### **Access Controls Worksheet**

**Note(s)**

1. The event log indicates that the suspicious transaction was performed from IP address 152.207.255.255 at 8:29:57 AM, and the user associated with it is "Legal\Administrator."
2. The account of "Robert Taylor Jr.," a contractor whose contract ended on 12/27/2019, was still active and allowed critical actions. This suggests that the account was not deactivated after the end of the contract.

**Issue(s)**

1. **Improper Contractor Account Management:**
   * The access for "Robert Taylor Jr.," a contractor whose contract ended on 12/27/2019, was still active, allowing critical actions. This indicates that the process for deactivating accounts of contractors and employees who are no longer with the company is not being followed properly.
2. **Inadequate Administrative Permissions:**
   * The account that performed the critical event had administrative permissions, even though it should not have access to such critical functions. This suggests a potential lack of adequate controls to ensure that administrative permissions are granted and reviewed according to the user's current role and status.

**Recommendation(s)**

1. **Implement an Account Review and Deactivation Process:**
   * **Actions:**
     + Establish a procedure to notify the IT team when an employee or contractor leaves the company.
     + Automate account deactivation at the end of contracts using an identity management system.
     + Conduct monthly audits to ensure inactive accounts have been deactivated.
   * **Benefit:** Reduces the risk of unauthorized access and ensures that only active users have access to critical resources.
2. **Establish a Rigorous Access Control Policy:**
   * **Actions:**
     + Define roles and responsibilities for assigning and managing permissions.
     + Implement a role-based access control (RBAC) system to ensure permissions align with job functions.
     + Conduct quarterly reviews of permissions to ensure they are appropriate and up-to-date.
   * **Benefit:** Minimizes the risk of privilege abuse and ensures that only authorized personnel have access to sensitive information.

### 

### **Hoja de control de acceso (spanish)**

**Nota(s)**

1. El evento del registro de eventos muestra que la transacción sospechosa se realizó desde la dirección IP 152.207.255.255 a las 8:29:57 AM, y el usuario asociado es "Legal\Administrator".
2. La cuenta del usuario "Robert Taylor Jr." tenía permisos administrativos activos a pesar de que su contrato terminó el 27/12/2019. Esto indica que su cuenta no se desactivó después de que su contrato terminó.

**Problema(s)**

1. **Cuenta de Contratista Activa Indevidamente:**
   * El acceso de "Robert Taylor Jr.", un contratista cuyo contrato finalizó el 27/12/2019, todavía estaba activo y permitía realizar acciones críticas. Esto sugiere que el proceso para desactivar cuentas de contratistas y empleados que ya no están en la empresa no se sigue adecuadamente.
2. **Permisos Administrativos Inadecuados:**
   * La cuenta que realizó el evento crítico tiene permisos administrativos, pero no debería tener acceso a funciones tan críticas. Esto indica una posible falta de controles adecuados para asegurar que los permisos administrativos se otorguen y revisen de acuerdo con el rol y el estatus actual del usuario.

**Recomendación(es)**

1. **Implementar un Proceso de Revisión y Desactivación de Cuentas:**
   * **Acciones:**
     + Establecer un procedimiento para notificar al equipo de TI cuando un empleado o contratista deje la empresa.
     + Automatizar la desactivación de cuentas al final de los contratos mediante un sistema de gestión de identidades.
     + Realizar auditorías mensuales para verificar que las cuentas inactivas hayan sido desactivadas.
   * **Beneficio:** Reduce el riesgo de accesos no autorizados y asegura que solo los usuarios activos tengan acceso a los recursos críticos.
2. **Establecer una Política de Control de Accesos Rigurosa:**
   * **Acciones:**
     + Definir roles y responsabilidades para la asignación y gestión de permisos.
     + Implementar un sistema de gestión de accesos basado en roles (RBAC) para asegurar que los permisos estén alineados con las funciones laborales.
     + Realizar revisiones de permisos trimestrales para garantizar que los accesos sean apropiados y estén actualizados.
   * **Beneficio:** Minimiza el riesgo de abuso de privilegios y asegura que solo el personal autorizado tenga acceso a información sensible.