Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: 1. Es evidente que el usuario que ingresó al sistema, es un usuario antiguo el cual ya no trabaja en la compañía. 2. Se añadió información de pago al sistema ejecutada como administrador. ● *Who caused this incident?* *Mala administración de perfiles y atribuciones de los empleados* ● *When did it occur?* *10/03/2023* ● *What device was used?* *Computer: Up2-NoGud*	**Objective:** Based on your notes, list 1-2 authorization issues: 1. Esta cuenta tiene autorización para realizar cambios de administrador . 2. La cuenta no debería tener acceso ya que puede ser utilizada por el usuario o por un atacante que haya encontrado esta informacion. ● *What level of access did the user have?* *Tenía nivel de acceso de administrador* ● *Should their account be active?* *Esta cuenta debería estar completamente inhabilitada*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: Lo principal sería una auditoría de los perfiles que tienen acceso a la compañía y con qué permisos cuenta, para así tomar las medidas correspondientes de administración de perfiles disminuyendo privilegios y superficie de ataque. ● *Which technical, operational, or managerial controls could help?* *Un operativo de gestión de perfiles y autorizaciones sería lo ideal, ya que este perfil no debería estar habilitado y menos con permisos de administrador, ya que un*

		desde hace al menos unos 4 años.	*atacante tendría una entrada muy fácil para hacer mucho daño a la compañía.*