**Análisis de Gestión del Riesgo**

**Interacción con AWS - Basado en norma ISO 31000**

La interacción del dispositivo IoT con AWS mediante certificados, almacenamiento en bucket S3 y la función Lambda para la publicación y suscripción de datos, introduce varios riesgos específicos.

Aplicando la norma ISO 31000, se pueden identificar y gestionar estos riesgos para asegurar la seguridad y fiabilidad de la transmisión y procesamiento de datos. A continuación, presentamos la matriz de riesgos enfocada en la interacción del dispositivo IoT con AWS.

**Matriz de Riesgos para la Interacción del Dispositivo IoT con AWS**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **ID** | **Descripción del Riesgo** | **Impacto** | **Probabilidad** | **Nivel de Riesgo** | **Estrategia de Mitigación** |
| IA1 | Compromiso de Certificados | Alto | Media | Alto | Implementar políticas de rotación de certificados. Utilizar certificados con fechas de expiración cortas. |
| IA2 | Fuga de Datos Sensibles a través de S3 | Alto | Media | Alto | Configurar políticas de acceso y permisos estrictos en S3. Utilizar cifrado para datos en reposo y en tránsito. |
| IA3 | Fallo en la Ejecución de Funciones Lambda | Alto | Media | Alto | Implementar pruebas exhaustivas y monitoreo continuo de funciones Lambda. Contar con planes de contingencia. |
| IA4 | Conexión Inestable entre el Dispositivo IoT y AWS | Alto | Media | Alto | Implementar mecanismos de reconexión automática y redundancia en las conexiones. |
| IA5 | Exposición a Ataques de Intermediarios (MITM) | Alto | Media | Alto | Utilizar cifrado fuerte para todas las comunicaciones. Configurar VPN de conexión. |
| IA6 | Fallos de Seguridad en la Publicación/Suscripción de Datos MQTT | Alto | Media | Alto | Asegurar la autenticación y autorización para todos los clientes MQTT. Utilizar TLS para las conexiones MQTT. |
| IA7 | Pérdida de Integridad de los Datos Transmitidos | Alto | Media | Alto | Implementar mecanismos de verificación de integridad, como firmas digitales o checksums. |
| IA8 | Configuración Incorrecta de Políticas IAM en AWS | Alto | Media | Alto | Revisar y auditar regularmente las políticas IAM. Implementar el principio de privilegio mínimo. |
| IA9 | Escalabilidad y Rendimiento de las Funciones Lambda | Medio | Alta | Alto | Monitorear el rendimiento y ajustar la configuración de escalado automático. Optimizar el código de las funciones. |
| IA10 | Falta de Monitoreo y Alertas en Tiempo Real | Alto | Media | Alto | Implementar servicios de monitoreo y alertas en tiempo real, como CloudWatch. Configurar notificaciones de eventos. |
| IA11 | Fallos en la Sincronización de Datos entre el Dispositivo y AWS | Alto | Media | Alto | Utilizar mecanismos de sincronización robustos y realizar pruebas de consistencia de datos periódicamente. |

Descripción Detallada de Estrategias de Mitigación

**IA1: Compromiso de Certificados**

**Estrategia para Mitigar:**

* Implementar políticas de rotación de certificados.
* Utilizar certificados con fechas de expiración cortas.

**Acciones:**

* Rotar los certificados regularmente y revocar los comprometidos.
* Configurar alertas para certificados próximos a expirar.

**IA2: Fuga de Datos Sensibles a través de Bucket S3**

**Estrategia para Mitigar:**

* Configurar políticas de acceso y permisos estrictos en Bucket S3.
* Utilizar cifrado para datos en reposo y en tránsito.

**Acciones:**

* Revisar y aplicar políticas de IAM estrictas para accesos a Bucket S3.
* Configurar cifrado automático para todos los datos almacenados en Bucket S3.

**IA3: Fallo en la Ejecución de Funciones Lambda**

**Estrategia para Mitigar:**

* Implementar pruebas exhaustivas y monitoreo continuo de funciones Lambda.
* Contar con planes de contingencia.

**Acciones:**

* Desarrollar y ejecutar pruebas unitarias y de integración para las funciones Lambda.
* Monitorear la ejecución de Lambda con CloudWatch y configurar alertas para fallos.

**IA4: Conexión Inestable entre el Dispositivo IoT y AWS**

**Estrategia para Mitigar:**

* Implementar mecanismos de reconexión automática y redundancia en las conexiones.

**Acciones:**

* Configurar el cliente IoT para reconectar automáticamente en caso de pérdida de conexión.
* Utilizar múltiples puntos de conexión para redundancia.

**IA5: Exposición a Ataques de Intermediarios (MITM)**

**Estrategia para Mitigar:**

* Utilizar cifrado fuerte para todas las comunicaciones.
* Configurar VPN de conexión.

**Acciones:**

* Implementar TLS para todas las comunicaciones entre el dispositivo IoT y AWS.
* Configurar VPN para asegurar la transmisión de datos.

**IA6: Fallos de Seguridad en la Publicación/Suscripción de Datos MQTT**

**Estrategia para Mitigar:**

* Asegurar la autenticación y autorización para todos los clientes MQTT.
* Utilizar TLS para las conexiones MQTT.

**Acciones:**

* Implementar autenticación basada en certificados para los clientes MQTT.
* Configurar TLS para asegurar las conexiones MQTT.

**IA7: Pérdida de integridad de los datos transmitidos**

**Estrategia para Mitigar:**

* Implementar mecanismos de verificación de integridad, como firmas digitales o checksums.

**Acciones:**

* Utilizar algoritmos de hash para verificar la integridad de los datos.
* Implementar firmas digitales para asegurar la autenticidad de los datos.

**IA8: Configuración incorrecta de políticas IAM en AWS**

**Estrategia para Mitigar:**

* Revisar y auditar regularmente las políticas IAM.
* Implementar el principio de privilegio mínimo.

**Acciones:**

* Realizar auditorías periódicas de las políticas IAM.
* Configurar políticas IAM con privilegios mínimos necesarios.

**IA9: Escalabilidad y rendimiento de las funciones Lambda**

**Estrategia para Mitigar:**

* Monitorear el rendimiento y ajustar la configuración de escalado automático.
* Optimizar el código de las funciones.

**Acciones:**

* Configurar CloudWatch para monitorear el rendimiento de las funciones Lambda.
* Ajustar las configuraciones de escalado automático según las necesidades.

**IA10: Falta de monitoreo y alertas en tiempo real**

**Estrategia para Mitigar:**

* Implementar servicios de monitoreo y alertas en tiempo real, como CloudWatch.
* Configurar notificaciones de eventos.

**Acciones:**

* Configurar CloudWatch para monitorear los servicios y recursos de AWS.
* Configurar SNS para notificaciones de eventos críticos.

**IA11: Fallos en la sincronización de datos entre el dispositivo y AWS**

**Estrategia para Mitigar:**

* Utilizar mecanismos de sincronización robustos y realizar pruebas de consistencia de datos periódicamente.

**Acciones:**

* Implementar colas de mensajes para asegurar la entrega de datos.
* Realizar pruebas periódicas para asegurar la consistencia y sincronización de los datos.

Este levantamiento de información basado en la norma ISO 31000 inicia con la identificación y evaluación de los riesgos asociados en el segundo sprint definido para nuestro proyecto. Los riesgos aquí mencionados pueden variar según las configuraciones en la cuenta de AWS utilizada para el registro, programación y pruebas para la transmisión de información desde el dispositivo IoT.