CIRCULAR MODIFICATORIA Nº 1

Ref.: EX-2019-68457181- APN-DA#EDUCAR

Por medio de la presente se hace saber de la enmienda del Pliego de Bases y Condiciones Particulares con referencia a la **LICITACION PUBLICA**, cuyo objeto es la provisión del: **"MANTENIMIENTO TECICO INTEGRAL"**. La presente Circular modificatoria Nº 1 deberá ser tenida en cuenta a la hora de presentar las ofertas, la cual se detalla a continuación:

Punto 1-

El punto 9.2 del Anexo B de las Especificaciones Técnicas. Quedará de la siguiente manera:

9.2 Servicio de Reparación de equipamiento en el centro de Reparación: Este servicio deberá estar incluido en el valor de la visita a los establecimientos. *En el caso que un establecimiento educativo lleve al centro de reparación 10 o más dispositivos el adjudicatario podrá facturar el valor de una visita una vez reparados y entregados los dispositivos.*

Punto 2-

El anexo II de las Especificaciones técnicas quedara conformado de la siguiente forma:

ANEXO II

HERRAMIENTAS DE CONTROL DE DISPOSITIVOS

ADMINISTRACION DE DISPOSITIVOS:

EDUCAR requiere de una solución que permita administrar los dispositivos informáticos que se encuentren en el ámbito escolar, tales como servidores, notebooks, tablets, etc.
Esta herramienta se instalará en todos los servidores destinados a alojar contenido educativo, como así también en los dispositivos entregados a partir de 2018 por el programa Aprender Conectados.

La solución deberá cumplir con las siguientes características técnicas:

HERRAMIENTAS DEL ADMINISTRADOR DE LA SOLUCIÓN:

- *Debe soportar distintos tipos de dispositivos, incluidas plataformas Windows, Android y iOS, sin limitarse a estos (en caso de que se adquieran otros tipos de dispositivos en el futuro).*
- *Debe poder administrarse desde la nube, sin requerir desplegar ningún servidor (físico o virtual) on-premises. El acceso a la consola de administración debe ser a través de un browser (HTML5)*

desde cualquier dispositivo y lugar, utilizando el protocolo HTTPS. No debe requerir software de terceros, como flash o java.

- *Debe ser escalable para administrar como mínimo 10 millones de dispositivos*
- *La consola de administración debe incorporar sus propias actualizaciones de manera automática cuando estas se encuentren disponibles, sin que el administrador deba hacerse cargo de instalarlas.*
- *Deberá integrarse (mediante APIs) a la misma consola de administración que EDUCAR utiliza para el resto de los dispositivos o infraestructura de red existente en las escuelas, tales como switches, Access Points y UTMs, ofreciendo administración centralizada desde la nube. De esta manera, EDUCAR contará con un system de gestión unidicado para las escuelas, que incluya todos los dispositivos desplegados en las mismas.*
- *Debe soportar doble factor de autenticación para poder acceder a la consola de administración.*
- *Debe soportar Security Assertion Markup Language (SAML) 2.0 para permitir poder acceder a la consola de administración utilizando soluciones de Single-Sign On (SSO).*
- *Debe proporcionar diferentes niveles de administración.*
- *Debe permitir que múltiples usuarios puedan acceder simultáneamente a la consola de administración.*
- *Debe permitir agregar, modificar o remover usuarios que puedan acceder a la consola de administración.*
- *Debe poder restringir que solo determinados administradores puedan administrar y controlar determinados dispositivos.*
- *Debe permitir modificar o remover los permisos dados a un determinado administrador.*
- *Debe ofrecer un listado de los usuarios que poseen privilegios de administrador, detallando el privilegio correspondiente, e información sobre la última vez que han accedido a la consola de administración.*
- *Debe registrar cada vez que un administrador realice un cambio referido a la configuración de la solución, brindando el detalle sobre qué administrador realizó el cambio y sobre qué configuración se ha realizado.*
- *Debe registrar cada vez que un administrador intente ingresar a la consola de administración, detallando si el login es exitoso o no, para poder tener visibilidad de manera sencilla sobre si hay algún intento de ingreso a la consola utilizando la cuenta de un administrador por parte de alguien externo en función del número de intentos fallidos.*
- *Debe ser capaz de bloquear el ingreso a la consola de administración a un administrador, luego de ingresar incorrectamente su contraseña un número definido de veces de manera consecutiva.*
- *Debe permitir definir criterios respecto de las contraseñas que los administradores utilizan para ingresar a la consola de administración, incluyendo que las contraseñas sean fuertes (imponiendo longitud mínima, inclusión de caracteres especiales, etc), que las contraseñas expiren luego de un número definido de días y que las contraseñas no puedan re-utilizarse hasta luego de un número definido de días.*
- *La solución debe contar con APIs.*

INVENTARIOS Y REPORTES:

- *Debe proporcionar un inventario de los dispositivos enrolados donde puedan aplicarse filtros para realizar una búsqueda determinada, por ejemplo, por tipo de dispositivo, sistema operativo, etiquetas asociadas a los dispositivos, entre otros.*
- *El inventario deberá poder exportarse en formato CSV o similar*
- *En el inventario se deberá detallar la condición del dispositivo frente las políticas de seguridad configuradas, de modo de poder visualizar rápidamente qué dispositivos, por ejemplo, carecen de un anti-virus, tienen instaladas aplicaciones no permitidas, entre otros.*
- *Deberá generar y enviar periódicamente (por ejemplo, diariamente, semanalmente o mensualmente) por correo electrónico a los administradores correspondientes, reportes que contengan información referida únicamente a dispositivos (o grupos de dispositivos a determinar por el administrador) que no cumplan con alguna política referida a su seguridad o postura.*
- *Deberá proporcionar un inventario de las aplicaciones (incluyendo su versión) que están corriendo en los dispositivos enrolados, para los distintos sistemas operativos. Dicho inventario debe poder exportarse en formato CSV.*
- *Deberá proporcionar la información recolectada correspondiente a un dispositivo determinado de manera consolidada, es decir, detallando el nombre del dispositivo, modelo, información del hardware (CPU, disco utilizado, etc), información del sistema operativo, información sobre la seguridad/postura del dispositivo, aplicaciones instaladas, información de conectividad (IPs y adaptadores de red), entre otros.*
- *Deberá proporcionar un mapa donde pueda visualizarse de manera estimada la ubicación de todos los dispositivos enrolados. Adicionalmente, debe ser posible visualizar la ubicación de un dispositivo enrolado en particular.*
- *Deberá poder envíar alertas a uno, varios o todos los administradores ante condiciones anónamalas detectadas en los dispositivos administrados, entre ellas: i) cuando se producen cambios en la configuración, ii) cuando se instala determinado software, iii) cuando se pierde el rastro de un cliente por más de un tiempo pre-establecido, iv) cuando se produce una violación en términos de geolocalización, entre otras.*
- *La solución debe ser capaz de enviar alertas de SNMP (SNMP traps).*

FUNCIONALIDADES COMO SOLUCIÓN DE EMM:

- *Describir en qué consiste el proceso de enrolamiento de un dispositivo en la solución.*
- *Debe ofrecer métodos para enrolar dispositivos de manera masiva.*
- *La solución debe ser capaz de soportar la funcionalidad de separación de data personal de comporativa mediante container para dispositivos móviles Android y iOS para casos de Bring Your Own Device (BYOD), donde el administrador pueda tener control del container dedicado a la data corporativa. Debe soportarse la tecnología nativa de container para Android mediante Android Enterprise (anteriormente conocido como Android for Work) y iOS mediante Apple's Managed Open-In.*
- *Debe soportar enrolar un dispositivo Android bajo Android Enterprise, soportando el modo de "device owner" y "work profile".*
- *Debe soportar que los dispositivos móviles (Android y iOS) se encuentren en modo kiosk, es decir, que solo se les permita a los usuarios tener acceso a una (o varias) aplicación/es específica/s, evitando que puedan acceder a otras funcionalidades del*

dispositivo que no hayan sido definidas en la configuración.

- *Debe permitir que un administrador acepte el enrolamiento de un dispositivo, previamente a que dicho dispositivo reciba el perfil y/o aplicaciones que le corresponden por haberse enrolado.*
- *Debe ser capaz de limitar desde qué red puede enrolarse un dispositivo.*
- *Deberá poder definir un intervalo de tiempo donde los dispositivos no deben recibir actualizaciones referidas a sus perfiles o aplicaciones.*
- *Debe ofrecer algún mecanismo para clasificar dispositivos en grupos. Por ejemplo, incluir dos o más dispositivos como parte de un mismo grupo para luego aplicarles alguna política en común.*
- *Debe permitir realizar esta clasificasificación de dispositivos en grupos de manera simultánea en dos o más dispositivos.*
- *Debe permitir definir perfiles (o similar) para poder aplicar una configuración común a un grupo de dispositivos (por ejemplo, a los dispositivos de los empleados Android, a los dispositivos corporativos Windows, etc).*
- *Debe permitir realizar autenticación a nivel de usuario al momento en que se desea enrolar un nuevo dispositivo, y luego poder utilizar esta información en políticas asociadas al dispositivo.*
- *Debe permitir utilizar Active Directory (AD) para realizar la autenticación a nivel de usuario al momento de enrolar un nuevo dispositivo, y debe ser capaz de utilizar la información sobre grupos de Active Directory (AD Groups), en las políticas que correspondan a los dispositivos de acuerdo al grupo de AD al que pertenecen sus dueños.*
- *Describir si la solución es capaz de realizar autenticación a nivel de usuario al momento en que se desea enrolar un nuevo dispositivo, utilizando otras integraciones con terceros (además de Active Directory).*
- *La solución debe ser capaz de desplegar aplicaciones públicas (provenientes de Google Play Store y Apple App Store) y aplicaciones privadas desarrolladas por la organización en los dispositivos móviles (Android y iOS) enrolados.*
- *Debe ser capaz de instalar aplicaciones/software desarrolados por la organización en computadoras Windows y Mac desde la consola de administración. Además, para el caso de Mac, la solución debe ser capaz de deplegar aplicaciones mediante la Mac App Store.*
- *La solución debe ser capaz de configurar una aplicación para un dispositivo móvil (Android y iOS) desde la consola de administración, para aplicaciones que implementen el estándar App Config (http://www.appconfig.org/).*
- *Debe incluir parámetros asociados a la postura de un dispositivo, para determinar si es compliant o no-compliant y utilizar esta información en el perfil donde se determina qué política está asociada a ese dispositivo (qué permisos y restricciones tiene el dispositivo).*
- *Debe verificar que un dispositivo no tenga instalada una aplicación definida en una lista negra por el administrador. En caso de encontrarse instalada, el dispositivo debe clasificarse como no-compliant.*
- *Debe verificar que un dispositivo tenga instalada una aplicación definida en una lista blanca. En caso de no encontrarse instalada, el dispositivo debe clasificarse como no-compliant.*
- *Deberá poder utilizar wildcards para definir aplicaciones a incluir en listas blancas o negras.*
- *Debe monitorear y alertar cuando software o aplicaciones no autorizadas se instalen.*
- *Debe permitir establecer una mínima versión de sistema operativo. Si un dispositivo cuenta con una versión anterior, debe clasificarse como no-compliant.*
- *Debe ser capaz de contemplar la ubicación geográfica de un dispositivo móvil, y utilizar esta información en el perfil donde se determine qué política está asociada a ese*

dispositivo.

- *Debe poder determinar la ubicación del dispositivo móvil a partir de distintos métodos, incluidos GPS, Wi-Fi y por IP pública.*
- *Debe ser capaz de contemplar el día de la semana y la hora, y utilizar esta información en el perfil donde se determina qué política está asociada a ese dispositivo (qué permisos y restricciones tiene el dispositivo) para ese día y hora. Es decir, la solución debe poder aplicar perfiles distintos, por ejemplo, a dos horas distintas si así se lo definiera.*
- *Debe poder modificar los permisos otorgados a un dispositivo de manera automática en función de información incluida en la política, como la hora del día, la geolocalización, la postura, entre otros.*
- *Deberá aprovisionar cuentas de correo electrónico de Exchange en dispositivos móviles (Android y iOS) enrolados.*
- *Permitirá que un administrador comparta archivos con dispositivos móviles (Android y iOS) enrolados.*
- *Deberá garantizar que los dispositivos enrolados puedan ser configurados y monitoreados desde la consola de administración, independientemente de la ubicación de dichos dispositivos.*
- *Debe poder establecer una sesión de remote-desktop en la computadora enrolada, para simplificar las tareas del departamento de IT a la hora de tener que realizar troubleshooting.*
- *Debe ser capaz de realizar una captura de pantalla en la computadora enrolada, para simplificar las tareas del departamento de IT a la hora de tener que realizar troubleshooting.*
- *Debe permitir ejecutar comandos en la computadora desde la consola de administración, para simplificar las tareas del departamento de IT a la hora de tener que realizar troubleshooting.*
- *Debe permitir acceder a la lista de procesos de la computadora desde la consola de administración, para simplificar las tareas del departamento de IT a la hora de tener que realizar troubleshooting.*
- *Deberá permitir el monitoreo activo de conexiones TCP, estadísticas TCP y tablas de enrutamiento de la computadora desde la consola de administración, para simplificar las tareas del departamento de IT a la hora de tener que realizar troubleshooting.*
- *Tendrá la capacidad de reiniciar o apagar una computadora desde la consola de administración, para simplificar las tareas del departamento de IT a la hora de tener que realizar troubleshooting.*
- *Debe permitir enviar una notificación instantánea definida por el administrador a un dispositivo desde la consola de administración. Esta notificación debe poder configurarse una única vez y enviarse a uno, dos o más dispositivos de manera simultánea.*
- *La solución debe ser capaz de ejecutar un wipe completo en un dispositivo desde la consola de administración (es decir, reestablecer la configuración de fábrica en el dispositivo, independientemente de su ubicación).*
- *La solución debe ser capaz de ejecutar un wipe selectivo en un dispositivo desde la consola de administración; es decir, eliminar la configuración y aplicaciones que se han aplicado al dispositivo desde esta solución de EMM sin necesidad de hacer un reseteo del dispositivo a su configuración de fábrica.*
- *LDebe permitir borrar la contraseña en dispositivos móviles (o computadoras) desde la consola de administración.*
- *Debe ser capaz de ejecutar bloqueo (lock) en un dispositivo móvil desde la consola de administración.*
- *La solución debe ser capaz de alertar cuando el consumo de datos móviles se aproxime a*

un valor configurable por el administrador.

- *La solución debe ser capaz de controlar el dispositivo, forzando que la contraseña (passcode) utilizada para desbloquear dispositivos móviles y computadoras personales cumpla, al menos con los siguientes requerimientos: i) que pueda determinarse una longitud mínima de caracteres, ii) que pueda determinarse una cantidad mínima de caracteres no alfanuméricos que deben incluirse y iii) que pueda determinarse un plazo luego del cual la contraseña debe modificarse.*
- *La solución debe mostrar las aplicaciones y perfiles instalados en un dispositivo.*
- *Debe ser capaz de desinstalar aplicaciones en dispositivos móviles Android y Apple, desde la consola de administración.*
- *La solución debe ser capaz de desinstalar aplicaciones y perfiles, para uno o varios dispositivos de manera simultánea, desde la consola de administración.*
- *Debe contar con herramientas para poder localizar un objeto perdido o robado.*
- *Debe contar con métodos para alertar y prevenir que se remueva la configuración o perfil de un dispositivo (dejando este de estar enrolado en la solución).*

INTEGRACIONES:

- *La solución debe ser capaz de controlar el dispositivo, permitiendo realizar su configuración inalámbrica, estableciendo a qué SSID debe conectarse, con el objetivo de que el dispositivo se una automáticamente a la red. Adicionalmente, es deseable que la solución de EMM se integre nativamente con la solución wireless implementada con el objetivo de simplificar este tipo de configuraciones.*
- *La solución debe ser capaz de controlar el dispositivo, permitiendo realizar la configuración inalámbrica del dispositivo, de acuerdo a información del dispositivo como el tipo de dispositivo, su ubicación, su cumplimiento con políticas de seguridad, entre otros.*
- *Es deseable que la solución sea capaz de controlar que los dispositivos que se conecten a la red inalámbrica corporativa cuenten con la solución de EMM instalada, previamente a darles acceso a dicha red. De lo contrario, la solución debería facilitar herramientas para que un usuario pueda instalar esta solución de EMM.*
- *Es deseable que la solución pueda integrarse con la infraestructura existente para asociar dispositivos con políticas configuradas, vinculadas, por ejemplo, a la limitación de ancho de banda por cliente, reglas de firewall de capa 3 y capa 7, traffic shaping, entre otras.*
- *Es deseable que la solución sea capaz de integrarse con la infraestructura wireless existente, y proporcione un certificado único EAP-TLS en un cliente para autenticación mediante certificado, sin necesidad de administrar una CA.*
- *Es deseable que la solución sea capaz de aprovisionar a un cliente VPN que se conectará con el concentrador VPN presente en la red. Adicionalmente, es deseable que la solución de EMM se integre nativamente con el concentrador de VPN implementado con el objetivo de simplificar este tipo de configuraciones.*
- *Debe poder integrarse con la infraestructura existente, siendo capaz de aprovisionar a un cliente VPN, de acuerdo a información del dispositivo como el tipo de dispositivo, su ubicación, su cumplimiento con políticas de seguridad, entre otros.*

SOPORTE

- *La solución ofrecida debe incluir soporte 24 x 7 x 365.*

REQUERIMIENTOS DE LA SOLUCIÓN SAAS

- *La solución debe incluir un Service Level Agreement (SLA) de 99,99% para garantizar el acceso a la consola de administración en la nube.*
- *Debe contar con infraestructura redundante que garantice disponibilidad a la consola de administración en caso de que ocurra una falla en un datacenter del cual la solución dependa.*
- *Debe realizar backups periódicos de la información perteneciente a un cliente.*

Punto 3-

En el punto v.7.5 del Pliego de Bases y Condiciones Particulares donde dice …. "Educ.ar S.E. solo aceptará Pólizas de Caución de instituciones financieras con mínima calificación crediticia a largo plazo de BBB con Standard y Poor's o un mínimo de crédito a largo plazo de Baa3 con Moody Investor Services o un mínimo de calificación de crédito a largo plazo de BBB con Fitch Ratings, la misma deberá ser acreditada por los oferentes".

Deberá decir:

"Educ.ar S.E. sólo aceptará pólizas de caución emitidas por Compañías de Seguros aprobadas por la Superintendencia de Seguros de la Nación, que no se encuentren en proceso de concurso / quiebra y que garanticen, a su satisfacción, el cumplimiento del crédito; reservándose el derecho de solicitar el cambio de la garantía presentada cuando la considere insuficiente."

Punto 4-

Conforme a la consulta realizada por la empresa Grupo Núcleo se detalla a continuación un cuadro a los efectos de brindar mayor claridad y visualización sobre las reparaciones y servicios contemplados en el servicio de mantenimiento integral por nivel educativo.

NIVEL	DISPOSITIVO	COBERTURA DE ST	COBERTURA POR VISITAS
INICIAL	**Tablet**	Pin de carga	Dos cambios de pantallas en

		Pantalla	Tablet o Notebook
	Notebook	HDD	Cambio de pin de carga de tablet (hasta 5)
		Cargador /Reposición	
		Pantalla	Un cambios de HDD en CAP, Notebook o Servidor con Restauración de Sistema
		Sistema operativo y contenidos	
	Pen Drive/Disco externo	NO CUBRE	
	Kit Robótica	NO CUBRE	Para el kit de robótica, micr/parlante, carro y pizarra validar la vigencia de la garantía y solicitarla si corresponde
	Micrófono + Parlante*1	NO CUBRE	
	Proyector	Toda la electrónica exceptuando la lámpara	
	Pizarra	NO CUBRE	Reposición de un Cargador de CAP o Notebook
	CAP	HDD	Restauraciones de sistemas de Tablet/ Notebook/Servidor
		Cargador	
		Sistema operativo y contenidos	Reparación de electrónica de proyector sin reposición de lámpara
	Carro Chico	Toda la electrónica de carga	
	Carro Grande		
	Servidor	Sistema operativo y contenidos	Reparación de electrónica del carro

NIVEL	DISPOSITIVO	COBERTURA DE ST	COBERTURA POR VISITA
PRIMARIA	Netbooks	100% del dispositivo	Hasta 5 reparaciones con cambios de hardware. Todos los dispositivos que presenten falla en el software. Todos las Netbooks que presenten problemas de pila de BIOS.
		Cargador	
	Pen Drive	NO CUBRE	1 Cambio de fuente de servidor
	Kit Robótica	NO CUBRE	Para el kit de robótica, y carro validar la vigencia de la garantía y solicitarla si corresponde
	Cámara Fotográfica	NO CUBRE	
	Proyector	Toda la electrónica exceptuando la lámpara	1 restauración de sistemas de Servidor
	Pizarra	NO CUBRE	
	AccesPoint	NO CUBRE	Reparación de electrónica de proyector sin reposición de lámpara
	Carro Chico	Toda la electrónica de carga	
	Carro Grande		
	Servidor	Fuente	Reparación de electrónica del carro

NIVEL	DISPOSITIVO	COBERTURA DE ST	COBERTURA POR VISITA
SECUNDARIA	Netbooks	100% del dispositivo	Reparación integral de todas las

		Cargador	Netbooks con los repuestos provistos por Educ.ar contra rendición de los mismos. Una vez consumidos los repuestos en stock de Educ.Ar la visita contemplará: Hasta 5 reparaciones con cambios de hardware. Todos los dispositivos que presenten falla en el software. Todos las netbooks que presenten problemas de pila de BIOS.
	Kit Raspberry	NO CUBRE	1 Restauración de sistemas de Servidor
	Sens hat	NO CUBRE	
	Kit Robótica	NO CUBRE	1 Cambio de fuente de servidor
	Carro Chico	Toda la electrónica de carga	Para el kit de robótica, y carro validar la vigencia de la garantía y solicitarla si corresponde
	Carro Grande		
	Servidor	Fuente	Reparación de electrónica del carro

Se notifica que la nueva fecha de apertura es el día lunes 30/09/2019 a las 11:00 hs

Fecha de Apertura: 30/09/2019 11:00 horas

Lugar de obtención del Pliego y la circular: vía Web ingresando en https://educar.com.ar/compra o personalmente en la Gerencia de Compras en AV. COMODORO RIVADAVIA 1151, C.A.B.A, de 10 a 18.00 Hs.

Presentación de ofertas: Hasta la fecha y hora fijadas por el acto de apertura a desarrollarse en el domicilio indicado en el Pliego.

Valor del Pliego: Sin costo.

República Argentina - Poder Ejecutivo Nacional
2019 - Año de la Exportación

Hoja Adicional de Firmas
Anexo

Número: IF-2019-83652844-APN-DA#EDUCAR

CIUDAD DE BUENOS AIRES
Lunes 16 de Septiembre de 2019

Referencia: CIRCULAR MODIFICATORIA N° 1

El documento fue importado por el sistema GEDO con un total de 9 pagina/s.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.09.16 11:11:58 -03'00'

Gabriela CISTERNAS
Directora
Dirección de Administración
Educ.ar S. E.

Digitally signed by GESTION DOCUMENTAL ELECTRONICA - GDE
DN: cn=GESTION DOCUMENTAL ELECTRONICA - GDE, c=AR, o=SECRETARIA DE GOBIERNO DE MODERNIZACION, ou=SECRETARIA DE MODERNIZACION ADMINISTRATIVA, serialNumber=CUIT 30715117564
Date: 2019.09.16 11:11:59 -03'00'