Máster Universitario en Ciberseguridad y Privacidad (MUCIP)

ANEXO 3

RESULTADOS ANÁLISIS DE RIESGOS

Universitat Oberta de Catalunya

Natividad García Lacárcel

ANÁLISIS DE RIESGOS

Una vez valorado el nivel de riesgo existente para cada activo, se deben comparar los resultados con el umbral del riesgo, es decir, cuándo considera que el nivel de riesgo obtenido es aceptable, y cuándo es necesario actuar sobre el mismo.
La Alta Dirección establece que el nivel de riesgo aceptable es 40, que corresponde al Nivel Medio, por lo tanto todo lo que esté por debajo de este nivel se considerará como una amenaza no crítica para la empresa.

Para gestionar los riesgos en una empresa pueden tomarse tres decisiones:

- Reducirlos:
  - Reducir la probabilidad: Mediante la búsqueda de mecanismos que ayuden a reducir la probabilidad de ocurrencia, a través de auditorías preventivas, formación, sensibilización, mantenimientos preventivos, etc. Así como la implementación de controles de detección, corrección y disuasión.
  - Reducir el impacto: Desarrollar planes de contingencia y continuidad de negocio, controles técnicos, administrativos. Implementación de controles de detección, corrección y disuasión.
- Transferirlos total o parcialmente: Se puede recurrir a pólizas y seguros, acuerdos de confidencialidad, transferencia física a otros lugares (división del riesgo), etc.
- Aceptarlos: Aquellos riesgos que se consideren residuales y puedan ser aceptados. Se aplicaría a riesgos bajos y moderados.

La empresa ha establecido los siguientes niveles para realizar el tratamiento del riesgo:

RIESGO	CRITERIO DE ACEPTACIÓN DEL RIESGO	DIRECTRICES GENERALES DE TRATAMIENTO
0-20 Muy bajo	Aceptable	No requiere tratamiento del riesgo, es decir, el riesgo se encuentra en un nivel que puede aceptarse.
20-40 Bajo	Tolerable	Mitigar el Riesgo: Riesgos que se puede permitir gestionar, que en caso de materialización la entidad se encuentra en la capacidad de asumirlo.
40-60 Medio	Moderado	Mitigar o Evitar el Riesgo: Riesgos para los cuales se requiere fortalecer los controles existentes y/o agregar nuevos controles.
60-80 Alto	Alto o importante	Mitigar o Evitar el Riesgo: Implementación de controles adicionales como parte del fortalecimiento de los actuales o como resultado de haberlo compartido o transferido.
80-100 Muy Alto	Crítico o inaceptable	Evitar el Riesgo: Se requiere de acciones inmediatas que permitan reducir la probabilidad y el impacto de materialización.

Umbral de riesgo

A continuación, se muestra la tabla con el cálculo del riesgo:

NUMERO	**ACTIVO**	**VALOR**	**RIESGO**
[L-01]	Oficina	Alto	9
[L-02]	CPD	Muy Alto	9
[L-03]	Recepción	Bajo	5
[HW-01]	Servidor de aplicaciones	Alto	7
[HW-02]	Servidor de desarrollo y pruebas	Medio	3
[HW-03]	Servidor de Web	Alto	7
[HW-04]	Servidor BBDD	Alto	9
[HW-05]	Servidor DNS/Proxy/Dominio	Medio	3
[HW-06]	Servidor de ficheros	Alto	9
[HW-07]	Servidor de Email	Alto	9
[HW-08]	Equipamiento de respaldo	Alto	7
[HW-09]	Enrutador de Internet	Medio	5
[HW-10]	Switch	Medio	5
[HW-11]	Cortafuegos	Muy alto	9
[HW-12]	Punto de acceso inalámbrico	Medio	3
[HW-13]	Equipos escritorio pc	Medio	7
[HW-14]	Portátiles	Medio	7
[HW-15]	Impresoras y escáneres	Bajo	3
[HW-16]	Centralita	Bajo	3
[HW-17]	Teléfonos fijos	Bajo	3
[HW-18]	Teléfonos móviles	Bajo	3
[HW-19]	Cámaras de vigilancia	Medio	3
[SW-01]	Sistemas operativos	Medio	70
[SW-02]	Paquete ofimático	Bajo	30
[SW-03]	Antivirus	Medio	50
[SW-04]	Software de desarrollo	Medio	70
[SW-05]	Software de contabilidad	Medio	70
[SW-06]	Email	Medio	50
[SW-07]	Servidores	Alto	100
[D-01]	Bases de datos	Muy alto	100
[D-02]	Datos de soporte y licencias	Bajo	30
[D-03]	Desarrollos propios	Medio	30
[D-04]	Backups (copias de seguridad)	Alto	70
[D-05]	Correo electrónico	Medio	30
[D-06]	Logs de servidores y clientes	Medio	80
[D-7]	Credenciales y datos de control de acceso.	Medio	80
[COM-01]	Internet	Alto	4,5
[COM-02]	Red inalámbrica	Medio	3,5
[COM-03]	Red cableada	Alto	4,5
[COM-04]	Telefonía fija	Medio	2,5
[COM-05]	Telefonía móvil	Medio	2,5

[SER-01]	Acceso remoto	Bajo	30
[SER-02]	Red de control e instrumentación	Bajo	10
[SER-03]	Acceso a internet	Bajo	30
[SER-04]	Correo electrónico	Bajo	30
[SER-05]	Servicio web	Medio	50
[SER-06]	Servicio aplicaciones	Medio	70
[SER-07]	Servicio ficheros	Bajo	70
[AUX-01]	Aire acondicionado	Alto	9
[AUX-02]	Archivadores	Bajo	3
[AUX-03]	Consumibles varios	Bajo	3
[AUX-04]	SAI	Alto	7
[AUX-05]	Corriente eléctrica	Muy alto	9
[P-01]	Director General	Muy alto	30
[P-02]	Director comercial	Medio	30
[P-03]	Director de proyectos	Medio	30
[P-04]	Director financiero	Medio	30
[P-05]	Director Sistemas TI	Alto	70
[P-06]	Responsable seguridad de la información.	Muy alto	70
[P-07]	Key Account Manager	Medio	30
[P-08]	Técnicos de sistemas	Medio	30
[P-09]	Personal del departamento comercial	Bajo	30
[P-10]	Personal del departamento de proyectos	Bajo	30
[P-11]	Personal del departamento financiero	Bajo	10

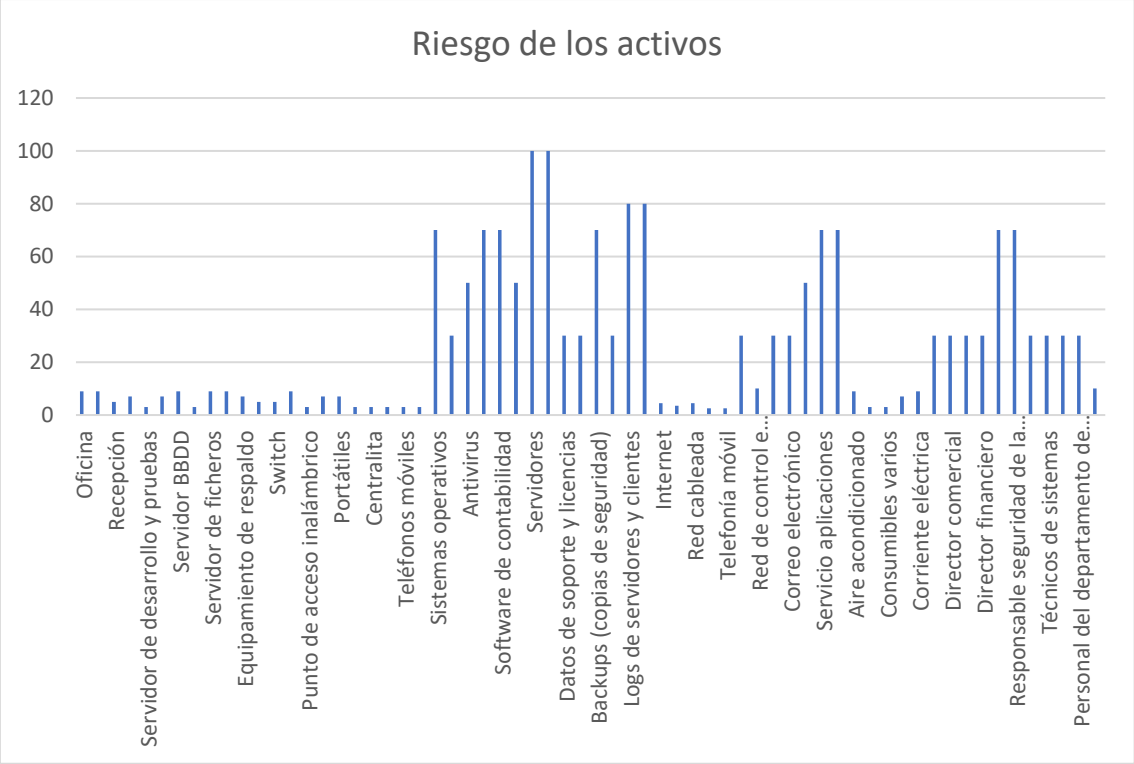
De forma resumida, se obtiene el nivel de tratamiento del riesgo de cada activo. A continuación, se muestran agrupados por nivel de tratamiento:

TRATAMIENTO DEL RIESGO CRÍTICO	
[SW-07]	Servidores
[D-01]	Bases de datos

TRATAMIENTO DEL RIESGO IMPORTANTE	
[SW-01]	Sistemas operativos
[SW-04]	Software de desarrollo
[SW-05]	Software de contabilidad
[D-04]	Backups (copias de seguridad)
[D-06]	Logs de servidores y clientes
[D-7]	Credenciales y datos de control de acceso.
[SER-06]	Servicio aplicaciones
[SER-07]	Servicio ficheros
[P-05]	Director Sistemas TI
[P-06]	Responsable seguridad de la información.

TRATAMIENTO DEL RIESGO MODERADO	
[SW-03]	Antivirus
[SW-06]	Email
[SER-05]	Servicio web

TRATAMIENTO DEL RIESGO TOLERABLE	
[SW-02]	Paquete ofimático
[SER-01]	Acceso remoto
[SER-03]	Acceso a internet
[SER-04]	Correo electrónico
[P-01]	Director General
[P-02]	Director comercial
[P-03]	Director de proyectos
[P-04]	Director financiero
[P-07]	Key Account Manager
[P-08]	Técnicos de sistemas
[P-09]	Personal del departamento comercial
[P-10]	Personal del departamento de proyectos



Riesgos de los activos

La agrupación de los activos permite estudiar de forma más clara el grado de riesgo en que se encuentra cada activo. Se observa un gran número de ellos en estado de riesgo tolerable y aceptable. Sin embargo, los catalogados como críticos o de alto riesgo demandan un tratamiento adecuado. Sobre ellos se implementarán los proyectos posteriores.

Para ello debe de gestionarse un plan de acción que debería de contener la siguiente información:

- Establecer prioridades, asignar prioridad a los riesgos que deben de reducirse en primer lugar.
- Planteamiento del análisis de coste / beneficio, para cada medida comprobar si el coste de la misma supera el beneficio.
- Selección de controles definitivos.
- Asignación de responsabilidades, asignar responsable para la implantación de los controles.
- Implantación de controles