ACTIVO			VALORACIÓN					
ID_PROCESO	ID_ACTIVO	ACTIVO DE INFORMACIÓN	C	I	D	TOTAL	VALOR 1	VALOR 2
	EMP_HW_01	Servidores de procesamiento	5	5	5	15	Alto	3
	EMP_DOC_01	Documentación de diagnóstico	4	4	3	11	Alto	3
EMP_IA_PROC_01	EMP_NET_01	Red interna corporativa	4	4	3	11	Alto	3
	EMP_SW_01	Modelos de IA	5	5	4	14	Alto	3
	EMP_DB_01	Bases de datos	5	5	5	15	Alto	3
EMP_IA_PROC_02	EMP_SW_02	Código fuente	5	4	4	13	Alto	3
	EMP_MON_01	Sistema de monitoreo	3	3	5	11	Alto	3
	EMP_TCK_01	Sistema de tickets	4	4	4	12	Alto	3
EMP_IA_PROC_03	EMP_LOG_01	Logs y bitácoras	4	5	4	13	Alto	3

VULNERABILIDADES	AMENAZAS	EVENTO DE AMENAZA (RIESGO)	CONTROLES
Acceso físico no controlado, fallas eléctricas, mala refrigeración, falta de capacitación	Error humano, sismo, incendio, ciberataque	Daño físico o indisponibilidad del servidor	Control de accesos físicos, UPS, monitoreo ambiental, capacitación
Falta de respaldo, accesos no controlados	Robo de información, error humano	Fuga de información	Control de accesos, respaldos
Configuración insegura	Ataque externo, malware	Interrupción de red	Firewall, segmentación
Falta de cifrado, control de versiones deficiente, errores humanos	Robo de información, error humano, ataque adversarial	Pérdida o manipulación de modelos	Cifrado, control de versiones, control de accesos
Falta de segmentación, accesos excesivos, respaldos insuficientes	Fuga de información, malware, error humano	Exposición o corrupción de datos	Cifrado, respaldos, roles y privilegios
Repositorios inseguros	Robo de código	Pérdida de propiedad intelectual	Control de repositorios
Configuración incorrecta, dependencia de red	Fallo de red, error humano	No detección de incidentes	Monitoreo redundante, validación de alertas
Configuración deficiente	Error humano	Mala gestión de incidentes	Capacitación
Falta de integridad	Manipulación	Ocultamiento de incidentes	Control de integridad

Análisis de vulnerabilidades			
Vulnerabilidades	Severidad	Exposición	Valor3
Acceso físico no controlado	3	3	5
Falta de cifrado en modelos	3	2	4
Accesos excesivos a bases de datos	3	3	5

Análisis de amenazas				
Amenazas	Eventos de amenaza	Capacidad	Motivación	Valor4
Error humano	Daño físico / lógico	2	2	3
Ciberataque	Robo o alteración de inf	3	3	5
Fallo de red	Indisponibilidad	2	2	3

Riesgo con control = Amenaza x Vulnerabilidad x Probabilidad x Impacto				
Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo Total
3	5	2	15	450
5	4	3	11	660
3	5	2	11	330

ACTIVO			VALORACIÓN						
ID_PROCESO	ID_ACTIVO	ACTIVO DE INFORMACIÓN	Área Geográfica	Periodo de Afectación	IMPACTO	Cantidad de Infraestructuras Críticas Afectadas	Campos Afectados	INTERDEPEN-DENCIA	CRITICIDAD
	EMP_HW_01	Servidores de procesamiento	3	3	3	3	3	5	V
	EMP_DOC_01	Documentación de diagnóstico	2	2	2	2	2	4	IV
EMP_IA_PROC_01	EMP_NET_01	Red interna corporativa	3	3	3	3	3	5	V
	EMP_SW_01	Modelos de IA	3	2	3	2	2	4	IV
	EMP_DB_01	Bases de datos	3	3	3	3	3	5	V
EMP_IA_PROC_02	EMP_SW_02	Código fuente	3	2	3	2	2	4	IV
	EMP_MON_01	Sistema de monitoreo	2	1	2	1	1	2	II
	EMP_TCK_01	Sistema de tickets	2	2	2	2	2	3	III
EMP_IA_PROC_03	EMP_LOG_01	Bitácoras y logs	2	2	3	2	2	4	IV

IDENTIFICACIÓN DE INFRAESTRUCTURAS CRÍTICAS		
INFRAESTRUCTURAS CRÍTICAS DETECTADAS	**GRADO DE CRITICIDAD**	**CONTROLES A IMPLEMENTAR**
Servidores de procesamiento	V	Redundancia, UPS, controles físicos
Documentación estratégica del cliente	IV	Cifrado, control de versiones, respaldos
Infraestructura de red corporativa	V	Cifrado, respaldos, firewall, segmentación
Modelos de IA productivos	IV	Control de versiones, cifrado, control de accesos
Bases de datos de entrenamiento y resultados	V	Cifrado, respaldos periódicos, control de roles
Repositorios de código fuente	IV	Repositorios privados, control de cambios
Plataforma de monitoreo	II	Redundancia, alertas automáticas
Sistema de gestión de incidentes	III	Respaldos, control de accesos
Registros de eventos y auditoría	IV	Integridad de logs, almacenamiento seguro

IDENTIFICACIÓN DE INFRAESTRUCTURAS CRÍTICAS		
INFRAESTRUCTURAS CRÍTICAS DETECTADAS	**GRADO DE CRITICIDAD**	**CONTROLES A IMPLEMENTAR**
Servidores de procesamiento	V	Redundancia, UPS, controles físicos
Documentación estratégica del cliente	IV	Cifrado, control de versiones, respaldos
Infraestructura de red corporativa	V	Cifrado, respaldos, firewall, segmentación
Modelos de IA productivos	IV	Control de versiones, cifrado, control de accesos
Bases de datos de entrenamiento y resultados	V	Cifrado, respaldos periódicos, control de roles
Repositorios de código fuente	IV	Repositorios privados, control de cambios
Plataforma de monitoreo	II	Redundancia, alertas automáticas
Sistema de gestión de incidentes	III	Respaldos, control de accesos
Registros de eventos y auditoría	IV	Integridad de logs, almacenamiento seguro