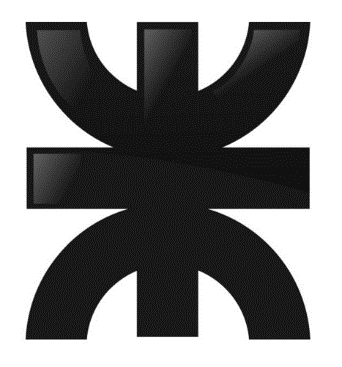
**TRABAJO PRACTICO N° 2**

**SEGURIDAD INFORMATICA**



Mariano Cerusico leg 21826

Carlos Bermúdez leg 20110

Cesar Paz leg 29247

Comisión: 3k3 Año: 2021

# Encuentre el coeficiente PPPI(Pérdida Potencial Por Incidencia), en el siguiente cuadro de Análisis de Riesgos y Exprese la Tabla en Orden decreciente en base a dicho coeficiente, que se calcula de la siguiente manera:

**P.P.P.I. = (FACTOR DE RIESGOS \* PERDIDA POTENCIAL)/ 1.000**

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgos** | **Factor de Riesgos** | **Perdida Potencial** | **PPPI** |
| Caída del Sistema | 1 | $15.000 | 15 |
| Sustracción de Información | 2 | $30.000 | 60 |
| Borrar información | 1 | $10.000 | 10 |
| Errores de Carga de Datos | 5 | $10.000 | 50 |
| Perdida de Documentación | 1 | $40.000 | 40 |
| Mala Aireación | 2 | $5.000 | 10 |
| Falla en la conectividad de la Red Informática | 2 | $10.000 | 20 |
| Fallas en los formularios y documentación administrada | 2 | $10.000 | 20 |
| Multas Vencimiento de licencias | 4 | $5.000 | 20 |

# En la Tabla del Ejemplo anterior, enumere medidas tendientes a minimiza o evitar los Riesgos analizados.

|  |  |  |
| --- | --- | --- |
| **Riesgos** | **PPPI** | **Contramedidas Alternativas** |
| Errores de Carga de Datos | 50 | Realizar una validación de datos y/o confirmación |
| Multas Vencimiento de licencias | 20 | Activar o instalar un sistema que nos indique los vencimientos próximos. Como estrategias de prevención. |
| Sustracción de Información | 60 | Plantear sistemas de recuperación, o instalar sistemas de copias de seguridad |
| Falla en la conectividad de la Red Informática | 20 | Buscar y tratar de cambiar de red realizar un estudio en donde nos permita realizar las mejoras de la red. |
| Fallas en los formularios y documentación administrada | 20 | Presentar un sistema de recuperación donde tenga incorporado, copias de seguridad. |
| Mala Aireación | 10 | Buscar la forma de mejorar la aireación buscando por el lado de la parte edilicia. Si por ese lado se presenta imposible la solución. Buscar de mejorar el sistema de ventilación o fuentes de ventilación alternativas. |
| Perdida de Documentación | 40 | Aplicar sistemas de recuperación o imponer copias de seguridad. Aplicar sistemas alternativos de recuperación geográficamente separados y protegidos. |
| Caída del Sistema | 15 | Aplicar sistemas de recuperación o imponer copias de seguridad. Aplicar sistemas alternativos de recuperación geográficamente separados y protegidos |
| Borrar información | 10 | Aplicar sistemas de recuperación o imponer copias de seguridad. Aplicar sistemas alternativos de recuperación geográficamente separados y protegidos |

# Enumere para cada incidencia siguiente, por lo menos tres contramedidas tendientes a anularlos o minimizar sus consecuencias

### Fallas en los Sistemas Informáticos desarrollados por el Área Informática

a) Revisión de registros de fallas para garantizar que las mismas fueron resueltas

Satisfactoriamente.

b) Revisión de medidas correctivas para garantizar que los controles no fueron comprometidos, y que las medidas tomadas fueron autorizadas.

c) Documentación de la falla con el objeto de prevenir su repetición o facilitar su resolución en caso de reincidencia.

#### Fallas en el tendido de comunicación coaxial de la Red Informática

a) Establecer los procedimientos para la administración del equipamiento remoto, incluyendo los equipos en las áreas usuarias, la que será llevada a cabo por el responsable establecido en el punto “Asignación de Responsabilidades en Materia de Seguridad de la Información”.

b) Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas.

c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

El Responsable del Área Informática implementará dichos controles.

##### Fallas en los soportes magnéticos de información.

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por el Organismo.

b) Requerir autorización para retirar cualquier medio del Organismo y realizar un control de todos los retiros a fin de mantener un registro de auditoría.

c) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

Se documentarán todos los procedimientos y niveles de autorización.

##### Fallas detectadas en Archivos de Datos Producidas por Fraude.

1. Revisar y proponer a la máxima autoridad del Organismo para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
2. Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
3. Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.
4. Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
5. Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
6. Garantizar que la seguridad sea parte del proceso de planificación de la información.
7. Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.