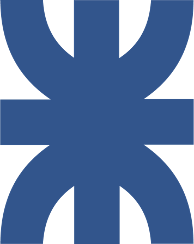
**UNIVERSIDAD TECNOLÓGICA NACIONAL**

**FACULTAD REGIONAL RESISTENCIA**



**TP 6.1 - “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

**Consignas:**

1. Realizar una lectura comprensiva del artículo ***“KRACK – La seguridad de las redes WiFi en entredicho”***. Luego, según los conceptos estudiados a partir de la bibliografía de Robson.
2. Identificar las vulnerabilidades, amenazas y riesgos referidos en el artículo.

**Vulnerabilidades**

* Falta de efectividad de la confidencialidad del protocolo de seguridad WP2, respecto a el acceso a las contraseñas de redes inalámbricas WIFI en los routers.
* Falta de procedimiento (o dificultad) de actualización de firmware en muchos routers que utilizan el protocolo WP2.

**Activos**

* Datos e información.

**Amenaza**

* Obtención de la contraseña de la red inalámbrica.
* Intercepción del tráfico WiFi que pasa entre ordenadores y router.
* Ataques a hosts específicos de la red WIFI (robo de información, control y configuración remota del dispositivo)

**Riesgos**

* Existe una *X* probabilidad de que personal no autorizado obtenga la contraseña de acceso de una red inalámbrica (amenaza), ingrese a la red y tenga acceso a nuestra información (activo) por culpa de la falta de efectividad en la confidencialidad del protocolo WP2 en routers inalámbricos (vulnerabilidad).
* Existe una *X* probabilidad de que personal no autorizado obtenga la contraseña de acceso de una red inalámbrica (amenaza), ingrese a la red y utilice nuestra conexión (activo) por culpa de la falta de efectividad en la confidencialidad del protocolo WP2 en routers inalámbricos (vulnerabilidad).

1. Clasificar las amenazas identificadas, indicando, además, si son ataques pasivos o activos.

Amenaza 1 y 2:

Obtención de la contraseña de la red inalámbrica.

Intercepción del tráfico WiFi que pasa entre ordenadores y router.

Estas amenazas son **pasivas** porque no alteran la comunicación, sino que únicamente la escucha o monitoriza para obtener la información que está siendo transmitida (en este caso la contraseña y el tráfico de datos). Es **deliberada** y **lógica**.

Amenaza 3: Ataques a hosts específicos de la red WIFI (robo de información, control y configuración remota del dispositivo)

* 1. Esta amenaza es **activa**, porque para que ocurra debe haber una acción **deliberada** por parte de un atacante, y es **lógica**, puesto que ocurre sobre y hacia medios de comunicación inalámbricos, y los activos involucrados también son lógicos.

1. Identificar y redactar adecuadamente las políticas y medidas enunciadas.
2. Clasificar las medidas indicadas.

Políticas:

* 1. (PROHIBITIVA) Mantener el firmware de todos los puntos de acceso) siempre lo más actualizado posible.
     1. (Prevención - Primera línea de defensa) En el RDP para la provisión de hardware se indicará la condición de que los dispositivos ofrecidos reciban actualización de firmware cada 6 meses.
     2. (Recuperación - Tercera línea de defensa) En el caso de que se haya detectado que se poseen puntos de acceso con la vulnerabilidad KRACK y no se tiene la posibilidad de actualizar el dispositivo afectado, se procederá a su inmediato reemplazo por un punto de acceso que sí sea invulnerable a dicha amenaza.
  2. (PROHIBITIVA) Toda navegación web u operación de red deben realizarse utilizando protocolos seguros o redes privadas virtuales.
     1. (Prevención - Primera línea de defensa) Solo se permitirá navegar por sitios web que usen el protocolo https.
     2. (Prevención - Primera línea de defensa) Los desarrollos internos de servicios web deben siempre utilizar el protocolo https
     3. (Prevención - Primera línea de defensa) Utilizar VPNs de acceso remoto para el acceso a los repositorios código fuente y demás información y sistemas sensibles de la empresa.

1. Leer detenidamente el artículo ***“Telefónica y otras empresas españolas sufren un ciberataque en sus redes internas”***. Luego:
   1. Realizar la etapa de identificación de riesgos (vulnerabilidades, amenazas, elementos amenazados y riesgos).

**Vulnerabilidades:**

* Los sistemas Windows instalados en algunos de los equipos del personal no poseen las últimas actualizaciones de seguridad, haciéndolas susceptibles a virus informáticos.
* Falta de capacitación en empleados para operar de forma segura en internet.
* Falta de un firewall configurado correctamente para evitar la propagación de los virus en las redes de trabajo de la organización.

Es a partir de estas vulnerabilidades, que notamos cuales activos están en riesgo a causa de las mismas.

**Activos Vulnerables:**

* Datos almacenados en las computadoras de trabajo de los empleados
* Horas de trabajo de los empleados
* Horas de servicio al cliente.
* Sistemas operativos

**Amenazas:**

* + 1. Inoperabilidad en el servicio de atención al cliente.
    2. Pérdida de los sistemas operativos de los ordenadores.
    3. Pérdida de los datos operativos (informes mensuales, reportes de actividad, planillas de asistencia, etc) de la organización almacenados en las computadoras de trabajo.
    4. Imposibilidad de uso de los ordenadores conectados a la red interna de la organización.

**Riesgos**

1. Probabilidad de inoperabilidad en la totalidad del servicio de atención al cliente e imposibilidad de uso de los ordenadores conectados a la red interna de la organización debido a la falta de un firewall configurado correctamente para evitar la propagación de virus en las redes de trabajo de la organización.
2. Probabilidad de pérdida de los datos operativos de la organización almacenados en las computadoras de trabajo y de los sistemas operativos de las mismas debido a la falta de capacitación de los empleados en materia de seguridad y falta de las últimas actualizaciones de seguridad de los SO en algunas computadoras de trabajo.
   1. Realizar el análisis de riesgos: identificar cuáles serían los ítems de pérdidas potenciales, evaluando además el costo que implicaría el daño producido. Basarse en el extracto bibliográfico ***“El aspecto económico de las medidas de seguridad”*** y el artículo “Alineados con el resto”4.

**Análisis de riesgo:**

El análisis de riesgo es el análisis de impacto potencial, donde intentamos evaluar la pérdida esperada, producida por una amenaza particular, donde:

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

Primero entonces, definimos las pérdidas potenciales relacionadas a cada riesgo, en la siguiente tabla

Suposiciones:

* Los datos de los clientes se guardan en los servidores de la compañía y están seguros frente a estas vulnerabilidades
* Los datos operativos como ser informes, registros contables, evaluaciones de personal, planillas de asistencia, entre otros, se almacenan en las computadoras de los empleados y se hacen backups en los servidores, una vez que están completas, en el transcurso de una semana.
* Al analizar pérdidas de datos no resguardados, se asume el peor valor posible, es decir, que los datos se pierden justo antes de realizar un nuevo back-up. Este monto es sumamente alto
* La empresa Telefónica no tiene seguro contra ransomware (es el caso del 36% de las organizaciones actuales)[[1]](#footnote-0)
* La empresa utiliza Windows 7, y los empleados no tienden a aceptar las actualizaciones en sus computadoras.

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | **Pérdida Potencial** | **Consecuencias primarias** | **Consecuencias secundarias** |
| Probabilidad de pérdida de los datos operativos de la organización almacenados en las computadoras de trabajo y sus sistemas operativos debido a la falta de capacitación de los empleados en materia de seguridad y falta de las últimas actualizaciones de seguridad de los SO en algunas computadoras de trabajo. | - Registros de la empresa almacenados en computadoras de trabajo  - Sistema operativo | Retraso de los procesos operativos de la organización (ej. evaluación del personal, informes diarios, registros de contabilidad recientes, etc) | - La capacidad de los sistemas de información se verá desaprovechada debido a la interrupción de las actividades.  -La actividad del personal de mantenimiento se incrementará drásticamente debido a los procesos de recuperación de datos y reinstalación de los sistemas operativos. |
| Probabilidad de inoperabilidad en la totalidad del servicio de atención al cliente e imposibilidad de uso de los ordenadores conectados a la red interna de la organización debido a la falta de un firewall configurado correctamente para evitar la propagación de virus en las redes de trabajo de la organización.  . | -horas de trabajo de los empleados  -horas de atención al cliente | Interrupción de la atención al cliente a corto plazo. | - Pérdida de la confianza de los clientes e inversores.  -Retraso en las entregas de servicios. |

**Aclaraciones**

* Todos los montos están en dólares estadounidenses

|  |  |  |  |
| --- | --- | --- | --- |
| **Elementos amenazados** | **Cantidad** | **Valor Unitario** | **Monto** |
| Sistemas operativos de los equipos afectados[[2]](#footnote-1) | 30.000 | $ 120 | $3.600.000 |
| Registros de datos operativos propios de la compañía almacenados en las computadoras de los empleados durante la última semana. [[3]](#footnote-2) [[4]](#footnote-3) [[5]](#footnote-4) | 30.000 | $ 584 | $17.500.000 |
| Horas del servicio brindado a los clientes interrumpido | 120 | $ 17800(abonos mensuales perdidos x hora) | $2.136.000 |
| Horas de trabajo interrumpido de los empleados | 40 horas x 30.000 empleados = 1.200.000 | $ 15(sueldo x hora prom) | $18.000.000 |
| **Total** |  |  | $41.236.000 |

Justificación del valor de las horas de servicio: Se suelen recibir 12 llamadas por hora por persona. Teniendo 1000 personas dedicadas a atención al cliente, son 12 mil llamadas perdidas por hora. De estas 12 llamadas no contestadas, 1 resulta en que el cliente deja de ser cliente, debido a que era una situación urgente. Por hora se están perdiendo 1000 clientes. Asumiendo que la restauración del servicio de atención al cliente tomará 5 días, estarán 120 horas inactivas Cada cliente en promedio paga 15 euros por mes. Por lo tanto Telefónica, al final de esa semana de inactividad perderá 120.000 clientes, lo que le costará 120.000 \* 15 = 1.800.000 euros. Por hora, los abonos perdidos son 15 euros \* 1000 clientes, 15 mil euros, o 17800 dolares.

Tras conocer las pérdidas posibles relacionadas con los riesgos considerados, es importante tener en cuenta la probabilidad de ocurrencia, para luego poder calcular las siguientes variables

**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%**

**Intermedio: 26% a 50%**

**Alto: 51% a 80%**

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Amenaza** | **Probabilidad de la agresión** | | **Probabilidad de éxito** | | **Frecuencia de pérdida** | **Pérdida potencial** | **Pérdida esperada** |
| Inoperabilidad en el servicio de atención al cliente. | Baja | 10% | Alta | 75% | 7.5% | $2.136.000 | $ 160.200 |
| Pérdida de los datos operativos (informes mensuales, reportes de actividad, planillas de asistencia, etc) de la organización almacenados en las computadoras de trabajo | Intermedia | 35% | Alto | 73%[[6]](#footnote-5) | 25,55% | $ 17.500.000 | $4.471.250 |
| Imposibilidad de uso de los ordenadores conectados a la red interna de la organización. | Bajo | 25% | Intermedio | 40% | 1% | $18.000.000 | $ 1.800.000 |
| Pérdida de los sistemas operativos de los ordenadores | Intermedio | 35% | Muy alta | 85% | 29.7% | $3.600.000 | $1.071.000 |

* 1. Identificar las consecuencias primarias y secundarias de las fallas de seguridad planteadas.

**Consecuencias primarias**

La principal consecuencia de un ataque ransomware es que todos los procesos operativos de la empresa, deben retrasarse, debido a que hay que cortar las redes de la empresa, hacer un análisis de la extensión de la infección y recien ahi puede volver la actividad. La actividad de atención al cliente, que es la cara visible de la compañía, se ve sumamente afectada, puesto que existen grandes cantidades de llamados por hora.

**Consecuencias secundarias**

Durante los procesos de recuperación de información y reinstalación de sistemas, la actividad del personal de mantenimiento se incrementará drásticamente. De no poseer suficiente personal de mantenimiento será necesario pagar horas extras al personal disponible para reestablecer los servicios esenciales con prontitud.

Cada hora en la que el servicio de atención al cliente no esté disponible, o esté disponible con capacidades reducidas, representan posibles clientes marchándose de la empresa y en general, una disminución de la imagen pública de la empresa, tanto desde el punto de vista de los consumidores como de sus inversores.

Los trámites de instalación de nuevos servicios y/o planes de mantenimiento se verán retrasados debido a que la administración de los mismos se realiza y regula desde las mismas computadoras del personal antes mencionadas.

Todo el equipo de hardware y sistema base que esté en pausa representa capacidad de los sistemas de información desaprovechada, lo cual retrasa los retornos de inversión en el equipamiento.

* 1. Cómo armaría la expresión de “riesgo”, propuesta por Robson?

*“Riesgo es el potencial de que una amenaza determinada explote las vulnerabilidades de un activo o de un grupo de activos, ocasionando su pérdida o daño (ISACA).”*

Cada vulnerabilidad afecta a distintos activos, en mayor o menor grado. Cada activo tiene relacionada una amenaza y una probabilidad de vulnerabilidad, llamada frecuencia de pérdida.

Lo que deberíamos hacer, es calcular el valor de cada activo vulnerable, multiplicarlo por la frecuencia de pérdida, y sumar todos estos productos.

* 1. ¿Identifica elementos que correspondan a otras etapas de la Administración de Riesgos? Justificar adecuadamente su respuesta.

*“Tras detectarse el ataque a la red interna, se ha puesto en marcha el protocolo de seguridad. Tras informar a los trabajadores, se ha apagado la red de ordenadores y de dispositivos electrónicos conectados a la red inalámbrica de su sede en Madrid, ubicada en Las Tablas, como medida de precaución.”*

Aca podemos ver que se está intentando hacer una recuperación contra desastres. No hubo detección porque cuando se noto la amenaza, esta ya estaba instalada en los equipos del personal de la compañía.

En la nota también está esta sección:

*“Cómo protegerse ante un «ransomware»*

***1.- Hacer copia de seguridad:*** *Los expertos recomiendan hacer «backups» o copias de seguridad de manera periódica para evitar perder los archivos importantes y mantenerla fuera del entorno online ante posibles intromisiones ilegales.*

***2.- No abrir archivos adjuntos ni correos electrónicos sospechosos****: Normalmente, este tipo de ataques se propagan entre los diferentes contactos produciendo un efecto dominó. En caso de desconocer la procedencia del remitente o ante cualquier duda evitar a toda costa abrir el correo.*

***3.- Tener instaladas las actualizaciones del sistema operativo y de los antivirus:*** *es necesario tener todo el software al día para evitar ataques.”*

Estas son consideraciones que pertenecen a una línea de prevención, pero no se aplicaron, razón por la cual la compañía fue infectada. En el articulo estan como consejos al lector.

1. Realizar una lectura comprensiva del artículo ***“Apagón informático en AFIP”*** . Luego:
2. Analizar los aspectos del “management responsable de SI”.

Los diferentes aspectos existentes son:

* “Seguros” desde el punto de vista organizacional (técnico)
* “Seguros” desde el punto de vista organizacional (ético)
* “Seguros” desde el punto de vista judicial (legal)

El análisis llevado a cabo en base al artículo desde cada punto de vista es:

**TÉCNICO**:

* *"Hoy en día la AFIP cuenta con un presupuesto equilibrado, y aun así faltan insumos básicos para el trabajo diario, no hay reglas claras de trabajo y se carece de un rumbo cierto en el ente recaudador más importante del país”*.

De esta manera se puede evidenciar en el artículo que con la falta de estos insumos y las escasas reglas de trabajo, aun teniendo un presupuesto considerable como para poder cubrir estos costos, la existencia de vulnerabilidades en el AFIP van a seguir estando presentes hasta que no se tomen medidas necesarias, como por ejemplo llevar a cabo una correcta documentación dejando en claro las reglas de trabajo y formas de proceder, realizando capacitaciones e insumos básicos para que los empleados no cometan errores a la hora de llevar a cabo su labor.

**ÉTICO**:

* Al carecer el AFIP de reglas de trabajo claras, en un organismo que es el ente recaudador más importante del País, no cumple con la seguridad ética que debería tener, teniendo en cuenta las funciones críticas que se llevan a cabo allí. Lo dicho anteriormente produce amenazas a todos los contribuyentes, en el que sus datos pueden quedar expuestos.

Es importante resaltar la falta de ética de los empleados que van a llevar a cabo el “apagón informativo” en este organismo, ya que se verán afectados tanto los turnos como los sistemas informáticos del AFIP, afectando tanto el funcionamiento de dicha empresa como a los activos de los contribuyentes.

**LEGAL**:

* Se evidencia en el artículo el reclamo realizado por el recorte a la cuenta de jerarquización del (0,65%), comunicado en la Disposición 204/2018 del Boletín Oficial de la República Argentina al 06/08/2018.
* En la constitución se reconoce como un derecho fundamental al Derecho de Huelga (**artículo 28.2**) para la defensa de los intereses de los trabajadores. En este caso se evidencia la convicción de los gremialistas a realizar el “apagón informático” el lunes 10 de septiembre.

1. Realizar la etapa de identificación de riesgos: identificar los principales elementos amenazados, las vulnerabilidades, amenazas y riesgos involucrados en el caso referido en el artículo.

**Activos Vulnerables**

* Datos de los contribuyentes
* Horas de trabajo de los empleados

**Vulnerabilidades:**

* Falta de normas y políticas de uso de los sistemas informáticos y de trabajo.
* Corte del servicio por la afectación de turnos, y de sistemas informáticos del AFIP.
* Disminución de control referido a los sistemas informáticos debido al personal reducido.

**Amenazas:**

* Fuga de datos de los contribuyentes y de la organización.
* Error en los procedimientos realizados por los empleados
* Falla en los equipos de trabajo y los servidores.

**Riesgos:**

* Probabilidad de fuga de datos de los contribuyentes y de la organización durante las 4 horas en las cuales se llevará a cabo el “apagón informático'', debido al corte total del servicio y de los sistemas informáticos del AFIP.
* Probabilidad de que los equipos de trabajo y servidores fallen debido a el corte del servicio y de los sistemas informáticos del AFIP.
* Probabilidad de error en los procedimientos realizados por los empleados, debido a falta de normas y políticas claras de trabajo y uso de sistemas informáticos.

1. Realizar el análisis de riesgos: identificar cuáles serían los ítems de pérdidas potenciales, evaluando además el costo que implicaría el daño producido.

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | **Pérdida potencial** | **Consecuencias primarias** | **Consecuencias secundarias** |
| Probabilidad de fuga de datos de los contribuyentes y de la organización durante las 4 horas en las cuales se llevará a cabo el “apagón informático'', debido al corte total del servicio y de los sistemas informáticos del AFIP. | * Extracción de datos confidenciales pertenecientes a la organización y a sus contribuyentes. | * Pérdida de confidencialidad de los datos de los contribuyentes. | * Pérdida de confianza como organización al ente recaudador más importante del país. |
| Probabilidad de que los equipos de trabajo y servidores fallen debido a el corte del servicio y de los sistemas informáticos del AFIP. | * Pérdida de datos de la organización. * Daños en el Hardware | * Pérdida de accesibilidad a los servidores. * Pérdida de disponibilidad de los datos. | * Retraso en las funciones de vital importancia en las que se utilizan datos. * Incapacidad de realización de las operaciones de forma completa. |
| Probabilidad de error en los procedimientos realizados por los empleados, debido a falta de normas y políticas claras de trabajo y uso de sistemas informáticos. | * Alteración y/o pérdida de datos de la organización. * Alteración de los sistemas de información. | * Pérdida de integridad de los datos | * Resultados obtenidos de los sistemas poco creíbles o erróneos. |

**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%**

**Intermedio: 26% a 50%**

**Alto: 51% a 80%**

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

El siguiente cuadro será definido y completado en base al conocimiento que posee cada uno de los integrantes del equipo al momento de la realización del trabajo, más la investigación realizada en internet referida a los elementos de hardware y sus precios actuales.

|  |  |  |  |
| --- | --- | --- | --- |
| **Elementos amenazados** | **Cantidad** | **Valor Unitario del elemento** | **Monto total** |
| Equipos de PC de escritorio | 20 | $ 23.000,00 | $ 460,000,00 |
| Impresora Láser HP 107A | 5 | $ 13.000,00 | $ 65.000,00 |
| Plotter Designjet T120 Con Sistema Continuo | 1 | $ 120.000,00 | $ 120.000,00 |
| Monitor Philips V 223V5LHSB2 LCD 21.5" negro 100V/240V | 7 | $ 17.000,00 | $ 119.000,00 |
| Servidor Dell Poweredge T140 Xeon E-2124 16gb 2tb No T130 | 2 | $ 151.000,00 | $ 302.000,00 |
| Mikrotik Router 4 Cores Rb1100ahx4 13x Gigabit Doble Fuente | 1 | $ 39.000,00 | $ 39.000,00 |
| Switch Full Administrable Cisco 48 Puertos 10/100/1000 - SG350X-48-K9 | 2 | $ 153.000,00 | $ 306.000,00 |
| Registro del sistema | 10.000 | $1700 | $ 17.000.000,00 |
| **Total** | **10.038** | **$ 517.500,00** | **$ 18.411.000,00** |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Amenaza** | **Probabilidad de agresión** | | **Probabilidad de éxito** | | **Frecuencia de la pérdida** | **Pérdida potencial** | **Pérdida esperada** |
| Fuga de datos de los contribuyentes y de la organización | Intermedio | 35% | Alto | 65% | 22% | $17.000.000,00 | $3.740.000 |
| Error en los procedimientos realizados por los empleados debido a la falta de normas y políticas de uso de los sistemas de información | Intermedio | 45% | Alto | 75% | 33% | $17.000.000,00 | $6.290.000,00 |
| Falla en los equipos de trabajo y los servidores. | Bajo | 23% | Alto | 55% | 12% | $1.441.000,00 | $172.000,00 |

Personal: 21191

(<http://www.afip.gob.ar/transparenciaactiva/documentos/nomiPersoAFIP_300618.pdf>)

1. **Identificar las consecuencias primarias y secundarias de la falla de seguridad planteada.**

**Consecuencias primarias**

La principal consecuencia producida luego de este “apagón informativo” consiste en la pérdida de los datos que contiene el AFIP, como así también su disponibilidad e integridad al estar expuestos a un hackeo durante las 4 horas en las cuales se produjo dicho apagón. A su vez, se puede ver afectada la confidencialidad de los datos correspondientes a los contribuyentes en caso de que ocurra un posible ciberataque, ya que este organismo se vio obligado a informar a todas las personas acerca del detalle del apagón.

A su vez, en lo referido a los sistemas informáticos, se podría ver afectada la accesibilidad a los servidores que forman parte de la organización, debido a la escasez de los empleados y la falta de reglas claras de trabajo durante el apagón y después del mismo.

**Consecuencias secundarias**

Las consecuencias secundarias existentes consistirán principalmente en la pérdida de confianza por parte de la población, lo cual terminaría brindando una mala imagen de esta organización que es la más importante del país.

Por otra parte, se habría disminuido la productividad y la operabilidad en el AFIP, ya que durante el apagón no se podrán realizar las funciones más importantes que requieren de la utilización de datos y los turnos se verían afectados.

Debido a la falla de los equipos y servidores como consecuencia del corte informático, los resultados obtenidos en las operaciones llevadas a cabo no podrán asegurar su credibilidad y seguridad, no se podrían asegurar su correcta actualización, y tampoco se podría llevar a cabo la carga de datos de manera correcta ya sea por errores de los empleados, por falta de reglas claras de trabajo y por falta de capacitación correspondiente.

1. **¿Qué estrategia de manejo del riesgo propondría utilizar? ¿Con qué esquema de seguridad?**

La estrategia de manejo de riesgo que proponemos utilizar es *“****Prevenir el riesgo****”*, ya que de esta manera podríamos documentar nuevas reglas claras, normas y políticas concretas de trabajo para que los empleados de la organización tengan bien definidas sus tareas y responsabilidades, evitando así errores por parte de ellos ante cualquier situación.

Se capacitará también a los empleados en las funciones más importantes que el AFIP debe llevar a cabo de manera más eficaz.

Por otra parte, se hará un análisis de los insumos que actualmente posee la organización para renovar o adquirir más y mejores, siempre y cuando sea necesario, ya que esto influye en la seguridad y en la eficiencia del trabajo y de las tareas de la organización.

|  |  |
| --- | --- |
| **Riesgo** | **Contra medida** |
| **Probabilidad de hackeo al AFIP durante las 4 horas durante las cuales se llevará a cabo el “apagón informático”.** | * Realizar copias de seguridad para tener un respaldo de toda la información según su prioridad. * Ejecutar periódicamente monitoreo de sistemas. * Activar el uso de Firewalls y hacer una nueva política de seguridad que aclare qué facultad tiene cada tipo de usuario. * Mantener actualizados nuestros softwares que nos proveen seguridad. |
| **Probabilidad de que los equipos de trabajo fallen.** | * Realizar diagnósticos periódicos para hacer recambios a insumos a equipos a los cuales se le está terminando su vida útil. * Contar con equipos de respaldo para que en caso de que se produzca una falla se los pueda usar inmediatamente. * Contar con backups de todos los archivos más relevantes. |
| **Probabilidad de error de los empleados por falta de reglas claras de trabajo.** | * Realizar capacitaciones sobre las funciones y tareas que deben llevar a cabo. * Contar con reglas de trabajo claras y documentación para que puedan acceder a ella en caso de necesitarlo. |

1. ¿Qué políticas de seguridad recomendaría?

Las políticas de seguridad que recomendaríamos son:

* Se debe informar de inmediato al responsable correspondiente sobre el mal funcionamiento de uno de los insumos. *(Prohibitiva)*
* Se debe dejar registrado en el caso de que haya un problema durante el horario laboral de cualquier empleado. *(Prohibitiva)*
* Se debe dejar registrado el recambio de algún insumo o equipo de trabajo. *(Prohibitiva)*
* Todos los accesos al sistema deben poder ser visibles únicamente por el Jefe de Seguridad de la organización.  *(Prohibitiva)*
* Todos los accesos al sistema deberán ser registrados automáticamente. *(Prohibitiva)*
* Ante un acceso sospechoso o no autorizado se deberá notificar inmediatamente al superior correspondiente. *(Prohibitiva)*

1. 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.

Etapas de Administración de Riesgos:

**Etapa 1 - Identificación del Riesgo**

Activos Vulnerables:

* PCs y terminales de trabajo
* Redes de información (Hardware y Software)
* 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.)
* Hardware de los servidores
* Información de causas, sentencias y documentación relevante para el PJCH.
* 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 en 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

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 por nuevos Virus, Ransomwares, Malwares
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 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*.*
* 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.
* Probabilidad de ciberespionaje con intenciones de fugar 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.
* 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
* Probabilidad de espionaje que afecte información sensible del PJCH

**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.

**Suposiciones**:

-El PJCH cuenta con múltiples back-ups distribuidos geográficamente

**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. [[7]](#footnote-6)

|  |  |  |  |
| --- | --- | --- | --- |
| **Riesgo** | **Pérdida Potencial** | **Consecuencias primarias** | **Consecuencias secundarias** |
| 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 | -PC  -Servidores  -Datos de las causas  -Datos operativos  -Horas de trabajo interrumpidas de los empleados | -Retraso en las operaciones llevadas a cabo en la organización | -Perdida de horas trabajadas de los empleados  -Retrasos en los procesos judiciales programados |
| 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. | -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 con intenciones de fugar información sensible | -Confidencialidad de los datos de las causas  -Horas de trabajo interrumpidas de los empleados | -Pérdida de confianza de los ciudadanos  -Posibles daños a la imagen de los ciudadanos implicados.  -Interrupción en los servicios brindados | -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. | -Servidores  -Datos de las causas  -Datos operativos  -PCs y terminales de trabajo  -Software  -Redes de información  -Horas de trabajo interrumpidas de los empleados | -Interrupción en los servicios brindados  -Reparación de los equipos con daño parcial  -Provisión de nuevo equipo de HW.  -Pérdida de disponibilidad de datos. | -Retraso de entrega de trabajos pendientes  -Retrasos en los procesos judiciales programados  -Carga excesiva en el área de mantenimiento. |
| 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 | -Hardware de los servidores  -Hardware de redes  -PCs y terminales de trabajo  -Horas de trabajo interrumpidas de los empleados | -Pérdida de disponibilidad de datos.  -Interrupción en los servicios brindados  -Provisión de los nuevos equipos necesarios | -Carga excesiva en el área de mantenimiento.  -Pérdida en la integridad y confiabilidad de los datos. |
| Probabilidad de espionaje que afecte información sensible del PJCH | -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. [[8]](#footnote-7)

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

**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. [[9]](#footnote-8) 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.

|  |  |  |  |
| --- | --- | --- | --- |
| **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%**

**Intermedio: 26% a 50%**

**Alto: 51% a 80%**

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Amenaza** | **Probabilidad de agresión** | | **Probabilidad de éxito** | | **Frecuencia de la pérdida** | **Pérdida potencial** | **Pérdida esperada** |
| Errores en la configuración en el SW o HW de los equipos empleados. | Alta | 70% | Intermedio | 34%[[10]](#footnote-9) | 24% | $ 700 +  $ 35.028  =  $ 35.728 | $ 8.574,72 |
| Evento catastrófico que afecte a la infraestructura de IS del PJCH (terremoto, tsunami, inundación, volcán) | Alta | 75% | Bajo | 10% | 7.5% | $ 700 +  $ 4.200 +  $ 3.890 +  $ 35.028 +  $ 250.200  =  $ 29.4018 | $ 22.051,35 |
| Fallas en los equipos causados por nuevos Virus, Ransomwares, Malwares | Baja | 20% | Alta | 73%[[11]](#footnote-10) | 15% | $ 35.028 +  $ 700  =  $ 35.728 | $ 5.359,2 |
| Espionaje que afecte a la información sensible del PJCH | Baja | 20% | Alta | 75% | 15% | $ 94.075 | $ 14.111,25 |
| Ciberespionaje que afecte a la información del PJCH | intermedio | 35%[[12]](#footnote-11) | Alta | 80%[[13]](#footnote-12) | 28% | $ 94.075 + $ 35.028  =  $ 129.103 | $ 36.148,84 |
| Fuga de información accidental debido a un error por parte de los empleados | Intermedia | 35% | Baja | 18% | 6.3% | $ 94.075 | $14.111,25 |

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.
* 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.
* El jefe de seguridad deberá realizar semanalmente la actualización de software de detección y reparación de software malicioso en las PCs y terminales de trabajo.
* Toda información relacionada a las causas o interna del PJCH deberá tener múltiples backup distribuidos geográficamente.
* La información relacionada a las causas y sus respectivos backup deberá estar encriptada.
* 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 PJCH.
* 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.
* En caso de observar violaciones de seguridad se deberá notificar inmediatamente al jefe de seguridad correspondiente, y existirá un canal anónimo para tal fin.
* Las contraseñas de cualquier rol que otorgue accesos al sistema, no podrán estar en blanco, deberán tener una longitud considerable y renovarse cada cierto periodo de tiempo.
* Cada acceso a información debe estar registrado con usuario, fecha y hora, para poder rastrear el uso de la misma en futuras auditorías.
* Los servidores y las zonas de backup estarán 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)
* Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o crítica, e instalaciones de manejo de información.
* Hacer un seguimiento de las condiciones meteorológicas de las jurisdicciones, para poder detectar amenazas medioambientales y reaccionar en consecuencia (tormentas eléctricas, incendios forestales, terremotos ,etc).
* Previo al contrato de cada empleado se deberá proceder a verificar su identidad y las certificaciones presentadas por el mismo, como así también sus antecedentes penales e información crediticia personal.
* Mantener el HW (servidores, red, equipos de personal) actualizado de acuerdo a los requerimientos de seguridad del PJCH. Los equipos deben ser capaces de correr los últimos sistemas operativos y/o firmware de red disponible en el mercado .

**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[[14]](#footnote-13)**

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.

--

**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 bloqueandola 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. https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf [↑](#footnote-ref-0)
2. Este monto podría no pagarse si Microsoft da nuevas licencias a aquellos infectados debido a que era una vulnerabilidad de su propio sistema, en el caso de que los parches de seguridad no hayan sido emitidos. [↑](#footnote-ref-1)
3. El valor de los registros de datos operativos se calcula en base al tiempo que le tomaría a un empleado rehacer o redactar un informe, planilla, registros contables, etc. Es una estimación. [↑](#footnote-ref-2)
4. El valor de la hora del empleado de telefonica se obtuvo de esta pagina: https://www.businessinsider.es/cuanto-gana-empleado-telefonica-espana-sueldo-condiciones-553420 [↑](#footnote-ref-3)
5. Una semana de trabajo, 30 mil empleados: 500 euros \* 30000 mil empleados: 15 millones de euros [↑](#footnote-ref-4)
6. 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-5)
7. http://secretariadegenero.pjud.cl/index.php/mujeres-y-hombres-en-numeros-en-el-poder-judicial [↑](#footnote-ref-6)
8. <http://secretariadegenero.pjud.cl/index.php/mujeres-y-hombres-en-numeros-en-el-poder-judicial> [↑](#footnote-ref-7)
9. http://repositorio.uchile.cl/bitstream/handle/2250/113165/de-inda\_m.pdf?sequence=1 [↑](#footnote-ref-8)
10. https://healthitsecurity.com/news/report-unsecured-misconfigured-databases-breached-in-just-8-hours [↑](#footnote-ref-9)
11. 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-10)
12. 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-11)
13. 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-12)
14. 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-13)