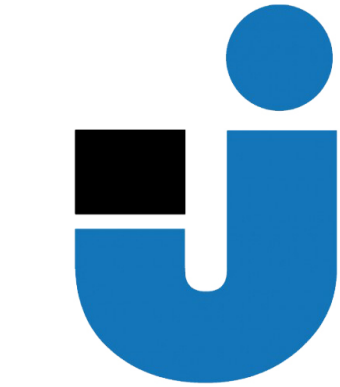

Universidad Nacional
ARTURO JAURETCHE

Seguridad de la Informacióna

TP nº 2

Salvatori Emiliano

Mayo del 2020

Índice

1. Introducción

En el siguiente informe identifican los incidentes de seguridad para la materia **Seguridad de la información Comisión nº 1** a distintos activos de la empresa ABC.

2. Objetivos

Se realiza el Análisis de Riesgo a los siguientes dispositivos, los cuales son parte de determinados activos de la empresa ABC.

3. Escenario

La empresa ABC tiene su sede en Capital Federal, posee alrededor de 400 empleados y cuenta con 10 sucursales ubicadas en diferentes ciudades del interior del país, con una totalidad de 20 empleados en cada una de estas sucursales. Para el desarrollo de sus operaciones ABC requiere realizar una evaluación de riesgo sobre alguno de sus activos. Una vez evaluados todos ellos, se logra dar con cinco, que serán los siguientes:

- Router de Sucursal Tucumán.
- HUB de Casa Central
- Servidor de Base de Datos nº 1.
- Servidor de Base de Datos nº 2.
- Servidor de Base de Datos nº 3.

4. Abordaje Metodológico

Cabe resaltar que para el siguiente informe se debe tener presente las siguientes definiciones acometidas en cada una de las tablas que siguen a cada dispositivo:

- **Impacto**: Trata de evidenciar cuánto afecta al negocio si la amenaza se concreta.
- **Vulnerabilidad**: Trata de evidenciar cada cuanto tiempo se genera una amenaza de forma efectiva. Los valores que se encontrarán en estos, son obtenidos de estudios de internacionales de seguridad.
- **Frecuencia**: cuán vulnerable es el activo a la amenaza considerando la situación actual. La situación actual depende de cada una de las circunstancias donde se encuentre el activo analizado.

La metodología a seguir será:

1. Determinar los activos

2. Determinar la importancia (entre 0 y 1) Por lo que 1 será sumamente crítico y 0 nada crítico.

3. Determinar las amenazas que afectan activos.

Por último, cabe tener en cuenta las siguientes sinónimos utilizados en las ecuaciones de ponderación:

- Para los riesgos ponderados como **Altos** se utilizará la letra griega α (alfa).
- Para los riesgos ponderados como **Medios** se utilizará la letra griega μ (mu).
- Para los riesgos ponderados como **Bajos** se utilizará la letra griega β (beta).
- Para el riesgo **Total** se utilizará la letra griega δ (delta).
- Para el riesgo **Ponderado** se utilizará la letra griega λ (lambda).

5. Evaluación por Activo

5.1. Router Sucursal Tucumán

Características

El recinto donde se encuentra ubicado el Router de la Casa central de la empresa ABC se encuentra en un subsuelo, a unos 100 metros debajo de la calle principal que da acceso a la empresa. Está situado en la esquina lateral, a mano izquierda de la única entrada.

El nivel de seguridad para adentrarse al recinto consta de dos niveles: el primero que es el del acceso general para todo empleado y el segundo para el personal de Administración IT. La habitación cuenta con está equipada con extintores para incendios, grupo electrógeno y estabilizador para los problemas con la luz. El grupo de electricidad alternativo, alimenta de forma indirecta también a las cámaras de seguridad que controlan tanto el subsuelo como el piso nº 1.

Sobre el equipo evaluado se tiene acceso restringido para personal del área de IT. Posee un firewall realizado bajo licencia Microsoft para todo su software.

Se cuenta con mantenimiento del personal de forma mensual, monitoreado por una empresa externa para la problemática de hardware o software. El personal firma un contrato de confidencialidad que le prohíbe divulgar la información. Los softwares utilizados tienen pruebas para evitar vulnerabilidades o amenazas.

Evaluación

Por las características antes mencionadas, resulta la siguiente tabla:

Amenazas	Impacto	Frecuencia	Vulnerabilidad	Riesgo
Inundaciones	Alto	Medio	Alto	**Alto**
Sobrevoltaje	Alto	Medio	Bajo	**Bajo**
Incendios	Alto	Bajo	Medio	**Medio**
Cortes de suministro eléctrico	Alto	Medio	Bajo	**Bajo**
Robo de equipamiento	Medio	Bajo	Bajo	**Bajo**
Acceso a Información no autorizado (Snnifing, SNMP, configuración de equipos, Bases de datos)	Alto	Medio	Bajo	**Bajo**
Destrucción de información (código malicioso)	Medio	Alto	Bajo	**Medio**
Instalación de software sin licencia	Alto	Bajo	Bajo	**Bajo**
Acceso no autorizado a recursos (Internet, PC, Impresoras, correo electrónico, acceso logico p/ cambio de configuracion)	Alto	Alto	Medio	**Alto**
Desconexión de equipamiento de red (voluntaria o involuntaria)	Alto	Medio	Medio	**Medio**
Divulgación de información confidencial (ingeniería social, correo electronico, messenger)	Medio	Medio	Medio	**Medio**
Desarrollo de software con vulnerabilidades	Alto	Medio	Medio	**Medio**
Indisponibilidad (por falla del software - ataque de denegacion de servicio)	Alto	Bajo	Medio	**Medio**
Indisponibilidad (por falla de hardware)	Alto	Bajo	Alto	**Medio**

Ponderación de Riesgos

Se calcula el Riesgo sobre el Activo de la siguiente manera:

$$\frac{\sum_{n=1}^{n=14} \beta * 1 + \sum_{n=1}^{n=14} \mu * 3 + \sum_{n=1}^{n=14} \alpha * 6}{\sum_{n=1}^{n=14} 14 * 6} = 0{,}38 \tag{1}$$

Se obtiene de lo anterior:

- El factor de **Riesgo Total** es de $\delta = 38\,\%$
- Siendo el **Riesgo Ponderado** es de $\lambda = 30\,\%$ debido a que es un activo de suma importancia para la compañía.

5.2. HUB de Casa Central

Características

El dispositivo HUB de Casa Central de la empresa ABC se encuentra ubicado en un tercer piso. Dada la altura no es propenso a sufrir inundaciones o filtraciones de agua. Las dimensiones del cubículo donde se encuentra el dispositivo hacen poco probable en caso de incendio que se pueda operar con facilidad y aún menos poder desmontar los equipos de forma correcta en caso de querer evitar algún desastre mayor. No se cuenta con extintores de fuego dentro de la habitación, pero si por fuera.

Se cuenta con un grupo electrógeno compartido para el primer y segundo piso, donde hay mayor cantidad de equipos eléctricos a los que responder. La misma gestión de licencias en software y mantenimiento realizado por el Router de la Sucursal

Tucumán, se ejecuta en este HUB. Se cuenta con soporte de personas de IT para su mantenimiento como también monitoreo remoto de otras sucursales

No se tienen normativas reguladas con respecto al trato de la información y la confidencialidad, así como tampoco se tiene un control riguroso de las personas que pueden acceder al cubículo donde se encuentra el dispositivo.

Evaluación

Por las características antes mencionadas, resulta la siguiente tabla:

Amenazas	Impacto	Frecuencia	Vulnerabilidad	Riesgo
Inundaciones	Medio	Medio	Bajo	**Medio**
Sobrevoltaje	Medio	Bajo	Alto	**Medio**
Incendios	Medio	Bajo	alto	**Medio**
Cortes de suministro eléctrico	Medio	Alto	Alto	**Alto**
Robo de equipamiento	Medio	Bajo	Medio	**Bajo**
Acceso a Información no autorizado (Snnifing, SNMP, configuración de equipos, Bases de datos)	Alto	Medio	Medio	**Medio**
Destrucción de información (código malicioso)	Alto	Bajo	Bajo	**Bajo**
Instalación de software sin licencia	Medio	Bajo	Bajo	**Bajo**
Acceso no autorizado a recursos (Internet, PC, Impresoras, correo electrónico, acceso logico p/ cambio de configuracion)	Alto	Medio	Medio	**Medio**
Desconexión de equipamiento de red (voluntaria o involuntaria)	Medio	Medio	Bajo	**Medio**
Divulgación de información confidencial (ingeniería social, correo electronico, messenger)	Alto	Bajo	Medio	**Medio**
Desarrollo de software con vulnerabilidades	Bajo	Bajo	Bajo	**Bajo**
Indisponibilidad (por falla del software - ataque de denegacion de servicio)	Medio	Bajo	Bajo	**Bajo**
Indisponibilidad (por falla de hardware)	Medio	Medio	Bajo	**Medio**

Ponderación de Riesgos

Se calcula el Riesgo sobre el Activo de la siguiente manera:

$$\frac{\sum_{n=1}^{n=14} \beta * 1 + \sum_{n=1}^{n=14} \mu * 3 + \sum_{n=1}^{n=14} \alpha * 6}{\sum_{n=1}^{n=14} 14 * 6} = 0{,}45 \tag{2}$$

Se obtiene de lo anterior:

- El factor de **Riesgo Total** es de $\delta = 45\,\%$
- Siendo el **Riesgo Ponderado** es de $\lambda = 40\,\%$

5.3. Servidor de Base de Datos SQL nº 1

Características

El Servidor de Base de Datos SQL de Casa Central de la empresa ABC se encuentra ubicado en un tercer piso. El mismo no es propenso a sufrir inundaciones. Cuenta con varios grupos de electricidad secundarios en la parte de informática y más específicamente en el subsuelo junto al enlace.

La seguridad física del Servidor se encuentra gestionada por dos niveles de seguridad: el nivel general hacia la empresa y el segundo gestionado por los empleados pertenecientes al Sector de IT. Por lo que sólo puede ingresar al lugar físico donde está el Servidor, personal autorizado y calificado.

El lugar también cuenta con cámaras de seguridad que controlan el acceso y el tiempo de permanencia de las personas en el recinto. El Servidor contiene tanto protección mediante antivirus como un firewall autorizado y con licencia original. Solo se permite software original, bajo patentes originales. . La clave del wifi se modifica semanalmente y pudiendo ocasionar que intrusos se conecten a la red y consuman recursos no autorizados.

Evaluación

Por las características antes mencionadas, resulta la siguiente tabla:

Amenazas	Impacto	Frecuencia	Vulnerabilidad	Riesgo
Inundaciones	Alto	Bajo	Alto	Bajo
Sobrevoltaje	Alto	Bajo	Bajo	Bajo
Incendios	Alto	Bajo	Bajo	Bajo
Cortes de suministro eléctrico	Medio	Medio	Bajo	Bajo
Robo de equipamiento	Alto	Bajo	Bajo	Bajo
Acceso a Información no autorizado (Snnifing, SNMP, configuración de equipos, Bases de datos)	Alto	Bajo	Bajo	Bajo
Destrucción de información (código malicioso)	Alto	Bajo	Bajo	Bajo
Instalación de software sin licencia	Alto	Bajo	Bajo	Bajo
Acceso no autorizado a recursos (Internet, PC, Impresoras, correo electrónico, acceso logico p/ cambio de configuracion)	Medio	Medio	Alto	Alto
Desconexión de equipamiento de red (voluntaria o involuntaria)	Alto	Bajo	Alto	bajo
Divulgación de información confidencial (ingeniería social, correo electronico, messenger)	Alto	Bajo	Alto	Bajo
Desarrollo de software con vulnerabilidades	Alto	Bajo	Bajo	Bajo
Indisponibilidad (por falla del software - ataque de denegacion de servicio)	Alto	Bajo	Alto	Bajo
Indisponibilidad (por falla de hardware)	Alto	Bajo	Bajo	Bajo

Ponderación de Riesgos

Se calcula el Riesgo sobre el Activo de la siguiente manera:

$$\frac{\sum_{n=1}^{n=14} \beta * 1 + \sum_{n=1}^{n=14} \mu * 3 + \sum_{n=1}^{n=14} \alpha * 6}{\sum_{n=1}^{n=14} 14 * 6} = 0{,}22 \tag{3}$$

Se obtiene de lo anterior:

- El factor de **Riesgo Total** es de $\delta = 20\,\%$
- Siendo el **Riesgo Ponderado** es de $\lambda = 22\,\%$

5.4. Servidor de Base de Datos SQL nº 2

Características

El Servidor de Base de Datos SQL de la Sucursal Tucumán de la empresa ABC se encuentra ubicado en un primer piso. El recinto cuenta con humedad no está equipada con seguridad para el caso de incendios, además el mismo se encuentra en una zona donde en los últimos años, la probabilidad de cortes de suministros de electricidad ha ido en aumento, no se encuentran grupos de electricidad secundarios.

Es un lugar cerrado con poco espacio para personas. El mismo cuenta con antivirus y Firewall para su protección.

Las licencias tanto de programas como de hardware no se renuevan tan a menudo como en los otros dispositivos debido a que cuenta con varios años en su haber. No se indica personal autorizado a acceder al dispositivo, por lo que redunda en un alto margen de peligrosidad.

Evaluación

Por las características antes mencionadas, resulta la siguiente tabla:

Servidor

Amenazas	Impacto	Frecuencia	Vulnerabilidad	Riesgo
Inundaciones	Medio	Medio	Alto	**Alto**
Sobrevoltaje	Medio	Bajo	Alto	**Medio**
Incendios	Medio	Bajo	Alto	**Medio**
Cortes de suministro eléctrico	Medio	Alto	Alto	**Alto**
Robo de equipamiento	Medio	Bajo	Medio	**Medio**
Acceso a Información no autorizado (Snnifing, SNMP, configuración de equipos, Bases de datos)	Alto	Medio	Bajo	**Medio**
Destrucción de información (código malicioso)	Alto	Bajo	Bajo	**Bajo**
Instalación de software sin licencia	Medio	Bajo	Medio	**Medio**
Acceso no autorizado a recursos (Internet, PC, Impresoras, correo electrónico, acceso logico p/ cambio de configuracion)	Alto	Medio	Medio	**Medio**
Desconexión de equipamiento de red (voluntaria o involuntaria)	Medio	Medio	Bajo	**Bajo**
Divulgación de información confidencial (ingeniería social, correo electronico, messenger)	Alto	Bajo	Medio	**Medio**
Desarrollo de software con vulnerabilidades	Bajo	Bajo	Medio	**Bajo**
Indisponibilidad (por falla del software - ataque de denegacion de servicio)	Medio	Bajo	Medio	**Medio**
Indisponibilidad (por falla de hardware)	Medio	Medio	Medio	**Medio**

Ponderación de Riesgos

Se calcula el Riesgo sobre el Activo de la siguiente manera:

$$\frac{\sum_{n=1}^{n=14} \beta * 1 + \sum_{n=1}^{n=14} \mu * 3 + \sum_{n=1}^{n=14} \alpha * 6}{\sum_{n=1}^{n=14} 14 * 6} = 0{,}54 \tag{4}$$

Se obtiene de lo anterior:

- El factor de **Riesgo Total** es de $\delta = 50\,\%$
- Siendo el **Riesgo Ponderado** es de $\lambda = 25\,\%$

5.5. Servidor de Base de Datos SQL nº 3

Características

El Servidor de Base de Datos SQL de la Sucursal Pueyrredón de la empresa ABC se encuentra ubicado en un primer piso de un edificio antiguo. No mantiene las medidas de seguridad requeridas para incendios. También carece de cámaras de seguridad en puntos vulnerables o de acceso a ciertos equipamientos.

En cuanto al suministro eléctrico posee grupos electrógenos y sistemas de alimentación ininterrumpida. El personal no está lo suficientemente capacitado en materia de seguridad de la información respecto a la ingeniería social y el manejo adecuado de la información.

No se permite el uso de software ilegal y en caso de requerir una licencia se realiza el pedido para que se incluya en el presupuesto. La contraseña del acceso a Internet

no se renueva periódicamente y el antivirus utilizado es el mismo que se utiliza para el Servidor de Casa Central descripto en el punto anterior.

Evaluación

Por las características antes mencionadas, resulta la siguiente tabla:

Amenazas	Impacto	Frecuencia	Vulnerabilidad	Riesgo
Inundación	Alto	Bajo	Bajo	**Bajo**
Sobrevoltaje	Alto	Medio	Bajo	**Bajo**
Incendio	Alto	Bajo	Alto	**Medio**
Cortes de suministro eléctrico	Alto	Alto	Bajo	**Bajo**
Robo de equipamiento	Alto	Bajo	Alto	**Medio**
Acceso a Información no autorizado (Snnifing, SNMP, configuración de equipos, Bases de datos)	Alto	Medio	Alto	**Alto**
Destrucción de información (código malicioso)	Alto	Medio	Bajo	**Bajo**
Instalación de software sin licencia	Alto	Bajo	Bajo	**Bajo**
Acceso no autorizado a recursos (Internet, PC, Impresoras, correo electrónico, acceso logico p/ cambio de configuracion)	Alto	Medio	Medio	**Medio**
Desconexión de equipamiento de red (voluntaria o involuntaria)	Alto	Bajo	Alto	**Medio**
Divulgación de información confidencial (ingeniería social, correo electronico, messenger)	Alto	Medio	Alto	**Alto**
Desarrollo de software con vulnerabilidades	Alto	Medio	Bajo	**Bajo**
Indisponibilidad (por falla del software - ataque de denegacion de servicio)	Alto	Medio	Bajo	**Bajo**
Indisponibilidad (por falla de hardware)	Alto	Bajo	Medio	**Medio**

Ponderación de Riesgos

Se calcula el Riesgo sobre el Activo de la siguiente manera:

$$\frac{\sum_{n=1}^{n=14} \beta * 1 + \sum_{n=1}^{n=14} \mu * 3 + \sum_{n=1}^{n=14} \alpha * 6}{\sum_{n=1}^{n=14} 14 * 6} = 0{,}50 \tag{5}$$

Se obtiene de lo anterior:

- El factor de **Riesgo Total** es de $\delta = 50\,\%$
- Siendo el **Riesgo Ponderado** es de $\lambda = 50\,\%$

6. Conclusiones

La función del **Análisis de Vulnerabilidad** es evidenciar cuan segura es la empresa o ente estatal ante riesgos de seguridad. Al abordar un proceso de este tipo se trata de razonar los puntos débiles de una organización, por los cuales pueden perder

información o comprometer su seguridad. Cabe resaltar que no se pueden asegurar todos los activos, sino que de todo el universo posible, se seleccionará unos pocos, que sean los más relevantes para el desarrollo de la actividad a la que se dedique la entidad.

El análisis anteriormente desarrollado sobre cinco dispositivos para la empresa ABC, da cuenta de la forma de abordar dicho Análisis y de esta forma, evaluar los activos que más puedan comprometer al trabajo de la organización.

7. Herramientas

7.1. Materiales utilizados para el presente trabajo

Para la resolución del presente Laboratorio se utilizaron las siguientes herramientas:

1. Arch Linux V5.1.11
2. Para la composición del presente Informe se utilizó el paquete *texlive-latexextra 2018.50031-1*