Tabla de tratamiento de riesgos

Activos /Amenzas/Vulnerabilidades					*Tratamiento del riesgo*	*Valores después del tratamiento*		
No.	**Nombre del activo**	**Propietario del activo**	**Amenaza**	**Vulnerabilidad**	**Selecciones de Controles**	**Consecuencia**	**Probabilidad**	**Riesgo**
R001	Correo electronico	Área administrativa/ Líder área de desarrollo	Difusion de software dañino	Falta de proteccion contra virus y codigo malicioso	A.13.2.1 Políticas y procedimientos de transferencia de información.	1	1	2
R002	WWW	Líder área de desarrollo	Errores de mantenimiento/actualizacion de programas	Falta de capacitación de trabajo	A.14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	2	1	3
R003	WWW	Líder área de desarrollo	Caida del sistema por agotamiento de recursos	Falta de planes de contingencia	A.12.6.1 Gestión de las vulnerabilidades técnicas	2	1	3
R004	Intercambio electronico de datos	Líder área de desarrollo	Escapes de información	Falta de politicas/normas/procedimientos	A.13.2.1 Políticas y procedimientos de transferencia de información.	2	0	2
R005	Intercambio electronico de datos	Líder área de desarrollo	Suplantacion de la identidad del usuario	Control de acceso inadecuado	A.13.2.3 Mensajería electrónica.	2	1	3
R006	Archivos de configuracion	Líder área de desarrollo	Suplantacion de la identidad del usuario	Falta de conciencia de seguridad	A.14.2.1 Política de desarrollo seguro de software	2	1	3
R007	Archivos de configuracion	Líder área de desarrollo	Acceso no autorizado	Administración deficiente de contraseña	A.9.1.1 Política de control de acceso	2	1	3
R008	Datos control de acceso	Líder área de desarrollo	Errores del administrador	Definicion de rol inadecuada	A.7.2.2 Sensibilización sobre seguridad de la información, educación y capacitación.	1	0	1
R009	Datos control de acceso	Líder área de desarrollo	Escapes de información	Falta de documentación	A.9.1.1 política de control de acceso	1	1	2
R010	Datos prueba	Líder área de desarrollo	Difusion de software dañino	Testeo inadecuado/insuficiente	A.14.2.6 Seguridad en entornos de desarrollo	2	1	3

R011	Backups	Líder área de desarrollo	Destrucción de información	Monitoreo insuficiente de medidas de seguridad	A.12.3.1 Copias de seguridad de la información	1	1	2
R012	Backups	Líder área de desarrollo	Errores de mantenimiento/actualizacion de programas	Instalación/Desisntalación no controlada	A.12.6.2 Restricciones en la instalación del software	2	1	3
R103	Backups	Líder área de desarrollo	Errores de mantenimiento/actualizacion de equipos	Protección fisica inadecuada	A.11.2.4 Mantenimiento de los equipos	1	1	2
R014	Codigo Fuente	Líder área de desarrollo	Difusion de software dañino	Monitoreo insuficiente de medidas de seguridad	A.9.4.5 Control de acceso al código fuente de los programas	2	1	3
R015	Codigo Fuente	Líder área de desarrollo	Errores de mantenimiento/actualizacion de programas	Falta de politicas/normas/procedimientos	A.9.4.5 Control de acceso al código fuente de los programas	1	1	2
R016	Bases de datos corporativas	Líder área de desarrollo	Errores del administrador	Definicion de rol inadecuada	A.7.2.1 Responsabilidades de gestión	0	0	0
R017	Bases de datos corporativas	Líder área de desarrollo	Suplantacion de la identidad del usuario	Administración deficiente de contraseña	A.9.2.3 Gestión de los derechos de acceso con privilegios especiales	1	1	2
R018	Credenciales	Líder área de desarrollo	Indisponibilidad de personal	Ausentismo y/o personal insuficiente	A.7.3.1 Terminación o cambio de responsabilidades laborales	1	0	1
R019	Credenciales	Líder área de desarrollo	Suplantacion de la identidad del usuario	Contraseñas no protegidas	A.9.4.1 Restricción del acceso a la información	1	0	1
R020	Routers	Líder de tecnología	Averia de origen fisico o lógico	Monitoreo insuficiente de medidas de seguridad	A.11.2.4 Mantenimiento de los equipos	1	1	2
R021	Servidor de correos	Líder de tecnología	Acceso no autorizado	Definicion de rol inadecuada	A.9.4.3 Gestión de contraseñas de usuario	1	0	1
R022	Servidor de BD	Líder de tecnología	Errores del administrador	Falta de conciencia de seguridad	A.6.1.1 Funciones y responsabilidades de seguridad de la información	1	0	1

R023	Servidor de BD	Líder de tecnología	Alteración accidental de la información	Falta de politicas/normas/procedimientos	A.12.3.1 Copias de seguridad de la información	1	1	2
R024	Informatica Personal	Líder de tecnología	Difusion de software dañino	Locación/almacenamiento no protegido	A.12.2.1 Controles contra malware	0	0	0
R025	Informatica Personal	Líder de tecnología	Perdida de equipos	Falla del hardware y sus componentes	A.8.3.3 Transferencia de medios físicos	1	0	1
R026	Informatica Movil	Líder de tecnología	Acceso no autorizado	Definicion de rol inadecuada	A.6.1.1 Funciones y responsabilidades de seguridad de la información	1	0	1
R027	Informatica Movil	Líder de tecnología	Robo	Protección fisica inadecuada	A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones	1	0	1
R028	Perifericos	Líder de tecnología	Averia de origen fisico o lógico	Monitoreo insuficiente de medidas de seguridad	A.11.2.4 Mantenimiento de los equipos	1	0	1
R029	Soporte de la red	Líder de tecnología	Errores de mantenimiento/actualizacion de equipos	Monitoreo insuficiente de medidas de seguridad	A.13.1.2 Mecanismos de seguridad asociados a servicios en red	1	0	1
R030	Red inalambrica	Líder de tecnología	Acceso no autorizado	Falta de conciencia de seguridad	A.13.1.2 Mecanismos de seguridad asociados a servicios en red	1	0	1
R031	Red local	Líder de tecnología	Acceso no autorizado	Administración de red inadecuada	A.13.1.1 Controles de red	1	1	2
R032	Gerencia	Área administrativa	Indisponibilidad de personal	Ausentismo y/o personal insuficiente	A.7.3.1 Terminación o cambio de responsabilidades laborales	1	0	1
R033	Bases de datos	Líder de tecnología	Acceso no autorizado	Control de acceso inadecuado	A.9.2.5 Revisión de los derechos de acceso de los usuarios	1	0	1
R034	Bases de datos	Líder de tecnología	Alteración accidental de la información	Control inadecuado de BD	A.9.4.1 Restricción del acceso a la información	1	1	2

R035	Sistema Operativo /Ofimatica	Líder de tecnología	Vulnerabilidades de los programas	Falta de conciencia de seguridad	A.7.2.2 Sensibilización sobre seguridad de la información, educación y capacitación.	1	0	1
R036	Navegador WEB	Líder de tecnología	Errores de mantenimiento/actualizacion de programas	Monitoreo insuficiente de medidas de seguridad	A.7.2.2 Sensibilización sobre seguridad de la información, educación y capacitación.	1	0	1
R037	Desarrolladores/programadores	Líder área de desarrollo	Indisponibilidad de personal	Falta de delegación/participación/secesión	A.7.1.2 Términos y condiciones de empleo	1	0	1
R038	Desarrolladores/programadores	Líder área de desarrollo	Abuso de privilegios de acceso	Falta de capacitación de trabajo	A.9.2.2 Provisión de acceso al usuario	0	0	0
R039	Proovedores	Área administrativa/ Líder área de desarrollo	Deficiencias en la organización	Falta de delegación/participación/secesión	A.15.1.2 Tratamiento del riesgo dentro de acuerdos de proveedores	1	1	2

Opciones de tratamiento de riesgo

Aceptación del riesgo
Evitar el riesgo
Transferencia del riesgo
Mitigación del riesgo

©2015 This template may be used by clients of EPPS Services Ltd. www.iso27001standard.com in accordance with the Licence Agreement.

Controles según el anexo A de la norma ISO / IEC 27001

A.5.1.1 Políticas para la seguridad de la información.
A.6.1.1 Funciones y responsabilidades de seguridad de la información
A.6.1.2 Segregación de funciones
A.6.1.5 Seguridad de la información en la gestión de proyectos
A.7.1.1 Proyección (Screening)
A.7.1.2 Términos y condiciones de empleo
A.7.2.1 Responsabilidades de gestión
A.7.2.2 Concienciación sobre la seguridad de la información, la educación y la formación
A.7.2.3 Proceso disciplinario
A.7.3.1 Terminación o cambio de las responsabilidades laborales
A.8.1.1 Inventario de activos
A.8.1.2 Propietarios de activos
A.8.1.3 Uso aceptable de activos
A.8.1.4 Retorno de activos
A.8.2.1 Clasificación de la información
A.8.2.2 Etiquetado de la información
A.8.2.3 Manejo de activos
A.8.3.1 Gestión de soportes extraíbles
A.8.3.2 Eliminación de los medios de comunicación
A.8.3.3 Transferencia de medios físicos
A.9.1.1 Política de control de acceso
A.9.1.2 Acceso a las redes y los servicios de red
A.9.2.1 Registro y salida de usuarios
A.9.2.2 Provisión de acceso al usuario
A.9.2.3 Gestión de los derechos de acceso con privilegios especiales
A.9.2.4 Gestión de información confidencial de autenticación de usuarios
A.9.2.5 Revisión de los derechos de acceso de los usuarios
A.9.2.6 Retirada o adaptación de los derechos de acceso
A.9.3.1 Uso de información confidencial para la autenticación
A.9.4.1 Restricción del acceso a la información
A.9.4.2 Procedimientos seguros de inicio de sesión
A.9.4.3 Gestión de contraseñas de usuario
A.9.4.4 Uso de herramientas de administración de sistemas
A.9.4.5 Control de acceso al código fuente de los programas
A.11.1.1 Perímetro de seguridad física
A.11.1.2 Controles físicos de entrada
A.11.1.3 Seguridad de oficinas, despachos y recursos
A.11.1.4 Protección contra las amenazas externas y ambientales
A.11.1.5 El trabajo en áreas seguras
A.11.1.6 Áreas de acceso público, carga y descarga
A.11.2.1 Emplazamiento y protección de equipos
A.11.2.2 Instalaciones de suministro
A.11.2.3 Seguridad del cableado
A.11.2.4 Mantenimiento de los equipos
A.11.2.5 Salida de activos fuera de las dependencias de la empresa
A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones
A.11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento
A.11.2.8 Equipo informático de usuario desatendido

©2015 This template may be used by clients of EPPS Services Ltd. www.iso27001standard.com in accordance with the Licence Agreement.

A.11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
A.12.1.1 Procedimientos operativos documentados
A.12.1.2 Gestión del cambio
A.12.1.2 Gestión de cambios
A.12.1.3 Gestión de capacidades
A.12.1.4 Separación de entornos de desarrollo, prueba y producción
A.12.2.1 Controles contra malware
A.12.3.1 Copias de seguridad de la información
A.12.4.1 Registro y gestión de eventos de actividad
A.12.4.2 Protección de los registros de información
A.12.4.3 Registros de actividad del administrador y operador del sistema
A.12.4.4 Sincronización de relojes
A.12.5.1 Instalación del software en sistemas en producción
A.12.6.1 Gestión de las vulnerabilidades técnicas
A.12.6.2 Restricciones en la instalación del software
A.12.7.1 Controles de auditoría de los sistemas de información
A.13.1.1 Controles de red
A.13.1.2 Mecanismos de seguridad asociados a servicios en red
A.13.1.3 Segregación de redes
A.13.2.1 Políticas y procedimientos de intercambio de información
A.13.2.2 Acuerdos de intercambio
A.13.2.3 Mensajería electrónica
A.13.2.4 Acuerdos de confidencialidad y secreto
A.14.1.1 Análisis y especificación de los requisitos de seguridad de la información.
A.14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas
A.14.1.3 Protección de las transacciones por redes telemáticas
A.14.2.1 Política de desarrollo seguro de software
A.14.2.2 Procedimientos de control de cambios en los sistemas
A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
A.14.2.4 Restricciones a los cambios en los paquetes de software
A.14.2.5 Uso de principios de ingeniería en protección de sistemas
A.14.2.6 Seguridad en entornos de desarrollo
A.14.2.7 Externalización del desarrollo de software
A.14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas
A.14.2.9 Pruebas de aceptación
A.14.3.1 Protección de datos de prueba
A.15.1.1 Política de seguridad de la información para proveedores
A.15.1.2 Tratamiento del riesgo dentro de acuerdos de proveedores
A.15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones
A.15.2.1 Supervisión y revisión de los servicios prestados por terceros
A.15.2.2 Gestión de cambios en los servicios prestados por terceros
A.16.1.2 Informe de eventos de seguridad de la información
A.16.1.4 Evaluación y decisión sobre eventos de seguridad de la información
A.16.1.6 Aprendiendo de incidentes de seguridad de la información
A.17.1.3 Verificar, revisar y evaluar la continuidad de la seguridad de la información.
A.18.1.2 Derechos de propiedad intelectual.
A.18.2.2 Cumplimiento de políticas y estándares de seguridad.
A.18.2.3 Revisión de cumplimiento técnico.

©2015 This template may be used by clients of EPPS Services Ltd. www.iso27001standard.com in accordance with the Licence Agreement.