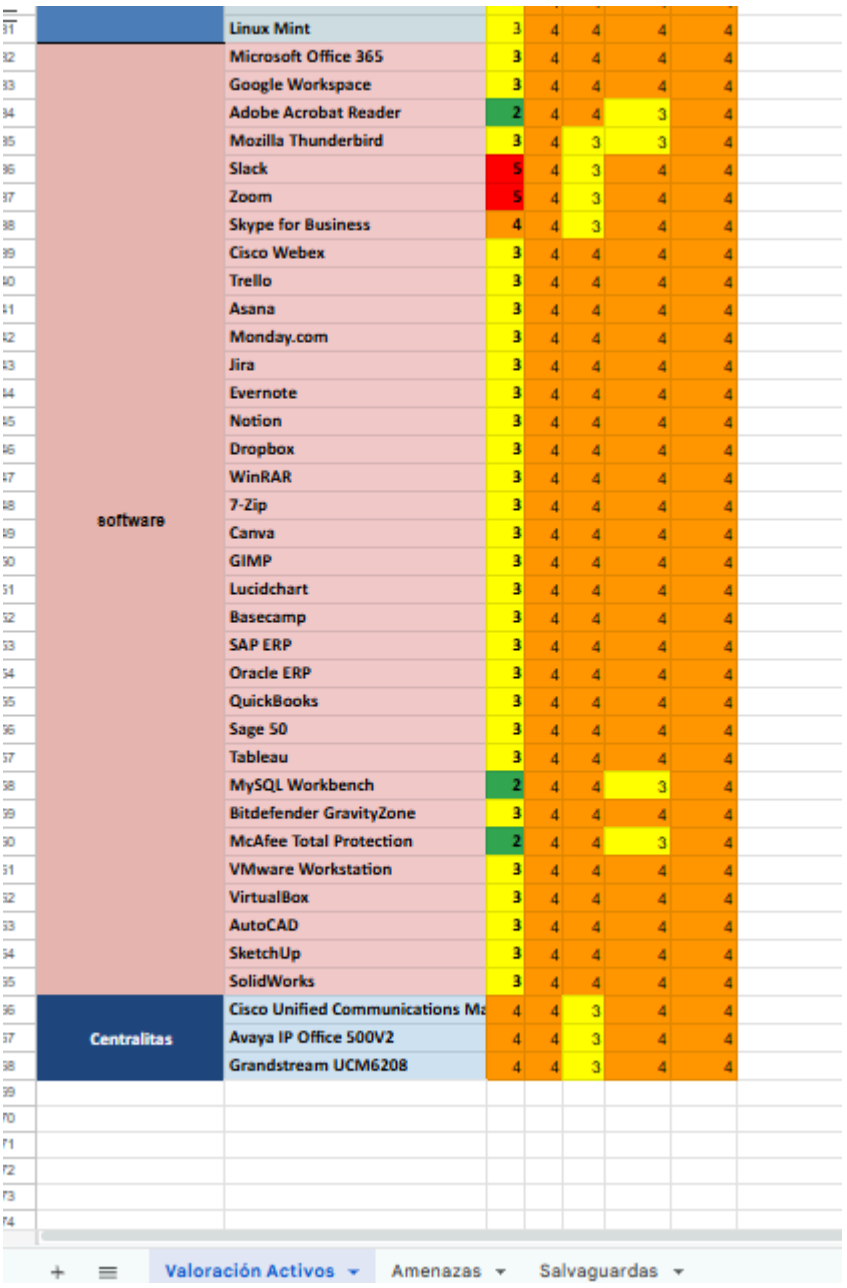
Familia activos	Activos	D	I	C	A	T
Servidores	Servidor NAS	5	4	3	4	4
	Servidor de base de datos	4	4	4	4	4
	Almacenamiento en red (SAN)	3	5	5	4	5
	Backup en cinta LTO	3	5	5	4	5
	Dell PowerEdge R750	4	4	4	4	4
	HPE ProLiant DL380 Gen10	4	4	4	4	4
	Lenovo ThinkSystem SR650	4	4	4	4	4
	Servidor de almacenamiento local	4	4	4	4	4
	Almacenamiento en la nube	4	5	4	4	5
	Servidor de archivos compartidos	3	4	5	4	5
	Almacenamiento en la nube	3	4	5	4	5
	Cisco UCS C240 M6	4	4	4	4	4
	Supermicro SuperServer 1029U	3	4	5	4	5
	IBM Power System S922	3	4	5	4	5
Personal	CEO	3	4	5	4	5
	Director	5	5	5	5	5
	Empleado	2	2	2	2	2
	Supervisor	4	4	4	4	4
	Técnico	3	3	3	3	3
Movil	iPhone	3	4	4	4	4
	Samsung Galaxy	3	4	4	4	4
	Google Pixel	3	4	4	4	4
	Xiaomi	3	4	4	4	4
	OnePlus	3	4	4	4	4
	Motorola	3	4	4	4	4
Sistema Operativo	Windows 11	3	4	4	4	4
	Ubuntu	3	4	4	4	4
	macOS	3	4	4	4	4
	Windows 10	3	4	4	4	4



31		Linux Mint	3	4	4	4	4
32	software	Microsoft Office 365	3	4	4	4	4
33		Google Workspace	3	4	4	4	4
34		Adobe Acrobat Reader	2	4	4	3	4
35		Mozilla Thunderbird	3	4	3	3	4
36		Slack	5	4	3	4	4
37		Zoom	5	4	3	4	4
38		Skype for Business	4	4	3	4	4
39		Cisco Webex	3	4	4	4	4
40		Trello	3	4	4	4	4
41		Asana	3	4	4	4	4
42		Monday.com	3	4	4	4	4
43		Jira	3	4	4	4	4
44		Evernote	3	4	4	4	4
45		Notion	3	4	4	4	4
46		Dropbox	3	4	4	4	4
47		WinRAR	3	4	4	4	4
48		7-Zip	3	4	4	4	4
49		Canva	3	4	4	4	4
50		GIMP	3	4	4	4	4
51		Lucidchart	3	4	4	4	4
52		Basecamp	3	4	4	4	4
53		SAP ERP	3	4	4	4	4
54		Oracle ERP	3	4	4	4	4
55		QuickBooks	3	4	4	4	4
56		Sage 50	3	4	4	4	4
57		Tableau	3	4	4	4	4
58		MySQL Workbench	2	4	4	3	4
59		Bitdefender GravityZone	3	4	4	4	4
60		McAfee Total Protection	2	4	4	3	4
61		VMware Workstation	3	4	4	4	4
62		VirtualBox	3	4	4	4	4
63		AutoCAD	3	4	4	4	4
64		SketchUp	3	4	4	4	4
65		SolidWorks	3	4	4	4	4
66	Centralitas	Cisco Unified Communications Ma	4	4	3	4	4
67		Avaya IP Office 500V2	4	4	3	4	4
68		Grandstream UCM6208	4	4	3	4	4
69							
70							
71							
72							
73							
74							

Valoración Activos | Amenazas | Salvaguardas

Familia activos	Amenazas	Frec	ID	II	IC	IA	IT	RD	RI	RC	RA	RT
Servidores	Fallo de hardware	M	5	3	1	2	2	5	3	1	2	2
	Ataques DDoS	M	5	1	1	1	1	5	1	1	1	1
	Malware	M	4	4	3	3	3	4	4	3	3	3
	Acceso no autorizado	A	3	4	5	5	4	6	8	10	10	8
	Elevación de privilegios	B	2	4	5	5	4	1	2	2,5	2,5	2
	Pérdida de energía	M	4	1	1	1	1	4	1	1	1	1
	Errores de configuración	M	4	3	3	3	3	4	3	3	3	3
Personal	Ingeniería social (phishing)	A	2	3	4	4	2	4	6	8	8	4
	Errores humanos	M	2	4	2	3	3	2	4	2	3	3
	Uso inadecuado de credenciales	M	3	3	4	4	4	3	3	4	4	4
	Fuga de información	B	1	2	5	4	3	0,5	1	2,5	2	1,5
	Falta de formación en seguridad	M	2	3	3	3	2	2	3	3	3	2
	Acceso indebido a información confidencial	B	2	2	5	4	4	1	1	2,5	2	2
Movil	Robo o pérdida del dispositivo	M	4	1	3	2	3	4	1	3	2	3
	Malware móvil	M	4	3	2	3	2	4	3	2	3	2
	Acceso no autorizado por redes Wi-Fi públicas	M	3	2	4	2	4	3	2	4	2	4
	Desactualización del sistema	M	2	2	2	2	2	2	2	2	2	2
	Sincronización insegura	M	3	2	2	2	2	3	2	2	2	2
	Apps maliciosas	B	4	3	3	3	3	2	1,5	1,5	1,5	1,5
Sistema Operativo	Vulnerabilidades no parcheadas	M	3	4	2	2	2	3	4	2	2	2
	Malware del sistema	M	3	3	3	2	2	3	3	3	2	2
	Ejecución de código malicioso	M	4	4	3	3	3	4	4	3	3	3
	Errores de configuración	M	4	4	2	2	2	4	4	2	2	2
	Escalada de privilegios	M	2	4	4	4	4	2	4	4	4	4
	Incompatibilidad de parches	B	3	2	1	2	2	1,5	1	0,5	1	1
software	Bugs de seguridad	M	3	3	2	2	2	3	3	2	2	2
	Uso de versiones obsoletas	M	3	3	2	2	2	3	3	2	2	2
	Inyecciones de código (SQL, XSS)	M	4	3	4	3	3	4	3	4	3	3
	Falta de validación de entradas	M	4	3	3	2	2	4	3	3	2	2
	Integridad comprometida	M	3	3	3	2	2	3	3	3	2	2
	Dependencias inseguras	B	4	4	3	3	3	2	2	1,5	1,5	1,5
Centralitas	Intercepción de llamadas	M	3	3	2	2	2	3	3	2	2	2
	Denegación de servicio (DoS)	M	3	3	2	2	2	3	3	2	2	2
	Acceso no autorizado a la configuración	M	5	2	1	2	2	5	2	1	2	2
	Vulnerabilidades en protocolos VoIP	M	4	3	3	2	2	4	3	3	2	2
	Ataques Man-in-the-Middle	M	4	3	4	3	3	4	3	4	3	3
	Phreaking (hackeo de líneas telefónicas)	M	4	3	3	3	2	4	3	3	3	2

Fre → Frecuencia
ID → Impacto en Disponibilidad
II → Impacto en Integridad
IC → Impacto en Confidencialidad
IA → Impacto en Autenticidad
IT → Impacto en Trazabilidad

RD → Riesgo Disponibilidad
RI → Riesgo Integridad
RC → Riesgo Confidencialidad
RA → Riesgo Autenticidad
RT → Riesgo Trazabilidad

MA → Muy frecuente, a diario (x2)
A → Frecuente, una vez al mes (x2)
M → Normal, una vez al año
B → Poco frecuente, cada varios años
MB → Muy poco frecuente, siglos

Valoración Activos | Amenazas | Salvaguardas

Familia activos	Amenazas	Salvaguardas técnicas	Salvaguardas organizativas	Riesgo Residual
Servidores	Fallo de hardware	RAID, sensores SMART, monitor de hardware	Política de renovación de hardware, inventario actualizado	3
	Ataques DDoS	Firewall perimetral, limitación de ancho de banda	Procedimiento anti-DDoS, acuerdos con ISP	3
	Malware	Antivirus, EDR, análisis en sandbox	Política antivirus y de comportamiento seguro	2
	Acceso no autorizado	MFA, control de accesos, IDS	Política de acceso, formación en uso de MFA	4
	Elevación de privilegios	Hardening, separación de privilegios, logs reforzados	Revisión periódica de privilegios y roles	-1
	Pérdida de energía	SAI, alimentación redundante, monitoreo eléctrico	Plan de contingencia, entrenamiento de respuesta	2
	Errores de configuración	Gestión de configuraciones, backups automáticos	Checklist de validación, política de cambios	2
Personal	Ingeniería social (phishing)	Antiphishing, filtros de correo, DNS seguro	Capacitación en ingeniería social	2
	Errores humanos	Control de errores, sistemas de tickets, backups frecuentes	Capacitación en errores comunes, cultura de reporte	0
	Uso inadecuado de credenciales	Gestión de credenciales, doble factor	Política de contraseñas, rotación obligatoria	1
	Fuga de información	Cifrado, DLP, control de dispositivos externos	Normas sobre confidencialidad y tratamiento de datos	-1,5
	Falta de formación en seguridad	Sistemas de formación en línea, actualizaciones forzadas	Cursos regulares de concienciación	0
	Acceso indebido a información confidencial	Cifrado, alertas de acceso no autorizado	Control de accesos físicos y digitales	-1
Movil	Robo o pérdida del dispositivo	MDM, cifrado, bloqueo remoto	Política BYOD, reporte inmediato de incidentes	2
	Malware móvil	Antivirus móvil, control de apps, MDM	Reglamento de uso de móviles corporativos	2
	Acceso no autorizado por redes Wi-Fi públicas	VPN obligatoria, alertas de conexión insegura	Política de teletrabajo, uso autorizado de redes	1
	Desactualización del sistema	WSUS, scripts de actualización automática	Política de actualización periódica	0
	Sincronización insegura	Control de sincronización en la nube, logs	Restricción de sincronización en dispositivos no aprobados	1
	Apps maliciosas	Bloqueo de apps desconocidas, listas blancas	Control de apps permitidas, auditorías internas	0
Sistema Operativo	Vulnerabilidades no parcheadas	Actualización automática, escáner de vulnerabilidades	Gestión de vulnerabilidades periódica	1
	Malware del sistema	Antivirus, protección de endpoints	Procedimiento de respuesta a incidentes	1
	Ejecución de código malicioso	Control de ejecución, AppLocker o similares	Plan de respuesta a código malicioso	2
	Errores de configuración	Backups automatizados, versionado de archivos	Procedimiento de recuperación ante fallo humano	2
	Escalada de privilegios	Auditoría de permisos, control por roles	Revisión de privilegios, auditoría periódica	0
	Incompatibilidad de parches	Monitoreo de parches, herramientas de inventario	Plan de actualización de software	-0,5
software	Bugs de seguridad	Escáner de seguridad, repositorios seguros	Política de calidad de software	1
	Uso de versiones obsoletas	Control de versiones, alertas de obsolescencia	Proceso de mantenimiento y desuso planificado	1
	Inyecciones de código (SQL, XSS)	WAF, validación del lado servidor	Formación en desarrollo seguro	2
	Falta de validación de entradas	Validaciones en frontend y backend	Normativa de codificación segura	2
	Integridad comprometida	Hashing, chequeo de integridad automatizado	Controles de integridad en procedimientos críticos	1
	Dependencias inseguras	Gestión de dependencias, escaneo de CVEs	Verificación de librerías de terceros	0
Centralitas	Intercepción de llamadas	SIP trunk seguro, cifrado de llamadas	Política de comunicaciones seguras	1
	Denegación de servicio (DoS)	Firewall con detección de DoS, balanceo de carga	Simulacros de contingencia, plan anti-DDoS	1
	Acceso no autorizado a la configuración	ACLs, hardening del panel de configuración	Normas de configuración segura	3
	Vulnerabilidades en protocolos VoIP	Actualización de firmware, protocolos seguros	Procedimientos de revisión de protocolos	2
	Ataques Man-in-the-Middle	WAF VoIP, SRTP, TLS	Formación en ataques VoIP y su prevención	2
	Phreaking (hackeo de líneas telefónicas)	Segmentación de red, detección de intrusiones	Guía de seguridad para redes segmentadas	2

Valoración Activos | Amenazas | Salvaguardas