**UNIVERSIDAD TECNOLÓGICA NACIONAL**

**FACULTAD REGIONAL RESISTENCIA**

Icono

Descripción generada automáticamente

**Administración de Sistemas de Información**

**Trabajo práctico 3.1: “Seguridad de SI”**

**Año:** 2025

**Profesores:**

* Claudia Alejandra Soria Ojeda
* Raúl Alejandro Montiel
* Rosina Sonia Analía Ramírez

**Integrantes:**

* Aguirre, Amilcar Nicolás
* Drose, Juan Ignacio
* Rivero, Bruno Sebastian
* Rosin, Zaira Antonella
* Sáez, Juliana
* Suarez, Tomás Alfonso

# Consignas

Suponiendo que AGUNSA cuenta con un depósito de almacenamiento en el Puerto de Barranqueras (Chaco), desarrollar los siguientes ejercicios:

i) Investigar en la W.W.W. casos de fallas de seguridad informática en organizaciones similares.

ii) Desarrollar las etapas de Administración de Riesgos, en forma completa, a fin de elaborar el esquema de seguridad informática que consideren más adecuado para la sede local de AGUNSA, sabiendo que la principal aplicación utilizada es el nuevo Sistema de Gestión de Almacenes (WMS). Las medidas deben incluir políticas de seguridad acorde. Puede tomarse como guías las líneas de actuación planteadas por la norma ISO 27002. También, para el caso de la cuarta etapa, puede tomarse como orientación general lo indicado en el artículo “Plan B: Estrategias de Contingencia”.

# Resolución

Suposiciones:

* Los almacenes utilizan sistemas locales conectados a sistemas centrales en la nube.

## i)ii) Investigación en la W.W.W y cuatro etapas del management de riesgos

### Identificación de riesgos

#### Activos vulnerables:

* + Datos de inventario.
  + Datos de los clientes.
  + Credenciales de acceso (niveles de acceso a la información por empleados).
  + Historial de movimientos realizados.
  + WMS (Sistema de Gestión de Almacenes).
  + Computadoras.
  + Red.
  + Base de datos (nube y propia).
  + Cableado de red.
  + Servidores

#### Debilidades:

* + Dispositivos personales no controlados.
  + Ausencia de protocolos claros de acceso físico y lógico.
  + Personal sin capacitación en seguridad de la información.
  + No existe un respaldo periódico de la base de datos.
  + Pobre visibilidad sobre accesos a los sistemas (falta de logs o monitoreo).
  + Dependencia de la nube

#### Amenazas:

* + Robos de información.
  + Robos de Hardware.
  + Ingeniería social.
  + Incendios.
  + Inundaciones.
  + Ransomware.
  + Virus.
  + Error del usuario.

| AMENAZAS | Físico | Lógico |
| --- | --- | --- |
| Accidental | Incendios, inundaciones. | Ingeniería social, Error del usuario. |
| Deliberada | Robos de Hardware. | Ransomware, Robos de información, Virus. |

### Análisis de riesgo

Frecuencia de pérdida= Probabilidad de agresión x Probabilidad de éxito.

Pérdida esperada = Pérdida potencial x Frecuencia de pérdida.

Probabilidades de agresión y éxito:

* + Robos de información

**Activos que afecta:** Datos de inventario, datos de clientes, historial de movimientos.

Probabilidad de agresión = 10%

Probabilidad de éxito = 30% Un trabajador deshonesto puede filtrar información confidencial si no se toman las medidas necesarias

Frecuencia de pérdida = 3% (0,30\*0,10=0,03)

Pérdida potencial = $4.500.000 porque IBM lo toma como el promedio https://www.ibm.com/reports/data-breach

Pérdida esperada = $1.500.000 ($4.500.000 \* 0,03)

* + Robos de Hardware

**Activos que afecta:** computadores, servidores, cableado de red.

Probabilidad de agresión = 5%

Probabilidad de éxito = 10%

Ya que en el almacén cuentan con cámaras de seguridad, un guardia, rejas y alarmas.

Frecuencia de pérdida = 0,005% (0,10\*0,05= 0,005)

Pérdida potencial = $2.000.000

Pérdida esperada = $10. 000 ($2.000.000 \* 0,005 ) porque un estudio de James Dertouzos afirma que el robo de hardware implica pérdidas en promedio de $20.000 para las empresas más grandes así que le bajamos un poco https://www.rand.org/content/dam/rand/pubs/monograph\_reports/2007/MR1070.pdf

* + Ingeniería social

**Activos afectados:** Base de datos, WMS.

Probabilidad de agresión = 90%

<https://www.incibe.es/ciudadania/blog/sabias-que-los-ataques-de-ingenieria-social-suponen-el-93-de-las-brechas>

Probabilidad de éxito = 5% porque tenemos empleados capaces de reconocer instancias de ingeniería social.

Frecuencia de pérdida = 4,5% (0,90\*0,05= 0,045),

Pérdida potencial = $10.000.000

Pérdida esperada = $450.000 ($10.000.000 \* 0,045)

* + Incendios

**Activos afectados:** servidores, computadores, base de datos, cableado de red

Probabilidad de agresión = 10%.

Probabilidad de éxito = 30% ya que cuentan con rociadores automáticos en el almacén.

Frecuencia de pérdida = 3% (0,10\*0,30= 0,03)

Pérdida potencial = $20.000.000 ya que afecta a toda la disposición física del depósito, afectando el registro o los terminales físicos de la base de datos, servidores y computadores asociados a los mismos, costos de inventario, etc.

Pérdida esperada = $600.000 ($20.000.000\*0,03)

* + Inundaciones

**Activos que afecta:** servidores, computadores, base de datos, cableado de red.

Probabilidad de agresión = 20% porque el almacén está cerca del río.

Probabilidad de éxito = 80% porque los activos de hardware están cerca del nivel del suelo y no se cuenta con seguro ante inundaciones.

Frecuencia de pérdida = 16% (0,20\*0,80= 0,16)

Pérdida potencial = $15.000.000

Pérdida esperada = $2.400.000 ($15.000.000 \* 0,16)

* + Ransomware

**Activos que afecta:** Datos de inventario, datos de los clientes. Historial de movimientos realizados. WMS (Sistema de Gestión de Almacenes) . Base de datos (nube y propia).

Probabilidad de agresión = 30%

Probabilidad de éxito = 70%, ya que los empleados ingresan a internet por medio de los computadores (no cuentan con protocolos de seguridad ante la navegacion web)

Frecuencia de pérdida = 21% (0.30 \* 0,70 = 0,21)

Pérdida potencial = $100.000.000

Pérdida esperada = $21.000.000 ( $100.000.000 \*0,21)

* + Virus

**Activos que afecta:** Datos de inventario, datos de los clientes. Historial de movimientos realizados. WMS (Sistema de Gestión de Almacenes) . Base de datos (nube y propia

Probabilidad de agresión = 40% debido a que en las computadoras los empleados pueden navegar por internet y utilizar dispositivos de almacenamiento externos a la empresa.

Probabilidad de éxito = 10% debido a que poseen un buen antivirus.

Frecuencia de pérdida = 4% (0,4\*0,10 = 0,04)

Pérdida potencial = 28.144 euros o $38.175.985 = $40.000.000

según <https://grupogaratu.com/perdidas-ataques-red-virus-empresas/> las perdidas en Pymes por virus es eso, podemos asumir q nuestro almacen tiene el tamaño de una pyme mas o menos

Pérdida esperada = $1.600.000($40.000.000 \* 0,04)

* + Error del usuario

**Activos que afecta:** WMS → datos de inventario, datos de los clientes

Probabilidad de agresión = 10% porque hubo una capacitación recientemente sobre el uso del sistema WMS.

Probabilidad de éxito = 50%

Frecuencia de pérdida = 5% (0,50\*0,10= 0,05)

Pérdida potencial = $2.000.000

Pérdida esperada = $100.000 ($2.000.000\*0,05)

Pérdidas de activo:

* + Datos de inventario.
  + Datos de los clientes.
  + Credenciales de acceso (niveles de acceso a la información por empleados).
  + Historial de movimientos realizados.
  + Empleados.
  + WMS (Sistema de gestión de almacenes) independiente.
  + Computadoras.
  + Red.
  + Base de datos (nube y propia).
  + Cableado de red (capaz está incluida en la red)

### Manejo del riesgo

| **Riesgo** | **Pérdida esperada** | **Estrategia genérica** |
| --- | --- | --- |
| Ransomware | $21.00.000 | Prevenir |
| Inundaciones | $2.400.000 | Transferir |
| Virus | $1.600.000 | Prevenir |
| Robos de información | $1.500.000 | Reducir |
| Incendios | $600.000 | Prevenir |
| Ingeniería social | $450.000 | Prevenir |
| Error del usuario | $100.000 | Reducir |
| Robos de hardware | $10.000 | Asumir |

| **Riesgo** | **Controles y contra medidas** | | **Línea de defensa** |
| --- | --- | --- | --- |
| Ransomware | Backups | | 3era(Recuperación) |
| Segmentación de red | | 1era(Prevención) |
| Inundaciones | Seguro | | 1era(Prevención) |
| Backups | | 3era(Recuperación) |
| Robos de información | Control del personal | | 2da(Detección) |
| Cifrar los datos | | 1era(Prevención) |
| Control de acceso a archivos vitales | | 2da(Detección) |
| Virus | Antivirus | | 1era(Prevención) |
| Filtrado de correo electrónico y web | | 2da(Detección) |
| Incendios | Prevención de incendios | | 1era(Prevención) |
| Backups | | 3era(Recuperación) |
| Ingeniería social | Capacitación | | 1era(Prevención) |
| Error del usuario | Capacitación | | 1era(Prevención) |
| Robos de hardware | Control de acceso físico | | 2da(Detección) |
| Seguimiento de activos | | 2da(Detección) |

Consecuencias primarias y secundarias (por amenaza)

* Primaria: se pierde el WMS

Políticas de seguridad:

* Las copias de seguridad se almacenarán en ubicaciones geográficamente diversas específicas y aisladas de la red de producción.
  + **Prohibitiva**: ya que se dispone específicamente las ubicaciones geográficas donde están almacenadas las copias de seguridad, todos los demás lugares se excluyen
* La infraestructura de red será segmentada en zonas lógicas (VLANs, subredes, etc.) para limitar la propagación de malware y ransomware en caso de una intrusión.
  + **Prohibitiva:** ya que especifica cómo será segmentado la infraestructura de red, todas las demás formas de segmentar la infraestructura se excluyen.
* Se mantendrán actualizados todos los sistemas operativos, aplicaciones y dispositivos de seguridad con los últimos parches y actualizaciones de seguridad.
  + **Prohibitiva:** se dispone que si o si se deben mantener siempre actualizado todos los medios de gestión de datos, sistemas, etc ya que una falta de actualización de alguno de estos medios, puede suponer una vulnerabilidad en la seguridad de los sistemas de la organización por lo tanto no pueden haber programas desactualizados.
* Los equipos de TI críticos (servidores, sistemas de almacenamiento, equipos de red) se ubicarán en soportes que los mantengan elevados del suelo.
  + **Prohibitiva:** se dispone que si o si los equipos críticos se ubicaran en soportes que los mantengan elevados del suelo para evitar que se estropeen en caso de inundaciones, sabiendo que se prohiben la otra forma de ubicación de los equipos de TI (suelo)
* Se instalarán sistemas de detección de agua y humedad en las áreas críticas donde se encuentran los activos de información, con alertas que notifiquen al personal responsable inmediatamente.
  + **Prohibitiva:** ya que se dispone específicamente es decir obligatoriamente que se instalarán sistemas en las áreas críticas por lo cual no se contará con ningún área sin sistema de detección de agua y humedad.
* Se contratarán y mantendrán pólizas de seguro adecuadas que cubran los daños a la infraestructura de TI y la interrupción del negocio resultantes de eventos como inundacione
* s.
  + **Permisiva:** Impone el uso de pólizas de seguro para proteger las TI, por lo cual no puede haber un solo equipo de TI sin seguro.
* Se proporcionará capacitación regular sobre la importancia de la protección de la información, las políticas de seguridad y las consecuencias de la divulgación no autorizada.
  + **Permisiva:** Medida formativa, no impone restricciones.
* La información sensible y confidencial debe ser cifrada tanto en tránsito como en reposo.
  + **Prohibitiva:** Prohíbe que la información sensible quede vulnerable.
* Se mantendrá un registro de los accesos a archivos y sistemas vitales, y se realizarán auditorías periódicas de los permisos de acceso.
  + **Permisiva:** Controla el acceso, no lo impide.
* Se programarán escaneos completos periódicos en todos los sistemas (detección de virus).
  + **Permisiva:** Control reactivo que no limita al usuario.
* Se implementarán soluciones de filtrado de correo electrónico para detectar y bloquear adjuntos maliciosos, enlaces a sitios web peligrosos y correos de phishing.
  + **Prohibitiva:** Solo se admiten los correos limpios, los demás se bloquean.
* Se implementarán y mantendrán sistemas de detección de incendios (detectores de humo, calor) en todas las áreas sensibles y centros de datos.
  + **Permisiva:** Medida de protección a la infraestructura, no restringe conductas.
* Los sistemas de alimentación eléctrica y aire acondicionado en los centros de datos deben ser revisados y mantenidos regularmente para prevenir sobrecargas y fallas que puedan causar incendios.
  + **Permisiva:** Asegura continuidad operativa, no prohíbe acciones.
* Se monitorizan las actividades de los usuarios y se realizan auditorías para identificar patrones de errores recurrentes y tomar medidas correctivas o de capacitación adicional.
  + **Permisiva:** Supervisa errores, pero no indica limitaciones estrictas.
* Se implementarán y mantendrán controles de acceso físico robustos en todas las instalaciones de la organización, incluyendo cerraduras, tarjetas de acceso, sistemas biométricos y guardias de seguridad, según el nivel de riesgo.
  + **Prohibitiva:** Acceso solo a personas autorizadas, las demás no pueden ingresar.
* El hardware crítico (servidores, equipos de red) debe ubicarse en salas de servidores o centros de datos con acceso restringido.
  + **Prohibitiva:** Indica una única ubicación válida.

### Plan de contingencia

Hay tres tipos de interrupciones:

* Catástrofe: destrucción de instalaciones y sus componentes físicos.
* Desastre: interrupciones durante más de un día.
* No desastre: interrupciones breves por fallas que deben corregirse inmediatamente.

Riesgos:

* Robo de información - Desastre
* Incendio - Catástrofe
* Inundación - Catástrofe
* Ransomware - Desastre
* Robo de HW - Desastre
* Ingeniería social - No desastre
* Error del usuario - No desastre
* Virus - No desastre

#### Riesgos - Priorización según tolerancia

| Prioridad | Riesgo | Justificación | Acciones de recuperación |
| --- | --- | --- | --- |
| Crítico | Robo de información | Constituye uno de los activos más valiosos para la empresa, afecta directamente a la competitividad, la confianza tanto con el cliente, proveedores y comerciales como así también la ventaja operativa, además de que su filtración y manipulación representa un incumplimiento legal. | Restauración de versiones  Revocar accesos y forzar cambios de credenciales  Notificar usuarios afectados |
| Crítico | Incendio | Compromete la integridad de la infraestructura física, como también es un riesgo para el personal, puede provocar una interrupción total del sistema de manera prolongada por lo que el negocio no puede operar sin una recuperación rápida. | Solicitar cobertura  Evaluar daños y recuperar equipos rescatables  Evaluar sitio alternativo |
| Crítico | Inundación | El depósito se encuentra cerca del río, por lo que la probabilidad de ocurrencia aumenta, se compromete la integridad de la infraestructura física debido a que los activos críticos están expuestos directamente lo que requiere una recuperación inmediata. | Solicitar cobertura  Evaluar daños y recuperar equipos rescatables  Evaluar sitio alternativo |
| Crítico | Ransomware | Paraliza las operaciones, dado que Agunsa depende del sistema WMS, para la trazabilidad del inventario y el movimiento de cargas, una interrupción prolongada afectaría tanto a la logística como al servicio al cliente. | Aislar equipos afectados  Restaurar copias de seguridad aisladas  Forzar cambio de credenciales de los usuarios |
| Vital | Robo de HW | La pérdida de equipos físicos representa un estado de alerta pero no paraliza completamente el negocio si existen backups HW de reemplazo. | Activar controles físicos y revisar cámaras  Reemplazar por equipos provisorios |
| Vital | Ingeniería social | No genera un daño directo pero es la vía de acceso a amenazas mayores, su impacto depende de la interacción del personal y su recuperación no requiere medidas técnicas complejas. | Evaluar usuarios afectados y bloquear accesos  Reforzar capacitación  Restaurar datos desde backup |
| Sensible | Error del usuario | Puede afectar la calidad de los datos pero generalmente son identificables a corto plazo, no compromete infraestructura ni paraliza procesos. | Identificar error  Reforzar capacitación  Implementar validaciones adicionales  Restaurar datos desde backup |
| Sensible | Virus | Puede afectar al rendimiento o integridad del sistema, pero las medidas periódicas pueden controlar el daño y su propagación. | Ejecutar escaneo completo  Aislar sistemas comprometidos  Restauración de versiones  Revisar y aplicar actualizaciones |

* el equipo de marain considero que no es lo mismo perder los datos de los paquetes que perder los datos de los clientes, ya que no genera el mismo valor en términos monetarios
* las empresas suelen proveer reportes de ransomware? de todos las amenazas supus, dijo rosina que podemos encontrar informes
* llevar al límite las situaciones hipotéticas para poder prevenir y generar medidas para las situaciones reales