FOCUS SYSTEMS PERU SAC
SEPTIEMBRE 2024

FOCUS business solutions
UNA EMPRESA DE GRUPO DATCO

MATRIZ DE RIESGOS

IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS								ANÁLISIS Y EVALUACIÓN DE RIESGOS			
Código Activo	Nombre del Activo	Descripción del Activo	Tipo de Activo	Clasificación			Valor del Activo	Vulnerabilidad	Amenaza	Descripción del Riesgo	Probabilidad
				C	I	D					
ACT-001	Microsoft 365	Suite de aplicaciones en la nube: Word, Excel, P.Point, Ms Project, etc.	Software	3	3	3	Muy Alto	Configuración inadecuada de permisos	Acceso no autorizado	Acceso indebido a información crítica o sensible	Media
ACT-002	Correo Electrónico Institucional	Aplicación de gestión de correos.	Servicio	3	3	3	Muy Alto	Correos de phishing, contraseñas débiles	Suplantación de identidad	Robo de credenciales y acceso a información confidencial	Alta
ACT-003	Microsoft Teams	Aplicación integral para comunicación y colaboración.	Software	2	2	3	Alto	Falta de control en la configuración de usuarios externos	Fuga de información	Acceso no autorizado a reuniones o documentos compartidos	Media
ACT-004	Windows 10 y 11	Sistema Operativo	Software	3	3	3	Muy Alto	Ausencia de actualizaciones de seguridad	Malware y exploits	Infección por malware o vulneración del sistema operativo	Alta
ACT-005	Sistema de Gestión de Tickets de Soporte	Aplicación en la que se registran las solicitudes de atención internas y externas (clientes)	Software	2	2	2	Medio	Contraseñas compartidas	Ataques de fuerza bruta	Robo de credenciales y manipulación de registros	Media
ACT-006	Sistema de Registro de Actividades	Aplicación en la que se registran las actividades diarias de cada consultor.	Software	1	1	1	Muy Bajo	Falta de políticas de respaldo	Pérdida de datos	Pérdida o corrupción de registros críticos	Media
ACT-007	Información Concernientes a Proyectos	Términos de Referencia, Estimaciones, Casos de Negocio, Propuestas, Contratos, Información Clientes, Actas de Inicio, Planes de Proyectos, Informes	Información	3	3	3	Muy Alto	Ausencia de cifrado de datos	Robo de información	Divulgación no autorizada de información confidencial	Alta
ACT-008	Servidor Físico 1	Servidor utilizado para la gestión de maquinas virtuales para realizar laboratorios, pruebas de concepto de herramientas de nuestros	Hardware	2	2	3	Alto	Falta de controles físicos	Robo físico	Robo o daño físico al servidor	Baja

ACT-009	Servidor Físico 2	Servidor utilizado para la gestión de maquinas virtuales para realizar laboratorios, pruebas de concepto de herramientas de nuestros	Hardware	2	2	3	Alto	Falta de respaldo eléctrico	Corte de energía	Pérdida de disponibilidad del servidor	Baja
ACT-010	Router Wifi	Enrutador de Internet para la generación de las IP's dinámicas en la oficina principal	Hardware	2	2	3	Alto	Configuraciones inseguras (contraseñas débiles, redes abiertas)	Ataques de red	Acceso no autorizado a la red y robo de información	Alta
ACT-011	Rack de Comunicaciones	Estructura que aloja los servidores, distribuir el cableado de redes y comunicaciones	Hardware	2	2	3	Alto	Ausencia de control físico	Sabotaje físico	Interrupción de servicios de comunicación	Baja
ACT-012	Red Inalámbrica	Red que permite la distribución del servicio de internet entre los equipos de la oficina principal	Redes	2	2	3	Alto	Ausencia de políticas de seguridad	Interceptación de datos	Robo de información sensible mediante ataques man-in-the-middle	Alta
ACT-013	VPN	Red que permite el acceso remoto a los servidores.	Comunicaciones	2	2	2	Medio	Configuraciones predeterminadas	Acceso indebido	Robo de información confidencial	Media
ACT-014	Lector de Huella Digital	Dispositivo que valida el accesos de los consultores a las instalaciones físicas.	Hardware	2	2	3	Alto	Mantenimiento inadecuado	Falla técnica	Pérdida temporal de capacidad de autenticar usuarios	Baja
ACT-015	Laptops	Equipos portátiles que emplean los consultores de la organización en sus actividades diarias.	Hardware	2	2	3	Alto	Falta de cifrado en discos	Robo de dispositivos	Robo de dispositivos con información confidencial	Alta
ACT-016	Consultores	Profesionales que llevan a cabo las actividades de consultoria.	Personal	3	3	3	Muy Alto	Falta de capacitación	Errores humanos	Exposición accidental de información	Media
ACT-017	Telefono Celular	Equipo celular para agilizar la comunicación entre los clientes y el equipo de soporte.	Comunicaciones	2	2	2	Medio	Aplicaciones no autorizadas	Malware	Pérdida de información confidencial	Media
ACT-018	Oficina Principal	Ambiente físico para actividades presenciales de los consultores	Amb.Físico	2	2	2	Medio	Falta de planes de contingencia	Incendios, inundaciones	Pérdida de activos físicos y documentos confidenciales	Baja

FOCUS SYSTEMS PERU SAC
SEPTIEMBRE 2024

IDENT				TRATAMIENTO DE RIESGOS				SEGUIMIENTO	
Código Activo	Nombre del Activo	Impacto	Severidad	Estrategia Respuesta	Control ISO 27001: 2022	Descripción de la Estrategia	Responsable	Estado	Actividades Realizadas
ACT-001	Microsoft 365	Alta	Alta	Mitigar	8.2. Derechos de acceso con privilegios	Configuración de políticas de acceso por roles y monitoreo continuo de actividades sospechosas	Responsable de TI	En Tratamiento	
ACT-002	Correo Electrónico Institucional	Alta	Alta	Mitigar	6.3. Concienciación, educación y formación en materia de seguridad de la información	Implementar autenticación de doble factor (2FA) y capacitación a los usuarios sobre detección de correos fraudulentos	Responsable de TI	En Tratamiento	
ACT-003	Microsoft Teams	Alta	Alta	Mitigar	5.34. Privacidad y protección de la información personal	Establecer políticas de acceso a invitados y restringir la compartición de datos confidenciales	Responsable de TI	En Tratamiento	
ACT-004	Windows 10 y 11	Alta	Alta	Mitigar	8.8. Gestión de las vulnerabilidades técnicas	Implementar actualizaciones automáticas y configurar un sistema de alertas para nuevas vulnerabilidades	Administrador de Sistemas	En Tratamiento	
ACT-005	Sistema de Gestión de Tickets de Soporte	Alta	Alta	Mitigar	8.5. Autenticación segura	Aplicar controles de contraseñas robustas y monitorear accesos al sistema	Responsable de TI	En Tratamiento	
ACT-006	Sistema de Registro de Actividades	Alta	Alta	Mitigar	8.13. Copia de seguridad de la información	Implementar un sistema de respaldo automatizado con validación periódica de recuperación	Responsable de TI	En Tratamiento	
ACT-007	Información Concernientes a Proyectos	Alta	Alta	Mitigar	5.33. Protección de registros	Cifrar información almacenada y en tránsito, y controlar los accesos a esta información	Responsable de Proyectos	En Tratamiento	
ACT-008	Servidor Físico 1	Alta	Media	Mitigar	7.1 Perímetro de seguridad física	Implementar controles físicos como cerraduras y sistemas de videovigilancia	Encargado de Infraestructura	En Tratamiento	

ACT-009	Servidor Físico 2	Alta	Media	Mitigar	5.30. Preparación de las TIC para la continuidad del negocio	Implementar sistemas UPS y generar un plan de contingencia para cortes prolongados	Encargado de Infraestructura	En Tratamiento	
ACT-010	Router Wifi	Alta	Alta	Mitigar	8.21. Seguridad de los servicios de red	Configurar contraseñas seguras, segmentación de red y monitoreo continuo	Administrador de Redes	En Tratamiento	
ACT-011	Rack de Comunicaciones	Alta	Media	Mitigar	7.2. Controles físicos de entrada	Implementar cerraduras, monitoreo y acceso restringido	Encargado de Infraestructura	En Tratamiento	
ACT-012	Red Inalámbrica	Alta	Alta	Mitigar	8.21. Seguridad de los servicios de red	Implementar WPA3 y restringir accesos por listas de control de acceso (MAC filtering)	Administrador de Redes	En Tratamiento	
ACT-013	VPN	Alta	Alta	Mitigar	8.21. Seguridad de los servicios de red	Configurar autenticación multifactor (MFA) y monitorear las conexiones activas	Responsable de TI	En Tratamiento	
ACT-014	Lector de Huella Digital	Media	Media	Mitigar	7.13. Mantenimiento de equipos	Implementar mantenimientos regulares y contar con un plan alternativo para fallos	Encargado de Infraestructura	En Tratamiento	
ACT-015	Laptops	Alta	Alta	Mitigar	7.13. Mantenimiento de equipos	Implementar cifrado completo de discos y seguimiento mediante herramientas de gestión de dispositivos	Responsable de TI	En Tratamiento	
ACT-016	Consultores	Alta	Alta	Mitigar	6.3. Concienciación, educación y formación en materia de seguridad de la información	Establecer programas de capacitación en seguridad informática	Responsable de Seguridad	En Tratamiento	
ACT-017	Telefono Celular	Alta	Alta	Mitigar	7.13. Mantenimiento de equipos	Configurar políticas de gestión de dispositivos móviles (MDM)	Responsable de TI	En Tratamiento	
ACT-018	Oficina Principal	Alta	Media	Mitigar	7.3. Seguridad de oficinas, salas e instalaciones	Implementar sistemas de protección como alarmas de incendio, respaldos físicos y planes de evacuación	Encargado de Infraestructura	En Tratamiento	