SOCIEDAD TEQUENDAMA

MATRIZ DE RIESGOS - MSPI

Activo	Vulnerabilidad	Amenaza		Riesgo	EVALUCION DEL RIESGO			
					Impacto (I)	Probabilidad (P)	IP	Riesgo Inherente I*P
Carpetas Usuarios Internos	Única copia, sólo una copia de la información	Modificación accidental de datos del sistema de información	R1	Usuario con permisos que accidentalmente modifica y/o elimina la información de Usuarios Internos.	4	3	43	12
Carpetas Usuarios Internos	Nivel de confidencialidad no definido con claridad	Acceso no autorizado al sistema de información	R2	Proprocionar acceso al sistema de información por no contar con niveles de confidencialidad claros en la carpetas de usuarios internos.	4	5	45	20
Backups Internos	Posibles riesgos electricos.	Interrupción del suministro eléctrico	R3	Fallas en el suministro eléctrico que impide la generación de backups o queden incompletas.	5	3	53	15
Contraseñas	Cuentas de usuario generadas por sistema en las que las contraseñas permanecen sin modificación	Moficación de información de los aplicativos	R4	Robo de contraseñas por falta de actualización y modificación de las mismas.	5	3	53	15
Contraseñas	Robo de información	Revelación de contraseñas	R5	Acceso a información por revelación de contraseñas.	5	4	54	20
Computadores	Acceso no autorizado a instalaciones	Robo	R6	Robo de equipos de cómputo o de soportes de información.	3	2	32	6
Computadores	Descargas de Internet sin control	Código malicioso	R7	Código malicioso por descargas sin control del servicio de internet	3	4	34	12
Servicio VPN.	Mal uso de las conexiones remotas	Identidad de usuario camuflada	R8	Funcionario camuflado haciendo mal uso de las conexiones remotas a través del servicio de VPN	3	1	31	3
Servicio de Correo Electrónico	Uso no controlado de sistemas de información	Perdida o filtrado de informacion sensible	R9	Perdida de información sensible por manejo inadecuado del correo electrónico	4	2	42	8
Ejecutables	Sistemas desprotegidos ante acceso no autorizado	Errores de aplicaciones	R10	Aplicación que no controla los intentos de acceso fallidos, permitiendo el ingreso no autorizado.	4	4	44	16
Servidores	Susceptibilidad del equipamiento a alteraciones en el voltaje	Colapso del servidor, información eliminada	R11	Colapso en los servidores e información elminada debido a la susceptibilidad del equipamiento a alteraciones en el voltaje.	5	3	53	15
Red Local	Inadecuada gestión de redes	Pérdida de conectividad	R12	Pérdida de conectividad por inadecuada gestion y capacidad de la red local.	4	4	44	16
Backups Internos	Perdida interna de informacion	Fallas en equipos	R13	Usuarios que no realizan copias de su información.	5	4	54	20
Cuartos de Telecomunicaciones	Posible daño a los servidores	Inundación	R14	Daño de servidores, switches, y equipos de cómputo y dispositivios de cmunicación por inundación en el cuarto de servidores.	4	2	42	8
Informacion	Ataques de phishing	Perdida de informacion	R15	El phishing se refiere al envio - recepcion de correos electronicos que pretender ser una fuente genuina.	5	4	54	20
Informacion	Ransomware	Perdida de informacion	R16	Sin acceso a determinadas partes o archivos del sistema	5	4	54	20
Informacion	DDoS	Perdida de informacion	R17	servicio o recursos no accesible a los usuarios principales.	5	4	54	20
Informacion	Perdida de datos (contraseñas)	Perdida de informacion	R18	Es importante cumplir con todos los requisitos para la creacion de contraseñas seguras.	5	4	54	20

ANALISIS DEL RIESGO			Riesgo asociado			Controles Implementados	TRATAMIENTO DEL RIESGO	
Tipo de impacto	Zona de riesgo	Medidas de respuesta	Confidencialidad	Integridad	Disponibilidad		Acciones	Responsable
A	#N/D	#N/D		X	X	Se dan permisos de escritura únicamente a los responsables	Quitar permisos a usuarios inactivos	Coordinador TI
E	Bajo	Asumir el riesgo	X				Dar acceso de lectura únicamente a los responsables	Coordinador TI
E	Bajo	Asumir el riesgo			X	UPS y Planta Eléctrica	Verificar Funcionamiento de UPS y Planta. Verificar los datos del backup Disponer de un sensor para control de energía	Coordinador TI
E	Bajo	Asumir el riesgo		X		Directorio Activo	Capacitar a funcionarios Aplicativos con poítica de actualización de contraseña	Jefe TIC
E	Bajo	Asumir el riesgo	X		X		Capacitar a funcionarios Aplicativos con poítica de actualización de contraseña	Jefe TIC
M	Moderado	Asumir el riesgo, reducir el riesgo				Vigilancia -- Autorización para retiro de equipos		Coordinador TI
E	Bajo	Asumir el riesgo			X	Antivirus - Gmail (control de Spam y Código malicioso)	Capacitación	Gloria Peña
B	Bajo	Asumir el riesgo	X	X		Control de Usuario		Coordinador TI
A	#N/D	#N/D	X	X	X		Capacitación	Jefe TIC
E	Bajo	Asumir el riesgo	X	X			Control de accesos fallidos en los aplicativos	Coordinador TI
E	Bajo	Asumir el riesgo				Planta, UPS	Análisis de energía (voltaje)	Coordinador TI
E	Bajo	Asumir el riesgo		X	X		Quitar Switches y habilitar puntos de red	Coordinador TI
E	Bajo	Asumir el riesgo	X	X	X	Gestión de información desde los aplicativos	Capacitar a funcionarios	Jefe TIC
A	#N/D	#N/D			X		Sensores de humedad	Coordinador TI
E	Bajo	Asumir el riesgo	X	X	X			Coordinador TI
E	Bajo	Asumir el riesgo	X	X	X			Coordinador TI
E	Bajo	Asumir el riesgo	X	X	X			Coordinador TI
E	Bajo	Asumir el riesgo	X	X	X			Coordinador TI