Informe de riesgos
Aprobado

AENZA

1.- Detalle de caso

Sobre el caso	
Fecha	01 julio 2025
Validez del informe	16 enero 2026
Código Interno	AS-15
Elaborado por	Yovana Reyes Delgado
Proceso Impactado	00 Control Y Gestión De Accesos
Área Impactada	TI Corporativo
Actividad	Que se altere o pierda información del negocio al otorgar accesos que presenten conflicto de segregación de funciones a cuentas con privilegios administrativos. El equipo de aplicaciones corporativas de AENZA SS.CC y los responsables de TI de las empresas del grupo AENZA tienen acceso con privilegio de administración en el sistema ICARUS, de acuerdo con la necesidad de realizar configuraciones propias de la herramienta para el funcionamiento en las empresas. La aprobación de los accesos se da de acuerdo a los lineamientos corporativo de gestión de accesos
Aplicativo	ICARUS
Referencia a la Política y/o norma	ANZ-TI-IN-005 Gestion de accesos ANZ-GR-MN-001 Manual de riesgos ANZ-TI-PC-001 Administracion de cuentas de usuarios, perfiles y asignación de accesos.

2.- Detalle de el/los riesgos evaluados

Sobre el/los riesgos evaluados				
Preocupación	**Riesgo**	**Probabilidad**	**Impacto**	**NRI**
Que se vulnere la integridad y confidencialidad de la información debido al uso inapropiado de cuentas con privilegio administrativos que ademas presentas conflicto de segregación de funciones.	Fuga de información confidencial de la empresa	3	4	3.46
Se mantengan perfiles administrativos con conflicto de segregación de funciones, pudiendose vulnerar la integridad y confidencialidad de la información del sistema ICARUS.	Fuga de información confidencial de la empresa	3	4	3.46

3.- Detalle de el/los controles evaluados

Sobre el/los controles evaluados						
Control	**Descripción**	**Frecuencia**	**Tipo**	**Manual**	**Formalidad**	**Fortaleza**

TI / 02.1	Creación – Modificación (1) 1) El Dueño del Proceso revisa la solicitud y aprueba o rechaza (2) bajo las siguientes consideraciones: - Validación de segregación de funciones: El Gestor de TI o el responsable del negocio según aplique verifica de manera manual o automática que no existe conflicto de segregación de funciones (3) de acuerdo a la matriz SOD registrada en el site de Control Interno según corresponda a la asignación/modificación de accesos. En caso de conflicto, el Dueño del Proceso o Dueño de Proceso Corporativo, según corresponda, procede a rechazar la solicitud o gestiona el acta de aceptación de riesgo según aplique con el área de Riesgos Corporativo de acuerdo a lo establecido en el Manual de Riesgos Corporativo. - Revisión del acceso solicitado en relación a las funciones laborales de usuario. 2) El Responsable de ejecutar la solicitud valida que la solicitud haya sido aprobada para proceder a realizar la actividad solicitada. En caso la solicitud sea rechazada se comunica al solicitante. (4) Notas: (1) Como excepción se tienen las altas automáticas mediante las cuales se realizan creaciones de cuentas de usuario y/o asignaciones de accesos por defecto de manera	Transaccional	Preventivo	Sí	Evidenciado	Moderado

	automática al momento de generar el alta del personal en el sistema de planillas u otro sistema. Aquellos accesos que no se asignan por defecto siguen las actividades indicadas como parte del control. (2) La aprobación / conformidad puede ser por correo electrónico, SharePoint, ICARUS o formato físico. (3) No aplica validación SOD para aquellos sistemas que por configuración no permitan la asignación de más de un perfil a una cuenta de usuario. (4) Como excepción se tienen las asignaciones de accesos generadas de manera automática. (5) Para el caso de cuentas de proveedores, estas cuentas se crearán ante una solicitud por parte del proveedor (excepción) o área interesada.					
TI / 02.7	1) El Gestor de TI extrae el historial de transacciones (1) ejecutadas por las cuentas privilegiadas del periodo de revisión.(2) 2) El Jefe de TI (3) revisa que las actividades se encuentren asociadas a las funciones que deberían desempeñarse, o que tengan como sustento un requerimiento aprobado por el dueño del proceso o se le haya notificado. 3) En caso se encuentren registros no conformes realizados por estas cuentas, se comunica al dueño del proceso. Caso contrario procede a emitir su aprobación. 4) El Dueño	Trimestral	Detectivo	Sí	Evidenciado	Débil

	de proceso revisa las transacciones identificadas (según aplique) y notificará la aceptación / acciones correctivas. 5) En caso de que el Dueño del proceso notifique acciones correctivas, el gestor de TI ejecutará las acciones correspondientes y documentará este proceso. 6) Posteriormente, se comunicará al dueño del proceso las acciones correctivas realizadas. 7) El jefe de TI revisará el informe y brindará su conformidad al informe realizado. Nota: (1) En caso de considerar sólo transacciones críticas estas deben ser definidas previamente por el Dueño del Proceso correspondiente y ejecutar el control con el último listado actualizado. La frecuencia de dicha actualización debe ser como mínimo trimestral para que sea input válido para la ejecución de este control. (2) Previamente debe obtenerse el listado de cuentas privilegiadas actualizado como parte de la ejecución del control 2.6 (3) El Jefe de TI encargado de la revisión no debe ser cuenta privilegiada en el sistema del alcance.						
TI / 02.9	1) El Gestor de TI extrae el listado de usuarios externos y proveedores configurados en los sistemas con sus respectivos accesos (roles, perfiles,	Semestral	Detectivo	Sí	Evidenciado	Débil

	responsabilidades) Para los usuarios externos: 1.1) Envía el listado de usuarios activos con accesos activos para revisión del GAF o Dueño de Proceso, con copia al responsable de TI de la compañía correspondiente. 1.2) El GAF o Dueño de Proceso valida las asignaciones bajo la premisa de que los accesos deben estar alineados a las funciones que desempeñan los usuarios en la compañía y envía comentarios/conformidad. (1) 1.3) En caso se detecten correcciones por hacer, el GAF o Dueño del Proceso solicita al área correspondiente que se realicen los cambios requeridos en el sistema. De requerirse desactivar la cuenta, se deberá solicitar la fecha fin de los accesos, posteriormente deberá revisarse la fecha de último logueo a fin de identificar si tuvo logueo posterior a la fecha en la que no debía contar con los accesos. De ser así deberán extraerse las transacciones realizadas en ese periodo de tiempo y enviarlas al GAF o Dueño de Proceso para su revisión/ análisis de impacto correspondiente hasta obtener su aprobación o acciones correctivas. Para los usuarios de proveedores: Revisa que los accesos otorgados correspondan únicamente al perfil correspondiente como						

	proveedor. (2) En caso de encontrarse diferencias se procede a corregir el acceso, extraer las posibles transacciones realizadas por el usuario y reportar a la Gerencia Corporativa de Contabilidad para su revisión/ análisis de impacto correspondiente hasta obtener su aprobación o acciones correctivas. Nota: (1) Si en el plazo de 5 días útiles el Dueño del proceso/GAF no remite respuesta, se escalará con el Gerente Corporativo del proceso correspondiente (6to día útil), VP del Proceso Corporativo correspondiente (8vo día útil) y VP de la empresa según corresponda (10mo día útil). (2) Previamente se debe validar que la asignación del perfil proveedor sea la adecuada quedando evidencia de los criterios considerados para la identificación.					
TI / 02.1	Creación – Modificación (1) 1) El Dueño del Proceso revisa la solicitud y aprueba o rechaza (2) bajo las siguientes consideraciones: - Validación de segregación de funciones: El Gestor de TI o el responsable del negocio según aplique verifica de manera manual o automática que no existe conflicto de segregación de funciones (3) de acuerdo a la matriz SOD registrada en el site de Control Interno según corresponda a la	Transaccional	Preventivo	Sí	Evidenciado	Moderado

	asignación/modificación de accesos. En caso de conflicto, el Dueño del Proceso o Dueño de Proceso Corporativo, según corresponda, procede a rechazar la solicitud o gestiona el acta de aceptación de riesgo según aplique con el área de Riesgos Corporativo de acuerdo a lo establecido en el Manual de Riesgos Corporativo. - Revisión del acceso solicitado en relación a las funciones laborales de usuario. 2) El Responsable de ejecutar la solicitud valida que la solicitud haya sido aprobada para proceder a realizar la actividad solicitada. En caso la solicitud sea rechazada se comunica al solicitante. (4) Notas: (1) Como excepción se tienen las altas automáticas mediante las cuales se realizan creaciones de cuentas de usuario y/o asignaciones de accesos por defecto de manera automática al momento de generar el alta del personal en el sistema de planillas u otro sistema. Aquellos accesos que no se asignan por defecto siguen las actividades indicadas como parte del control. (2) La aprobación / conformidad puede ser por correo electrónico, SharePoint, ICARUS o formato físico. (3) No aplica validación SOD para aquellos sistemas que por configuración no permitan la asignación de más de un perfil a una cuenta de						

	usuario. (4) Como excepción se tienen las asignaciones de accesos generadas de manera automática. (5) Para el caso de cuentas de proveedores, estas cuentas se crearán ante una solicitud por parte del proveedor (excepción) o área interesada.					
TI / 02.7	1) El Gestor de TI extrae el historial de transacciones (1) ejecutadas por las cuentas privilegiadas del periodo de revisión.(2) 2) El Jefe de TI (3) revisa que las actividades se encuentren asociadas a las funciones que deberían desempeñarse, o que tengan como sustento un requerimiento aprobado por el dueño del proceso o se le haya notificado. 3) En caso se encuentren registros no conformes realizados por estas cuentas, se comunica al dueño del proceso. Caso contrario procede a emitir su aprobación. 4) El Dueño de proceso revisa las transacciones identificadas (según aplique) y notificará la aceptación / acciones correctivas. 5) En caso de que el Dueño del proceso notifique acciones correctivas, el gestor de TI ejecutará las acciones correspondientes y documentará este proceso. 6) Posteriormente, se comunicará al dueño del proceso las acciones correctivas realizadas. 7) El jefe de TI revisará el	Trimestral	Detectivo	Sí	Evidenciado	Débil

	informe y brindará su conformidad al informe realizado. Nota: (1) En caso de considerar sólo transacciones críticas estas deben ser definidas previamente por el Dueño del Proceso correspondiente y ejecutar el control con el último listado actualizado. La frecuencia de dicha actualización debe ser como mínimo trimestral para que sea input válido para la ejecución de este control. (2) Previamente debe obtenerse el listado de cuentas privilegiadas actualizado como parte de la ejecución del control 2.6 (3) El Jefe de TI encargado de la revisión no debe ser cuenta privilegiada en el sistema del alcance.					
TI / 02.9	1) El Gestor de TI extrae el listado de usuarios externos y proveedores configurados en los sistemas con sus respectivos accesos (roles, perfiles, responsabilidades) Para los usuarios externos: 1.1) Envía el listado de usuarios activos con accesos activos para revisión del GAF o Dueño de Proceso, con copia al responsable de TI de la compañía correspondiente. 1.2) El GAF o Dueño de Proceso valida las asignaciones bajo la premisa de que los accesos deben estar alineados a las funciones que desempeñan los usuarios en la compañía y envía	Semestral	Detectivo	Sí	Evidenciado	Débil

	comentarios/conformidad. (1) 1.3) En caso se detecten correcciones por hacer, el GAF o Dueño del Proceso solicita al área correspondiente que se realicen los cambios requeridos en el sistema. De requerirse desactivar la cuenta, se deberá solicitar la fecha fin de los accesos, posteriormente deberá revisarse la fecha de último logueo a fin de identificar si tuvo logueo posterior a la fecha en la que no debía contar con los accesos. De ser así deberán extraerse las transacciones realizadas en ese periodo de tiempo y enviarlas al GAF o Dueño de Proceso para su revisión/ análisis de impacto correspondiente hasta obtener su aprobación o acciones correctivas. Para los usuarios de proveedores: Revisa que los accesos otorgados correspondan únicamente al perfil correspondiente como proveedor. (2) En caso de encontrarse diferencias se procede a corregir el acceso, extraer las posibles transacciones realizadas por el usuario y reportar a la Gerencia Corporativa de Contabilidad para su revisión/ análisis de impacto correspondiente hasta obtener su aprobación o acciones correctivas. Nota: (1) Si en el plazo de 5 días útiles el Dueño del proceso/GAF no remite respuesta, se escalará con el Gerente						

	Corporativo del proceso correspondiente (6to día útil), VP del Proceso Corporativo correspondiente (8vo día útil) y VP de la empresa según corresponda (10mo día útil). (2) Previamente se debe validar que la asignación del perfil proveedor sea la adecuada quedando evidencia de los criterios considerados para la identificación.					

4.- Controles por implementar y sus responsables

Sobre el/los controles por implementar			
Control	**Estado**	**Fecha de Implementación**	**Responsable**

5.- Detalle de riesgos residuales

Sobre el/los riesgos y controles				
Riesgo	**Control**	**Objetivo**	**NRI**	**NRR**
Fuga de información confidencial de la empresa	TI / 02.1	Toda creación y modificación (interno o externo) así como asignación o modificación de accesos en los sistemas de información (aplicaciones, sistemas operativos, bases de datos) es revisada y aprobada	3.46	2.24
Fuga de información confidencial de la empresa	TI / 02.7	Las transacciones críticas ejecutadas por usuarios privilegiados de TI, son revisadas y aprobadas	3.46	2.24
Fuga de información confidencial de la empresa	TI / 02.9	Validación de que los accesos se encuentren asignados adecuadamente a las cuentas de usuarios externos y proveedores	3.46	2.24
Fuga de información confidencial de la empresa	TI / 02.1	Toda creación y modificación (interno o externo) así como asignación o modificación de accesos en los sistemas de información (aplicaciones, sistemas	3.46	2.24

		operativos, bases de datos) es revisada y aprobada		
Fuga de información confidencial de la empresa	TI / 02.7	Las transacciones críticas ejecutadas por usuarios privilegiados de TI, son revisadas y aprobadas	3.46	2.24
Fuga de información confidencial de la empresa	TI / 02.9	Validación de que los accesos se encuentren asignados adecuadamente a las cuentas de usuarios externos y proveedores	3.46	2.24

6.- Descripción del riesgo que va a ser aceptado (de ser el caso)

Sobre el/los riesgos a aceptar
Que se altere o pierda información del negocio al otorgar accesos que presenten conflicto de segregación de funciones a cuentas con privilegios administrativos. El equipo de aplicaciones corporativas de AENZA SS.CC y los responsables de TI de las empresas del grupo AENZA tienen acceso con privilegio de administración en el sistema ICARUS, de acuerdo con la necesidad de realizar configuraciones propias de la herramienta para el funcionamiento en las empresas. La aprobación de los accesos se da de acuerdo a los lineamientos corporativo de gestión de accesos

7.- Historial de aprobación

Sobre el/los aprobadores
Ines Tang Muñoz - 30 junio 2025