Ministerio de Educación
Gobierno de Chile

UNIVERSIDAD CATÓLICA DE TEMUCO

Recursos compartidos a través de una red de área local: *Vulnerabilidades, matriz de riesgo y plan de acción*

Módulo 5: **Configuración de la seguridad en redes de área local.**

Conectividad y Redes

Objetivos de Aprendizaje de la Especialidad

Módulo 1	**OA1** Leer y utilizar técnicamente proyectos de conectividad y redes, considerando planos o diagramas de una red de área local (red LAN), basándose en los modelos TCP/IP y OSI. **OA3** Instalar y mantener cableados estructurados, incluyendo fibra óptica, utilizados en la construcción de redes, basándose en las especificaciones técnicas correspondientes. **OA7** Instalar y configurar una red inalámbrica según tecnologías y protocolos establecidos.
Módulo 2	**OA2** Instalar y configurar sistemas operativos en computadores personales con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos. **OA11** Armar y configurar un equipo personal, basándose en manuales de instalación, utilizando las herramientas apropiadas y respetando las normas de seguridad establecidos.
Módulo 3	**OA8** Aplicar herramientas de software que permitan obtener servicios de intranet e internet de manera eficiente.
Módulo 4	**OA4** Realizar pruebas de conexión y señales en equipos y redes, optimizando el rendimiento de la red y utilizando instrumentos de medición y certificación de calidad de la señal, considerando las especificaciones técnicas.
Módulo 5	OA5 Aplicar métodos de seguridad informática para mitigar amenazas en una red LAN, aplicando técnicas como filtrado de tráfico, listas de control de acceso u otras.
Módulo 6	**OA9** Mantener y actualizar el hardware de los computadores personales y de comunicación, basándose en un cronograma de trabajo, de adcuerdo a las especificaciones técnicas del equipo.
Módulo 7	**OA10** Mantener actualizado el software de productividad y programas utilitarios en un equipo personal, de acuerdo a los requerimientos de los usuarios.
Módulo 8	**OA6** Aplicar procedimientos de recuperación de fallas y realizar copias de respaldo de los servidores, manteniendo la integridad de la información.
Módulo 9	No esta asociado a Objetivos de Aprendizaje de la Especialidad (OAE), sino a Genéricos. No obstante, puede asociarse a un OAE como estrategia didáctica.

Perfil de Egreso – Objetivos de Aprendizaje Genéricos

A- Comunicarse oralmente y por escrito con claridad, utilizando registros de habla y de escritura pertinentes a la situación laboral y a la relación con los interlocutores.	**B-** Leer y utilizar distintos tipos de textos relacionados con el trabajo, tales como especificaciones técnicas, normativas diversas, legislación laboral, así como noticias y artículos que enriquezcan su experiencia laboral.	**C-** Realizar las tareas de manera prolija, cumpliendo plazos establecidos y estándares de calidad, y buscando alternativas y soluciones cuando se presentan problemas pertinentes a las funciones desempeñadas.
D- Trabajar eficazmente en equipo, coordinando acciones con otros in situ o a distancia, solicitando y prestando cooperación para el buen cumplimiento de sus tareas habituales o emergentes.	**E-** Tratar con respeto a subordinados, superiores, colegas, clientes, personas con discapacidades, sin hacer distinciones de género, de clase social, de etnias u otras.	**F-** Respetar y solicitar respeto de deberes y derechos laborales establecidos, así como de aquellas normas culturales internas de la organización que influyen positivamente en el sentido de pertenencia y en la motivación laboral.
G- Participar en diversas situaciones de aprendizaje, formales e informales, y calificarse para desarrollar mejor su trabajo actual o bien para asumir nuevas tareas o puestos de trabajo, en una perspectiva de formación permanente.	**H-** Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.	**I-** Utilizar eficientemente los insumos para los procesos productivos y disponer cuidadosamente los desechos, en una perspectiva de eficiencia energética y cuidado ambiental.
J- Emprender iniciativas útiles en los lugares de trabajo y/o proyectos propios, aplicando principios básicos de gestión financiera y administración para generarles viabilidad.	**K-** Prevenir situaciones de riesgo y enfermedades ocupasionales, evaluando las condiciones del entorno del trabajo y utilizando los elementos de protección personal según la normativa correspondiente.	**L-** Tomar decisiones financieras bien informadas, con proyección a mediano y largo plazo, respecto del ahorro, especialmente del ahorro previsional, de los seguros, y de los riesgos y oportunidades del endeudamiento crediticio así como de la inversión.

Marco de Cualificaciones Técnico Profesional (MCTP) Nivel 3 y su relación con los OAG

HABILIDADES

1. Información
1. Analiza y utiliza información de acuerdo a parámetros establecidos para responder a las necesidades propias de sus actividades y funciones.
2. Identifica y analiza información para fundamentar y responder a las necesidades propias de sus actividades.

2. Resolución de problemas
1. Reconoce y previene problemas de acuerdo a parámetros establecidos en contextos conocidos propios de su actividad o funcion.
2. Detecta las causas que originan problemas en contextos conocidos de acuerdo a parámetros establecidos.
3. Aplica soluciones a problemas de acuerdo a parámetros establecidos en contextos conocidos propios de una función.

3. Uso de recursos
1. Selecciona y utiliza materiales, herramientas y equipamiento para responder a una necesidad propia de una actividad o función especializada en contextos conocidos.
2. Organiza y comprueba la disponibilidad de los materiales, herramientas y equipamiento.
3. Identifica y aplica procedimientos y técnicas específicas de una función de acuedo a parámetros establecidos.

4. Comunicación
4. Comunica y recibe información relacionada a su actividad o función, a través de medios y soportes adecuados en contextos conocidos.

APLICACIÓN EN CONTEXTO

5. Trabajo con otros
1. Trabaja colaborativamente en actividades y funciones coordinándose con otros en diversos contextos.

6. Autonomía
1. Se desempeña con autonomía en actividades y funciones especializadas en diversos contextos con supervisión directa.
2. Toma decisiones en actividades propias y en aquellas que inciden en el quehacer de otros en contextos conocidos.
3. Evalua el proceso y el resultado de sus actividades y funciones de acuerdo a parámetros establecidos para mejorar sus prácticas.
4. Busca oportunidades y redes para el desarrollo de sus capacidades

7. Ética y responsabilidad
1. Actúa de acuerdo a las normas y protocolos que guían su desempeño y reconoce el impacto que la calidad de su trabajo tiene sobre el proceso productivo o la entrega de servicios.
2. Responde por cumplimiento de los procedimientos y resultados de sus actividades.
3. Comprende y valora los efectos de sus acciones sobre la salud y la vida, la organización, la sociedad y el medio ambiente.
4. Actúa acorde al marco de sus conocimientos. experiencias y alcance de sus actividades y funciones

CONOCIMIENTO

8. Conocimientos
1. Demuestra conocimientos especificos de su área y de las tendencias de desarrollo para el desempeño de sus actividades y funciones.

Metodología seleccionada

Simulación de contextos laborales

- Esta presentación te servirá para avanzar paso a paso en el desarrollo de la actividad propuesta.

Aprendizaje Esperado

- **5.1** Gestiona recursos compartidos de la red de área local según estándares o procedimientos técnicos y de seguridad establecidos

¿Qué vamos a lograr con esta actividad para llegar al Aprendizaje Esperado (AE)?

Clasificar recursos factibles de ser compartidos, así como identificar y analizar los potenciales daños que esto puede generar usando una matriz de riesgos.

Pregunta o actividad de motivación:

Si tuvieras que compartir tu computador
¿dejarías que vieran todos tus archivos, o preferirías que sólo algunas personas pudieran verlos?

¿Qué recursos se pueden compartir a través de una red de área local?

- **Una red de área local** permite compartir recursos tales como archivos, unidades de disco, dispositivos de red, etc.
- El **compartir recursos** permite el ahorro de tiempo y recursos económicos, que a la larga se traduce en una reducción de costos para la empresa.
- **Un ejemplo de lo anterior**, sería compartir una impresora en lugar de comprar una para cada miembro de la organización.

Imagen: https://sobretodoredes.wordpress.com/redes-cableadas/elementos-de-una-red/recursos-compartidos/

¿Cómo se clasifican los recursos compartidos?

Los recursos compartidos pueden clasificarse en:

- **Hardware:** Escáner, Impresoras, Unidades de disco, Dispositivos de red, etc.

- **Software:** Archivos, Carpetas, Aplicaciones, etc.

Para definir si un recurso debe ser compartido o no, debe estar establecido en las políticas de seguridad de la empresa

¿Qué riesgos o vulnerabilidades existen al compartir estos recursos?

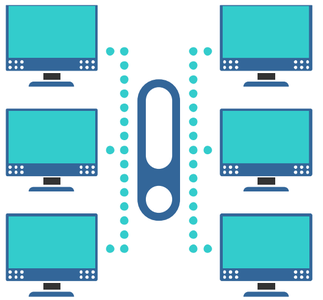
Al compartir recursos en área local, existen potenciales vulnerabilidades como por ejemplo:

01

- **Al compartir un archivo**, éste puede ser modificado y poner en riesgo alguna configuración importante.

02

- **Al compartir el disco duro**, pueden borrarse archivos importantes del disco, si los permisos no corresponden a los categorías de los usuarios (administrador, invitado, etc.).



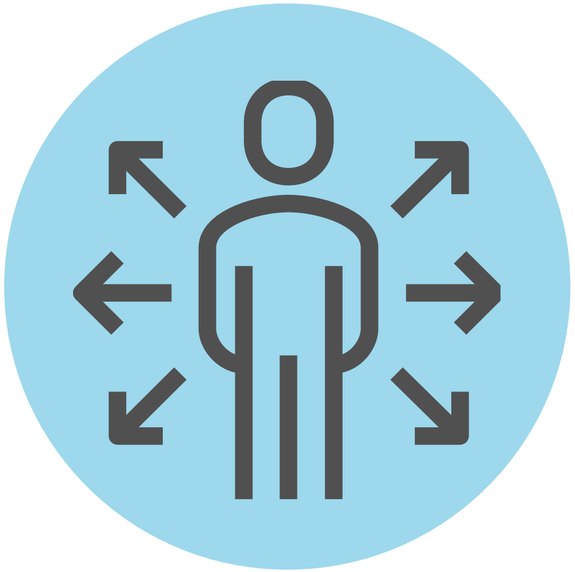
¿Cuáles son las características y condiciones de conectividad de un recurso?

- **La decisión de compartir** recursos, ya sean hardware o software, está directamente relacionada con las políticas de seguridad que se implementarán para minimizar las vulnerabilidades y posibles amenazas que ésta pudiera causar.

- Un ejemplo de lo anterior sería:

  - Si se ha compartido un equipo que da conectividad a una oficina de dos empleados, al dejar de funcionar, sólo afectará la conectividad de dos personas, en cambio,

  - Si se ha compartido el equipo principal que da conectividad una casa matriz con sus sucursales, el impacto que se genera al dejar de funcionar es mucho mayor ya que la conectividad y por lo tanto el acceso a los recursos de toda la organización se vería afectada.



¿Cuáles son las características y condiciones de conectividad de un recurso?

La decisión de compartir recursos, ya sean hardware o software, está directamente relacionada con las políticas de seguridad que se implementarán para minimizar las vulnerabilidades y posibles amenazas que ésta pudiera causar.
Un ejemplo de lo anterior sería:

01

- Si se ha compartido un equipo que da conectividad a una oficina de dos empleados, al dejar de funcionar, sólo afectará la conectividad de dos personas, en cambio,

02

- Si se ha compartido el equipo principal que da conectividad una casa matriz con sus sucursales, el impacto que se genera al dejar de funcionar es mucho mayor ya que la conectividad y por lo tanto el acceso a los recursos de toda la organización se vería afectada.

Tipos de seguridad

Previo a hacer la clasificación de recursos compartidos en una red e **identificar la vulnerabilidad** que éste genera en la organización, es necesario entender los tipos de seguridad existentes:

Seguridad Física

Se refiere a proteger físicamente la información de posibles amenazas, por ejemplo controles de acceso, torniquetes.

Seguridad Lógica

Se refiere a proteger por medio de autorización, autenticación y registro a un sistema, además de permisos para la manipulación de la información ya sea de lectura, escritura y ejecución.

Seguridad Backup

Se refiere a proteger la información realizando respaldos, ya sean simultáneos, diarios, para así asegurar ante un incidente no perder la información.

¿Cuáles son las áreas claves que requieren medidas de protección?

- **Las vulnerabilidades** corresponden a una debilidad en un sistema que pueda transformarse en una amenaza y causar daño.

- Es importante considerar que las vulnerabilidades corresponden a **fallos físicos** y **lógicos principalmente**.

¿Cuáles son las áreas claves que requieren medidas de protección?

01

- Estos fallos pueden tener su origen en la **ubicación, instalación, configuración** y **mantenimiento de los equipos**. Estos pueden estar relacionadas con aspectos de organizativos, como por ejemplo, una definición de políticas de seguridad deficiente.

02

- **El factor humano** también es una componente importante, ya que el personal posee acceso a los recursos, y es muy común que por falta de capacitación el mismo personal, de forma accidental provoque problemas de seguridad en la organización.

Pregunta de reflexión

¿A que miembros de su familia le darían permisos para acceder a sus recursos?

¿Qué riesgos podrían haber?

¿Se puede compartir recursos a través de internet?

- Los recursos que se pueden compartir a través de **una red de área local** de igual manera pueden compartirse a través de internet, poniendo especial atención ya que internet es un medio inseguro, por lo que se recomienda utilizar una **VPN** para darle mayor seguridad a esta conexión, y poder acceder a los recursos compartidos y disminuir potenciales vulnerabilidades.

Imagen: https://userscontent2.emaze.com/images/1a8e762e-d8c7-46cc-b1e9-e1092acc24a0/866092be-244c-4331-ba8f-a7982cc93754.jpg

Identificar riesgos al compartir recursos

01

- Dadas las potenciales **vulnerabilidades de seguridad** que existen al compartir recursos, se hace necesario identificar los riesgos, y para ello se sugiere generar una matriz de riesgos.

02

- Es **importante** a la hora de generar una matriz, poseer un grupo de profesionales que tengan criterios comunes sobre el impacto que puede generar algún problema de hardware o software en la organización.

03

- **Por ejemplo**, no es lo mismo el impacto que produce el fallo de una impresora en una organización, al fallo del equipo de comunicación principal en el centro de datos de la empresa. El daño en el segundo caso es mucho más extenso y complejo.

¿Cuales son los Componentes básicos de valoración de riesgo?

El riesgo informático se evalúa en base a dos variables, estas corresponden a la **Probabilidad de amenaza** y la Magnitud de daño. La metodología más utilizada para la valoración del riesgo corresponde a la utilización de la siguiente fórmula para el análisis de riesgos:

- $\boldsymbol{Riesgo = Probabilidad\ x\ Magnitud\ de\ daño}$

Matriz de riesgo

Luego, los datos obtenidos se grafican en base al valor obtenido en riesgo alto, medio y bajo, como se observa en la figura:

- En el proceso de realización del análisis, la percepción del riesgo no es vista por todos los miembros de la organización de igual forma. Debido a ésto, se recomienda la incorporación de diferentes colaboradores de la organización para lograr un mejor resultado.

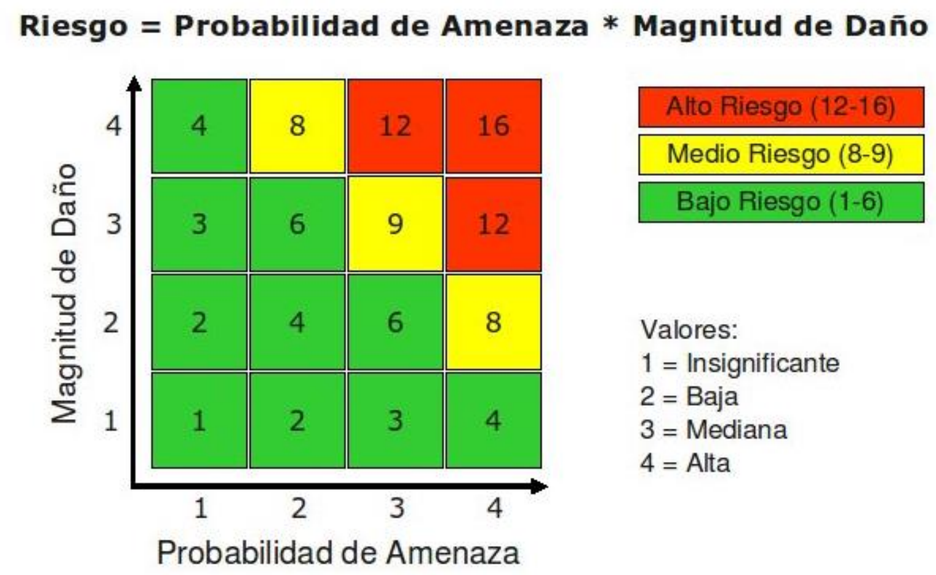


Imagen: https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

¿De qué manera pueden afectar en una empresa el impacto de riesgo?

El impacto de riesgo puede afectar directamente a las siguientes componentes del negocio:

- **Monetarios:** Se pueden ver afectados de forma directa a los ingresos de dinero a la empresa, y generar pérdidas.

- **Imagen/Reputación:** La imagen corporativa de la empresa se puede ver afectada perdiendo reputación con los clientes, por ejemplo un ataque cibernético a un banco genera desconfianza en los usuarios de dicho banco.

1. **Jurídicos/legales:** Se materializa cuando existen multas, demandas laborales, incumplimientos regulatorios, etc.

2. **Operaciones:** Operaciones de la organización se ven interrumpidas.

¿Cuál es el plan de acción ante un riesgo?

- **Los riesgos** en una organización o empresa requieren una administración, la cual tiene como objetivo principal minimizar la magnitud del daño. Para ello se necesita un enfoque reactivo o proactivo.

¿Cuáles son las formas para administrar el riesgo?

Aceptar

Evitar/Eliminar el riesgo

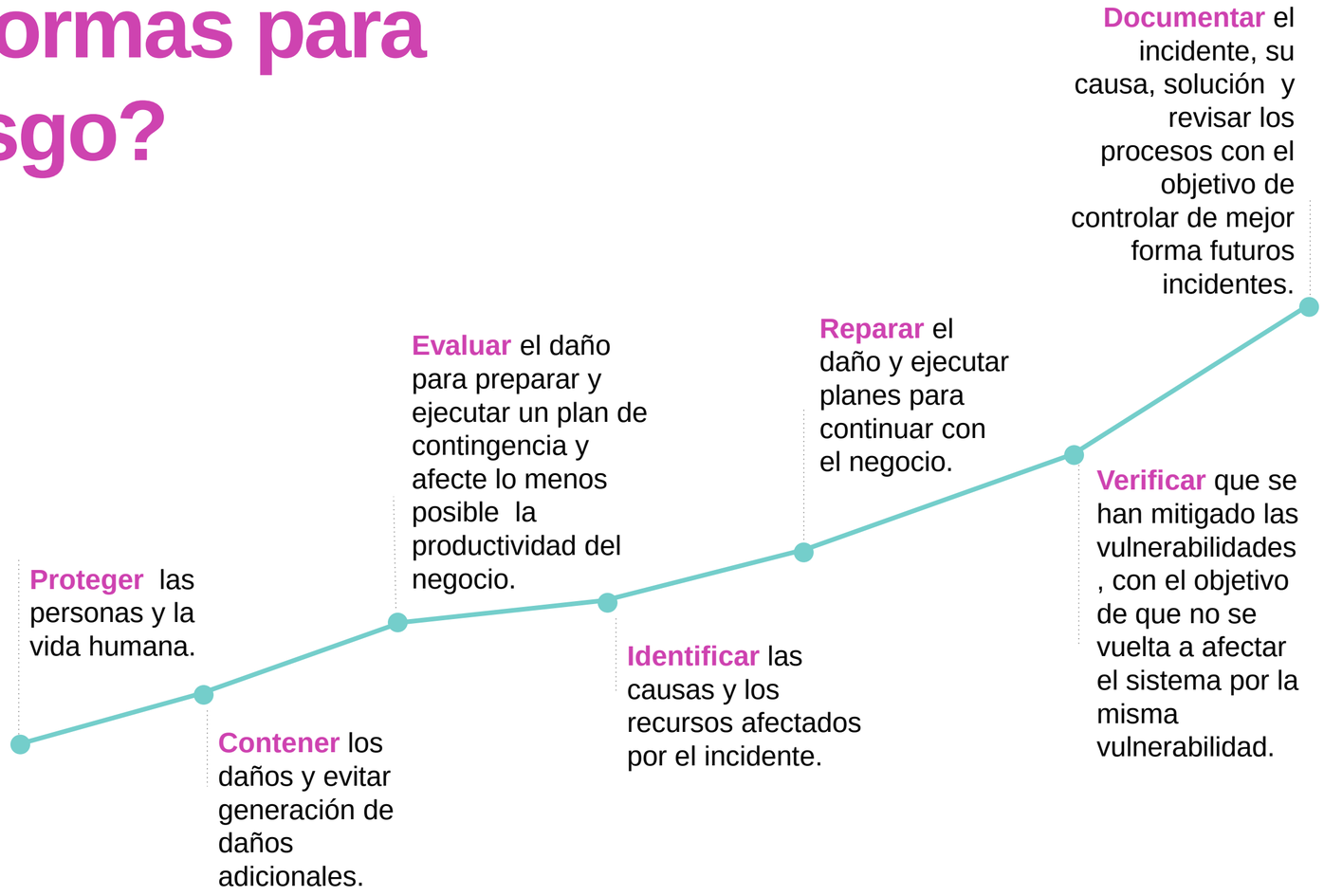
Mitigar

Tercerizar

¿Cuáles son las formas para administrar el riesgo?

1. **Aceptar**

Es esperar que se materialice el incidente para tomar una acción correctiva. Las organizaciones que realizan una respuesta ante un incidente de forma ordenada responderán de forma más eficiente al problemas. Cuando se decide enfrentar un incidente, se deben seguir los siguientes pasos:



Evitar/Eliminar el riesgo

- Significa evitar las oportunidades de riesgo. Por ejemplo, si una empresa quiere evitar la posible infección por una pendrive en la organización se toma como política de seguridad deshabilitar todos los puertos USB de los equipos.

Mitigar

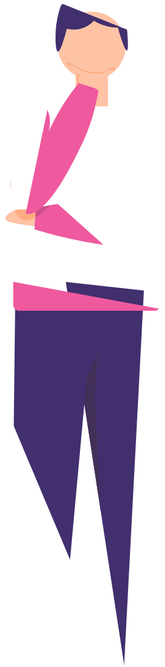
- Se busca la disminución de la probabilidad de que un incidente ocurra, o disminuir las consecuencias de éste.
- **Por ejemplo**, una empresa desea disminuir la probabilidad de infectarse por un virus, para ellos mantiene el antivirus actualizado y los parches de seguridad actualizados de los sistemas operativos.

Tercerizar

- Se busca una disminución del impacto, sin embargo esto no evade la responsabilidad, pero permite reducir los costos en caso de un incidente. Un ejemplo es la contratación de seguros.

Pregunta de reflexión

De las formas de administración de riesgo, ¿cuál es la que ustedes utilizan en su computador? ¿Por qué?



Ticket de salida

01

Seleccione 3 conceptos sobre matriz de riesgo, y en sus propias palabras explique en qué consisten.

02

Realiza dos recomendaciones:

1. Un hardware o software **que recomendarías** compartir porque implica bajo riesgo.
2. Un hardware o software que **no recomendarías** compartir por ser de alto riesgo.
3. Presenta al menos dos argumentos para apoyar tus recomendaciones.

03

¿En qué caso recomendarías tercerizar para disminuir el impacto de un daño?

Referencias

https://www.ciscopress.com/store/ccna-cyber-ops-secfnd-210-250-official-cert-guide-9781587147029

https://protejete.wordpress.com/gdr_principal/analisis_riesgo/

¿Preguntas?