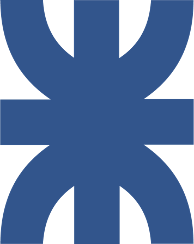
**UNIVERSIDAD TECNOLÓGICA NACIONAL**

**FACULTAD REGIONAL RESISTENCIA**



**TP 6.1 (Ej. 4) - “Seguridad de SI”**

* **Asignatura:** Administración de Recursos – Integradora del 4to nivel

* **Cátedra:** Ing. Claudia A. SORIA OJEDA – Profesora Titular

Ing. Rosina RAMIREZ – Jefe de Trabajos Prácticos

Ing. Jorge ROA – Auxiliar Docente de 1ra

**Integrantes:**

* Budzovsky, Gerardo
* Cuevas, Rodrigo
* Diaz Duarte, Nicolas
* Nadal, Alejandro
* Rouvier, Selene Susana
* Silva, Otto

**Carrera:** Ingeniería en Sistemas de Información

**Año:** 2020

**Aclaración**: Todo lo que está tachado, son cosas que cambiamos con respecto al envío anterior. Existen secciones (entre ellas, las políticas del

**4.** Desarrollar, de manera específica y ajustada al escenario, las diferentes etapas de Administración de Riesgos, a fin de elaborar el esquema de seguridad que considere más adecuado para el PODER JUDICIAL DE CHILE, incluyendo la redacción de las políticas de seguridad que correspondan, basándose en las líneas de actuación planteadas por la norma ISO 27002. (Puede tomarse como lineamiento general lo indicado en el artículo ***“Plan B: Estrategias de Contingencia”*** )

**Suposiciones:**

* La configuración del firewall no es la correcta
* El PJCH no tiene sus sistemas operativos actualizados a las últimas versiones.
* El firmware de los routers del PJCH no es actualizable
* Se posee equipos de trabajo desactualizado y con fallas
* El PJCH se encuentra en una zona de actividad sísmica.
* El PJCH no ha redactado protocolos claros de manejo de información confidencial de las causas.
* El PJCH tiene backups de respaldo de datos distribuidos geográficamente.

Etapas de Administración de Riesgos:

**Etapa 1 - Identificación del Riesgo**

Activos Vulnerables:

1. PCs y terminales de trabajo
2. Redes de información (Hardware y Software)
3. Software interno del PJCH (sw contable, sistemas de manejo de archivos, sistema de registro, entre otros)
4. Software para ofrecer servicios externos del PJCH (abogados, peritos, acusados, fiscales, etc.)
5. Hardware de los servidores
6. Información de causas, sentencias y documentación relevante para el PJCH.
7. Datos operativos en general, es decir, información que requiere el PJCH para funcionar ej. planillas de cobros, registros de empleados, registros contables, etc.

Vulnerabilidades**:**

* 1. Falta de políticas y reglas claras al momento de manejar información sensible de las causas y procesos judiciales.
  2. Falla en la seguridad de los software que podría ser usada para filtrar datos sensibles
  3. Falta de medios de recuperación que permitan al PJCH disponer la replicación de los sistemas
  4. Falta de capacitación técnica de los empleados ~~para operar de forma segura en internet~~.
  5. Falta de las últimas actualizaciones de seguridad en los sistemas operativos
  6. Falta de procedimiento (o dificultad) de actualización de firmware en algunos routers del PJCH.
  7. Falta de planificación para renovar los equipos
  8. Falta de protección física de los servidores.

Amenazas:

1. Errores en la configuración en el SW o HW de los equipos empleados.
2. Evento catastrófico que afecte a la infraestructura de IS del PJCH (terremoto, tsunami, inundación, volcán)
3. ~~Fallas en los equipos causados~~ Ataques por nuevos Virus, Ransomwares y Malwares en los equipos
4. Espionaje que afecte a la información sensible del PJCH
5. Ciberespionaje que afecte a la información del PJCH
6. Fuga de información accidental debido a un error por parte de los empleados

Riesgos:

* Probabilidad de ataques por nuevos virus, ramsomwares y malwares en los equipos que extraiga Información de causas, sentencias y documentación relevante para el PJCH debido a la falta de actualización en los sistemas operativos, software de protección desactualizados o por falta de capacitación de los empleados sobre cómo operar de forma segura en internet*.*
* Probabilidad de ataques por nuevos virus, ramsomwares y malwares en los equipos que afecte el software interno y el software para ofrecer servicios externos del PJCH debido a la falta de actualización en los sistemas operativos, software de protección desactualizados o por falta de capacitación de los empleados sobre cómo operar de forma segura en internet*.*
* Probabilidad de fuga de información de las causas, sentencias y documentación relevante para el PJCH accidental por parte de los empleados debido a la falta de reglas y políticas claras al momento de manejar la información sensible referida a los casos y procesos judiciales.
* Probabilidad de ciberespionaje que extraiga Información de causas, sentencias y documentación relevante para el PJCH debido a falla en la seguridad de los software
* Probabilidad de que la infraestructura de IS del PJCH se vea afectada por eventos catastróficos debido a faltas de medios de recuperación que permitan replicarlos no permitiendo la disponibilidad de información de causas, sentencias y documentación relevante para el PJCH.
* Probabilidad de que la infraestructura de IS del PJCH se vea afectada por eventos catastróficos, debido a la falta de protección física de los servidores, dañandolos.
* Probabilidad de errores en la configuración en el SW o HW que afecte PCs, terminales de trabajo y redes debido a falta de capacitación técnica de empleados
* Probabilidad de espionaje que extraiga datos operativos en general debido a la falta políticas y reglas claras al momento de manejar información sensible de las causas y procesos judiciales. listo

**Etapa 2 - Análisis del Riesgo**

Una vez determinados los posibles riesgos, los listamos en la siguiente tabla, analizando sus posibles consecuencias y las pérdidas potenciales en términos de activos, que podrían generar.

**Aclaración:**

* Pérdida potencial de SW: Se requiere instalación del SW y durante este tiempo, las transacciones que estos realizan se verán interrumpidas, lo que conlleva a que los procesos y funciones de negocio se vean interrumpidas.
* El PJCH cuenta, en el 2020, con 12513 personas contratadas. [[1]](#footnote-0)

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | **Pérdida Potencial** | **Consecuencias primarias** | **Consecuencias secundarias** |
| Probabilidad de ataques por nuevos virus, ransomwares y malwares en los equipos que extraiga Información de causas, sentencias y documentación relevante para el PJCH debido a la falta de actualización en los sistemas operativos, software de protección desactualizados o por falta de capacitación de los empleados sobre cómo operar de forma segura en internet. | -PC  -Servidores  -Datos de las causas  -Datos operativos | -Retraso en las operaciones llevadas a cabo en la organización  -Horas de trabajo interrumpidas de los empleados | -Perdida de horas trabajadas de los empleados  -Retrasos en los procesos judiciales programados |
| Probabilidad de ataques por nuevos virus, ransomwares y malwares en los equipos que afecte el software interno y el software para ofrecer servicios externos del PJCH debido a la falta de actualización en los sistemas operativos, software de protección desactualizados o por falta de capacitación de los empleados sobre cómo operar de forma segura en internet. | Software interno del PJCH (sw contable, sistemas de manejo de archivos, sistema de registro, entre otros)  Software para ofrecer servicios externos del PJCH (abogados, peritos, acusados, fiscales, etc.) | -Retraso en las operaciones llevadas a cabo en la organización  -Horas de trabajo interrumpidas de los empleados | -Perdida de horas trabajadas de los empleados  -Retrasos en los procesos judiciales programados |
| Probabilidad de fuga de información de las causas, sentencias y documentación relevante para el PJCH accidental por parte de los empleados debido a la falta de reglas y políticas claras al momento de manejar la información sensible referida a los casos y procesos judiciales. | -Confidencialidad de los datos de las causas | -Pérdida de confianza de los ciudadanos  -Posibles daños a la imagen de los ciudadanos implicados. | -Demandas judiciales por parte de los ciudadanos |
| Probabilidad de ciberespionaje que extraiga Información de causas, sentencias y documentación relevante para el PJCH debido a falla en la seguridad de los software. | -Confidencialidad de los datos de las causas | -Pérdida de confianza de los ciudadanos  -Posibles daños a la imagen de los ciudadanos implicados.  -Interrupción en los servicios brindados  -Horas de trabajo interrumpidas de los empleados | -Demandas judiciales de los ciudadanos al exponer información sensible |
| Probabilidad de que la infraestructura de IS del PJCH se vea afectada por eventos catastróficos debido a faltas de medios de recuperación que permitan replicarlos no permitiendo la disponibilidad de información de causas, sentencias y documentación relevante para el PJCH. | -Datos de las causas  -Datos operativos  -PCs y terminales de trabajo  -Software | -Interrupción en los servicios brindados  -Reparación de los equipos con daño parcial  -Provisión de nuevo equipo de HW.  -Pérdida de disponibilidad de datos.  -Horas de trabajo interrumpidas de los empleados | -Retraso de entrega de trabajos pendientes  -Retrasos en los procesos judiciales programados  -Carga excesiva en el área de mantenimiento. |
| Probabilidad de que la infraestructura de IS del PJCH se vea afectada por eventos catastróficos, debido a la falta de protección física de los servidores, dañandolos. | -Hardware de los servidores  -Hardware de redes  -PCs y terminales de trabajo  -Redes de Información | -Pérdida de disponibilidad de datos.  -Interrupción en los servicios brindados  -Provisión de los nuevos equipos necesarios  -Horas de trabajo interrumpidas de los empleados | -Carga excesiva en el área de mantenimiento.  -Pérdida en la integridad y confiabilidad de los datos. |
| Probabilidad de errores en la configuración en el SW o HW que afecte PCs ,terminales de trabajo y redes debido a falta de capacitación técnica de empleados | -Hardware de los servidores  -Hardware de redes  -PCs y terminales de trabajo | -Pérdida de disponibilidad de datos.  -Interrupción en los servicios brindados | -Carga excesiva en el área de mantenimiento. |
| Probabilidad de espionaje que extraiga datos operativos en general debido a la falta políticas y reglas claras al momento de manejar información sensible de las causas y procesos judiciales. | -Confidencialidad de los datos de las causas | -Pérdida de confianza de los ciudadanos  -Posibles daños a la imagen de los ciudadanos implicados. | -Demandas judiciales de los ciudadanos al exponer información sensible |

Luego, en esta tabla, se establece el valor de los activos que pueden perderse debido a los riesgos. Recordar que no siempre se puede establecer un valor exacto, puesto que el valor de la información depende de un gran conjunto de atributos y de las políticas de la organización en materia de balance de costo-beneficio de la información. Los responsables deben establecer un criterio de manera racional para determinar estos valores.

**Suposiciones:**

Cuando ocurre una interrupción de la actividad, solo ocurre para el 10% de los empleados. Una correlación de esto con la estructura del PJCH es que una de estas problemáticas ocurra en un área, o en un jurisdiccion. [[2]](#footnote-1)

En promedio, la actividad se recupera, al menos parcialmente, en un día.

Los desastres naturales ocurren en una sola jurisdicción a la vez.

**Aclaraciones**

Los montos están en dólares estadounidenses.

Se hizo un promedio de las demandas al estado chileno por daños y perjuicios. La cifra demandada fue, en promedio, de 18815 dólares. Esta cifra varía enormemente dependiendo del caso y situación particular. [[3]](#footnote-2) La cantidad de juicios se hizo viendo la cantidad de juicios ocurridos por fuga de información del año anterior.

El cálculo del registro de procesos judiciales y el software se hace teniendo en cuenta lo siguiente. El personal de mantenimiento deberá trabajar arduamente para restaurar lo perdido en el transcurso de un día. Para ello, trabajarán sus ocho horas normales más 4 horas extra. Solo contamos el monto de las horas extra, asumiendo 25 empleados en promedio.

El hardware de redes tenido en cuenta son switches marca Cisco. Consideramos que debido a la capacidad de los mismos, cada jurisdicción no tendrá más de dos (estos equipos son modulares y pueden tener más de 200 conexiones.

|  |  |  |  |
| --- | --- | --- | --- |
| **Elementos amenazados** | **Cantidad** | **Valor Unitario del elemento** | **Monto total** |
| PC | 1251 | $ 200 | $ 250.200 |
| Horas de trabajo interrumpidas de los empleados | 8hs \* 1251empleados = 10008hs | $ 3,5 | $ 35.028 |
| Hardware de los servidores | 2 | $ 1.945 | $ 3.890 |
| Hardware de redes | 2 | $ 2.100 | $ 4.200 |
| Registros de procesos judiciales  Software | (4 hs extra) \* 25empleados = 100hs | $ 7 | $ 700 |
| Confidencialidad de los datos de las causas | 5 juicios | $18.815 | $ 94.075 |
| **Total** | | $ 23.070,5 | $ 338.093 |

Finalmente, con esta tabla de costos, queda determinar la frecuencia de las amenazas, su frecuencia de éxito, e intentar determinar cuánto valor podría perderse a causa de las amenazas.

**Pérdida esperada = Pérdida Potencial \* Frecuencia de pérdida**

**Frecuencia de pérdida = Probabilidad agresión \* Probabilidad de éxito.**

Las probabilidades son estimadas a partir de suposiciones y eventos históricos, en base a un año.

Rango de probabilidad:

**Bajo: 0% a 25%**

**Medio: 26% a 50%**

**Alto: 51% a 80%**

**Muy Alta: 81% a 100%**

Abreviaciones:

**B**: Baja

**M**: Media

**A**: Alta

**A+**: Muy Alta

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Riesgos** | **Probabilidad de agresión** | | **Probabilidad de éxito** | | **Frecuencia de la pérdida** | **Pérdida potencial** | **Pérdida esperada** |
| Probabilidad de errores en la configuración en el SW o HW que afecte PCs ,terminales de trabajo y redes debido a falta de capacitación técnica de empleados. | A | 70% | M | 34%[[4]](#footnote-3) | 24% | $ 700 +  $ 35.028  =  $ 35.728 | $ 8.574,72 |
| Probabilidad de que la infraestructura de IS del PJCH se vea afectada por eventos catastróficos debido a faltas de medios de recuperación que permitan replicarlos no permitiendo la disponibilidad de información de causas, sentencias y documentación relevante para el PJCH. | A | 75% | B | 10% | 7.5% | $ 700 +  $ 3.890 +  $ 35.028 +  $ 250.200  =  $ 29.4018 | $ 22.051,35 |
| Probabilidad de que la infraestructura de IS del PJCH se vea afectada por eventos catastróficos, debido a la falta de protección física de los servidores, dañandolos. | A | 75% | B | 10% | 7.5% | $4200 + 3890 = 8090 | $606.75 |
| Probabilidad de ataques por nuevos virus, ransomwares y malwares en los equipos que extraiga Información de causas, sentencias y documentación relevante para el PJCH debido a la falta de actualización en los sistemas operativos, software de protección desactualizados o por falta de capacitación de los empleados sobre cómo operar de forma segura en internet. | B | 20% | A | 73%[[5]](#footnote-4) | 15% | $ 35.028 +  $ 700  +  94075  =  $ 129775 | $ 19.466.25 |
| Probabilidad de espionaje que extraiga datos operativos en general debido a la falta políticas y reglas claras al momento de manejar información sensible de las causas y procesos judiciales. | B | 20% | A | 75% | 15% | $ 94.075 | $ 14.111,25 |
| Probabilidad de ciberespionaje que extraiga Información de causas, sentencias y documentación relevante para el PJCH debido a falla en la seguridad de los software. | M | 35%[[6]](#footnote-5) | A | 80%[[7]](#footnote-6) | 28% | $ 94.075 +  $ 35.028  =  $ 129.103 | $ 36.148,84 |
| Probabilidad de fuga de información de las causas, sentencias y documentación relevante para el PJCH accidental por parte de los empleados debido a la falta de reglas y políticas claras al momento de manejar la información sensible referida a los casos y procesos judiciales. | M | 35% | B | 18% | 6.3% | $ 94.075 | $14.111,25 |
| Probabilidad de ataques por nuevos virus, ransomwares y malwares en los equipos que afecte el software interno y el software para ofrecer servicios externos del PJCH debido a la falta de actualización en los sistemas operativos, software de protección desactualizados o por falta de capacitación de los empleados sobre cómo operar de forma segura en internet. | B | 20% | A | 73%[[8]](#footnote-7) | 15% | $700  +  $ 35.028  =  $ 35.728 | $5359,2 |

El riesgo, definido en dólares, para el poder judicial, durante un año, es de 100356,61 dólares. Este es el monto que podría perderse por los diversas amenazas existentes y debe tenerse en cuenta al momento de planificar el presupuesto anual.

**Etapa 3 - Manejo del Riesgo**

**Políticas de seguridad**:

* La creación de usuarios y asignación de los permisos se realizará únicamente por el jefe de seguridad.
* ~~Los usuarios de las computadoras del PJCH, en sus diversas áreas, no poseerán acceso de administrador en sus sesiones, lo cual impedirá la instalación de software no autorizado por el DIC.~~
* Solo el jefe de seguridad tendrá acceso de administrador en las computadoras del PJCH, lo cual impedirá que otros usuarios instalen software no autorizado por el DIC
* ~~Si los usuarios requieren de algún SW no instalado por el DIC en las computadoras, deberán mandar una solicitud al DIC, aclarando el motivo y el programa en cuestión.~~
* Solo el DIC podrá instalar SW en los equipos del PJCH. Cualquier necesidad del nuevo SW deberá ser reportada al DIC y este llevará a cabo la instalación después de determinar su seguridad.
* El Jefe de seguridad será el único encargado de realizar semanalmente la actualización de software de detección y reparación de software malicioso en las PCs y terminales de trabajo.
* Toda la información relacionada a las causas o interna del PJCH deberá tener múltiples backup distribuidos geográficamente. *(permisiva)*
* La información relacionada a las causas y sus respectivos backup deberá estar encriptada. *(permisiva)*
* Toda persona que ingrese al PJCH recibirá un usuario para los sistemas, con un rol determinado y permisos asociados a dicho rol.
* El rol y sus permisos solo incluyen acceso a la información necesaria para el cumplimiento de las funciones del cargo.
* ~~Existirá una clasificación de la información de acuerdo a su nivel de confidencialidad, y los accesos a la misma se darán en base a roles con permisos que los usuarios de los sistemas recibirán al momento de ingresar al PJC~~H.
* Al momento de que un miembro del PJCH abandone el poder judicial, se deberá informar al DIC para eliminar el usuario del miembro en el sistema, o incluso bloquear temporalmente al usuario cuando el mismo se encuentre fuera del trabajo. (*permisiva)*
* *Cualquier empleado que abandone el PJCH, deberá informar al DIC para eliminar su usuario automáticamente y bloquearlo temporalmente. (phohibitivo)*
* En caso de observar violaciones de seguridad se deberá notificar inmediatamente al jefe de seguridad correspondiente, y existirá un canal anónimo para tal fin. *(permisiva)*
* *Las contraseñas de cualquier rol que otorgue accesos al sistema, deberá tener al menos 8 caracteres y renovarse cada cierto periodo de tiempo. (prohibitiva)*
* Cada acceso a información debe estar registrado con usuario, fecha y hora, para poder rastrear el uso de la misma en futuras auditorías. (prohibitiva)
* Todos los los servidores y las zonas de backup deberán estar en salas con control ambiental, minimizando el daño por agua, polvo, humedad, calor, etc. Las cuales deberán ser resistentes a la mayor cantidad de catástrofes posibles (antisísmicas, ignífugas, difícilmente inundables, etc). (prohibitiva)
* *Las áreas que contengan información sensible o crítica tendrán perímetros de seguridad*
* Toda jurisdicción deberá hacer un seguimiento de las condiciones meteorológicas de su área.
* Ninguna jurisdicción podrá no declarar estado de emergencia bajo condiciones de amenazas meteorológicas.
* Una persona podrá integrarse al PJCH solamente tras pasar por un intenso chequeo de sus antecedentes penales, información crediticia personal y sus certificaciones.
* *En el PJCH se permitirán únicamente equipos que puedan correr los últimos sistemas operativos y/o firmware del mercado. (prohibitiva)*

**Riesgo**: Probabilidad de fallas en los equipos causadas por diversos malwares debido a la falta de actualización en los sistemas operativos, software de protección desactualizados o por falta de capacitación de los empleados sobre cómo operar de forma segura en internet*.*

Contramedidas:

**Primera línea de defensa (prevención)**

Los sistemas operativos se actualizan ni bien el fabricante libere una nueva actualización

Diariamente se controlará que los sistemas de detección y antivirus estén activados y actualizados

El DIC instalará todo el software necesario para las funciones y procesos de negocio de cada área, los usuarios no podrán instalar software. Si necesitan algún nuevo SW, deberán solicitarlo al DIC.

Se instruirá a los empleados del PJCH respecto de los riesgos acarreados al abrir correos provenientes de fuentes desconocidas o acceder a sitios no seguros.

Las redes de intranet del PJCH tendrán firewall instalados, bloqueando todos los puertos salvo aquellos necesarios para el funcionamiento de los protocolos de comunicación entre los equipos.

**Segunda línea de defensa (detección)**

Diariamente se ejecutarán análisis automáticos de virus en background para no interrumpir las tareas de los usuarios.

**Tercera línea de defensa (recuperación)**

En caso de que los equipos fallen a causa de un malware, se procederá a formatear el sistema, reinstalar el sistema operativo y realizar la recuperación de los datos mediante los backups realizados semanalmente, junto a los backups incrementales, que se realizarán diariamente.

En caso de que en el equipo haya algunos archivos que sean del dia de la deteccion de infeccion, personal del DIC aplicará un proceso avanzado de recuperación para garantizar la no infección de los mismos y luego aplicará las medidas normales antes mencionadas.

**Riesgo:** Fuga de información accidental por parte de los empleados debido a la falta de reglas y políticas claras al momento de manejar la información sensible referida a los casos y procesos judiciales.

Contramedidas:

**Primera línea de defensa (prevención)**

Antes de enviar un correo electrónico, el sistema mostrará un aviso de confirmación donde se mostrará el mail del destinatario, para evitar envíos a direcciones equivocadas. También podrá deshacer el envío durante 1 minuto.

No se podrá ingresar con memorias usb propias (tarjetas SD, pendrives), a las instalaciones. En las instalaciones, habrá numerosos pendrives para mover información entre las computadoras de trabajo. Estos pendrive tendrán SW que registrara su uso y dejará registros de cada movimiento realizado. Si este SW es eliminado del pendrive, las computadoras darán una alerta al DIC al momento de intentar usarlo.

**Segunda línea de defensa (detección)**

En las auditorías, se revisarán los correos para comprobar los destinatarios y así descubrir posibles fugas accidentales de información, analizando usuarios, fecha y hora, e información enviada.

**Tercera línea de defensa (recuperación)**

En el caso de que la fuga se haya dado a una persona o un grupo reducido de personas, un representante del PJCH conversará con los mismos y se les solicitará firmar un acuerdo de confidencialidad sobre la información adquirida. Se lanzará una auditoría para rastrear el camino de la información y detectar la causa. Dependiendo de la causa se aplicarán las soluciones o medidas pertinentes.

**Riesgo:** Probabilidad de que la infraestructura de IS del PJCH se vea afectada por eventos catastróficos debido a faltas de medios de recuperación que permitan replicarlos.

**Contramedidas:**

**Primera línea de defensa (prevención)**

Las regiones de cada jurisdicción harán seguimiento meteorológico, para detectar condiciones climáticas adversas, como ser frentes de tormenta severos y/o incendios forestales cuando los centros de manejo de información están en zonas no urbanas.

**Segunda línea de defensa (detección)**

En la sala, habrá sensores que detectarán fenómenos como incendios, elevados niveles de monóxido de carbono, humedad, etc. Al detectar estas amenazas, sonará una alarma específica, notificando al DIC.

En caso de detectar eventos meteorológicos graves, las salas de los servidores/backup podrán cerrarse de forma hermética.

**Tercera línea de defensa (recuperación)**

Se iniciará la recuperación de los backup existentes, la reparación de los equipos con daño parcial, se iniciaran procesos de provisión para los equipos completamente dañados, y se reinstalan los sistemas operativos en los equipos reparados si es necesario.

**Riesgo:** Probabilidad de ciberespionaje con intenciones de fugar información sensible.

**Primera línea de defensa (prevención)**

Los sistemas operativos se actualizan ni bien el fabricante libere una nueva actualización

Diariamente se controlará que los sistemas de detección y antivirus estén activados y actualizados

El DIC instalará todo el software necesario para las funciones y procesos de negocio de cada área, los usuarios no podrán instalar software. Si necesitan algún nuevo SW, deberán solicitarlo al DIC.

Se instruirá a los empleados del PJCH respecto de los riesgos acarreados al abrir correos provenientes de fuentes desconocidas o acceder a sitios no seguros.

Las redes de intranet del PJCH tendrán firewall instalados, bloqueando todos los puertos salvo aquellos necesarios para el funcionamiento de los protocolos de comunicación entre los equipos.

**Segunda línea de defensa (detección)**

Diariamente se ejecutarán análisis automáticos de virus en background para no interrumpir las tareas de los usuarios.

Se monitoreará de forma constante el funcionamiento de la red, en concreto, de la conexión de la intranet del PJCH con el internet exterior, a fin de detectar tráfico no autorizado, no asociado con usuarios o con procesos y funciones de negocio.

**Tercera línea de defensa (recuperación)**

En caso de que se detecten equipos que, mediante software malicioso, están enviando información no autorizada, se procederá a formatear el sistema, reinstalar el sistema operativo y realizar la recuperación de los datos mediante los backups realizados semanalmente, junto a los backups incrementales, que se realizarán diariamente. Se deberán hacer análisis exhaustivos de los demás equipos para cerciorarse de que no hayan sido infectados.

En caso de que en el equipo haya algunos archivos que sean del dia de la deteccion de infeccion, personal del DIC aplicará un proceso avanzado de recuperación para garantizar la no infección de los mismos y luego aplicará las medidas normales antes mencionadas.

**Riesgo:**Probabilidad de fallas en las redes y equipos de trabajo antiguos debido a la falta de planificación para renovación de equipos y por error en la configuración

**Contramedidas:**

**Primera línea de defensa (prevención):**

Periódicamente, revisar el listado de hardware del PJCH y determinar cuales están desactualizados al punto de ser vulnerables en materia de seguridad. El criterio será que el HW debería poder correr los últimos protocolos de red, y los últimos sistemas operativos disponibles en el mercado.

Al momento de preparar nuevo equipo o realizar mantenimiento, estas tareas se realizarán de a pares, uno hará la tarea concretamente y otro personal revisará luego que se haya realizado correctamente. El que revisa será el responsable del correcto funcionamiento de los equipos.

**Segunda línea de defensa (detección):**

En caso de que un equipo no funcione, el personal que lo utiliza notificará al DIC de la cuestión. Se cuenta también con un sistema de monitoreo constante que alertará inmediatamente ante cualquier inconveniente

**Tercera línea de defensa (recuperación):**

Se contará con equipos de respaldo, para que en el caso de recuperación no se deba suspender las tareas durante tanto tiempo y se proceda a una rápida recuperación ante cualquier situación como esta.

Se realizará mantenimiento a todos los equipos que cuenten con una falta de renovación, para poder utilizar en un futuro esos mismos equipos como respaldo a los actuales.

Se iniciaran procesos de provisión para los equipos completamente dañados.

**Riesgo:** Probabilidad de espionaje que afecte información sensible del PJCH

Contramedidas**:**

**Primera línea de defensa (prevención)**:

Se establecerán perímetros en áreas donde se maneja información confidencial, donde para ingresar se deberá presentar identificación.

También habrá un canal anónimo donde se podrá notificar ante una violacion de seguridad por parte de cualquier persona

**Segunda línea de defensa (detección)**

Videovigilancia en accesos clave y en áreas críticas.

**Tercera línea de defensa (recuperación)**

Se realizará una auditoría para descubrir quién fue el encargado de filtrar la información. Si se descubre al culpable, se iniciarán los procesos penales correspondientes.

**Etapa 4 - Recuperación del Desastre[[9]](#footnote-8)**

En base a los montos determinados al momento del análisis de riesgo, consideramos que el riesgo más grave que podría suceder es el Ciberespionaje, debido a que pone en peligro no solo la infraestructura del PJCH sino también, la información de los ciudadanos, violando los derechos civiles de la población.

Es por esto que definimos aquí un plan detallado, con los pasos a seguir, al momento de detectar esta situación.

Para ver la información concreta que llevó a esta decisión, véanse los puntos de **análisis y manejo de riesgo.**

--

**Detalle de pasos:**

*Paso 1: Detección del tráfico no autorizado*

Incluye la terminal en la cual fue registrada la detección de tráfico no autorizado por el monitor, identificando la IP de la máquina, registrandola y bloqueándola para frenar su ataque. Puede ir desde la afectación parcial como pérdida total del servicio (crítico)

*Paso 2: Notificación del ataque*

Se notificará al Jefe de seguridad en primera instancia y luego este informará a los usuarios internos y de las diferentes áreas para la detención inmediata de labores y para el apago de los equipos afectados.

*Paso 3: Determinación del alcance del incidente detectado*

En este paso se evalúan los daños causados con la mayor recopilación de información posible. Se debe proceder lo más rápido ya que ante este tipo de ciberataques el tiempo es valioso para poder evitar daños irrecuperables en datos e intrusiones más profundas que conlleven a robos de información y comprometan la integridad e imagen de la organización

Aquí, el Jefe de Seguridad ordenará a un personal de seguridad, analizar el tráfico que estaba siendo enviado al exterior para determinar el tipo de información que fue emitida al exterior, e intentar determinar el destino de la misma. El tráfico debe estar registrado para tal fin. Se analizarán los demás equipos conectados a la intranet, buscando instancias del proceso que se ejecutaba en la máquina infectada. Si se encuentran otras, también deberán ser desconectadas de la red y apagadas.

*Paso 4: Ejecución del plan*

El jefe de seguridad comienza con la aplicación del plan movilizando los equipos de cada área para que cada uno de ellos comience realizando las acciones ya preestablecidas para detener sus labor y empezar con las acciones de recuperación.

Tras aislar los equipos de la red, se encenderán los equipos en un entorno controlado para analizar el virus e intentar determinar su origen.

El Jefe de Seguridad hará copias completas del disco para futuros análisis y auditorias. El personal de operaciones comprobará la integridad de los archivos almacenados en los servidores, comparándolos con últimos backups existentes.

*Paso 5: Recuperación del ataque*

Por último, los equipos y dispositivos que fueron afectados en el ataque deberán ser revisados y reconfigurados para que vuelvan a funcionamiento cuanto antes. Abarcando así los procedimientos definidos, respaldos de información relacionada a la organización, manuales y documentación de sistemas. Una vez mitigado el ataque se debe evaluar la magnitud del ataque y los daños producidos, como así también, tener en cuenta cual seria el tiempo necesario para la recuperación de los equipos que presentaron fallos importantes.

1. http://secretariadegenero.pjud.cl/index.php/mujeres-y-hombres-en-numeros-en-el-poder-judicial [↑](#footnote-ref-0)
2. <http://secretariadegenero.pjud.cl/index.php/mujeres-y-hombres-en-numeros-en-el-poder-judicial> [↑](#footnote-ref-1)
3. <http://repositorio.uchile.cl/bitstream/handle/2250/113165/de-inda_m.pdf?sequence=1> [↑](#footnote-ref-2)
4. https://healthitsecurity.com/news/report-unsecured-misconfigured-databases-breached-in-just-8-hours [↑](#footnote-ref-3)
5. Casos de exito de ransomware destinado a encriptacion de archivos https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf [↑](#footnote-ref-4)
6. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html [↑](#footnote-ref-5)
7. https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/3767-ccn-cert-ia-13-19-ciberamenazas-y-tendencias-resumen-ejecutivo-2019/file.html [↑](#footnote-ref-6)
8. Casos de exito de ransomware destinado a encriptacion de archivos https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf [↑](#footnote-ref-7)
9. Al momento de desarrollar este plan, nos guiamos por un documento emitido por la Escuela Superior Politécnica del Litoral: “Plan de Contingencia ante Ciberataques”. https://www.dspace.espol.edu.ec/retrieve/102439/D-106279.pdf [↑](#footnote-ref-8)