## Access controls worksheet

|  | **Note(s)** | **Issue(s)** | **Recommendation(s)** |
| --- | --- | --- | --- |
| **Authorization /authentication** | **Objective:** Make 1-2 notes of information that can help identify the threat:   * *Who caused this incident?*   *Se identfico que los la IP del equipo que fue Robert Taylor Jr., corresponde a un Usuario con rol Administrador fue el que origino el incidente que generó la orden de pago de origen extraño.*   * *When did it occur?*   *El incidente ocurrio el 10/03/2023 sobre las 8:29:57 AM.*   * *What device was used?*   *El equipo utilizado corresponde al equipo con la IP 152.207.255.255 que es utilizado por Robert Taylor Jr.* | **Objective:** Based on your notes, list 1-2 authorization issues:   * *What level of access did the user have?*   *El usuario tenia nivel de admin.*   * *Should their account be active?*   *Esta cuenta no debería de haber estado activa, se tuvo que dar de baja el 27/12/2019.* | **Objective:** Make at least 1 recommendation that could prevent this kind of incident:   * *Which technical, operational, or managerial controls could help?*   *Las cuentas inactivas deberian de expirar despues de 30 días.*  *Establecer SSO y MFA para autorizar las ordenes de pago futuras.*  *Los contratistas deben tener acceso limitado a los recursos.* |