

PLIEGO DE ABSOLUCIÓN DE CONSULTAS Y OBSERVACIONES

Entidad convocante : UNIVERSIDAD NACIONAL SAN MARTIN

Nomenclatura : LP-ABR-1-2025-UNSM/C-1

Nro. de convocatoria : 1

Objeto de contratación : Bien

Descripción del objeto : ADQUISICION DE UN SISTEMA DE CIBERSEGURIDAD CON FIREWALL DE NUEVA GENERACION PARA LA UNIVERSIDAD NACIONAL DE SAN MARTIN

Ruc/código :	20602691617	Fecha de envío :	04/07/2025
Nombre o Razón social :	CLOUD INFRASTRUCTURE AND TELECOM PERU SOCIEDAD ANONIMA CERRADA - CLOUD IT PERU S.A.C.	Hora de envío :	18:10:43

Consulta: Nro. 1

Consulta/Observación:

Se pide confirmar como y en que parte de la oferta o momento se acreditara las especificaciones técnicas requeridas, a fin de que la entidad pueda validar el cumplimiento y todos los postores puedan ser evaluados en igualdad de condiciones.

Acápite de las bases : Sección: Especifico **Numeral:** III **Literal:** 3.4 **Página:** 22

Artículo y norma que se vulnera (En el caso de Observaciones):

Estado: Se acoge

Análisis respecto de la consulta u observación:

Se debe presentar una declaracion jurada para la admision de la oferta, indicando la marca y modelos ofertados, y su direccion web para acreditar al menos las características de hardware y rendimiento requeridos para los firewall de campus y rectorado, con el objetivo de que las ofertas presentadas contemplen lo requerido por la entidad y optimizar los plazos de contratacion.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

Se agrega en la documentacion para la admision de la oferta 2.2.1.1. del capitulo II de la seccion especifica: H) Se debe presentar una declaracion jurada para la admision de la oferta, indicando la marca y modelos ofertados, y su direccion web para acreditar al menos las características de hardware y rendimiento requeridos para los firewall de campus y rectorado

Entidad convocante : UNIVERSIDAD NACIONAL SAN MARTIN

Nomenclatura : LP-ABR-1-2025-UNSM/C-1

Nro. de convocatoria : 1

Objeto de contratación : Bien

Descripción del objeto : ADQUISICION DE UN SISTEMA DE CIBERSEGURIDAD CON FIREWALL DE NUEVA GENERACION PARA LA UNIVERSIDAD NACIONAL DE SAN MARTIN

Ruc/código :	20602691617	Fecha de envío :	04/07/2025
Nombre o Razón social :	CLOUD INFRASTRUCTURE AND TELECOM PERU SOCIEDAD ANONIMA CERRADA - CLOUD IT PERU S.A.C.	Hora de envío :	18:10:43

Observación: Nro. 2

Consulta/Observación:

Consideramos que la identificación y prevención de vulnerabilidades CVE en los equipos de seguridad es una buena practica, la cual debe ser incluida en el presente requerimiento. Sin embargo, consideramos que debemos enfocarnos en aquellas vulnerabilidades que representan un riesgo mayor y que requieren necesariamente ser mitigadas a nivel de actualizaciones y/o parches de seguridad, es decir aquellas que son de nivel alto o critico. Por lo cual, solicitamos favor se consideren para el presente requerimiento, solo las vulnerabilidades CVE de nivel alto o critico, es decir que tenga un valor de CVSS igual o superior a 7.0.

Acápite de las bases : **Sección:** Especifico **Numeral:** III **Literal:** 3.4 **Página:** 24

Artículo y norma que se vulnera (En el caso de Observaciones):

ART 2, 3, 4 LCE

Estado: Se acoge

Análisis respecto de la consulta u observación:

Se precisa que, se evaluaran las vulnerabilidades que implicarían un riesgo en la continuidad operativa de los servicios de la entidad, considerando aquellas que requerirán necesariamente ventanas de mantenimiento y/o cortes de servicio (debido a la aplicación de parches y/o actualizaciones para dichos equipos firewall) y con la finalidad de no restringir la participación de potenciales postores, se considera que se evaluaran solo aquellas vulnerabilidades (CVE) con un nivel de criticidad: alto y/o crítico, establecido a través del valor CVSS (Vulnerability Scoring System) de la vulnerabilidad.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

"De esta manera, se considera que el requerimiento deberá quedar redactado de la siguiente manera:
Los equipos firewall ofertados que conforman el servicio de seguridad perimetral gestionada, no deberán tener en sus respectivos sistemas operativos y/o firmware, más de diez (10) vulnerabilidades (CVE) de nivel alto y/o critico (igual o superior a CVSS 7.0) anunciadas y/o publicadas, acumuladas entre sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de propuestas."

Entidad convocante : UNIVERSIDAD NACIONAL SAN MARTIN

Nomenclatura : LP-ABR-1-2025-UNSM/C-1

Nro. de convocatoria : 1

Objeto de contratación : Bien

Descripción del objeto : ADQUISICION DE UN SISTEMA DE CIBERSEGURIDAD CON FIREWALL DE NUEVA GENERACION PARA LA UNIVERSIDAD NACIONAL DE SAN MARTIN

Ruc/código :	20602691617	Fecha de envío :	04/07/2025
Nombre o Razón social :	CLOUD INFRASTRUCTURE AND TELECOM PERU SOCIEDAD ANONIMA CERRADA - CLOUD IT PERU S.A.C.	Hora de envío :	18:10:43

Observación: Nro. 3

Consulta/Observación:

Consideramos que la identificación y prevención de vulnerabilidades CVE en los equipos de seguridad es una buena practica, la cual debe ser incluida en el presente requerimiento. Sin embargo, consideramos que debemos enfocarnos en aquellas vulnerabilidades que representan un riesgo mayor y que requieren necesariamente ser mitigadas a nivel de actualizaciones y/o parches de seguridad, es decir aquellas que son de nivel alto o critico. Por lo cual, solicitamos favor se consideren para el presente requerimiento, solo las vulnerabilidades CVE de nivel alto o critico, es decir que tenga un valor de CVSS igual o superior a 7.0.

Acápite de las bases : **Sección:** Especifico **Numeral:** III **Literal:** 3.4 **Página:** 31

Artículo y norma que se vulnera (En el caso de Observaciones):

ART 2, 3, 4 LCE

Estado: Se acoge

Análisis respecto de la consulta u observación:

Se precisa que, se evaluaran las vulnerabilidades que implicarían un riesgo en la continuidad operativa de los servicios de la entidad, considerando aquellas que requerirán necesariamente ventanas de mantenimiento y/o cortes de servicio (debido a la aplicación de parches y/o actualizaciones para dichos equipos firewall) y con la finalidad de no restringir la participación de potenciales postores, se considera que se evaluaran solo aquellas vulnerabilidades (CVE) con un nivel de criticidad: alto y/o critico, establecido a través del valor CVSS (Vulnerability Scoring System) de la vulnerabilidad.

Precisión de aquello que se incorporará en las bases a integrarse, de corresponder:

"De esta manera, se considera que el requerimiento deberá quedar redactado de la siguiente manera:
Los equipos firewall ofertados que conforman el servicio de seguridad perimetral gestionada, no deberán tener en sus respectivos sistemas operativos y/o firmware, más de diez (10) vulnerabilidades (CVE) de nivel alto y/o critico (igual o superior a CVSS 7.0) anunciadas y/o publicadas, acumuladas entre sus diferentes versiones durante los últimos 12 meses anteriores a la fecha de presentación de propuestas."