ON.
- La solución provee un esquema de roles basados en acceso que permite asignar de manera granular los privilegios en el portal de administración.
- La solución propuesta maneja conexiones seguras para el acceso al portal de administración para la solución VoIP y los teléfonos (HTTPS, SSH).

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

- La solución provee logs de auditoria
Requerimientos de Licencias y Soporte
La propuesta debe incluir al menos 1,000 licencias para Knowledge Workers en modo suscripcion.
Licenciamiento de colaboracion para al menos 45 mil estudiantes
- el modelo de licenciamiento debe permitir funcionalidades avanzadas y registrar al menos 10 dispositivos para dicho usuario
- Los usuarios anteriores deben tener la capacidad de poder utilizar IPAD, PC, LAPTOP o ANDROID como dispositivos de usuario
- Todos los usuarios deben contar con mensajería instantánea y presencia
- el licenciamiento debe permitir hasta un 20% de crecimiento sobre el licenciamiento propuesto.
- el licenciamiento dede permitir e incluir el registo de telefonos para espacio publicos sin exceder el 50% de las licencias propuestas.
- el licenciamiento dede permitir e incluir el registro de telefonos en la nube.
- Todos los usuarios deben contar con el licenciamiento necesario para funciones VPN-less.
Debe incluirse la funcionalidad de mensajería instantánea y presencia para todos los usuarios licenciados.
Este componente debe contar con al menos 3 año de soporte por parte del fabricante, acceso a actualización de software y mantenimiento, no debe estar fuera de venta y/o vida por parte del mismo. Para el remplazo de partes en los componentes de hardware se deben incluir un soporte SLA de 8 horas, 5 días semana, siguiente día laborar
**** Se debe demostrar en un ambiente de producción similar al propuesto las funcionalidades de: conferencias, llamadas de video externas/internas y cliente móvil sin VPN.**

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

**** Debe incluir encripción entre los telefonos.**
**** La central Telefonica debe Soportar integracion de manera nativa con soluciones de video conferencias en la nube**
SISTEMA DE MENSAJERÍA DE VOZ
la Solucion propuesta debe ser del mismo fabricante de la PBX propuesta, a fines de garantizar un funcionamiento optimo.
Debe ser e incluir escalabilidad de mínimo 48 puertos y 5,000 usuarios.
Se deben incluir las licencias necesarias para buzones de voz para todos los usuarios licenciados.
Solución virtualizada en VMware.
Debe soportar la funcionalidad de Single Sign ON.
Se deben incluir los servidores físicos necesarios para alojar la solución propuesta, se debe brindar redundancia y alta disponibilidad física, lógica. Además de redundancia de servidores se debe incluir redundancia eléctrica en los mismos.
La Solucion debe estar configurada en HA.
Soportar grabaciones de saludos de audio
Debe cumplir con los requerimientos de la certificación del Departamento de Estado de los Estados Unidos de Joint Interoperability Test Command (JITC)
Enviar un mensaje a múltiples destinatarios.
Soportar la funcionalidad de Text-to-Speech (TTS), y poder accesar los correos electrónicos desde el teléfonos.
Debe soportar al menos los siguientes codec para la reproducción de mensajes: G.711 mu-law, G.711 a-law, G.722, G.729, iLBC, entre otros.
Debe soportar IPv6.
Debe soportar al menos los siguientes codec para la grabación de los mensajes: PCM linear, G.711 mu-law, G.711 a-law, G.729a, G.726, entre otros.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Debe soportar la funcionalidad de reglas de transferencias de llamadas de llamadas entrantes por llamante, tiempo del día, o estado (libre u ocupado) en el calendario.
Soportar mínimo 5 saludos personales (alternativo, ocupado, interno, fuera de horario, o estándar) en los buzones de usuario.
La solución debe proveer mensajería unificada (soportada con Microsoft Exchange 2016, 2019 y Microsoft Office 365).
Soportar e incluir el acceso por varias vías de a los mensajes de voz (telefónica, web, correo electrónico, aplicaciones y servicios).
Debe permitir graduar la velocidad y volumen de las grabaciones durante la reproducción.
Soportar el formato de extensión completo en E.164.
Soportar Directorio con búsqueda por nombre de usuario.
Soportar Caller ID (identificación del llamante).
Los administradores deben poder crear usuarios de manera individual o en volumen (plantillas) o a través de LDAP.
Debe soportar el protocolo de señalización SIP.
Los usuarios pueden ser provistos por un mensajería unificada (un único buzón) o integrada (IMAP).
La solución debe soportar SNMP versión 1,2 y 3.
Este componente debe contar con al menos 3 año de soporte por parte del fabricante, acceso a actualización de software y mantenimiento, no debe estar fuera de venta y/o vida por parte del mismo. Para el remplazo de partes en los componentes de hardware se deben incluir un soporte SLA de 8 horas, 5 días a la semana, siguiente dia laborar
Debe soportar lo siguiente: música en espera, alertas de envejecimiento de mensajes, aviso de buzón lleno, registro de eventos, formatos de 12 o 24 horas

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

para estampar la hora, números telefónicos en formato E.164, entre otros.
**** Se debe demostrar en un ambiente de producción similar al propuesto las funcionalidades de mensajería de voz.**
SISTEMAS DE CENTRO DE CONTACTO
Sistema de manejo de llamadas en el centro de contacto que incluya soporte para 10 agentes con las siguientes características:
la Solucion propuesta debe ser del mismo fabricante de la PBX propuesta, a fines de garantizar un funcionamiento optimo.
Debe incluir enrutamiento condicional de las llamadas basado en selección en los menues, estadísticas en tiempo real de las colas, hora del día, día de la semana, ANI, numero marcado y a través de datos de archivos de texto XML.
Debe contar con un cliente para los agentes y supervisores fácil de usar basado en Web 2.0.
Se deben incluir los servidores físicos necesarios para alojar la solución propuesta, se debe brindar redundancia y alta disponibilidad física, lógica. Además de redundancia de servidores se debe incluir redundancia eléctrica en los mismos.
Debe seleccionar a los agentes basado en mayor disponibilidad, linear, mayor cantidad de contactos manejados, tiempo menor de manejo de contactos y algoritmo circular.
Debe incluir la personalización de audios de la cola.
Debe incluir la reinserción de la llamada a la cola ante una llamada no contestada.
Debe colectar entradas de selección de las personas que llaman en el IVR.
El IVR debe Soportar consultas a Base de Datos
Debe soportar e incluir funcionalidades de colas de Correo Electronico.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Debe soportar e incluir funcionalidades de Web-Chat como canal de Servicio.
Debe soportar IPv6.
Debe contar con una aplicación que permita a los agentes poder autenticarse y des autenticarse en el sistema, ponerse listos y no listos dentro del sistema.
Debe incluir estadísticas en tiempo real disponibles para los agentes.
Se deben incluir las siguientes funciones para los supervisores:
- Ver y cambiar el estado de los agentes.
- Estadísticas en tiempo real de los agentes supervisados.
- Monitoreo Silencioso: Todas las interacciones deben poder permitir el monitoreo por parte de los supervisores, esto quiere decir que se pueden poder ver en tiempo real.
- Intervención de la llamada por supervisor en tiempo real en línea con el agente y el cliente.
- Capacidad de adicionar o eliminar agentes a grupos en tiempo real.
- Dashboard con principales indicadores en tiempo real.
Este componente debe contar con al menos 3 años de soporte por parte del fabricante, acceso a actualización de software y mantenimiento, no debe estar fuera de venta y/o vida por parte del mismo. Para el remplazo de partes en los componentes de hardware se deben incluir un soporte SLA de 24 horas al día por 7 días de la semana con tiempo de respuesta máximo de 4 horas.
TELÉFONOS
Teléfono Básico
Remplazo 450 teléfono por el modelo Cisco 7821 MODELO: CP-7821-K9, Smartnet SNTC-8X5XNBD por 1 año

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

Nuevo para la plataforma 410 telefono Cisco 7821 MODELO: CP-7821-K9, Smartnet SNTC-8X5XNBD por 1 año
Debe contar con dos puertos RJ-45, uno para la conexión de red y otro para la PC, con velocidad 10/100 Mbps.
Modelo de tener Capacidad de registro Onpremise,si en un fututo se quiere tambien en la nube
Este tipo de teléfono debe tener teclas o botones dedicados para las funciones de seleccionar, volver, volver a marcar, transferir, espera / Reanudar, silencio, volumen arriba / abajo, altavoz, entre otros.
Indicador LED para notificaciones.
Debe contar con una Pantalla gráfica monocromática antideslumbrante con retroiluminación blanca con una resolución no menor a 384 x 106 pixeles.
IEEE 802.3af Clase 1.
Posibilidad de ser montado en la pared.
Full dúplex altavoz.
Soportar los siguientes codecs: G.711a/μ, G.722, G.729a, iLBC and OPUS
Encripción de la media usando SRTP y de la señalización con TLS.
Debe soportar varios idiomas incluidos ingles y español.
El protocolo de señalización debe ser SIP.
Debe permitir autenticación basado en IEEE 802.1X
Debe contar con garantía del fabricante de 1 año
Debe soportar IPv6.
No debe estar fuera de venta y/o vida por parte del fabricante. No puede ser reconstruido ni reparado.
Debe soportar minimo 2 lineas
SUPLIDOR
El suplidor de la solución debe presentar una certificación PREMIER O GOLD por parte del fabricante indicando que el mismo esta autorizado a

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

ser representante de la ofertada marca en Republica Dominicana.
El suplidor de la solución debe presentar una certificación por parte del fabricante indicando que esta certificado para vender e instalar los componentes propuestos.
El Suplidor debe Contar la especializacion Contact Center Express
El suplidor debe incluir evidencia de experiencias locales en solucion de Contact Center IP de al menos 10 Agentes (incluir cartas del Cliente). Se validaran los datos suministrados con el Cliente.
El suplidor debe contar con los ingenieros locales certificados capaces de instalar la solución.
El suplidor debe contar con una metodología de manejo de proyectos avalada por el Project Management Institute, es decir, debe contar con personal con la certificación PMP para el manejo de los proyectos.
El Suplidor debe considerar los servicios de profesionales para le implementacion y actualizacion de toda la solucion propuesta
El Suplidor debe ofrecer un servicio de soporte 24/7 con niveles de atencion de 30min para casos prioritarios.
El suplidor debe reliazar una DEMOSTRACION de las funciones incluidas en este RFP considerando lo siguiente:
Telefonia:
- Video llamadas con Telefonos Fisicos.
- Voicemail, Presencia, Grupos de Caza, colas nativas, Movilidad.
- Applicativo de Mensajeria instantanea y Softphone.
- Chat Persistente
Centro de Contacto:

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		- Interface de Agente y Supervisor	
		- Monitoreo en Vivo de llamadas	
		-Repuesta interactiva de voz : manejo de llamadas entrantes, coleccion y visualisacion de datos en los agentes.	
		- Web-Chat : interacion externa, manejo de colas, respuestas predefinidas, estadisticas.	
		- Colas de Email : Manejo de Correcos entrantes, Asignaciones y Distribucion por skill, plantillas predefinidas busqueda de correos, estadisticas.	
		- Reporteria: llamadas, Chat Email, Agentes, Customizacion y tipos de reportes por Tabla y Graficos, Dashboard	
		Adquisición de Servicios de Nube Computacional, Nota: la institución actualmente usa los servicios de Azure en la modalidad pospago anual en modelo CSP (Cloud Solution Provider).	
		Los oferentes deben tomar en cuenta que la institución actualmente usa los servicios de Azure en la modalidad pospago anual en modelo CSP (Cloud Solution Provider).	
		Que deben cubrir costos aproximados de US$72,000 dólares anuales en estos servicios, y con capacidad de crecimiento proyectado a 20% anual (sujeto a revisión anual).	
Lote X-TELEFONIA			
XII-Servicios Nube Computacional	**1**	**Los recursos son mostrados a continuación:**	**1**
		Maquinas Virtuales:	
		4x Standard D8s v3 (8 vcpus, 32 GiB memory)	
		3x Standard B2ms (2 vcpus, 8 GiB memory)	
		2x Standard D2s v3 (2 vcpus, 8 GiB memory)	

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		1x Standard D16s v3 (16 vcpus, 64 GiB memory)
		3x Standard D4s v3 (4 vcpus, 16 GiB memory)
		Otros:
		3x Load Balancer
		2x Azure Database for MySQL
		Disponibilidad
		La plataforma debe ofrecer un 99.9% de disponibilidad en todos sus servicios.
		Administracion
		Se requiere que el servicio ofertado tenga un Portal de Autoservicio con roles de administración
		Conectividad
		El servicio de conectividad ofertado debe proveer a los servicios por lo menos 100MBps (Megabytes por segundo) de conexión a internet con un SLA de 99.9%.
		Licenciamiento
		El licenciamiento debe ser tipo “Academic Licensing for Microsoft Education” (Microsoft Open Value Subscription Education Solutions).
		Interfaz de Monitoreo
		Ser compatible con los navegadores más comunes Safari, Chrome, Firefox y IE.
		Indicar el estado de todos los Centros de datos del proveedor.
		Tener un panel con los estados de los servicios contratados.
		Poder configurar cada uno de los recursos contratados y cambiar las diferentes alertas
		Configurar auto escalamiento a demanda según la disponibilidad de recursos.
		Emisión de reportes de consumo de recursos a demanda y periódicos con retardo máximode 5 días
		Cobro de consumo por hora de los recursos procesamiento, almacenamiento y red.

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Capacidad para crear máquinas virtuales de diferentes tamaños con sistema operativo Windows. Debe incluir la licencia del sistema operativo en su OFERTA.
		Las máquinas virtuales deben tener la posibilidad de correr Linux.
		Capacidad para crear bases de datos SQL de diferentes tamaños y desempeños con la licencia del producto incluida en el servicio.
		Capacidad de sincronización con el directorio activo (Active Directory) en modalidad software como servicio (SaaS) a fin de proveer validación de usuarios en las aplicaciones desde la nube
		Capacidad de integración en modalidad hibrida con la finalidad de mover recursos transparentemente entre nuestro Centro de Datos y el servicio contratado.
		Capacidad de establecer conexiones virtuales privadas (VPN) sitio a sitio para integración con la red local.
		Capacidad de monitoreo de los recursos actuales con funcionalidades de control de cambio auditoria, análisis antimalware y automatización de tareas.
		Capacidad de integración son soluciones de recuperación de desastres y respaldo de información (debe incluir licenciamiento del agente a utilizar).
		Interfaz de administración de autoservicio con capacidad de administración de permisos a diferentes niveles y roles.
		Soporte
		Gestión vía consola web de los casos abiertos y progreso de los mismos.
		La Plataforma deba tener un plan de mantenimiento donde el cliente este informado con por lo menos 20 días de antelación de todas las ventanas de mantenimiento que afecten la infraestructura

Tel.: +1 (809) 286 1009
Web: www.ogtic.gob.do
RNC: 430-01950-1
ogticrd

		Consultas para análisis y recomendaciones de mejoras en la plataforma
		8 horas de soporte local para ser utilizadas en consultas durante el primer año de servicio
		Proveedores
		Los oferentes deben presentar la certificación del fabricante, que acredite que están autorizados a comercializar los productos de Microsoft.
		Gold Cloud Productivity
		Gold Cloud Platform
		Gold Small and Midmarket Cloud Solutions
	XII-Servicios Nube Computacional	

Conclusión:

Luego de revisar la documentación aportada, verificar la solicitud y sus soportes, evaluamos las especificaciones técnicas y consideramos que cumplen con todos los aspectos necesarios requeridos y no solapan ningún proyecto que haya de ejecutarse desde la Agenda Digital 2030.

Mario Adames
Encargado de División de Consultoría Digital
Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC)