

ACTIVO			VALORACIÓN						VULNERABILIDADES	AMENAZAS	EVENTO DE AMENAZA (RIESGO)	CONTROLES
ID_PROCESO	ID_ACTIVO	ACTIVO DE INFORMACIÓN	C	I	D	TOTAL	VALOR 1	VALOR 2				
NUBE_MIG_01	NUBE_APP_01	Aplicaciones críticas (IaaS/PaaS)	4	5	5	14	Alto	3	Configuraciones inseguras por defecto; Dependencia de claves/API mal gestionadas; Falta de endurecimiento del servidor	Ciberdelincuencia; Falla tecnológica	Indisponibilidad o compromiso de la aplicación	Gestión de secretos e IAM; Parches y hardening; Monitoreo y WAF
	NUBE_DB_01	Base de datos gestionada en nube	5	5	5	15	Alto	3	Falta de cifrado de información sensible; Controles de acceso insuficientes a la base de datos; Respaldos no verificados periódicamente	Error humano; Ciberdelincuencia	Eliminación o modificación de evidencias/registros	Cifrado en reposo y tránsito; Control estricto de accesos y auditoría; Respaldos automáticos y pruebas de restauración
	NUBE_NET_01	VPC y Conectividad (IPSec/DirectConnect)	4	4	5	13	Alto	3	Reglas de firewall demasiado permisivas; Canales sin cifrado adecuado; Falta de segmentación de red	Falla tecnológica; Ciberdelincuencia	Interrupción de conectividad o intrusión	Políticas de red cero confianza; VPN/IPSec y cifrado TLS; Segmentación y listas de control de acceso
	NUBE_STO_01	Almacenamiento institucional en la nube	5	4	4	13	Alto	3	Accesos públicos no intencionales; Falta de políticas de retención; Permisos heredados excesivos	Error humano; Ciberdelincuencia	Divulgación o pérdida de datos	Bloqueo de acceso público; Lifecycle y retención; Políticas IAM y cifrado
	NUBE_CICD_01	Pipeline CI/CD e Infra como Código	3	4	3	10	Medio	2	Configuración incorrecta de pipelines; Credenciales embebidas; Falta de revisión de cambios	Ciberdelincuencia; Error humano	Alteración maliciosa del flujo de despliegue	Firmado de artefactos; Secretos seguros; Políticas de revisión y auditoría
NUBE_SEC_02	NUBE_IAM_01	Servicio de Autenticación / IAM	5	5	4	14	Alto	3	Cuentas privilegiadas sin MFA; Roles con permisos excesivos; Falta de rotación de credenciales	Ciberdelincuencia; Error humano	Acceso no autorizado o escalamiento de privilegios	MFA obligatorio; Principio de menor privilegio; Auditoría y rotación
	NUBE_SIEM_01	Monitoreo de seguridad / auditoría	4	4	4	12	Alto	3	Fuentes de logs incompletas; Reglas de correlación desactualizadas; Almacenamiento sin cifrado	Ciberdelincuencia; Falla tecnológica	Detección tardía de incidentes	CoBERTura de fuentes; Afinamiento continuo; Cifrado y retención
	NUBE_POL_01	Políticas y procedimientos (CAB)	2	3	3	8	Medio	2	Procesos no formalizados; Falta de CAB; Escasa trazabilidad	Error humano	Cambios no autorizados	Gestión de cambios; Flujos de aprobación; Bitácoras
NUBE_BAK_03	NUBE_BAK_01	Plataforma de respaldos y DR	4	5	5	14	Alto	3	Respaldos no cifrados; Pruebas de restauración poco frecuentes; Copias en misma zona	Ciberdelincuencia; Falla tecnológica	Compromiso o indisponibilidad de copias	Cifrado y segregación; Pruebas regulares; Versionado
	NUBE_MON_01	Monitoreo de disponibilidad	3	4	4	11	Alto	3	Alertas deshabilitadas; Falta de procedimientos de incidencia; Dependencia de intervención manual	Error humano; Falla tecnológica	No atención oportuna de alertas	Runbooks y capacitación; Monitoreo continuo; Automatización de respuesta

Análisis de vulnerabilidades			
Vulnerabilidades	Severidad	Exposición	Valor3
Alertas deshabilitadas	2	2	3
Dependencia de intervención manual	2	2	3
Falta de procedimientos de incidencia	2	2	3

Análisis de amenazas				
Amenazas	Eventos de amenaza	Capacidad	Motivación	Valor4
Error humano	No atención de alertas	2	2	3
Falla tecnológica	Fallas de agente/sondas	2	2	3
Ciberdelincuencia	Accesos no autorizados	2	3	4

Riesgo con control = Amenaza x Vulnerabilidad x Probabilidad x Impacto				
Amenaza	Vulnerabilidad	Probabilidad	Impacto	Riesgo Total
3	3	2	14	252
3	3	1	15	135
4	3	2	13	312

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
NUBE_MIG_01	NUBE_APP_01	Aplicaciones críticas (IaaS/PaaS)	1	2	2	2	2	3	III
	NUBE_DB_01	Base de datos gestionada en nube	1	2	2	2	2	3	III
	NUBE_NET_01	VPC y Conectividad (IPSec/DirectConnect)	1	2	2	2	2	3	III
	NUBE_STO_01	Almacenamiento institucional en la nube	1	2	2	2	2	3	III
	NUBE_CICD_01	Pipeline CI/CD e Infra como Código	1	1	1	1	1	1	I
NUBE_SEC_02	NUBE_IAM_01	Servicio de Autenticación / IAM	1	2	2	2	2	3	III
	NUBE_SIEM_01	Monitoreo de seguridad / auditoría	1	2	2	2	2	3	III
	NUBE_POL_01	Políticas y procedimientos (CAB)	1	1	1	1	1	1	I
NUBE_BAK_03	NUBE_BAK_01	Plataforma de respaldos y DR	1	2	2	2	2	3	III
	NUBE_MON_01	Monitoreo de disponibilidad	1	2	2	2	2	3	III

IDENTIFICACIÓN DE INFRAESTRUCTURAS CRÍTICAS		
INFRAESTRUCTURAS CRÍTICAS DETECTADAS	GRADO DE CRITICIDAD	CONTROLES A IMPLEMENTAR
Aplicaciones críticas (IaaS/PaaS) (Activo de TIC)	III	Gestión de secretos e IAM; Parches y hardening; Monitoreo y WAF
Base de datos gestionada en nube (Activo de TIC)	III	Cifrado en reposo y tránsito; Control estricto de accesos y auditoría; Respaldos automáticos y pruebas de restauración
VPC y Conectividad (Redes)	III	Políticas de red cero confianza; VPN/IPSec y cifrado TLS; Segmentación y listas de control de acceso
Almacenamiento institucional en la nube (Activo de TIC)	III	Bloqueo de acceso público; Lifecycle y retención; Políticas IAM y cifrado
Pipeline CI/CD e Infra como Código (Activo de TIC)	I	Firmado de artefactos; Secretos seguros; Políticas de revisión y auditoría
Servicio de Autenticación / IAM (Activo de TIC)	III	MFA obligatorio; Principio de menor privilegio; Auditoría y rotación
Plataforma de Monitoreo de seguridad / auditoría (Activo de TIC)	III	Coertura de fuentes; Afinamiento continuo; Cifrado y retención
Políticas y procedimientos (CAB) (Activo de TIC)	I	Gestión de cambios; Flujos de aprobación; Bitácoras
Plataforma de respaldos y DR (Activo de TIC)	III	Cifrado y segregación; Pruebas regulares; Versionado
Plataforma de Monitoreo de disponibilidad (Activo de TIC)	III	Runbooks y capacitación; Monitoreo continuo; Automatización de respuesta

VULNERABILIDADES		
	Valor	
Severidad	1	Poca o nula severidad en el grado de vulnerabilidad
	2	Severidad moderada por el grado de vulnerabilidad
	3	Altamente severo el nivel de vulnerabilidad
Exposición	1	Poco o nula exposición
	2	Nivel moderado de exposición
	3	Altamente expuesto

AMENAZA		
	Valor	Descripción
Capacidad	1	Poca o nula capacidad de realizar el ataque.
	2	Capacidad moderada. Se tiene el conocimiento y habilidades para realizar el ataque, pero pocos recursos. O, tiene suficientes recursos, pero conocimiento y habilidades limitadas.
	3	Altamente capaz. Se tienen los conocimientos, habilidades y recursos necesarios para realizar un ataque.
Motivación	1	Poca o nula motivación. No se está inclinado a actuar.
	2	Nivel moderado de motivación. Se actuará si se le pide o provoca.
	3	Altamente motivado. Casi seguro que intentará el ataque.

PROBABILIDAD		
	Valor	Descripción
Probabilidad de ocurrencia	1	Baja, no hay historial y es raro que la amenazas ocurra.
	2	Media, se han presentado casos y puede ocurrir la amenaza.
	3	Alta, se han presentado suficientes casos y la amenaza seguramente ocurrirá.