ADENDA #1
ADENDA ACLARATORIA
RETO LÍNEAS DE TRANSMISIÓN
17/06/2024

De acuerdo con la sección **"5. CONVOCATORIA: CRONOGRAMA Y FASES DEL PROCESO"** de los términos de referencia, que en su numeral 5.2, Nota 1, reza: *"Las Entidades Operadoras, cuando así lo estimen conveniente y sin justificación alguna, se reservan en cualquier momento el derecho a declarar desierta, suspender o terminar la presente convocatoria, o modificar el cronograma anterior y/o los términos y condiciones, sin que haya lugar a reclamación alguna o reconocimiento de indemnización para los Participantes."*, el equipo operador de la Convocatoria Retos Econova 2024 #HubTransiciónEnergética, procede a expedir la presente **ADENDA**, con la cual se da **aclaración a la ficha del reto de líneas de transmisión (Anexo 1: Retos de Innovación – Líneas de transmisión)**.

Cabe resaltar que las siguientes consideraciones se refieren a los temas de ciberseguridad y la integración de la solución a la arquitectura de ECOPETROL. Estas consideraciones no representan una adición a los requerimientos de la convocatoria para la selección de la idea innovadora, pero si serán de obligatorio aseguramiento en el marco de la ejecución del piloto de experimentación.

Consideración general:

- Se puede implementar cualquier tecnología (IaaS, PaaS o SaaS)
- La nube preferente es AZURE.
- Todos los componentes que utilicemos en la red deben ser intrínsecamente seguros.

Consideración #1: Seguridad de los datos

- Contemplar el cumplimiento normativo de la Ley 1581 de 2012 protección de datos personales.
- Contemplar la implementación de controles de cifrado para la información en tránsito y en reposo que sea catalogada como RESERVADA, CLASIFICADA o DATO PERSONAL.
- Dentro de las bases de datos, es importante garantizar el control de accesos a la información ya sea por usuarios o por aplicaciones o servicios.
- En los casos que aplique, garantizar un borrado seguro: Eliminar toda la información entregada por ECOPETROL. El proceso deberá registrarse en acta donde se especifique el mecanismo utilizado y el tipo de datos usados.
- Cifrar las imágenes: El cifrado de blobs de Azure protege las imágenes en reposo mediante el cifrado AES de 256 bits.

- Utilizar claves de acceso con cuidado: Generar claves de acceso seguras y almacenarlas de forma segura en Azure Key Vault. Restringir el acceso a las claves de acceso y rotarlas periódicamente.

Consideración #2: Seguridad de las aplicaciones

Para toda plataforma o aplicación que no se encuentre vinculada al directorio activo para la administración de la autenticación, implementar:

- Políticas de contraseñas fuertes.
- Uso de MFA (Multiple Factor de autenticación).
- Almacenamiento seguro de credenciales, usando algoritmos de cifrado con SALT y siguiendo las pautas establecidas por OWASP para el almacenamiento de credenciales.

Consideración #3: Seguridad en la plataforma Azure

- Revisar las características de seguridad integradas de Azure: La nube ofrece una amplia gama de funciones de seguridad integradas, como Azure Active Directory (Azure AD) para la autenticación y autorización, Azure Key Vault para la administración segura de claves y Azure Security Center para la supervisión y protección contra amenazas.

- Utilizar redes virtuales (VNet) para aislar sus recursos: Las VNet le permiten crear redes privadas dentro de la nube de Azure, lo que le brinda un mayor control sobre el acceso a sus recursos de almacenamiento de imágenes.

- Implementar firewalls de aplicaciones web (WAF) para protegerse contra ataques web: Los WAF pueden filtrar el tráfico malicioso y proteger sus imágenes de ataques como inyección de código SQL y ataques de secuencias de comandos entre sitios (XSS)

Consideración #4: Seguridad de la red

- Protección perimetral: mediante sistemas de firewalls, proxis, detectores de intrusos, gestión de los logs y alarmas que producen estos equipos.

- Garantizar el uso de protocolos seguros como (SSL, TLS, HTTPS, HSTS, entre otros) para las integraciones o conexiones que se realizan actualmente, o las nuevas que vayan a ser contempladas dentro de este proyecto, independientemente de si son conexiones internas o externas.

- Garantizar el uso de protocolos cifrados desde el acceso seguro a las redes Cloud, para ello es importante centralizar el uso de un sistema de gestión de acceso VPN y el uso de máquinas y/o servicios bastión bajo esquemas Tier 0,1 y 2. Como elemento alternativo a los mecanismos de comunicación VPN tradicionales para conectar la nube con los servicios on- premise, se podrá utilizar mecanismos SDP (software defined perimeter).

- Segmentación de redes: evitar que el tráfico de un grupo de usuarios y equipos se mezcle con otros. Utilizar VLANs (Redes Locales Virtuales). También es muy común separar distintas redes IP mediante routers con reglas de filtrados, lo que permite diferenciar tráficos.

Consideración #5: Control de acceso

- Contemplar controles para la gestión de Control de Accesos y Gestión de Usuarios, siguiendo los procedimientos establecidos por Ecopetrol para evitar accesos no autorizados, suplantación de usuarios y dispositivos, pérdida y fuga de información, para toda infraestructura, plataforma y/o aplicaciones diseñadas e implementadas.

- Considerar la autorización, según el principio de menor privilegio. Por lo tanto, es importante incluir en el diseño, la definición de los roles y funciones asignadas a cada rol.

Consideración #5: Gestión de vulnerabilidades

- Implementar configuraciones de seguridad, para todos los sistemas, plataformas y aplicaciones que hacen parte del alcance para el proyecto.
- Planear y ejecutar la remediación de vulnerabilidades antes de la salida en vivo del proyecto, en el cual se realice la identificación, análisis - priorización, remediación y verificación de las vulnerabilidades TI con sus respectivos planes, acciones, mediciones y evidencias.

Consideración #5: Ciberseguridad en cadena de suministro

- Reportar todas las novedades (Ingresos, vacaciones, licencias, retiros), del personal que disponga para la ejecución del contrato, con el fin de mantener únicamente los accesos requeridos para cumplir con el objeto del contrato.

- Contar con controles de acceso sobre las aplicaciones, bases de datos, sistemas operativos y dispositivos de red que aseguren una segregación de funciones y que los usuarios dispongan de los mínimos privilegios.

- Garantizar que todo software usado en su infraestructura tecnológica se encuentra debidamente licenciado.

- Implementar controles y procedimientos para garantizar el borrado seguro de la información de Ecopetrol a la que tenga acceso, en tanto esta ya no sea requerida para el producto o servicio prestado.

- Certificar la ejecución de verificación de antecedentes de los empleados de la organización, que tendrán acceso a información de Ecopetrol.

- Habilitar en los equipos de los usuarios limitaciones, políticas de seguridad, antivirus, antimalware, etc. Entre estas limitaciones destaca el uso de Wifi cifrada, la imposición de utilizar VPNs desde accesos públicos, negar al usuario la posibilidad

de instalar aplicaciones, deshabilitar los puertos USB para que no se puedan conectar dispositivos de memoria, etc

Consideración #6: Pruebas y validación

- Pruebas exhaustivas de la capacidad de detección y clasificación de fallas, validación de la precisión del sistema mediante inspecciones reales, se debe cuantificar la especificidad, sensibilidad del modelo, además de estadísticos de ajuste de modelos y clasificadores (ej. Métricas AUC).

- Aplicación de técnicas predictivas (Inspección coronografía o ultrasonido)

Consideración #7: Mantenimiento y actualizaciones

- Actualizaciones de modelos de inteligencia artificial /Machine Learning, monitoreo constante de la infraestructura desplegada en Azure para garantizar rendimiento y disponibilidad.