Dirección Nacional de Contrataciones Públicas
E.E.U.U. 961 c/ Tte. Fariña - Asunción, Paraguay
Tel. y Fax +595 21 4154000 - dncp@contrataciones.gov.py

Consultas Realizadas

Licitación 438168 - Adquisición de Solución de Seguridad para Accesos Privilegiados y Clúster de Bóveda de Contraseñas (SBE) - Ad Referéndum.

Consulta 1 - Experiencia Requerida

Consulta	Fecha de Consulta	05-04-2024

En el PBC se solicita: Demostrar la experiencia en la provisión e instalación de las soluciones y/o herramientas de gestión de usuarios y privilegios, con contratos, facturas, y/o recepciones finales por un monto equivalente al 25% como mínimo del monto total ofertado en la presente licitación, de los últimos 3 (tres) años (2020, 2021, 2022).

CONSULTA: Las bases definen en la EETT, sobre la experiencia y teniendo en cuenta que son soluciones muy poco comercializados Solicitamos respetuosamente a la convocante que sean aceptadas experiencia del 15% como mínimo de los Últimos 4 años, agregando al año (2020,2021,2022,2023) a fin de fomentar los principios de la Ley de compras públicas (anterior y actual), conforme a su art. 4° - Economía, Eficacia y Eficiencia e IGUALDAD y LIBRE COMPETENCIA.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: Considerando la gran envergadura del proyecto que implica adquisición e implementación de nuevas tecnologías, así como la amplitud de los servicios críticos a ser vinculados a la solución PAM, nos resulta indispensable que la empresa oferente cuente mínimamente con experiencia demostrable en la provisión y/o instalación de soluciones o herramientas de seguridad y/o gestión de cuentas de usuarios y/o gestión de accesos, con contratos, facturas, y/o recepciones finales por un monto equivalente al 40% como mínimo del monto total ofertado en la presente licitación, dentro de los últimos 3 (tres) años (2021, 2022 y 2023). Remitirse a la Adenda enumerada.

Consulta 2 - CAPACIDAD TÉCNICA

Consulta	Fecha de Consulta	05-04-2024

En el PBC se solicita: El oferente debe contar con al menos 1 (uno) técnico que realizará la instalación y puesta en marcha de las soluciones ofertadas

CONSULTA: Solicitamos que la convocante pueda aclarar si el técnico solicitado, deberá tener una especialización técnica del fabricante y si la misma deberá ser parte del plantel del oferente y/o si aceptaran técnico certificado del representante? ¿Nivel de certificación?

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: Considerando la gran envergadura del proyecto que implica adquisición e implementación de nuevas tecnologías, así como la amplitud de los servicios críticos a ser vinculados a la solución PAM, el oferente debe contar con al menos 2 (dos) técnicos certificados en despliegue o instalación de la solución PAM ofertada, pudiendo ser personal subcontratado. Remitirse a la Adenda enumerada.

Consulta 3 - Experiencia requerida

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN, Experiencia requerida, se solicita:
Demostrar la experiencia en la provisión e instalación de las soluciones y/o herramientas de gestión de usuarios y privilegios, con contratos, facturas, y/o recepciones finales por un monto equivalente al 25% como mínimo del monto total ofertado en la presente licitación, de los últimos 3 (tres) años (2020, 2021, 2022).
Solicitamos que sea aceptada la experiencia en la provisión y/o instalación de soluciones o herramientas de seguridad y/o gestión de cuentas de usuarios y/o gestión de accesos y/o gestión de activos de TI y/o monitoreo de infraestructura de TI, con contratos, facturas, y/o recepciones finales por un monto equivalente al 40% como mínimo del monto total ofertado en la presente licitación, dentro de los últimos 3 (tres) años (2021, 2022 y 2023), de manera a dar mayor apertura de participación a los proveedores y potenciales oferentes.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: Considerando la gran envergadura del proyecto que implica adquisición e implementación de nuevas tecnologías, así como la amplitud de los servicios críticos a ser vinculados a la solución PAM, nos resulta indispensable que la empresa oferente cuente mínimamente con experiencia demostrable en la provisión y/o instalación de soluciones o herramientas de seguridad y/o gestión de cuentas de usuarios y/o gestión de accesos, con contratos, facturas, y/o recepciones finales por un monto equivalente al 40% como mínimo del monto total ofertado en la presente licitación, dentro de los últimos 3 (tres) años (2021, 2022 y 2023).Remitirse a la Adenda enumerada.

Consulta 4 - Capacidad Técnica

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN, Capacidad Técnica, se solicita:
2. Referencias satisfactorias de clientes finales, como mínimo 1 (uno), que contengan la debida identificación y suscripción del emisor, de haber proveído e instalado soluciones y/o herramientas de gestión de usuarios y privilegios, en el periodo comprendido entre los años 2020 al 2022.
Solicitamos que sea aceptada referencias satisfactorias, como mínimo 1 (uno), en provisión y/o instalación de soluciones o herramientas de seguridad y/o gestión de cuentas de usuarios y/o gestión de accesos y/o gestión de activos de TI y/o monitoreo de infraestructura de TI, dentro de los últimos 3 (tres) años (2021, 2022 y 2023), de manera a dar mayor apertura de participación a los proveedores y potenciales oferentes.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: Considerando la gran envergadura del proyecto que implica adquisición e implementación de nuevas tecnologías, así como la amplitud de los servicios críticos a ser vinculados a la solución PAM, se aceptará referencias satisfactorias, como mínimo 1 (una) carta y/o nota originales firmadas por el cliente, en provisión y/o instalación de soluciones o herramientas de seguridad y/o gestión de cuentas de usuarios y/o gestión de accesos, dentro de los últimos 3 (tres) años (2021, 2022 y 2023). Remitirse a la Adenda enumerada.

Consulta 5 - Técnicos Certificados

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN, Capacidad Técnica, se solicita:
1. El oferente debe contar con al menos 1 (uno) técnico que realizará la instalación y puesta en marcha de las soluciones ofertadas
Dada la envergadura del proyecto licitado, recomendamos a la convocante considerar ampliar la exigencia de 2 (dos) técnicos certificados en el despliegue de la solución PAM ofertada, pudiendo ser estos, personal subcontratado específicamente para el proyecto.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: Considerando la gran envergadura del proyecto que implica adquisición e implementación de nuevas tecnologías, así como la amplitud de los servicios críticos a ser vinculados a la solución PAM, la solicitud de que la empresa oferente cuente con mínimamente 2 (dos) técnicos certificados en el despliegue de la solución PAM ofertada, pudiendo ser estos, personal subcontratado específicamente para el proyecto. Remitirse a la Adenda enumerada.

Consulta 6 - Técnicos Certificados

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN, Capacidad Técnica, se solicita:
1. El oferente debe contar con al menos 1 (uno) técnico que realizará la instalación y puesta en marcha de las soluciones ofertadas
Dada la envergadura del proyecto licitado, recomendamos a la convocante considerar incluir certificaciones de las diferentes plataformas que forman parte de la solución, pudiendo ser estos, personal subcontratado específicamente para el proyecto.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: Considerando la envergadura del proyecto que implica adquisición e implementación de nuevas tecnologías, así como la criticidad de las prestaciones que brinda el BNF, en donde la presentación de errores podría desembocar en un perjuicio patrimonial para la entidad, nos resulta indispensable que la empresa oferente cuente mínimamente con un (1) técnico con las siguientes certificaciones: Ethical Hacking Essentials (EHE) o superior, CompTIA Cybersecurity Analyst (CySA+) o superior, Cyber Securiry Foundation Professional Certificate (CSFPC) o superior, Windows Server Hybrid Administrator Associate o superior, Microsoft Certification Solutions Associate - Windows Server 2016 o superior, Microsoft Certification Solutions Expert - Server Infraestructure o superior, Microsoft Certification Solutions Expert - Private Cloud o superior, VMware Certified Professional - Data Center Virtualization 2023 o superior, Red Hat Certified System Administrator (RHCSA) o superior, pudiendo ser estos, personal subcontratado específicamente para el proyecto. Remitirse a la Adenda enumerada.

Consulta 7 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Capacidades generales de la herramienta PAM, solicita:

Posibilidad de realizar búsquedas dentro de los videos de auditoría.

Sugerimos que sea aceptada la posibilidad de realizar búsquedas basadas en lista de comandos o queries (query) para trazabilidad y seguimiento de los mismos para futuras consultas sobre la biblioteca de videos generadas por las sesiones de usuarios para identificar tiempos exactos de los queries (query) o comandos que ocurren en dichos videos.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: Hemos considerado exigir la capacidad de realizar búsquedas basadas en lista de comandos (querys) para trazabilidad y seguimiento de los mismos para las futuras consultas sobre la biblioteca de videos generadas por las sesiones de usuarios para identificar tiempos exactos de los queries (querys) o comandos que ocurren en dichos videos. Remitirse a la adenda enumerada.

Consulta 8 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Capacidades generales de la herramienta PAM, se requiere:

Debe tener la capacidad de detectar automáticamente nuevos dispositivos Laptops o PCs Windows, Servicios Windows (Windows Services), Scheduled Tasks, IIS Service Accounts, para su administración en la solución.

Sugerimos a la convocante que la herramienta tenga la capacidad de detectar automáticamente dispositivos como máquinas virtuales, servidores físicos, estaciones de trabajo con sistema operativo Microsoft Windows, para su administración en la solución.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe tener la capacidad de detectar dispositivos como máquinas virtuales, servidores físicos, estaciones de trabajos con sistema operativo Microsoft Windows, para su administración en la solución. Remitirse a la adenda enumerada.

Consulta 9 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Capacidades generales de la herramienta PAM, dice:

Debe soportar integración con soluciones de análisis de vulnerabilidades.

Solicitamos que la herramienta soporte integración con al menos una solución de análisis de vulnerabilidades.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe soportar integración con al menos una solución de análisis de vulnerabilidades. Remitirse a la adenda enumerada.

Consulta 10 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Capacidades generales de la herramienta PAM, dice:

Debe proporcionar un acceso remoto seguro (fuera de la red corporativa) a los administradores sin necesidad de instalar clientes VPN en los dispositivos de los usuarios remotos, garantizando un acceso seguro con MFA sin modificar los recursos de autenticación corporativos como el AD..

Sugerimos que la herramienta proporcione acceso remoto seguro (fuera de la red corporativa) sin necesidad de instalar clientes VPN en los dispositivos de los usuarios remotos, a fin de reducir la superficie de ataque y optimizar la administración de VPNs.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe proporcionar un acceso remoto seguro (fuera de la red corporativa) sin necesidad de instalar clientes VPN en los dispositivos de los usuarios remotos, conforme a ser garantizado el acceso seguro con MFA sin modificar los recursos de autenticación corporativos como el AD. Remitirse a la adenda enumerada.

Consulta 11 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Capacidades generales de la herramienta PAM, dice:

Debe contar con la opción de bloquear todo el tráfico de entrada o salida desde y hacia cualquier destino

Sugerimos que la herramienta cuente con bloqueo de inicio de sesiones en los dispositivos, configurable para grupos de roles o grupos de usuarios, considerando que el control de tráfico se realiza en el Firewall con la finalidad de agregar una capa de seguridad adicional.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe contar con bloqueo de inicio de sesiones en los dispositivos, configurable para grupos de roles o grupos de usuarios. Remitirse a la adenda enumerada.

Consulta 12 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Reportes y Auditoría, dice:

Debe cumplir con las siguientes normativas: GDPR, ISO27001, NIST 800-53

Recomendamos que los reportes y auditoria de la solución cumpla mínimamente con las siguientes normativas: GDPR, ISO27001.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe cumplir con las siguientes normativas: GDPR e ISO27001. Remitirse a la adenda enumerada.

Consulta 13 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Integración de la Solución, dice:

Integración con soluciones de Scanner de vulnerabilidades

Recomendamos que la herramienta PAM soporte integración con al menos una solución de Scanner de vulnerabilidades.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe soportar la integración con al menos una solución de Scanner de vulnerabilidades. Remitirse a la adenda enumerada.

Consulta 14 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Análisis de Comportamiento de Usuario (UBA), dice:

Debe evaluar el riesgo de autenticación mediante la verificación del comportamiento histórico de la identidad a través de los siguientes atributos: GeoVelocidad, Geolocalización, Día de la semana, Horario de acceso, Sistema operativo y Fallas de inicio de sesión consecutivas

Recomendamos que la herramienta PAM pueda evaluar el riesgo de autenticación mediante la verificación del comportamiento histórico de la identidad, mínimamente a través de los siguientes atributos: Día de la semana, Horario de acceso, origen y longitud de la sesión.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe evaluar el riesgo de autenticación mediante la verificación del comportamiento histórico de la identidad a través de los siguientes atributos: Día de la semana, Horario de acceso, origen y longitud de la sesión. Remitirse a la adenda enumerada.

Consulta 15 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Análisis de Comportamiento de Usuario (UBA), dice:

Debe permitir configurar dashboards personalizados.

Recomendamos que la herramienta PAM permita como mínimo, personalizar las vistas de los dashboards predefinidos mediante la aplicación de filtros de manera local en la plataforma y permitir la extracción de datos para conectar mediante APIs a herramientas de BI a fin de permitir ampliar el manejo de información generada por la herramienta.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe permitir personalizar las vistas de los dashboards predefinidos mediante la aplicación de filtros de manera local en la plataforma y permitir la extracción de datos para conectar mediante APIs a herramientas de BI. Remitirse a la adenda enumerada.

Consulta 16 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES
TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Monitoreo/Grabación de Actividad Privilegiada, dice:

Debe ser capaz de realizar búsquedas de comandos privilegiados dentro de las grabaciones de video..

Sugerimos que sea aceptada la posibilidad de realizar búsquedas basadas en lista de comandos o queries (query) para trazabilidad y seguimiento de los mismos para futuras consultas sobre la biblioteca de videos generadas por las sesiones de usuarios para identificar tiempos exactos de los queries (query) o comandos que ocurren en dichos videos.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe ser capaz de realizar búsquedas basadas en lista de comandos o queries (query) para trazabilidad y seguimiento de los mismos para futuras consultas sobre la biblioteca de videos generadas por las sesiones de usuarios para identificar tiempos exactos de los queries (query) o comandos que ocurren en dichos videos. Remitirse a la adenda enumerada.

Consulta 17 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES
TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Acceso Remoto Privilegiado a Terceros, dice:

Para otorgar accesos privilegiados remotos la solución debe proveer autenticaciones de factor humano basadas en biométricos.

Sugerimos que para otorgar accesos privilegiados remotos, la solución provea autenticaciones de multifactor basadas en al menos una de las siguientes opciones: biométricos, SMS, correo electrónico o Tokens.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe otorgar accesos privilegiados remotos la solución debe soportar autenticación multifactor basadas en al menos una de las siguientes opciones: biométricos, SMS, correo electrónico o Tokens. Remitirse a la adenda enumerada.

Consulta 18 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Acceso Remoto Privilegiado a Terceros, dice:

La solución debe contar con una aplicación de autenticación biométrica para teléfonos inteligentes iOS y Android

Sugerimos que la solución cuente con la posibilidad de integrarse con aplicaciones de terceros para agregar una capa adicional de seguridad en la autenticación de usuarios externos, mediante biométricos o algún otro factor para teléfonos inteligentes iOS y Android.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada deberá contar con la posibilidad de integrarse con aplicaciones de terceros para agregar una capa adicional de seguridad en la autenticación de usuarios externos, mediante biométricos o algún otro factor para teléfonos inteligentes iOS y Android. Remitirse a la adenda enumerada.

Consulta 19 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Acceso Remoto Privilegiado a Terceros, dice:

La seguridad de la plataforma de autenticación para accesos remotos debe estar acorde a estándares de seguridad OWASP, NIST y CAIQ

Sugerimos que la seguridad de la plataforma de autenticación para accesos remotos esté acorde con al menos uno de los siguientes estándares de seguridad: OWASP, NIST o CAIQ.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la seguridad de la plataforma de autenticación para accesos remotos de la solución PAM ofertada debe estar acorde a uno de los siguientes estándares de seguridad: OWASP, NIST o CIS. Remitirse a la adenda enumerada.

Consulta 20 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Gestión de Privilegios para Endpoints (EPM), dice:

Debe permitir la configuración de señuelos" tales como contraseñas y credenciales falsas del administrador local para la detección de ataques en curso y el bloqueo proactivo.

Sugerimos a la convocante, que esta exigencia sea reformulada y que en su lugar la plataforma exija las directivas de control de acceso a los usuarios, de tal forma a ampliar las opciones de control de seguridad para la protección de la herramienta.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada deberá permitir directivas de control de acceso a los usuarios, de tal forma a ampliar las opciones de control de seguridad para la protección de la herramienta. Remitirse a la adenda enumerada.

Consulta 21 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Autenticación Multifactor (MFA), dice:

Debe ser capaz de ofrecer mínimamente los siguientes métodos para múltiples factores de autenticación:
Usuario y contraseña de los directorios admitidos en la solución. Exigido
A través de la aplicación móvil iOS y Android, que ofrece soporte para (Biometría FaceID, Biometría a través del lector digital, notificación para aprobar o rechazar una autenticación, Geolocalización a través de GPS coordenadas e IDatabase). Exigido
Soporte tokens OATH OTP. Autenticación en la pantalla de inicio de sesión a través de QRcode (Passwordless) sin necesidad de introducir el usuario y la contraseña, con la opción de forzar la biometría en el dispositivo móvil. Exigido
Entrega de código a través de SMS y llamada de voz. Exigido
Preguntas de seguridad Notificaciones de correo electrónico y teléfono móvil. Exigido.
OTP tokens (en línea, fuera de línea, por correo electrónico y Hardware). Exigido

Sugerimos a la convocante, sea aceptado que la herramienta sea capaz de ofrecer al menos uno de los métodos para múltiples factores de autenticación listados.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe ser capaz de ofrecer al menos uno de los siguientes métodos para múltiples factores de autenticación:
A) Usuario y contraseña de los directorios admitidos en la solución.
B) A través de la aplicación móvil iOS y Android, que ofrece soporte para (Biometría FaceID, Biometría a través del lector digital, notificación para aprobar o rechazar una autenticación, Geolocalización a través de GPS coordenadas e IDatabase)
C) Soporte tokens OATH OTP. Autenticación en la pantalla de inicio de sesión a través de QRcode (Passwordless) sin necesidad de introducir el usuario y la contraseña, con la opción de forzar la biometría en el dispositivo móvil.
D) Entrega de código a través de SMS y llamada de voz.
E) Preguntas de seguridad Notificaciones de correo electrónico y teléfono móvil
F) OTP tokens (en línea, fuera de línea, por correo electrónico y Hardware). Remitirse a la adenda enumerada.

Consulta 22 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Autenticación Multifactor (MFA), dice:

Debe ser capaz de soportar autenticadores que admiten FIDO2 / U2F, que admiten mínimamente:
Windows Hello. Exigido
Google Titan Key Exigido
MacOS TouchID. Exigido

Sugerimos que sean aceptadas herramientas capaces de soportar autenticadores que admiten FIDO2 / U2F / OTP, que admiten al menos uno de los siguientes: Google Authenticator, Microsoft Authenticator, Windows Hello, Google Titan Key, MacOS TouchID.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe ser capaz de soportar autenticadores que admiten FIDO2 / U2F / OTP, que admiten al menos uno de los siguientes: Google Authenticator, Microsoft Authenticator, Windows Hello, Google Titan Key, MacOS TouchID. Remitirse a la adenda enumerada.

Consulta 23 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Autenticación Multifactor (MFA), dice:

Debe ser capaz de soportar confirmación de código por correo electrónico.

Sugerimos que la herramienta pueda soportar confirmación de código mediante al menos una de las siguientes opciones: biométricos, SMS, correo electrónico o Tokens.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe ser capaz de soportar confirmación de código por medio de al menos una de las siguientes opciones: biométricos, SMS, correo electrónico o Tokens. Remitirse a la adenda enumerada.

Consulta 24 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Autenticación Multifactor (MFA), dice:

Debe ser capaz de soportar preguntas y respuestas previamente configuradas.

Sugerimos a la convocante, que esta exigencia sea reformulada y que en su lugar la plataforma exija integraciones con soluciones de seguridad de terceros robustas como: Cisco Duo Security, de tal forma a ampliar aún más las opciones de seguridad compatibles con MFA.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe ser capaz de soportar integraciones con soluciones de seguridad de terceros robustas como: Cisco Duo Security, de tal forma a ampliar aún más las opciones de seguridad compatibles con MFA. Remitirse a la adenda enumerada.

Consulta 25 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Autenticación Multifactor (MFA), dice:

Debe permitir que los usuarios realicen el restablecimiento de contraseña y el desbloqueo del usuario, autoservicio mediante los múltiples métodos de factor de autenticación citados para la verificación positiva a través del portal de soluciones, Windows y la pantalla de inicio de sesión del sistema operativo MacOS, y a través de las API de REST que ofrece la solución.

Recomendamos que la herramienta PAM permita el restablecimiento de contraseña y el desbloqueo del usuario desde el panel de administración, considerando que al ser una solución de servicios privilegiados no es conveniente el restablecimiento de la contraseña mediante autoservicio.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe permitir el restablecimiento de contraseña y el desbloqueo del usuario desde el panel de administración. Remitirse a la adenda enumerada.

Consulta 26 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Autenticación Multifactor (MFA), dice:

Debe soportar autenticación dinámica basada en el contexto de riesgo y seguridad aprendido por la solución, permitiendo la creación de un perfil para cada usuario, aprovechando los atributos históricos y situacionales específicos del mismo, como la ubicación, el dispositivo, la red, el horario y el índice de riesgo de comportamiento.

Sugerimos a la convocante que la solución PAM soporte la autenticación dinámica basada en el contexto de riesgo y seguridad, permitiendo la creación de un perfil para cada usuario, aprovechando los atributos históricos y situacionales específicos del mismo, como la ubicación, el dispositivo, la red, el horario y el índice de riesgo de comportamiento.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe soportar autenticación dinámica basada en el contexto de riesgo y seguridad, permitiendo la creación de un perfil para cada usuario, aprovechando los atributos históricos y situacionales específicos del mismo, como la ubicación, el dispositivo, la red, el horario y el índice de riesgo de comportamiento. Remitirse a la adenda enumerada.

Consulta 27 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Single Sign On (SSO), dice:

Debe permitir la configuración de las aplicaciones web mínimamente a través de los siguientes protocolos y métodos, para por lo menos 20 usuarios administradores:
SAML 2.0 Exigido;
Modo cliente Oauth 2.0 Exigido;
WS-Federation Exigido;
Conexión OpenID Exigido;
Ntlm Exigido;
Modo de servidor Oauth 2.0 Exigido;
HTTP Basic Exigido;
Extensión en el navegador para capturar aplicaciones web que utilizan el formulario con el usuario y la contraseña y realizar la finalización automática del inicio de sesión y la contraseña de forma automatizada. Esta información debe almacenarse de forma segura en la solución para la finalización automática en futuros inicios de sesión en estas aplicaciones. Exigido

Solicitamos respetuosamente que la herramienta PAM permita la configuración de las aplicaciones web a través de al menos uno de los protocolos y métodos listados, para por lo menos 20 usuarios administradores.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe permitir la configuración de las aplicaciones web a través de al menos uno de los siguientes protocolos y métodos, para por lo menos 20 usuarios administradores: SAML 2.0, Modo cliente Oauth 2.0, WS-Federation, Conexión OpenID, Ntlm, Modo de servidor Oauth 2.0, HTTP Basic, Extensión en el navegador para capturar aplicaciones web que utilizan el formulario con el usuario y la contraseña y realizar la finalización automática del inicio de sesión y la contraseña de forma automatizada. Esta información debe almacenarse de forma segura en la solución para la finalización automática en futuros inicios de sesión en estas aplicaciones. Remitirse a la adenda enumerada.

Consulta 28 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Single Sign On (SSO), dice:

Debe proporcionar una extensión avanzada del explorador solo para los administradores de soluciones, con el fin de asignar los campos de los formularios (normalmente inicio de sesión y contraseña) para que después de asignar el usuario administrado pueda incluir como una aplicación web para SSO en el catálogo general, lo que permite el SSO de aplicaciones que no admiten protocolos más modernos como SAML y Oauth.

Sugerimos a la convocante que la solución permita la inyección de usuario y contraseña para los administradores de sesiones web con el fin de asignar los campos de los formularios (normalmente inicio de sesión y contraseña).

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe permitir la inyección de usuarios y contraseña para los administradores de sesiones web con el fin de asignar los campos de los formularios (normalmente inicio de sesión y contraseña). Remitirse a la adenda enumerada.

Consulta 29 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Single Sign On (SSO), dice:

Debe soportar SSO a través de la autenticación integrada de Windows (IWA) que reutiliza el inicio de sesión de red para la autenticación en aplicaciones web, sin necesidad de introducir el usuario y la contraseña de nuevo.

Sugerimos a la convocante, que esta exigencia sea reformulada y que en su lugar la plataforma exija al usuario la autenticación para el acceso a las aplicaciones web, conforme a cumplir con las mejores prácticas para la protección de accesos y las concesiones de privilegios a usuarios.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe exigir al usuario la autenticación para el acceso a las aplicaciones web, conforme a cumplir con las mejores prácticas para la protección de accesos y las concesiones de privilegios a usuarios. Remitirse a la adenda enumerada.

Consulta 30 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES
TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Single Sign On (SSO), dice:

Debe admitir la personalización de respuestas SAML, como la asignación de atributos de directorio a atributos SAML, la capacidad de incluir lógica compleja para controlar las respuestas SAML y habilitar la visualización de la respuesta SAML configurada antes de su
implementación.

Sugerimos a la convocante, sea excluida de esta exigencia, la personalización de respuestas SAML así como la asignación de atributos de directorio a atributos SAML, la capacidad de incluir lógica compleja para controlar las respuestas SAML y habilitar la visualización de la respuesta SAML configurada antes de su implementación, y en su lugar sea exigida la autenticación para iniciar sesiones web de manera nativa sin necesidad que el usuario conozca las credenciales.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe admitir respuestas SAML y autenticación para iniciar sesiones web de manera nativa sin necesidad que el usuario conozca las credenciales. Remitirse a la adenda enumerada.

Consulta 31 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES
TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Single Sign On (SSO), dice:

El servicio de directorio de soluciones debe tener la capacidad de ampliar su esquema configurando atributos personalizados para satisfacer requisitos empresariales complejos

Sugerimos a la convocante, que esta exigencia sea reformulada y que en su lugar se exija que la personalización de atributos pueda ser realizada en las credenciales y dispositivos gestionados en la plataforma, de manera a tener mayor flexibilidad en la creación de grupos de usuarios.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe tener la capacidad de realizar la personalización de atributos de las credenciales y los dispositivos gestionados en la plataforma. Remitirse a la adenda enumerada.

Consulta 32 - Especificaciones Técnicas

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, SUMINISTROS REQUERIDOS - ESPECIFICACIONES
TÉCNICAS, ITEM N° 1 - SOLUCION DE SEGURIDAD PARA ACCESOS PRIVILEGIADOS (PAM), Single Sign On (SSO), dice:

Debe tener la capacidad de configurar LOS PROVEEDORES DE IDENTIDAD (IDP) de los socios comerciales de la organización para dar acceso a identidades federadas en aplicaciones empresariales de la organización sin necesidad de crear una nueva identidad en la infraestructura, a través de la federación realizada a través del protocolo SAML.

Sugerimos a la convocante, que esta exigencia sea reformulada y que en su lugar se exija que la plataforma tenga la capacidad de INTEGRARSE a LOS PROVEEDORES DE IDENTIDAD (IDP) de los socios comerciales de la organización mediante la federación realizada por la plataforma, sin la necesidad de crear nuevas identidades en la infraestructura. De forma tal que los protocolos como: LDAP, SAML, OpenID y otros puedan ser empleados para brindar acceso a las identidades federadas.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: la solución PAM ofertada debe tener la capacidad de INTEGRARSE a LOS PROVEEDORES DE IDENTIDAD (IDP) de los socios comerciales de la organización mediante la federación realizada por la plataforma, sin la necesidad de crear nuevas identidades en la infraestructura. De forma tal que los protocolos como: LDAP, SAML, OpenID y otros puedan ser empleados para brindar acceso a las identidades federadas. Remitirse a la adenda enumerada.

Consulta 33 - Técnicos Certificados

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN, Capacidad Técnica, se solicita:
1. El oferente debe contar con al menos 1 (uno) técnico que realizará la instalación y puesta en marcha de las soluciones ofertadas
Dada la envergadura del proyecto licitado, recomendamos a la convocante considerar incluir como mínimo 1 (un) personal con las siguientes certificaciones: Ethical Hacking Essentials (EHE) o superior, CompTIA Cybersecurity Analyst (CySA+) o superior, Cyber Securiry Foundation Professional Certificate (CSFPC) o superior, Windows Server Hybrid Administrator Associate o superior, Microsoft Certification Solutions Associate - Windows Server 2016 o superior, Microsoft Certification Solutions Expert - Server Infraestructure o superior, Microsoft Certification Solutions Expert - Private Cloud o superior, VMware Certified Professional - Data Center Virtualization 2023 o superior, Red Hat Certified System Administrator (RHCSA) o superior, pudiendo ser estos, personal subcontratado específicamente para el proyecto.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: Considerando la envergadura del proyecto que implica adquisición e implementación de nuevas tecnologías, así como la criticidad de las prestaciones que brinda el BNF, en donde la presentación de errores podría desembocar en un perjuicio patrimonial para la entidad, nos resulta indispensable que la empresa oferente cuente mínimamente con un (1) técnico con las siguientes certificaciones: Ethical Hacking Essentials (EHE) o superior, CompTIA Cybersecurity Analyst (CySA+) o superior, Cyber Securiry Foundation Professional Certificate (CSFPC) o superior, Windows Server Hybrid Administrator Associate o superior, Microsoft Certification Solutions Associate - Windows Server 2016 o superior, Microsoft Certification Solutions Expert - Server Infraestructure o superior, Microsoft Certification Solutions Expert - Private Cloud o superior, VMware Certified Professional - Data Center Virtualization 2023 o superior, Red Hat Certified System Administrator (RHCSA) o superior, pudiendo ser estos, personal subcontratado específicamente para el proyecto. Remitirse a la adenda enumerada

Consulta 34 - Capacidad Técnica

Consulta	Fecha de Consulta	05-04-2024

En el Pliego de Bases y Condiciones, REQUISITOS DE PARTICIPACIÓN Y CRITERIOS DE EVALUACIÓN, Capacidad Técnica, no se observa que la convocante solicite certificaciones de calidad ISO 9001, ni certificación de seguridad ISO 27001. Dado que este proyecto se trata de una implementación que involucra la gestión de derechos de acceso privilegiados y que la Norma ISO 27001, contempla lo siguiente: Gestión de los derechos de acceso y derechos de acceso privilegiados, incluyendo la adición de cambios y las revisiones periódicas., recomendamos a la convocante se exija que el oferente cuente ambas certificaciones: ISO 9001/2015 o similar e ISO 27001/2013 o similar.

Respuesta	Fecha de Respuesta	19-06-2024

Conforme a lo expuesto por la dependencia requirente y responsable del servicio informamos que: Haciendo mención a la envergadura del proyecto que implica adquisición e implementación de las nuevas tecnologías, así como la criticidad de los servicios y su dependencia con la solución PAM a ser implementada, hemos requerido que la herramienta cumpla con los requisitos de auditoría y de los estándares más exigentes, como ser GDPR e ISO27001. Remitirse a la adenda enumerada.